SIKRINGSHÅNDBOKA

Håndbok i sikring av eiendom,
bygg og anlegg mot terror, sabotasje,
spionasje og annen kriminalitet.

Forsvarsbygg

SIKRINGSHÅNDBOKA

Håndbok i sikring av eiendom,
bygg og anlegg mot terror, sabotasje,
spionasje og annen kriminalitet.

Forsvarsbygg

Forord

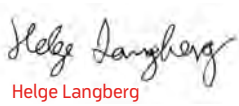
Sikringshåndboka ble første gang utgitt av Forsvarsbygg i 2005 og har siden dette kun blitt oppdatert med mindre justeringer og rettelser. Dagens trusselbilde og sikkerhetslovens forskrift om objektsikkerhet stiller nye krav til beskyttelse og sikring av viktige funksjoner i samfunnet. Det har derfor vært behov for å foreta en omfattende revidering av boken slik at den er oppdatert på alle fagfelt.

Sikringshåndboka er laget for å formidle kunnskap om hvordan sikre verdier i eiendom, bygg og anlegg (EBA) mot terror, sabotasje, spionasje og annen kriminalitet. Boken gir oppdaterte råd og veiledning når det gjelder planlegging, gjennomføring og kontroll av sikringstiltak og er ment å kunne brukes både som et oppslagsverk og som en lærebok innenfor sitt fagfelt. Vi håper at dette vil bidra til en mer enhetlig og helhetlig håndtering av sikkerhetstiltak, samt mer gjennomtenkte sikringsløsninger i og rundt sentrale bygninger og funksjoner.

Sikringshåndboka er tenkt å være et hjelpemiddel både for sikkerhetsledere og andre som jobber med forebyggende sikkerhet, beslutningstakere i forbindelse med byggeprosjekter og berørte fagpersoner. Boken er også tenkt å kunne brukes i undervisnings- og kurssammenheng.

Nasjonalt kompetansesenter for sikring av bygg (NKSB) ble opprettet i 2012 som statens rådgiver for beskyttelse og sikring av eiendommer, bygg og anlegg mot eksplosjonsulykker, terrorhandlinger, spionasje, sabotasje og annen kriminalitet. NKSB er organisert som en egen enhet i Forsvarsbygg og leverer sikkerhetsfaglig rådgivning til alle større byggeprosjekter i forsvarssektoren og staten for øvrig. Det er dette fagmiljøet som har utarbeidet den reviderte Sikringshåndboka.

Vi vil takke alle som har bidratt til at en ny bok nå er på plass, spesielt gjelder dette bidrag fra Forsvarsdepartementet, Forsvaret og Kommunal- og moderniseringsdepartementet. Vi vil også takke Nasjonal sikkerhetsmyndighet som viktig samarbeidspartner.



Helge Langberg
Leder Nasjonalt
kompetansesenter
for sikring av bygg

Innhold

DEL 1

INTRODUKSJON

DEL 2

PLANLEGGING OG PROSJEKTGJENNOMFØRING

DEL 3

METODER FOR SIKRING

Forts. neste side →

→ Forts.

DEL 3

METODER FOR SIKRING

DEL 4

SPESIELLE FUNKSJONER OG SPESIALROM

DEL 5

VEDLEGG

DEL 1

INTRODUKSJON

Del 1 Introduksjon gir deg en innføring i grunnleggende forhold som sikringsteori, sikkerhetskultur og hvilke lover og regelverk som er gjeldende for sikring av eiendom, bygg og anlegg.

Kapittel 1

Innledning

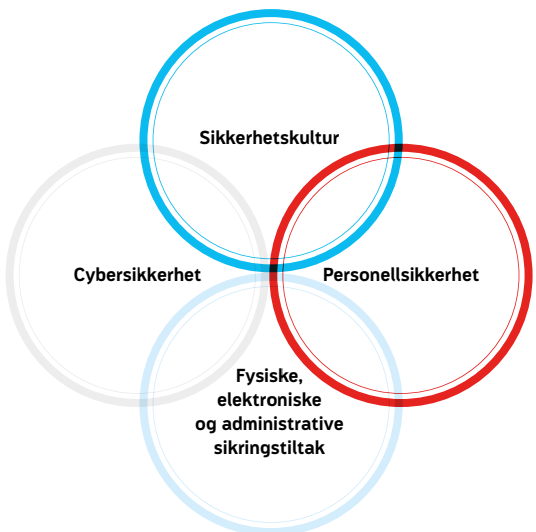
Sikkerhetssituasjonen er i kontinuerlig endring og behovet for å sikre verdier har økt. Etter 22. juli 2011 kan vi se et mer bevisst forhold til sikring, og det stilles flere spørsmål om omfanget og utformingen av sikringstiltak.

Sikringshåndboka handler om hvordan skader som følge av uønskede handlinger kan begrenses. Boken beskriver veien fra identifisering av verdier til riktig sikring, og har hovedfokus på metoder og løsninger for fysisk og elektronisk sikring av eiendommer, bygninger og anlegg. Vi håper at boken vil være nyttig og øke kompetansen blant dem som skal bestille og planlegge bygg og anlegg med behov for sikring.

Generelt

Sikringshåndboka formidler kunnskap om hvordan forhindre eller begrense skader på verdier i eiendom, bygg og anlegg (EBA) som følge av terror, sabotasje, spionasje og annen kriminalitet. Boken gir råd og veiledning når det gjelder planlegging, gjennomføring og kontroll av sikringstiltak.

Sikring - helhetlig perspektiv



Tidligere utgave av Sikringshåndboka har vært rettet særlig mot sikringstiltak i tilknytning til Forsvarets bygninger og anlegg, mens denne utgaven har en bredere vinkling og retter seg også mot sivile aktører. Boken er et referanseverk både i forbindelse med oppføring av nye bygg og ved oppgradering av eksisterende bygg. For virksomheter og objekter omfattet av sikkerhetsloven, er det konkrete krav til sikring nedfelt i lover, forskrifter og veiledere. Sikringshåndboka omfatter imidlertid råd og veiledning om prosesser og tiltak som har en bredere relevans, og som er aktuelle også for aktører som ikke er underlagt sikkerhetsloven.

Sikring av bygg og anlegg spenner fra å forsterke allerede eksisterende konstruksjoner til større planmessige grep. Nøkkelen til suksess er at sikkerhet raskt blir et tema i prosjektplanleggingen, slik avdekkes viktige muligheter og utfordringer tidlig i prosessen.

Sikringshåndboka er bygget opp mest mulig i samsvar med de ulike trinnene i en slik prosess. Boken er delt i fire deler i tillegg til en del med vedlegg:

1. ***Introduksjon*** *tar for seg grunnleggende forhold som sikringsteori, sikkerhetskultur og hvilke lover og regelverk som er gjeldende for sikring av eiendom, bygg og anlegg.*
2. ***Planlegging og prosjektgjennomføring*** *går gjennom de grunnleggende elementene som må ivaretas før konkrete sikringstiltak kan prosjekteres. Gjennomføring av risikoanalyse er sentralt, og verdivurdering og trusselvurdering er utdypet i egne kapitler. Det er også en beskrivelse av planlegging av sikringstiltak i byggeprosjekter.*
3. ***Metoder for sikring*** *belyser fagvis en rekke måter å sikre eiendom, bygg og anlegg på mot ulike trusler.*
4. ***Spesielle funksjoner og spesialrom*** *gir innsikt i hvordan oppnå ønsket sikringsnivå for enkelte konkrete spesialfunksjoner.*
5. ***Vedlegg*** *omfatter definisjoner, samling av alle sikringsklassene, eksempel på skjema for verdivurdering og en kategorisering av trusselaktører på forskjellige nivåer.*

Sikring i et helhetlig perspektiv

Sikringshåndboka handler om å sikre bygg og verdier i bygg mot tilsiktede uønskede handlinger. Det er imidlertid viktig og nyttig å forstå at sikring handler om mer enn å etablere sikringstiltak. Hvis vi ser på sikring på et mer overordnet nivå, er det en viktig samfunnsoppgave å rette tiltak mot samfunnsforhold som kan danne grobunn for terror og annen kriminalitet. Slike tiltak ligger på et politisk nivå og vil kunne være med på å redusere truslene og omfanget av kriminelle handlinger, men aldri fjerne dem helt.

Effektiv sikring handler om å få mennesker, teknologi og organisasjon til å spille sammen på en god måte. Skal en organisasjon ha en god forebyggende sikkerhet, så omfatter det sikringstiltak innenfor følgende delområder: cybersikkerhet, personellsikkerhet, fysiske, elektroniske, menneskelige og organisatoriske tiltak og en god sikkerhetskultur. Disse må ses i sammenheng.

For å redusere risikoen for utro tjenere må det eksempelvis være et godt system for personellsikkerhet med bakgrunnssjekk og oppfølging av ansatte. En god sikkerhetskultur må etableres, der de ansatte har kunnskap og gode holdninger slik at de har en god sikkerhetsmessig adferd. Cybersikkerhet handler om å beskytte seg mot trusler rettet mot informasjonssystemer. Fysiske, elektroniske og administrative sikringstiltak er nødvendig for å redusere risikoen for tilsiktede handlinger som spionasje, terror, sabotasje og andre kriminelle handlinger.

Siden alle disse områdene er gjensidig avhengig av hverandre, er det vesentlig å sørge for at det ikke er noen «svake ledd» i systemet når det gjel-

SENTRALE BEGREPER

Overordnet mål
SIKKERHET
Reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare.

Aktivitet
SIKRING «SECURITY»
Risikohåndtering forbundet med tilsiktede uønskede handlinger (NS 5830).

SIKRING «SAFETY»
Risikohåndtering forbundet med utilsiktede uønskede handlinger. (Behandles ikke videre i Sikringshåndboka.)

der personell, praktisering av sikkerhetsrutiner eller å sikre informasjonssystemer. Sikringshåndboka gir i hovedsak råd om sikring av bygg. For å få et helhetlig perspektiv på sikring må andre kilder benyttes for mer kunnskap om sikringstiltak innenfor cybersikkerhet og personellsikkerhet.

Begreper og definisjoner i Sikringshåndboka

Sikringshåndboka inneholder en rekke faguttrykk og begreper som er forklart i vedlegget ***Ordliste og definisjoner.*** Målet med definisjonene er å oppnå en klar og entydig kommunikasjon mellom personer som arbeider med sikring, beslutningstakere og andre interessenter.

Enkelte sentrale begreper innen sikringsfaget har ikke en enhetlig eller entydig stadfestet definisjon eller bruk. På engelsk brukes betegnelsene «security» og «safety» som begge blir oversatt til norsk med sikkerhet. Vanlige ord i det norske språket som sikring, beskyttelse og skjerming er ofte brukt i sikkerhetsarbeidet, men brukes om hverandre og betyr i utgangspunktet det samme. Den enkelte eller organisasjoner legger forskjellige betydninger i ordet.

Sikkerhetsloven med forskrifter og veiledninger medfører også utfordringer for definisjonene. En rekke begreper fra sikkerhetsloven er sentrale, og definisjonene der er viktige i mange sammenhenger. I loven benyttes imidlertid også en del sentrale begreper uten at de er definert, og andre definisjoner er naturlig nok generelt avgrenset til å gjelde sikkerhetslovens virkefelt. Sikringshåndboka ønsker i første rekke å benytte definisjoner som gjør at sikringstiltakene ikke avgrenses til lovens virkefelt.

Sikkerhet er et mål eller en overordnet tilstand og defineres som reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare.[1] Det vil si at begrepet omfatter både tilsiktede (security) og utilsiktede hendelser (safety). ***Sikring*** brukes også ofte om begge typer aktiviteter, men i Sikringshåndboka avgrenser vi sikring[2] til å gjelde risikohåndtering forbundet med tilsiktede uønskede hendelser. Det vil si hendelser forårsaket av en aktør som handler med hensikt.

I Sikringshåndboka er begrepet sikkerhet brukt som et overordnet mål eller tilstand, og all aktivitet for å oppnå sikkerhet er sikring. Sikring omfatter også begrepene beskyttelse og skjerming, og disse er benyttet i fagkapitler som en språklig variasjon ut fra følgende forutsetning: Beskyttelse benyttes om sikring mot våpenvirkninger, og skjerming benyttes om sikring mot etterretningstrusler (avlytting, stråling) og elektromagnetiske trusler (EMP, HPM og Tempest).

I listen med definisjoner og forkortelser har vi både tatt noen valg og utformet nye definisjoner som vi mener er de riktige for sikringsarbeidet. Definisjonene inneholder også referanser og merknader.

1
Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger. Definisjon fra: Norsk Standard NS 5830:2012

2
Ibid.

Kapittel 2

Sikringsteori

I dette kapitlet vil vi se nærmere på allmenne, veletablerte prinsipper som gjelder for sikring av verdier i bygg og anlegg.

Opplevelse av trygghet og stabilitet er et av menneskets mest grunnleggende behov. Følelsen av trygghet henger sammen med fravær av trusler og muligheten til å beskytte seg mot farer. Helt siden oldtiden har mennesker gått sammen i et organisert forsvar for å kunne stå imot angrep fra rivaliserende folkegrupper som var ute etter å plyndre, ødelegge, ta slaver eller kontroll over et territorium. Et av de første forsvarsanleggene vi kjenner til, er bymuren rundt Uruk i oldtidens Sumer (nå Irak). Uruk er sammen med Jeriko regnet som en av verdens eldste byer som var omringet av en bymur.

I takt med utviklingen av moderne våpen og byggeteknikk har forsvarsanlegg blitt stadig mer avansert, og med tradisjonell fortifikasjon kan det konstrueres fjellanlegg som gir svært god beskyttelse mot et konvensjonelt angrep. De fleste sivile funksjoner med sikringsbehov gir andre utfordringer i etableringene av godt sikrede bygg i byområder. Dette er krevende og vil ofte innebære behov for langsiktig planlegging, utforskning av tomtens muligheter, utvendig og innvendig forsterkning av bygget, elektronisk sikring, vakthold og administrative tiltak.

Sikring i dybden

Sikring i dybden er et av de eldste sikringsprinsippene, som også er vel så viktig og hyppig benyttet i moderne tid. Av illustrasjonene nedenfor ser vi tydelig at både forsvarsanlegget i oldtidens Uruk og i Camp Meymaneh i Afghanistan er utformet med sikring i dybden som hovedprinsipp for sikring, til tross for at de er konstruert med over 4500 års mellomrom. Det samme prinsippet er også brukt for sikring av den amerikanske ambassaden i London (2016).

Tanken bak sikring i dybden er dels å avskrekke en angriper ved at det er flere lag med sikringstiltak. Flere lag med sikringstiltak vil gjøre det vanskeligere og mer tidkrevende for en inntrenger å komme seg forbi sikringstiltakene, og forsvarerne vil da kunne vinne tid til å få på plass en utrykningsstyrke som kan settes inn for å stoppe angrepet.

Prinsippet med sikring i dybden brukes i dag både i forbindelse med utvendig perimetersikring (f.eks. gjerder, mur og kjøretøysperrer) og innvendig sikring (f.eks. sluser ved innganger og spesielle soner rundt de viktigste verdiene inne i et bygg). Alle sikringssoner vil ha en form for fysisk forsterkning og representerer således en barriere som en inntrenger må ta

1
Perimetersikring før og nå: Perimetersikringen i Uruk (ca. år 2600 f.Kr.).

FOTO Wiki Commons

2
Perimetersikringen i Camp Meymaneh i Afghanistan (2007).

FOTO Forsvarets mediesenter

3
Den amerikanske ambassaden i London.

FOTO/RENDER Kieran Timberlake

seg forbi. I tillegg til den fysiske sikringen er det anbefalt å etablere vakthold, deteksjon, alarmer, adgangskontroll og kontrollrutiner i forbindelse med sonene. Prinsippet om sikring i soner er like relevant om man planlegger å sikre et militært område, et høysikkerhetsfengsel, et lite kontorbygg eller eget hjem. Antall soner og omfang av sikringstiltak vil imidlertid være forskjellig.

I ***figuren Sikring i dybden*** illustrerer hvert lag en sikringssone. Innerst er de viktigste verdiene som vi ønsker å beskytte, plassert.

Grunnsikring

Det er angriperen som velger tid og sted, og til tross for at ulike sikkerhetstjenester bruker mye ressurser på å avdekke terroranslag, må det påregnes at det i noen tilfeller ikke er mulig å få noen varsling i forkant av en hendelse. Vi må derfor ha en god grunnsikring som kan motstå et overraskende angrep. Grunnsikringen må omfatte tiltak innenfor fysisk sikring, elektronisk sikring og menneskelige og organisatoriske tiltak som kan håndtere potensielle trusselscenarioer som kan oppstå i fremtiden. Grunnsikringen må være til stede permanent, men i tillegg må

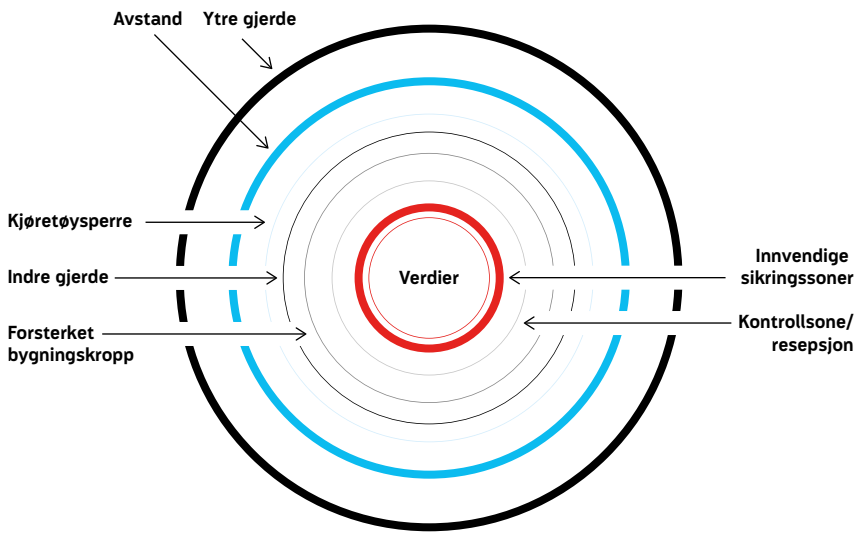
GRUNN-SIKRING

Grunnsikring innebærer at sikkerhets-tiltakene rundt verdiene i bygget eller på eiendom-men er på plass og er i daglig drift, slik at vi kan håndtere en trussel som kan oppstå uten forvarsel.

Av sikkerhets-loven fremgår at grunnsikring skal omfatte en kom-binasjon av bar-rierer, deteksjon, verifikasjon og reaksjon tilpas-set verdiene som skal sikres.

Sikring i dybden

Hvert lag representerer én sikringssone. Innerst er de viktigste verdiene som vi ønsker å beskytte.



Sikring i dybden med eksempler på ulike sikringstiltak som ligger lagvis utenfor verdiene. Sikring i dybden innebærer at sikringstiltak etableres i flere lag, slik at det blir vanskeligere for en inntrenger å komme forbi alle sonene og inn til verdiene. Sikring i dybden betyr at sikringstiltakene ligger lagvis innover i et areal eller volum. Tiltakene kan være adgangskontroll, autorisasjonsskiller, dører, vegger, hvelv m.m.

det være planlagt med ulike beredskapstiltak som kan forsterke sikringen ved behov.

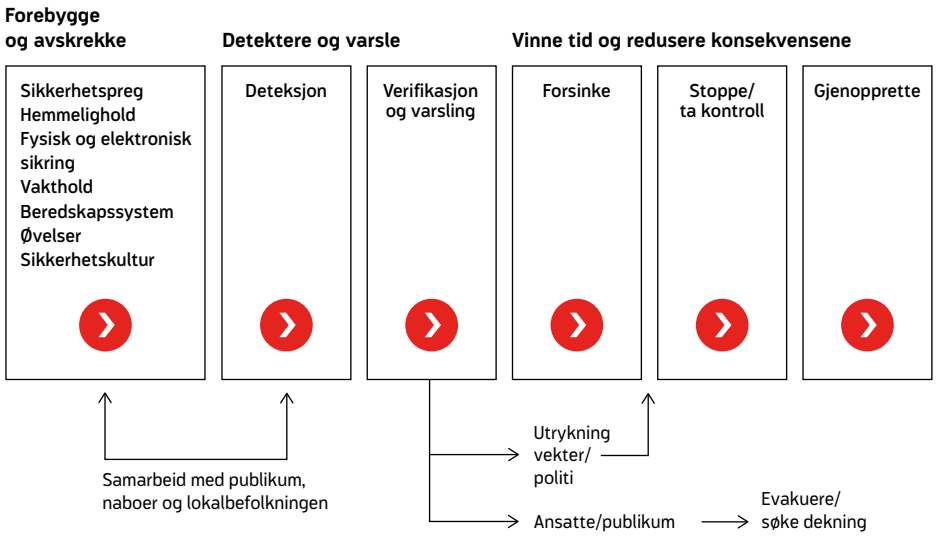
For å forsikre oss om at vi har en tilstrekke-lig grunnsikring, må vi øve på håndtering av aktuelle trusselscenarioer. En god grunnsikring innebærer imidlertid ikke at vi kan se bort fra ulike beredskapstiltak. De vil spesielt være aktuelle ved ulike krisesituasjoner der det f.eks. er en konflikt med en fremmed makt, og vi kan bli utsatt for målrettede sabotasjehandlinger.

Overraskelse

Overraskelse er et av de viktigste krigsprin-sippene, men det er også et prinsipp som kan benyttes av den som skal beskytte eller sikre sine bygg og anlegg. En trusselaktør har som regel planlagt angrepet på forhånd, og dersom han blir overrasket under aksjonen, kan dette forsinke ham, gjøre ham usikker og kanskje medføre at han gir opp. Noen overraskelses-elementer som kan være effektive i sikrings-sammenheng, er listet opp nedenfor:

- *Nye sikringselementer som er ukjent for inntrengeren, eksempelvis en ekstra eller ny type sikkerhetsdør*
- *En lyskaster som tennes av bevegelses-detektor, vil signalisere til inntrengeren at han er detektert og gjør at han blir lett synlig*
- *En sirene vil signalisere til inntrengeren at han er detektert, samtidig som omgivel-sene varsles. Enkelte sirener har et så høyt lydnivå at det vil være svært ubehagelig å oppholde seg i nærheten av dem uten hørselsvern*

Helhetlig sikring



Helhetlig sikring illustrerer et helhetlig sikringssystem med viktige elementer som det å forebygge, avskrekke, forsinke, detektere, verifisere, varsle, utrykning, stoppe/ta kontroll og gjenopprette. **Helhetlig sikring** er en videreutvikling av sikringselementene: barriere, deteksjon, verifikasjon og reaksjon, som blant annet nevnes i sikkerhetsloven.

- → *En høyttaler kan brukes til å kommunisere med inntrengeren og varsler også om at han er oppdaget, og informere om at politiet er på vei*
- → *En røykgenerator vil kunne røyklegge et rom relativt raskt og gjøre det svært vanskelig for en inntrenger å orientere seg*
- → *Forsterkninger av veggkonstruksjoner, vinduer, dører som ikke er synlig*

Skal sikringselementer ha en overraskende virkning, krever dette skjerming av opplysninger om plassering og kapasitet.

Spredning eller konsentrasjon

Spredning kan være et effektivt tiltak for å redusere sårbarheten til en viktig verdi, men det vil i mange tilfeller medføre økte sikringskostnader i forhold til en konsentrasjon av verdiene. På den andre siden vil en spredning gjøre det mer ressurskrevende for en angriper å sette alle verdiene ut av spill. Det er således både fordeler og ulemper med et spredningskonsept. En konsentrasjon av viktige verdier vil gjøre det mer kosteffektivt å sikre disse ved at omfanget og kostnadene for sikringstiltak blir mindre i forhold til en spredt plassering. Ulempen med dette er imidlertid at alle verdiene samles, og at det generelt sett vil være mindre ressurskrevende for en angriper å angripe ett objekt enn flere objekt.

Helhetlig sikring

Sikringstiltak bør fremstå som så gode og effektive at en angriper vil vurdere muligheten for å lykkes med et angrep som lav. Sikringstiltakene vil da ha en forebyggende og avskrekkende effekt. Dersom en angriper

likevel forsøker seg, må vi raskt kunne detektere angrepet slik at vi kan sette inn mottiltak for å forsøke å stoppe angrepet og å begrense skadevirkningene.

Forebygge og avskrekke

Sett fra et sikringsperspektiv er det ønskelig at noen sikringstiltak er synlige for å oppnå en avskrekkende virkning. Dette må imidlertid balanseres mot behovet for å skjule sikringstiltakene for å skape overraskelse. Typiske eksempler på bygg og anlegg der det er lagt stor vekt på å la sikringstiltak virke avskrekkende, er fengsler og forsvarsanlegg. I et bymiljø bør hensyn til en tiltalende estetikk og tilgjengelighet for byens borgere som oftest være viktigere enn at sikringstiltakene skal se robuste og avskrekkende ut. Dette innebærer at sikringstiltakene integreres i arkitektur og landskapsarkitektur, slik at man kan unngå at et godt sikret bygg fremstår som en festning som begrenser folks bevegelsesfrihet og opplevelse av et godt bymiljø. Bruk av vakter rundt et bygg kan virke avskrekkende, men kan også gi befolkningen en følelse av trygghet, uten at dette begrenser bevegelsesfriheten.

Trusselvurderinger vil gi oss bedre kunnskap om potensielle trusler og vil være viktig for å regulere beredskapsnivået opp eller ned. Økt beredskap og øvelser innebærer i praksis en bedre sikring og vil kunne medføre at en angriper utsetter angrepet eller kanskje velger et annet enklere mål.

Eksempler på noen sikringstiltak som kan virke avskrekkende, er:

- *Gjerder og skilt med advarsler som: «Området er kameraovervåket», «Adgang forbudt» og «Forhøyet beredskap» signaliserer at sikringstiltak er iverksatt, og at overtredelse vil kunne medføre straff eller andre negative konsekvenser.*
- *Kameraovervåkning og alarmsensorer gir økt risiko for å bli oppdaget. Bildene fra kameraovervåkningen kan dessuten brukes til å identifisere gjerningspersonene og som bevismateriale i en straffesak.*
- *Avsperringer som gjør at det ikke er mulig å komme så nær objektet som man ønsker.*
- *Forsterket vakthold på objektet.*

Hvor omfattende og gode de avskrekkende tiltakene er, vil ofte være begrenset av hvilke ressurser som er tilgjengelige. Med god planlegging kan man imidlertid ofte oppnå akseptabel effekt selv med begrensede midler.

Selv om de fleste trusselaktører vil tenke seg om noen ekstra ganger før de går til angrep på et mål som er godt sikret, må man ta i betraktning at det finnes aktører som ikke lar seg avskrekke. Aktører med stor vilje, som ikke demotiveres av tanken på negative konsekvenser (for eksempel en selvmordsbomber) eller aktører med stor kapasitet (for eksempel spesialstyrker) vil kanskje gjennomføre angrepet uavhengig av sikringsnivå, dersom målet fremstår som symboltungt eller på andre måter svært attraktivt.

Detektere

Deteksjon er normalt en forutsetning for å kunne avverge et angrep, eller begrense skadene av det. Tidlig deteksjon skaper tid og mulighet for å mobilisere aktive og passive mottiltak. Deteksjon kan utføres av ulike elektroniske sensorer (kameraer, termiske kameraer, bevegelsesdetektorer, radarer, lasere, trykksensorer og akustiske sensorer) eller av mennesker (vakter, ansatte, publikum og naboer).

Ofte vil en angriper spane på objektet i forkant av angrepet. Ved å gi ansatte og publikum opplæring i å gjenkjenne mistenkelig adferd eller gjenstander, har virksomheten bedre muligheter til å detektere at et angrep er i emning. For ubemannede anlegg som ligger øde til, kan det være en god idé å alliere seg med lokalbefolkning og naboer for rapportering av uvanlige hendelser.

Verifikasjon og varsling

Ved alarm er det viktig å kunne verifisere enten med tv-overvåkning eller personell på stedet, slik at riktig reaksjon kan iverksettes. Vanligvis sender vaktsentralen ut spesielt trenede ansatte eller vaktmannskaper, eller det brukes kamera eller andre sensorer for å forsikre seg om at det er en reell alarm. Verifikasjon ved bruk av kamera er å foretrekke, slik at man unngår å sende egne ansatte eller vaktmannskaper inn i en farlig situasjon. Dersom alarmen viser seg å være reell, varsles reaksjonsapparatet. I tillegg vil det i noen tilfeller være nødvendig å varsle ansatte, besøkende og publikum slik at de kan søke dekning, evakuere eller få informasjon om hvordan de skal forholde seg.

Forsinke

De fysiske sikringstiltakene er designet for å forsinke eller aller helst stoppe en inntrenger fra å nå inn til verdier.

For å lykkes med å hindre inntrengeren i å nå frem til verdiene må forsinkelsen forårsaket av de fysiske sikringstiltakene være større enn reaksjonsstyrkens utrykningstid. Dette kalles balansert sikring. For å dokumentere at man har en balansert sikring, lages det vanligvis et tidsregnskap, se mer om dette nedenfor.

Forsinkelsen de fysiske sikringstiltakene gir, skal også gi ansatte, publikum og VIP muligheter til å evakuere eller rømme til sikre områder.

Utrykning

Utrykningsstyrken kan bestå av egne spesielt trenede ansatte, vektere, politi eller militære vaktsoldater. For et samfunnskritisk objekt vil det normalt være politiet som rykker ut, mens det på militære objekter i mange tilfeller vil være en militær vaktstyrke som brukes som utrykningsstyrke. Selv om politiet teoretisk har en kort utrykningstid, kan andre pågående oppdrag gjøre at den reelle utrykningstiden kan bli vesentlig lengre. For å få bedre bilde av den reelle utrykningstiden må det gjennomføres realistiske øvelser.

Det er viktig at størrelsen på utrykningsstyrken og bevæpningen av denne står i forhold til en potensiell trusselaktør, og det er bare politiet og militære vakter som har mulighet for å bære våpen. En effektiv inngripen av politi krever at det er tilrettelagt for dette, og at politiet er kjent på sikringsobjektet og jevnlig øver på håndtering av aktuelle trusselscenarioer som kan skje på objektet.

Stoppe, ta kontroll og sikre bevis

Kommer utrykningsstyrken (her politi eller militær vaktstyrke) raskt på plass, har den mulighet til å avverge at angriperen tar seg inn på anlegget eller i bygningen, tar gisler eller skader viktige verdier.

Dersom responstiden er lang og/eller man har få eller svake fysiske barrierer, vil utrykningsstyrken ofte ha begrenset mulighet til å avverge en trusselsituasjon. Styrken må da fokusere på å få oversikt og ta kontroll over situasjonen ved å lokalisere inntrengerne, vurdere behov for forsterkning, evakuering og minimere skade.

Et angrep vil ikke automatisk stoppe selv om reaksjonsstyrken kommer frem til objektet. Situasjonen kan være svært uoversiktlig og kompleks, noe som kan medføre at det vil ta tid før utrykningsstyrken får kontroll på situasjonen. Dette gjelder spesielt dersom det er mistanke om utplasserte bomber på objektet og/eller en gisselsituasjon.

Det er viktig å sikre tv/video-opptak, både som hjelp under en pågående aksjon, og for senere etterforskning og bevisførsel.

Gjenopprette

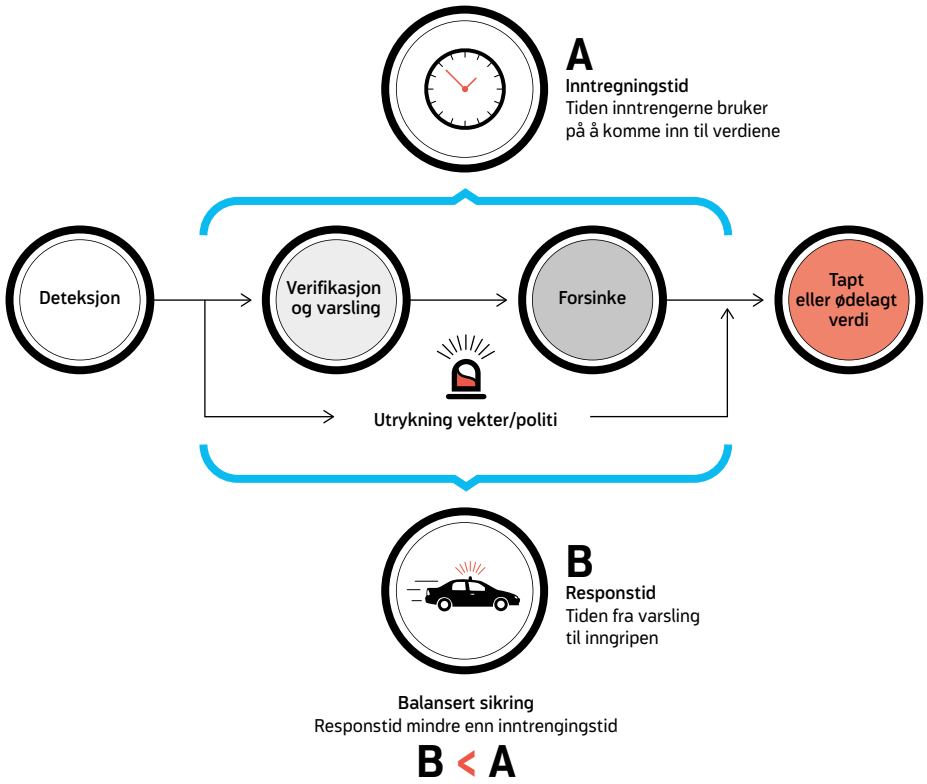
Beredskapsplaner vil være nødvendig for å kunne håndtere spesielle hendelser og krisesituasjoner på en god måte. Alle virksomheter bør

BALANSERT SIKRING

Balansert sikring betyr at den totale forsinkelsen de ulike sikringstiltakene gir, er større enn responstiden. Snakker man om balanse i sikringstiltakene, er dette en helhetlig sikring mot en trussel, og at for eksempel dører, vegger og vinduer har samme motstandskraft mot inntrengning.

Tidsregnskap brukes som et verktøy for å dokumentere at man har etablert en effektiv sikring mot en definert trusselaktør. I et tidsregnskap vurderes inntrengingstid mot responstid. Dersom responstiden vurderes å være kortere enn inntrengningstiden, så har man oppnådd en balansert sikring.

Balansert sikring – tidsregnskap

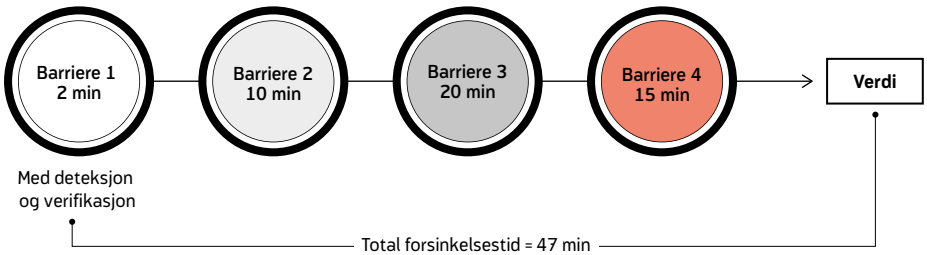


ha en plan som beskriver hvordan virksomheten skal håndtere en sikkerhetstruende hendelse. Det vil i den forbindelse være viktig å samarbeide tett med politi og redningsetatene for å få kontroll over situasjonen, redusere skadeomfanget, hindre følgeskader og raskt kunne gjenopprette en tilfredsstillende tilstand. Ved en større hendelse vil det være aktuelt å etablere en krisestab. Etter en sikkerhetstruende hendelse må det også settes av ressurser for oppfølging av ansatte, andre berørte samt pårørende. Håndtering av presse vil også være viktig for å unngå å skape unødvendig frykt samt for å skjerme de som er blitt rammet og deres pårørende.

Balansert sikring

Balansert sikring betyr at den totale forsinkelsen de ulike sikringstiltakene gir, er større enn responstiden. Dette betyr at tiden det tar å få utrykningsstyrken på plass, må være mindre enn tiden angriperen bruker på å komme frem til verdiene eller ta kontroll over et område. Dette forutsetter at inntrengningen blir detektert og verifisert, og at størrelsen på utrykningsstyrken og bevæpningen av denne står i forhold til aktuell trusselaktør. Dersom sikringstiltakene (eks. gjerde, dører, vinduer, vegger) er vurdert til å forsinke en inntrenger i 20 min og responstiden for utrykningsstyrken

Eksempel på tidsregnskap



Figuren viser eksempel på forsinkelsestid som kan oppnås for de ulike barrierene mot en definert trusselaktør. Dersom det ikke lykkes å detektere og verifisere ved Barriere 1, men f.eks. først ved Barriere 3, blir total forsinkelsestid redusert til 35 min.

er 40 min, er ikke balansert sikring oppnådd, og det vil være en god sjanse for at inntrengeren lykkes.

Tidsregnskap

For å dokumentere at man har balansert sikring, må det utarbeides et tidsregnskap. I et tidsregnskap gjør man en kvalifisert beregning av hvor lang tid en definert trusselaktør vil bruke på å komme forbi de aktuelle fysiske sikringselementene, eks. gjerde, vindu, dører eller vegger. En slik beregning krever kunnskap om inntrengningstider, noe man vanligvis får gjennom å gjennomføre realistiske inntrengingsforsøk.

Det er viktig å poengtere at tidsregnskap ikke er ikke noen eksakt beregning, da flere av verdiene som brukes, er basert på en subjektiv faglig vurdering. Utrykningstid kan man relativt greit få en oversikt over gjennom f.eks. møter med politiet og gjennomføring av realistiske øvelser. Kapasiteten til ulike sikringselementer mot en definert inntrenger er litt mer krevende å estimere, fordi det kan være stor forskjell på kapasiteten til en terrorist eller vinningskriminell. Sikkerhetsdører er f.eks. testet mot et sett av verktøy som kanskje ikke er den type verktøy en inntrenger ville brukt. Den beste kunnskapen om inntrengingstider får man kun gjennom å gjennomføre realistiske innbruddstester, se ***kapittel 11, Fysisk sikring mot inntrengning.***

Kapittel 3

Sikkerhetskultur

Dette kapitlet beskriver prosesser og mekanismer som kan etablere god sikkerhetskultur. Hva er egentlig god sikkerhetskultur, hvorfor er det viktig, og hvordan kan det oppnås i praksis?

Nasjonal sikkerhetsmyndighet (NSM) oppsummerer sikkerhetskultur på følgende måte: «Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.»[1] Forenklet kan en si at god sikkerhetskultur er når alle i en organisasjon har et bevisst og aktivt forhold til sikkerhet. Sikkerhet skal være en integrert del av alle prosesser i virksomheten, og alle må ha god nok kompetanse til å utføre sine oppgaver på en hensiktsmessig måte med tanke på sikkerheten.

Hvorfor er god sikkerhetskultur viktig?

Dårlig sikkerhetskultur vil raskt redusere effekten av kostbare fysiske og elektroniske sikringstiltak ved at de motarbeides av ansatte som ikke forstår hvorfor, eller er uenige i at de er etablert. Et typisk eksempel på dette er at ansatte omgår sikringstiltak «av praktiske hensyn», som ved å holde en sikringsdør åpen for personen som kommer rett etter uten å sjekke at denne har riktig adgangskort. Det virker kanskje både tidsbesparende og høflig for den ansatte, men det kan også forenkle arbeidet til en trusselaktør som vil ha tilgang til det som skulle være en sikret sone. Andre eksempler er dører som settes åpne, fordi de er så tungvinte å åpne eller ansatte som selv deaktiverer alarmer.

Hvordan skape god sikkerhetskultur?

Å bygge god sikkerhetskultur er et omfattende arbeid. Det kan være vanskelig å snu en negativ trend, og god sikkerhetskultur må pleies og ivaretas kontinuerlig. Medarbeidere må stadig motiveres til å ta gode valg, og sikkerhet må være i fokus på samme måte som andre viktige områder i virksomhetens hverdag. Et viktig steg på vei mot bedre sikkerhetskultur er å informere om hvilket sikringsnivå virksomheten har behov for, og hvorfor. Riktig sikringsnivå kan kartlegges ved å gjennomføre en risikoanalyse som anbefaler fysiske, elektroniske og administrative sikringstiltak. Se ***kapittel 5, Risikoanalyse*** for mer om denne prosessen.

Britiske Centre for the Protection of National Infrastructure (CPNI) deler tiltak for å skape god sikkerhetskultur inn i to hovedkategorier: myke og harde tiltak. Mens de myke tiltakene handler om at medarbeiderne i en organisasjon skal forstå hvorfor sikringstiltak er implementert, og hvordan man utviser god sikkerhetsatferd, handler de harde tiltakene om klare retnings-

1 NSMs nettsider, «Hvordan skape en god sikkerhetskultur?» *www.nsm.stat.no*

linjer for hva som skjer når man utviser dårlig sikkerhetsatferd.[2]

God sikkerhetskultur er et lederansvar. For at den enkelte ansatte skal kunne utføre sine arbeidsoppgaver med god sikkerhetsatferd, er det viktig at virksomhetens ledelse går foran som gode eksempler, som en del av de myke tiltakene for god sikkerhetskultur. Det er ledelsen som beslutter hvilke sikringstiltak som skal implementeres, og hvilke rutiner som skal være gjeldende på arbeidsplassen. Ledelsen må forklare for de ansatte hvorfor de fysiske, elektroniske og administrative tiltakene er viktige,[3] og hvorfor de ikke skal søke å omgå implementerte sikringstiltak «av praktiske hensyn».

Det er viktig å huske på at en ikke kan lære av sine feil om en ikke er klar over dem. Denne tankegangen må implementeres i hele virksomheten. Det er først da alle kan bli bevisste på eventuelle sikkerhetsmessige feil som gjøres, og i andre rekke forbedre seg. Det er også viktig å huske hvilke forutsetninger de enkelte ansatte har, spesielt med tanke på opplæring. En person kan ikke lastes for de feil han eller hun begår hvis en ikke har blitt opplært på riktig måte eller fått tilstrekkelig opplæring.[4] Det er de ansatte som kjenner egen arbeidsplass best, og det er derfor lurt at de opplæres i hvordan de skal reagere og varsle ved mistenkelig atferd. Årvåkne medarbeidere kan ofte enklere identifisere atferd som strider mot det normale, enn det vaktpersonell har mulighet til å gjøre via kameraovervåkning og vaktrunder. Denne typen årvåkenhet blant de ansatte kan både representere en sikringsbarriere i seg selv og være med på å danne et sikringspreg som vil virke avskrekkende på noen typer trusselaktører.[5] Slik årvåkenhet gjelder også overfor kolleger. I Norge er den generelle tilliten i samfunnet blant de høyeste i verden,[6] og det sitter nok for mange langt inne å konfrontere en kollega med det som oppfattes som dårlig sikkerhetsatferd. Det avsløres imidlertid utro tjenere også her til lands, og Kriminalitets- og sikkerhetsundersøkelsen for 2015 viste at tre av ti virksomheter har avdekket utro tjenere blant sine ansatte.[7]

De harde tiltakene handler om å skape gode rutiner for å håndtere dårlig sikkerhetsatferd. Det skal være klare retningslinjer for hvordan oppgaver skal utføres på en sikkerhetsmessig tilfredsstillende måte, og retningslinjene må håndheves på en synlig og effektiv måte. Det må kommuniseres tydelig til medarbeiderne at dårlig sikkerhetsatferd får konsekvenser, og at det forventes at retningslinjene etterleves.[8]

2
CPNIs nettsider, «Passport to Good Security» *www.cpni.gov.uk*

3
NSMs nettsider, «Hvordan skape en god sikkerhetskultur?» *www.nsm.stat.no*

4
Reason, James, «High Reliability Organisations», 2007

5
CPNIs nettsider, «Personell security – employee vigilance» *www.cpni.gov.uk*

6
Helge Skirbekk og Harald Grimen, «Tillit i Norge», Res Publica, 2012

7
Næringslivets sikkerhetsråd, «KRISINO – Kriminalitets- og sikkerhetsundersøkelsen i Norge», 2015

8
CPNIs nettsider, «Passport to Good Security» *www.cpni.gov.uk*

Ledelsen etablerer et system med rutiner som skal fange opp sikkerhetsbrudd, sikkerhetstruende hendelser og nesten-hendelser i alle ledd i organisasjonen. Ansatte må forplikte seg til å rapportere inn til riktig instans, og de må få tilbakemelding i etterkant. Dersom det ikke blir gitt tilbakemelding på innrapporterte sikkerhetsbrudd, kan det være vanskelig for de ansatte å se hensikten med å rapportere. Det er også viktig at det finnes prosedyrer for hva som er ledelsens neste steg ved innmeldte sikkerhetsbrudd, slik at dette ikke kun blir håndtert ad hoc, basert på mer eller mindre tilfeldige individuelle vurderinger.

I en hektisk hverdag er det lett å ikke ta årsakene til sikkerhetsbrudd innover seg og ta lærdom av dem. Det blir med andre ord ofte ikke tid til evaluering av hendelser og eventuell iverksettelse av tiltak som følge av hendelser.[9] Om ikke sikkerhetsbrudd følges opp med tilpasset opplæring av de ansatte, vil man kunne komme i en situasjon der samme dårlige sikkerhetsatferd utøves gang på gang, og med det resultat at virksomhetens sikkerhet gradvis blir dårligere.

Følgende tiltak anbefales for å forbedre sikkerhetskulturen:[10]

- *Ledelsen må ha fokus på sikkerhet og fremheve at sikkerheten er viktig*
- *Generell opplæring av alle ansatte med tanke på sikkerhetsrutiner og sikkerhetsbrudd*
- *Obligatoriske opplæringspakker f.eks. ved bruk av e-læring med en avsluttende test for å kontrollere at man har oppnådd et tilfredsstillende kunnskapsnivå*
- *Informasjon om implementerte fysiske og elektroniske sikringstiltak*
- *Bevisstgjøring rundt hva som utgjør sensitiv og skjermingsverdig informasjon*
- *Bevisstgjøring rundt hvordan ulike typer informasjon skal oppbevares og behandles*
- *Utarbeidelse av planverk og instrukser for sikkerhetstruende hendelser*
- *Øve på håndtering av sikkerhetstruende hendelser og evakuering*
- *Fokus på trusselscenarioer og årvåkenhet overfor mistenkelig atferd, inkludert innsidetrussel*

God sikkerhetskultur er en forutsetning for et godt sikkerhetssystem. Virksomheter som er underlagt sikkerhetsloven, plikter å utøve det som kalles «forebyggende sikkerhetstjeneste». NSM beskriver i den anledning en rekke forhold som er en del av god sikkerhetsadministrasjon, inkludert sikkerhetsledelse, sikkerhetsorganisering og løpende sikkerhetsoppfølging.[11] Dette skal være organisert i et styringssystem for sikkerhet, slik at den forebyggende sikkerhetstjenesten i virksomheten kan planlegges, gjennomføres, kontrolleres og kontinuerlig forbedres.[12]

Oppsummert handler en god sikkerhetskultur om å bevisstgjøre og motivere de ansatte til god sikkerhetsatferd. Rapportering av sikkerhetsbrudd og oppfølging av disse må ikke handle om å henge ut personer for feil de har gjort, men om å skape systemer og rutiner som fanger opp og retter opp i dårlig sikkerhetsatferd.

Uavhengig av metode kreves det at ledelsen går foran som et godt eksempel, er «på ballen» og setter krav til at rutiner følges. Ledelsen må arbeide kontinuerlig med å skape bevisstgjøring og årvåkenhet, og hele virksomheten må være med på øvelser.

For å lykkes med å skape og opprettholde god sikkerhetskultur anbefales en helhetlig tilnærming og samarbeid på tvers av avdelinger i virksomheten. På denne måten kan virksomheten få frem det fulle potensialet i både egne medarbeidere og i de fysiske og elektroniske sikringstiltakene som etableres.

Hvordan bedre sikkerhetskultur oppnås, beskrives nærmere i ***kapittel 15, Menneskelige og organisatoriske tiltak.***

9
Reason, James, «High Reliability Organisations», 2007

10
Listen er ikke uttømmende

11
NSM, «Veiledning til Risikostyring» *www.nsm.stat.no*

12
NSM, «Hvordan skape en god sikkerhetskultur?» *www.nsm.stat.no*


NORGES LOV
1687-20

Kapittel 4

Samfunnssikkerhet, lover og regelverk

LOVER OG FOR-SKRIFTER

Gjeldende lover med forskrifter kan hentes på www.lovdata.no, og se ellers siste del av dette kapitlet for nærmere henvisninger.

→
www.lovdata.no

Dette kapitlet tar for seg de lover, forskrifter og andre bestemmelser som kan ha innvirkning på sikring og beskyttelse av eiendom, bygg og anlegg (EBA) i normal fredstilstand. Oppgaver og beføyelser i krise og krig vil ikke bli behandlet, da det er andre lover og fullmakter som vil gjelde.

Generelt

Det er en rekke lover, forskrifter og andre bestemmelser som gir pålegg om sikring og beskyttelse av kritiske verdier, sikkerhetsgradert informasjon og militært materiell.

Figuren Ulike lover og regelverk viser en del lovverk som kan gjøre seg gjeldende i planleggingen av sikringstiltak.

Det er ikke alltid like lett å vite hvilke lover som gjelder for ens egen virksomhet, men sikkerhetsloven vil være utgangspunktet for all forebyggende sikkerhetstjeneste. Ved for eksempel objektsikkerhet vil det være flere lover og forskrifter som gjør seg gjeldende, og i ulike sektorer i samfunnet vil det være egne regelverk som regulerer sikkerheten. Dette omtales som sektorlovverk, som igjen kan ha egne forskrifter.

I noen tilfeller kan det være vanskelig å vite hvilket lovverk man skal forholde seg til.

Er det sikkerhetsloven, sektorlovgivningen eller forskriftene som gjelder?

Ulike lover og regelverk

Person-opplysnings-loven

Sikkerhets-loven

Brannvern-loven

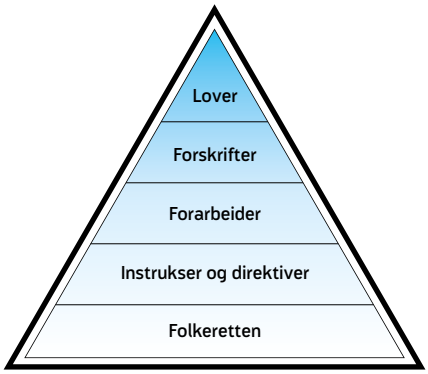
Plan- og bygnings-loven

Beskyttelses-instruksen

Instruks om sikring og beskyttelse av objekter ved bruk av sikrings-styrker fra Forsvaret og politiet i fred, krise og krig

Forsvars-sjefens direktiv for sikring av Forsvarets materiell

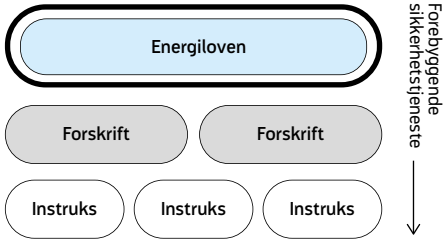
Hierarki lovverk



Lovverk

Eksempel på lovverk for skjermingsverdige objekter

Eksempel på en virksomhet som har eget sektorregelverk



Sikkerhetsloven og sektorregelverk

Sikkerhetslovens virkeområde er definert i lovens § 2. Hovedregelen er at loven gjelder for forvaltningsorganer og for alle leverandører som leverer varer eller tjenester til et forvaltningsorgan i forbindelse med sikkerhetsgradert anskaffelse. Loven får også anvendelse på forvaltningsorganer i utlandet, blant annet norske utenriksstasjoner og militære enheter som deltar i internasjonale operasjoner.[1]

Sikkerhetsloven skal fungere som en sektorovergripende lov, der den gjelder på tvers av alle samfunnssektorer. Det er i dag virksomheter i alle sektorer som er underlagt sikkerhetslovens bestemmelser om sikring av skjermingsverdige objekter.

I forarbeidene til sikkerhetsloven er det uttalt at der hvor det mangler et eget sektorregelverk som omhandler objektsikkerhet, må man benytte seg av sikkerhetsloven. Videre er det slik at der det er eget sektorregelverk som harmonerer med sikkerhetsloven[2] eller er strengere, skal sikkerhetsloven stå tilbake, og der sektorregelverket er mangelfullt, vil sikkerhetsloven virke reparerende.

Objektsikkerhet og forholdet til sektorregelverk

Der det ikke finnes et eget sektorregelverk som omhandler objektsikkerhet, vil hovedregelen være at man følger bestemmelsene i sikkerhetsloven kapittel 5, samt forskrift om objektsikkerhet. I de tilfellene der det foreligger et sektorregelverk, må man kontrollere at bestemmelsene gir like eller strengere føringer for objektsikkerhet. Er dette tilfelle og det er etablert et tilsynsorgan, går sektorlovgivningen foran bestemmelsene i sikkerhetsloven og objektsikkerhetsforskriften[3].

Nasjonal sikkerhetsmyndighet (NSM), som er fagmyndighet innen forebyggende sikkerhetstjeneste, kan bistå ved usikkerhet rundt hvilke regler som gjelder for en gitt virksomhet.

1 Jf. Ot.prp. nr. 49 s. 64

2 Ot.prp.nr. 21 (2007–2008) Om lov om endringer i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven)

3 Jf. forskrift om objektsikkerhet (objektsikkerhetsforskriften) § 1–3

4 Jf. kronprinsregentens resolusjon 4. juli 2003 om fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet

5 Med «virksomhet» menes et forvaltningsorgan eller annet rettssubjekt som sikkerhetsloven gjelder for, jf. sikkerhetsloven § 3 nr. 6

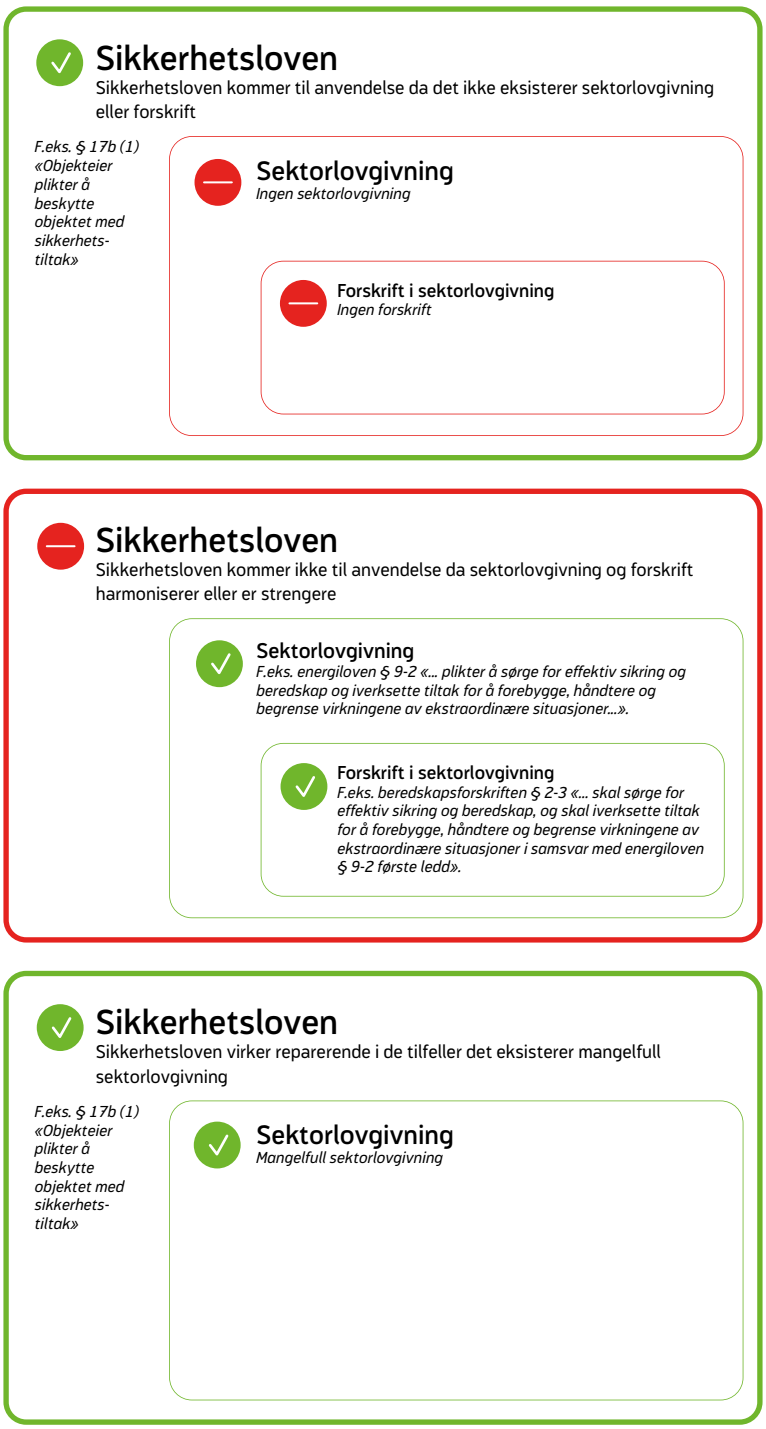
6 Jf. sikkerhetsloven § 5

7 Jf. sikkerhetsloven § 17 og forskrift om objektsikkerhet 22. okt. 2010 nr. 1362 §§ 2-1 og 2-2

8 Som «objekteier» menes virksomhet eller person som eier eller på annen måte råder over skjermingsverdige objekt, jf. sikkerhetsloven § 3 nr. 14

9 Se kapittel 6 Verdivurdering

Sikkerhetsloven og sektorlovgiving



Forpliktelser

Det overordnede ansvaret for forebyggende sikkerhet i militær og sivil sektor ligger hos henholdsvis Forsvarsdepartementet og Justis- og beredskapsdepartementet,[4] men den utøvende funksjonen ivaretas av Nasjonal sikkerhetsmyndighet. Med forebyggende sikkerhet menes «planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet», jf. sikkerhetsloven § 3 nr. 1. Den enkelte virksomhet[5] plikter å utøve forebyggende sikkerhetstjeneste i henhold til bestemmelsene gitt i, eller i medhold av, sikkerhetsloven[6]. Samtidig stiller objektsikkerhetsforskriften krav til objekteiere om å iverksette sikkerhetstiltak slik at skjermingsverdige objekter er tilfredsstillende beskyttet i henhold til gitt klassifisering (VIKTIG, KRITISK og MEGET KRITISK). Sikkerhetsloven har definert skjermingsverdige objekter som «eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser», jf. sikkerhetsloven § 3 nr. 12. Begrepet «eiendom» skal forstås som områder, bygninger, anlegg, transportmidler eller annet materiell, eller deler av slik eiendom, jf. sikkerhetsloven § 3 nr. 13. Sikkerhetstiltakene som implementeres, skal utgjøre en permanent grunnsikring av objektet, og må kunne justeres opp dersom risikoen øker.

Virksomhetens forpliktelser

Det er det enkelte sektordepartementet som skal utpeke og klassifisere skjermingsverdige objekter innen sine myndighetsområder,[7] men som objekteier[8] skal du foreslå overfor departementet hvilke objekter som kan være skjermingsverdige og utarbeide en skadevurdering[9]. Etter at fagdepartementet har fastsatt en klassifiseringsgrad, plikter objekteier å beskytte objektet med forebyggende sikkerhetstiltak, jf. sikkerhetsloven § 17b første ledd.

Loven gir ingen føringer på hvilke forebyggende sikkerhetstiltak som må være til stede, men presiserer at de må bestå av en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon. Dette kalles grunnsikringstiltak[10] og blir en skjønnsmessig avveining av den enkelte objekteier. Sikkerhetstiltakene som implementeres, skal planlegges, gjennomføres og vedlikeholdes etter en permanent grunnsikring for objektet, der objekteier også skal planlegge for og gjennomføre påbygging av grunnsikring ved økt risiko.[11] Hvilke sikringstiltak som velges, må fastsettes på bakgrunn av objektes klassifiseringsnivå, samt risikovurdering og sikkerhetsrevisjon.[12] Uavhengig om man følger bestemmelsene om objektsikkerhet eller egen sektorlovgivning, har objekteier meldeplikt etter forskrift om objektsikkerhet[13].

Skjermingsverdig objekt

Meget kritisk[14]

Klassifiseringsgraden benyttes dersom «det kan få helt avgjørende skadefølger for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse av uvedkommende».

Objekter klassifisert som MEGET KRITISK skal «beskyttes slik at tap av funksjon, ødeleggelse og rettstridig overtakelse avverges», jf. sikkerhetsloven § 17b annet ledd bokstav a.

Hva innebærer «tap av funksjon», «ødeleggelse» og «rettstridig overtakelse avverges»? Loven gir ingen veiledning om hva som ligger i begrepene, men en naturlig språklig forståelse av begrepet «tap av funksjon» tilsier at objekteier plikter å beskytte sitt objekt slik at tilsiktede/utilsiktede hendelser ikke gjør at objektet mister sin funksjon[15] permanent. Hvis det er mulig å gjenopprette funksjonen etter en viss tid ved en form for redundans, kan dette være tilstrekkelig. En naturlig språklig forståelse av begrepet «ødeleggelse» tilsier at objekteier plikter å beskytte sitt objekt slik at tilsiktede/utilsiktede hendelser ikke gjør at noen deler av objektet fysisk blir satt ut av spill. Hvis det for eksempel er fare for at en del av objektet er utsatt for eksplosjonsvirkninger fra vei, må objektet enten sikres mot dette eller flyttes. En naturlig språklig forståelse av begrepet «rettstridig overtakelse avverges» tilsier at handlingen må være ulovlig, og at objekteier plikter å beskytte objektet slik at ingen deler av objektet kan overtas/beleires av uvedkommende.

Kritisk[16]

Klassifiseringsgraden nyttes dersom «det alvorlig kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse av uvedkommende».

Objekter klassifisert som KRITISK skal «beskyttes slik at tap av funksjon og ødeleggelse begrenses og rettstridig overtakelse av vesentlige funksjoner avverges», jf. sikkerhetsloven § 17b annet ledd bokstav b.

Hva ligger i begrepene «tap av funksjon og ødeleggelse begrenses» eller «rettstridig overtakelse av vesentlige funksjoner avverges»? Heller ikke her gir loven veiledning om hva som ligger i begrepene. En naturlig språklig forståelse av begrepet «begrenses» tilsier at objekteier plikter å beskytte sitt objekt slik at tilsiktede/utilsiktede hendelser ikke påvirker hele objektet, men at noe kan mistes. Hvis det er mulig å reparere eller bare deler av objektet påvirkes ved at det har tilstrekkelig avstand/skjermet fra eksplosjoner eller tyngre våpen, kan dette være tilstrekkelig. En naturlig språklig forståelse av begrepet «rettstridig overtakelse av vesentlige funksjoner avverges» tilsier at deler av objektet kan bli rettstridig overtatt/beleiret, men ikke de viktigste funksjonene som gjør at objektet kan opprettholde drift/funksjon.

10 Jf. objektsikkerhetsforskriften § 3-1 annet ledd

11 Jf. objektsikkerhetsforskriften § 3-1

12 Ibid.

13 Objektsikkerhetsforskriften §§ 2-4 og 4-3

14 Jf. sikkerhetsloven § 17a første ledd bokstav a

15 Med funksjon/funksjonalitet menes: «produksjon, forsyning, kommunikasjon eller annen rettmessig bruk eller aktivitet tilknyttet eiendommen», jf. sikkerhetsloven § 3 første ledd nr. 15

16 Jf. sikkerhetsloven § 17a første ledd bokstav b

Viktig[17]

Klassifiseringsgraden nyttes dersom «det kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse av uvedkommende».

Objekter klassifisert som VIKTIG skal «beskyttes slik at tap av vesentlig funksjon og ødeleggelse begrenses», jf. sikkerhetsloven § 17 b annet ledd bokstav c. Tolkningen av begrepene er det samme som over, men det er ikke krav til beskyttelse mot «rettstridig overtakelse».

Ansattes forpliktelser

Ikke alle har et bevisst forhold til sikkerhet. Noen tenker at det er bare lederen eller en som er utpekt til å ha dette ansvaret, som sørger for at jeg er trygg på jobb. Mange av oss opplever sikkerhetstruende hendelser hver eneste dag. Det kan være en kollega som glemmer å låse datamaskinen, en kortleser som er i ustand, eller en dør som ikke lukker seg ordentlig. Det kan være mer alvorlige hendelser som virusangrep eller hacking i virksomheten, eller det kan være en mistenkelig person som tar notater, fotograferer og utarbeider skisser over arbeidsplassen din. Felles for alle sammen er at det er sikkerhetstruende hendelser og kan være sikkerhetsbrudd. Mange vil rapportere når det oppleves avvik fra den fastsatte sikkerhetsstandarden, men ikke alle. Vi tenker ofte at det er andre som har oppdaget avviket, og vi vil ikke involvere oss fordi vi ikke vil fremstå som den som overreagerer.

Sikkerhetsloven er helt klar når det gjelder ansvar for forebyggende sikkerhet:

«Alt ansatt eller engasjert personell har i sitt arbeid eller oppdrag for virksomheten ansvar for å ivareta sikkerhetsmessige hensyn, og plikter å bidra til forebyggende sikkerhet», jf. sikkerhetsloven § 5 fjerde ledd.

Sikkerhetsgradert/sensitiv informasjon

Sikkerhetsloven stiller krav om at informasjon som defineres som sikkerhetsgradert[18], skal merkes og beskyttes. Virksomheter som ønsker å beskytte informasjon av andre grunner, kan benytte graderingen FORTROLIG og STRENGT FORTROLIG i henhold til beskyttelsesinstruksen. Dette forutsetter at informasjonen kan unntas fra offentlighet i medhold av offentlighetsloven, og at det vil kunne ha skadevirkninger at dokumentets innhold blir kjent for uvedkommende.[19]

For tilgang til informasjon gradert KONFIDENSIELT eller høyere, kreves en sikkerhetsklarering[20] av en klareringsmyndighet (KM). Enhver som skal ha befatning med sikkerhetsgradert informasjon BEGRENSET, KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG, må på forhånd autoriseres.[21] Personen som skal sikkerhetsklareres, sender en personopplysningsblankett via anmodningsmyndigheten (AM) til klareringsmyndigheten. De største klareringsmyndighetene i Norge er Forsvarets sikkerhetsavdeling (FSA) og Nasjonal sikkerhetsmyndighet (NSM). Sikkerhetsklarering omfatter en bakgrunnssjekk som varierer, avhengig av hvilket nivå man skal klareres for. For STRENGT HEMMELIG innhentes det opplysninger om hovedpersonen og alle nærstående personer.[22] Etter vedtatte endringer i sikkerhetsloven vil det fra 1.1.2017 primært være to klareringsmyndigheter; én for forsvarssektoren (FSA) og én for den sivile sektoren (NSM).[23]

Noen eksempler på hva som kan være sikkerhetsgradert informasjon:

- *Tegninger, foto, kart, skisser o.l. over militære anlegg, kritisk infrastruktur, nøkkelpunkt*
- *Oversikt over sikkerhetstiltak*
- *Beredskapsplanverk*
- *Trusselvurderinger*
- *Risikovurderinger*
- *Operasjonsordrer*

17 Jf. sikkerhetsloven § 17a første ledd bokstav c

18 Jf. sikkerhetsloven § 11

19 Jf. beskyttelsesinstruksen §§ 3 og 4

20 Definisjon av begrepet sikkerhetsklarering: «avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad», jf. sikkerhetsloven § 3 første ledd nr. 19

21 Jf. sikkerhetsloven § 19

22 NSMs nettsider, informasjon om sikkerhetsklarering *www.nsm.stat.no*

23 Jf. Innst. 352 L (2015–2016)

NØKKEL-PUNKT

I krise og krig trer nøkkelpunktdirektivet i kraft. Dette utarbeides av Forsvaret for å sikre personer og objekter som er av betydning for forsvarsevnen ved utløst nasjonal krisetilstand eller væpnet konflikt.

Det stilles særlige krav til sikring av nøkkelpunkt, og på lik linje med objektsikkerhetsforskriften vil også nøkkelpunktdirektivet legge føringer for risikovurdering av et objekt.

- *Personopplysninger*
- *Informasjon som sier noe om kapasitet og størrelse*
- *Systembeskrivelser*

Merking[24]

Det er den personen som utarbeider eller endrer informasjonen/dokumentet, som har ansvar for å påføre riktig sikkerhetsgrad og det skal merkes med høyeste sikkerhetsgrad av informasjon i dokumentet. På pc-er, USB, SD-kort eller andre lagringsmedier skal gjenstanden merkes med høyeste sikkerhetsgrad av informasjon som er eller har vært på mediet. Merkingen skal være i rødt og plasseres lett synlig. På dokumenter av papir eller annet materiale med sider skal merkingen være synlig både øverst og nederst på alle sider av dokumentet.

Oppbevaring[25]

Etter sikkerhetsloven § 11 har «enhver som får tilgang til sikkerhetsgradert informasjon som ledd i arbeid, oppdrag eller verv», plikt til å beskytte informasjonen. I dette ligger det ulike krav til oppbevaring. Se ***tabell Oppbevaring av sikkerhetsgradert informasjon.***

Sikkerhetsgraderte anskaffelser

- *Ved bruk av leverandører for anskaffelser av varer eller tjenester hvor disse skal få tilgang til skjermingsverdig informasjon eller objekt, og virksomheten er underlagt sikkerhetsloven, vil det være ulike lovfestede krav:*
- *Om virksomheten skal utveksle informasjon som er gradert, må det foreligge en sikkerhetsavtale*[26]*. Avtalen skal blant annet inneholde nærmere detaljer om ansvar og plikter om anskaffelsens sikkerhetsgrad, praktisk gjennomføring av undersøkelser hos leverandør for å vurdere sikkerhetstilstanden og konsekvenser ved brudd på sikkerhetsavtalen.*
- *Videre må det foreligge en leverandørklarering for oppdrag som gir tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere.*
- *For minimumsvilkår og -krav til sikkerhetsavtale, utlevering og tilbakelevering av skjermingsverdig informasjon, leverandørklarering, internasjonale sikkerhetsgraderte anskaffelser m.m. vises det til forskrift om sikkerhetsgraderte anskaffelser av 1. juli 2001 nr. 753. For Forsvaret vises det også til forskrift om forsvars- og sikkerhetsanskaffelser.*

Plan- og bygningsloven

Forskrift om tekniske krav til byggverk setter krav til blant annet rømningsveier, dagslysforhold og konstruksjonssikkerhet. Dette er typiske eksempler på forhold som kan komme i konflikt med kravene til sikring:

Krav om tilbakerømning

Eksempelvis kan krav til sikring av BESKYTTET og SPERRET OMRÅDE være i konflikt med krav om tilbakerømning. Det anses som lite hensiktsmessig å bruke penger på en sikkerhetsdør hvis en inntrenger kan komme inn ved å utløse brannalarmen eller trykke inn glasset på en nødbryter for at låsen skal slippe. I veiledning til TEK10 § 11-13 syvende ledd er det fastsatt følgende minstekrav:

«Dør til rømningsvei skal prosjekteres og utføres slik at den sikrer rask rømning og slik at det ikke oppstår fare for oppstuving. Følgende skal minst være oppfylt:

a) Dør skal ha tilstrekkelig bredde og høyde, og den skal være lett å åpne uten bruk av nøkkel.

b) Dør skal slå ut i rømningsretningen. Dør til rømningsvei kan likevel slå mot rømningsretningen dersom det ikke er fare for oppstuving ved rømning».

Flammer og skadelige gasser kan gjøre det umulig å bruke rømningsveien slik at perso-

24 Forskrift om informasjonssikkerhet av 1. juli 2001 nr. 744 kap. 4 A

25 Ibid. § 6-9 til § 6-12

26 Jf. sikkerhetsloven § 27

Oppbevaring av sikkerhetsgradert informasjon

Gradering	Krav
BEGRENSET	Skal oppbevares i avlåst rom eller i låsbart skap/skuff
KONFIDENSIELT	Skal oppbevares i sperret område (sperret KONFIDENSIELT), eller i godkjent oppbevaringsenhet i beskyttet område.
HEMMELIG	Skal oppbevares i sperret område sikret som hvelv (sperret HEMMELIG), eller i godkjent oppbevaringsenhet for HEMMELIG i beskyttet område.
STRENGT HEMMELIG	Skal oppbevares i sperret område sikret som hvelv. I tillegg må området sikres med permanent vakthold eller godkjent elektronisk sikringsanlegg. Det er her krav til balansert sikring.

Det finnes også andre måter å oppbevare sikkerhetsgradert informasjon på.
Se forskrift om informasjonssikkerhet av 1. juli 2001 nr. 744 kap. 6.

ner må rømme tilbake. Dette kan løses ved at man har en manuell utløser av lås med alarm på utsiden av nødutgangen. I noen tilfeller er ikke dette mulig fordi det er lovmessig krav til sikring av rom eller område, og det må derfor gjøres en risikovurdering i hvert tilfelle.

Dagslys

Etter TEK10 § 13-12 annet ledd så skal rom med varig opphold gi tilfredsstillende tilgang på dagslys. Dette kan fravikes hvis «virksomheten tilsier noe annet», jf. annet ledd. Regelen kan fravikes hvis det for eksempel gjelder fjellanlegg, rom som ikke kan ha vindu på grunn av sikringsklassen, eller områder som må være skjermet for innsyn. En bør i slike tilfeller sørge for å legge til rette for god kunstig belysning.

Konstruksjonssikkerhet

Tekniske forskrifter til plan- og bygningsloven (pbl) stiller krav om at bygningskonstruksjoner i Norge prosjekteres og utføres slik at det oppnås tilfredsstillende sikkerhet mot brudd og tilstrekkelig stivhet og stabilitet for laster som kan oppstå under forutsatt bruk. Grunnleggende krav til mekanisk motstandsevne og stabilitet kan oppfylles ved prosjektering av konstruksjoner etter NS-EN-1990 Eurokode: Grunnlag for prosjektering av konstruksjoner og underliggende standarder i serien NS-EN 1991 til NS-EN 1999, med tilhørende nasjonale tillegg.

De grunnleggende kravene til konstruksjonssikkerhet for bygninger i Norge, innebærer at bygninger prosjekteres og utføres for å gi tilfredsstillende sikkerhet både mot kjente, men også ikke-kjente ulykkeslaster fra ulike hendelser som eksplosjoner, støt eller konsekvenser av menneskelige feil. Eurokoden omfatter ikke ulykkeslaster forårsaket av utvendige eksplosjoner eller reststabilitet av bygninger som er skadet av seismiske påvirkninger, brann osv. Eurokoden stiller likevel krav om at en konstruksjon skal prosjekteres og utføres, slik at den ikke vil bli skadet ved ulike hendelser i et omfang som ikke står i forhold til den opprinnelige årsaken.

Se ***kapittel 16 Beskyttelse mot eksplosiver*** for mer inngående beskrivelser av krav til konstruksjonssikkerhet.

Forslag til ny sikkerhetslov

I mars 2015 ble det oppnevnt et utvalg for å utrede og foreslå et nytt lovgrunnlag for forebyggende nasjonal sikkerhet. Noe av bakgrunnen for en ny revidering av sikkerhetsloven var blant annet at trusselbildet har endret seg fra en typisk trussel til å stadig bli mer atypisk og komplekst. Den økte digitaliseringen i samfunnet har bidratt til en positiv utvikling, men har også gjort oss mer sårbare. Utvalget har derfor foreslått en rekke konkrete tiltak for å møte nye trusler og nye sårbarheter. Dette vil legge til rette for en styrket samhandling i det forebyggende sikkerhetsarbeidet.

Hele forslaget til ny lov kan leses i NOU 2016:19 «Samhandling for sikkerhet – beskyttelse av grunnleggende samfunnsfunksjoner».

Relevante lover og forskrifter m.m.

Lover	
Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) med forskrifter	→ Sikkerhetsloven omhandler sikkerhetsadministrasjon, personellsikkerhet, objektsikkerhet, informasjonssikkerhet og sikkerhetsgraderte anskaffelser. Loven med forskrifter omhandler blant annet sikring av områder, deler av bygg og/eller rom i bygning hvor sikkerhetsgradert informasjon/materiell skal behandles, samt anskaffelse av tjenester der tjenesteyter får tilgang til sikkerhetsgradert informasjon.
Lov om elektronisk kommunikasjon (ekomloven)	→ Det er ulike krav til tilbydere av elektronisk kommunikasjonsnett og –tjeneste i fred, krise og krig. I lovens kapittel 2 finner man regler som omhandler sikkerhet og beredskap. Relevante forskrifter er forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) og forskrift om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett (klassifiseringsforskriften).
Lov om havner og farvann (havne- og farvannsloven)	→ Lovens § 43 omhandler sikkerhet og terrorberedskap i havner og havneterminaler. Relevante forskrifter er forskrift om sikring av havner og forskrift om sikring av havneanlegg.
Lov om luftfart (luftfartsloven)	→ For å sikre nødvendig nasjonal beredskap i krig, ved krise, og i andre ekstraordinære situasjoner, kan departementet pålegge aktører innen luftfarten blant annet å yte bistand i beredskapsplanlegging, fysisk sikring, samarbeid med nasjonale og internasjonale aktører og gjennomføre eller delta på militære øvelser.
Lov om forsvarshemmeligheter (opphevet) Midlertidig lov om beskyttelse av og kontroll med geografisk informasjon av hensyn til rikets sikkerhet	→ Lov om forsvarshemmeligheter er opphevet. For å videreføre enkelte forskriftshjemler i den opphevede loven er en midlertidig lov vedtatt, midlertidig lov om beskyttelse av og kontroll med geografisk informasjon av hensyn til rikets sikkerhet. Denne loven fungerer foreløpig som hjemmelsgrunnlag for blant annet forskrift om fotografering mv. fra luften og kontroll av luftfotografier og opptaksmateriale fra luftbårne sensorsystemer. Loven gjelder i to år fra ikraftsettingstidspunktet.

Lover forts.	
Plan- og bygningsloven	→ Loven omhandler blant annet unntak fra offentlig byggesaksbehandling når anlegget er å anse som militært objekt.
Lov om behandling av personopplysninger	→ Loven omhandler blant annet meldeplikt ved bruk av tv-overvåkning, automatiske adgangskontrollanlegg og i enkelte tilfeller automatiske innbruddsalarmanlegg. (Systemer hvor personopplysninger, herunder bilder, registreres og behandles.)
Lov om vern mot brann, eksplosjon og ulykker med farlig stoff og om brannvesenets redningsoppgaver (brannvernloven)	→ Loven omhandler blant annet krav til rømningsveier. Loven er aktuell når det gjelder bruk av automatiske adgangskontrollanlegg.
Lov om politiet (politiloven)	→ I loven finnes det bestemmelser om politiets oppgaver, hvem som kan inneha politimyndighet, og hvordan politiet kan få bistand fra Forsvaret.
Lov om vaktvirksomhet	→ I loven finnes det bestemmelser om ervervsmessig vaktvirksomhet og egenvakthold for forvaltningsorganer. Videre finnes det bestemmelser om krav til ansatte, legitimasjon, bruk av makt, bruk av hund, krav til kommunikasjonsutstyr m.m.
Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)	→ Loven er primært for å legge til rette for åpen og gjennomsiktig offentlig informasjon. I loven finnes det bestemmelser for å unnta informasjon fra innsyn. Dette kan blant annet være informasjon som bør unntas grunnet nasjonale forsvars- og sikkerhetshensyn.
Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven)	→ Loven har bestemmelser om blant annet hvem som inngår i Kraftforsyningens beredskapsorganisasjon (KBO), plikter med hensyn til sikring av kraftforsyning og informasjonssikkerhet. Forskrift til energiloven (beredskapsforskriften) harmoniserer godt med sikkerhetsloven.
Lov om petroleumsvirksomhet (petroleumsloven)	→ Loven har bestemmelser om blant annet beredskap mot bevisste anslag, sikkerhetssoner rundt oljeinstallasjoner og krav til sikkerhetsdokumentasjon. Forskrift til petroleumsloven har ikke lovfestede sikringstiltak som harmoniserer med sikkerhetsloven.
Forskrifter	
Sikkerhetsloven	→ Forskrift om objektsikkerhet (objektsikkerhetsforskriften) → Forskrift om informasjonssikkerhet (informasjonssikkerhetsforskriften) → Forskrift om personellsikkerhet → Forskrift om sikkerhetsgraderte anskaffelser → Forskrift om sikkerhetsadministrasjon
Havne- og farvannsloven	→ Forskrift om sikring av havner → Forskrift om sikring av havneanlegg
Energiloven	→ Beredskapsforskriften
Klassifiseringsforskriften	→ Forskriften gjelder for nettilbydere som tilbyr elektronisk kommunikasjonsnett og -tjeneste for brukere i fred, krise og krig.

Forts. neste side →

→ Forts.

Folkeretten	
Tilleggsprotokoll til Genèvekonvensjonene av 12-08-49 (TP I)	→ Tilleggsprotokollen omhandler beskyttelse av ofre for internasjonale væpnede konflikter (Protokoll I), som blant annet har bestemmelser om plassering av militære anlegg i forhold til sivil bebyggelse. Etter konvensjonen kan en motstander bare angripe det som er definert som «lovlige mål». Se også Del IV Vedlegg nr. 22: Strafferettslig vern av militær EBA med særlig vekt på fysisk sikring.
Forarbeider	
Sikkerhetsloven	→ Prop. 97 L (2015–2016) → Ot.prp. nr. 21 (2007–2008) → Ot.prp. nr. 49 (1996–1997)
Instruks, retningslinjer og direktiver	
Beskyttelsesinstruksen	→ Instruksen kommer til anvendelse ved beskyttelse av andre dokumenter enn de som omfattes av sikkerhetsloven med forskrifter. Beskyttelsesgradene som nyttes, er STRENGT FORTROLIG og FORTROLIG. Det spiller ingen rolle hvilket medium dokumentet er lagret på.
Instruks om sikring og beskyttelse av objekter ved bruk av sikringsstyrker fra Forsvaret og politiet i fred, krise og krig (kgl.res. 24. august 2012)	→ Instruksen fastsetter ansvarsforhold og samarbeid om politiets og Forsvarets objekt-sikring ved bruk av sikringsstyrker. Formålet med objektsikringen er at viktige objekter skal opprettholde sin virksomhet og funksjonalitet i kritiske situasjoner. Instruksen sier også noe om hvem som har beslutningsmyndighet for iverksettelse av objektsikring ved bruk av sikringsstyrker fra Forsvaret og politiet.
Direktiv for sikkerhetstjenesten i Forsvarets militære organisasjon	→ Direktivet beskriver hvordan sikkerhetstjenesten, herunder også fysisk og elektronisk sikring, skal utføres i Forsvarets militære organisasjon.
Forsvarssjefens direktiv for krav til sikkerhetsstyring i Forsvaret	→ Direktivet beskriver roller og ansvarsområder knyttet til beskyttelse av Forsvarets operative evne og dets grunnlag (materiell, ytre miljø, personell, informasjon, infrastruktur og aktivitet).
Forsvarssjefens direktiv for beskyttelse mot terrorisme	→ Direktivet beskriver hvordan Forsvarets militære organisasjon skal sikre og beskytte seg ved innføring av terrorberedskap.
Forsvarsdepartementets retningslinjer for tjenestefeltet eiendommer, bygg og anlegg, av 6. september 2004	→ Retningslinjene beskriver ansvarsforhold ved blant annet anskaffelse, leie, drift, vedlikehold og avhending av EBA i Forsvaret.
Direktiv for uttak og sikring av nøkkelpunkt (nøkkelpunktdirektivet)	→ Direktivet omfatter føringer for hvordan Forsvaret skal sikre befolkningen og viktige objekt ved krise eller væpnet konflikt. Disse objektene blir betegnet som «lovlige mål» ved en væpnet konflikt, og må derfor sikres ved hjelp av militære styrker.
Veiledninger	
NSM Veileder for objektsikkerhetsforskriften	→ I NSMs veileder for objektsikkerhet beskrives det hvilken trusselaktør som skal legges til grunn for vurderingene av et skjermingsverdig objekt. Det er derfor viktig at man i starten av en risikovurdering undersøker om hele eller deler av objektet man skal gjøre en risikovurdering av, er skjermingsverdig, og eventuelt hvilken klassifisering objektet har, fordi det vil legge føringer for arbeidet med risikovurderingen og tiltakene som anbefales.

Veiledninger forts.	
NSM Veileder i fysisk sikring mot ulovlig inntrengning	→ I denne veilederen beskrives det hvordan man behandler og oppbevarer sikkerhetsgradert informasjon. Dette gjelder særlig krav til oppbevaringsenheter, adgang til områder, håndtering av nøkler og koder, låser, dører og elektronisk sikring.
NSM Veiledning i sikring mot avlytting	→ I denne veilederen beskrives hvordan man kan sikre rom mot uønsket avlytting og innsyn av sikkerhetsgradert informasjon.
NSM Veiledning for sikring av kryptorom	→ Denne veilederen gir informasjon om hvordan man kan planlegge og sikre et kryptorom. Dette gjelder blant annet krav til vegger, vinduer, dører, låser og ventiler, samt tempest-tiltak.
NSM Veileder for sikkerhetsgraderte anskaffelser	→ Denne veilederen gir informasjon og føringer som omhandler forskrift om sikkerhetsgraderte anskaffelser samt enkelte paragrafer i sikkerhetsloven kapittel 7. Veilederen går blant annet inn på graderingsspesifikasjon, sikkerhetsavtale, utvelgelse av leverandører, leverandørklarering, levering av graderte varer og tjenester til utenlandsk anskaffelsesmyndighet og omvendt.
NSM Veiledning til sikkerhetslovens kapittel 6 og forskrift om personellsikkerhet	→ Veilederen gir en innføring i sikkerhetsloven kapittel 6 og forskrift om personellsikkerhet som blant annet omhandler sikkerhetsklarering og autorisasjon, klareringsmyndighet og autorisasjonsansvarlig.
NSM Veiledning i sikkerhetsadministrasjon	→ Det finnes to veiledere i temaet sikkerhetsadministrasjon. Dette er verdivurdering og sikkerhetsstyring. Veiledning i verdivurdering omfatter en klargjøring av hva som kan være verdier, når man benytter en verdivurdering, og redegjørelse for regler rundt forhold knyttet til verdivurdering. Veiledning i sikkerhetsstyring gir råd i blant annet styringssystemet for sikkerhet, herunder ledelsesforankring, styringshjul og organisering og roller.
Veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger – Terrorsikring utgitt av Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste	→ Veilederen er ment som et hjelpemiddel til offentlige og private virksomheter, slik at virksomheten kan planlegge og iverksette sikringstiltak mot terrorhandlinger. Den kan også benyttes som et hjelpemiddel for å sikre seg mot spionasje, sabotasje og annen alvorlig kriminalitet. Veilederen beskriver generelle, kjente prosesser og eksempler på allmenne tiltak.
Aktuelle NATO bestemmelser	
C-M(2002)49 Security within The North Atlantic Treaty Organisation	→ Dette er sikkerhetsbestemmelsene til NATO. De beskriver i hovedsak hvordan sikkerhetsgradert informasjon i NATO skal sikres og beskyttes.
C-M(2002)50 Protection Measures For NATO Civil And Military Bodies Deployed NATO Forces And Installations (Assets) Against Terrorist Threats	→ Direktivet gir føringer om beskyttelse av NATO-personell og installasjoner mot terrortrusler.

DEL 2

PLANLEGGING OG PROSJEKTGJENNOMFØRING

Del 2 Planlegging og prosjektgjennomføring går gjennom de grunnleggende elementene som må ivaretas før konkrete sikringstiltak kan prosjekteres.

Gjennomføring av risikoanalyse er sentralt, og verdivurdering og trusselvurdering er utdypet i egne kapitler. Her får du også en beskrivelse av hvordan planlegging av sikringstiltak i byggeprosjekter bør skje.

Kapittel 5

Risikoanalyse

Dette kapitlet beskriver risikoanalyse, som er en systematisk måte å fremskaffe og fremstille kunnskap på om en usikker fremtid.

Det er en utfordrende oppgave for virksomheter å vurdere hvilke verdier de skal beskytte, hvilke mulige trusler de står overfor, hvor sårbare de er overfor truslene, og hvilken risiko de bør håndtere i fremtiden.

Gjennomføring av en risikoanalyse er en viktig oppgave for private og offentlige virksomheter. Terrorangrepet 22. juli 2011 viste behovet for grunnsikringstiltak rundt viktige samfunnsinstitusjoner som kan være terrormål. Andre virksomheter i privat og offentlig sektor har også et behov for å etablere grunnsikringstiltak for å forhindre innbrudd, etterretning, hærverk og sabotasje. Grunnsikringstiltak er permanente, til forskjell fra sikringstiltak som opprettes ut fra en beredskapssituasjon. Første steg i prosessen med å vurdere hvilke grunnsikringstiltak som må etableres, er gjennomføring av en risikoanalyse. For å finne riktig grunnsikringsnivå må virksomhetene:[1]

- *Identifisere hvilke verdier som trenger særlig beskyttelse – og begrunne hvorfor*
- *Kartlegge hva slags trusler disse verdiene er stilt overfor, herunder ta hensyn til at det kan være rasjonelle aktører man står overfor*
- *Vurdere hvilke sårbarheter som kan utnyttes eller forsterke skadevirkningene av en hendelse*
- *Håndtere risiko (akseptere, redusere mv.)*

Definisjon av risiko

Risiko handler om usikkerhet. Vi skal beskrive noe som ikke har skjedd ennå, noe som vi ikke vil skal skje. Derfor finnes det ikke objektive «fakta» om risiko. Risiko kan defineres som muligheten for at noe ubehagelig skal skje, og at det dreier seg om noe negativt for den som rammes. Dette samsvarer med NS 5814:2008[2], der risiko defineres som et «uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse». Risiko er altså en kombinasjon av to størrelser, sannsynlighet og konsekvens. En alternativ definisjon på risiko er NS 5830:2012, som definerer risiko som «forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifikke trusselen». Her er ikke sannsynlighet spesifikt nevnt og med hensikt utelatt i definisjonen, ettersom denne standarden ikke forholder seg eksplisitt til sannsynlighetsvurderinger. I dette kapitlet benytter vi begrepet risikoanalyse for hele prosessen, og risikovurdering i det steget i prosessen som vurderer risiko.

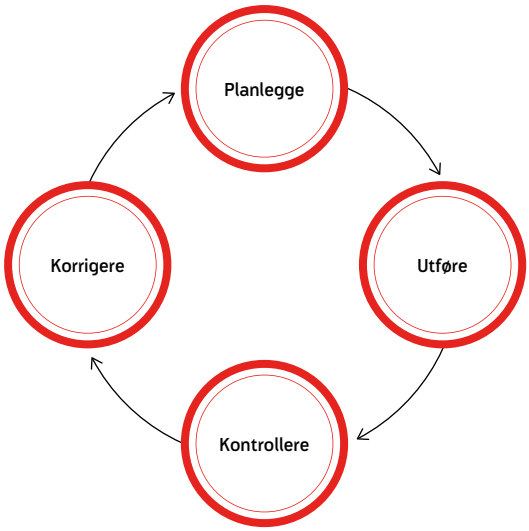
Risikostyring

Risikostyring og håndtering av usikkerhet er i dag et viktig tema på styremøter og i ledelsen i de fleste større bedrifter og etater. Risikoanalysen er et trinn i risikostyringsstrategien for virksomheten. Utfordringene er mange. Hvor-

1 St.meld. 21 (2012–2013) Terrorberedskap

2 Krav til risikovurderinger. Norsk standard NS 5814: 2008

Styringsprosess



dan skal man på best mulig måte balansere konflikten mellom det å utforske muligheter på den ene siden og unngå uønskede hendelser på den andre siden?

Med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko.[3]

Risikostyring handler på den ene siden om å få innsikt i risikoforhold, effekt av tiltak, grad av styrbarhet av risiko mv., og på den andre siden metoder, prosesser og strategier for å kunne kartlegge og styre risikoene.[4] Formålet med risikostyring er med andre ord å skape den riktige balansen mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap.[5]

Risikostyring gjennomføres som en tradisjonell styringsprosess, se ***figuren Styringsprosess***. Denne prosessen omfatter kartlegging av situasjonen og problemformulering. Neste steg i prosessen er å gjennomføre en risikoanalyse basert på planleggingsfasen.

Risikoanalysen danner grunnlaget for å vurdere tiltak som reduserer risikoen. I løpet av prosjektutviklingen bør risikovurderingen benyttes til å vurdere gjenstående risiko. Vurderingene bør knyttes opp til de ulike prosjektfasene, slik at det kan inngå i beslutningsunderlaget for eventuell revisjon og oppdatering. Avvikene bør rapporteres internt i organisasjonen og eksternt til virksomheter der virksomheten har en rapporteringsplikt.

Sikringshåndboka belyser prosessene fra planlegging og risikoanalyse til tiltak.

Hva kan risikoanalyser brukes til?

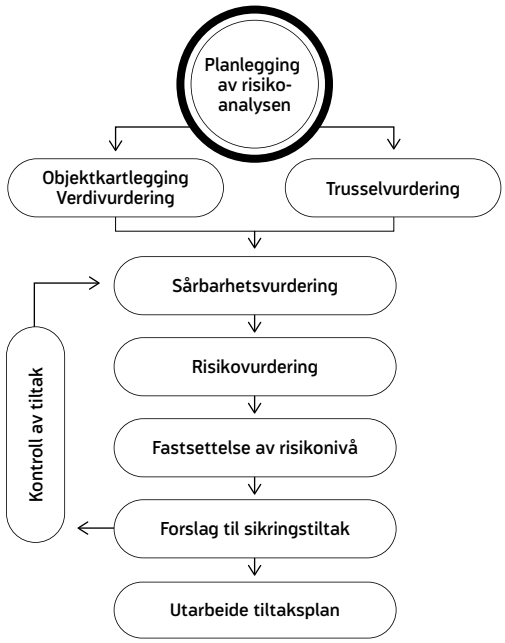
Risikoanalyser kan benyttes til flere ulike formål:[6]

- → *Etablere et risikobilde*
- → *Sammenligne ulike alternativer og løsninger for risikostyring*

3, 4, 5
Aven, Terje (2007) Risikostyring

6
Terje Aven mfl. (2010) Risikovurdering. Universitetsforlaget: Oslo

Modell for gjennomføring av risikoanalyse



- → *Identifisere faktorer (aktiviteter, systemer, komponenter osv.) som har stor betydning når det gjelder risiko*
- → *Gi et bilde av hvordan ulike sikringstiltak kan redusere risikoen*

Resultatene fra risikoanalysene kan videre benyttes i alt fra å kontrollere at virksomheten tilfredsstiller lov- og forskriftskrav til valg mellom alternative løsninger og sikringstiltak. Risikoanalyser kan med fordel gjennomføres i flere ulike faser av en byggeprosess, fra tidlig idéfase, planleggingsfase og konstruksjonsfase til driftsfase og avviklingsfase. Formålet er hele tiden det samme: Å utarbeide et beslutningsgrunnlag som kan brukes for å balansere ulike hensyn, som sikkerhet, økonomi og andre forhold som vil kunne gjøre seg gjeldende som vurderingskriterier.

Modell for risikoanalyse

De ulike standardene benytter ulike definisjoner på risiko. Vi benytter begrepet risikoanalyse for hele prosessen, og begrepet risikovurdering for den delen av risikoanalysen som vurderer risiko. Risikoanalyser kan gjerne være et prosjekt med en planleggingsfase, gjennomføringsfase og en avslutningsfase. Målsettingen bør være en systematisk prosess med deltakelse av fagpersoner, prosessleder og personer fra virksomheten (eier av analyseobjektet).

Vi ser av ***figuren Modell for gjennomføring av risikoanalyse*** hvilke trinn i prosessen vi vurderer før risiko fastsettes, og tiltak for å redusere risikoen beskrives. Dette kapitlet vil gå gjennom de ulike prosesstegene og har til

hensikt å gi leseren et godt utgangspunkt for å gjennomføre en risikoanalyse uavhengig av standard som benyttes.

Standarder og veiledninger for risikoanalyser

Det er utviklet flere standarder og veiledninger for utførelse av risikovurderinger både nasjonalt og internasjonalt.[7] I Norge er det tre standarder som i hovedsak benyttes for risikoanalyse i forbindelse med sikring av bygg: ISO 31000 (Risikostyring – Prinsipper og retningslinjer), NS 5814 (Krav til risikovurdering) og NS 5832 (Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse). I tillegg finnes det en rekke andre relevante standarder og veiledere, som blant annet omtaler internkontroll og informasjonssikkerhet, og andre fagspesifikke modeller. Forsvarets forskningsinstitutt (FFI) har i rapporten «Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger»[8] identifisert noen fellestrekk for de ulike metodene:

- *Alle tilnærmingene har som formål å «finne risikoen knyttet til at noe skal kunne skje»*
- *Begrepet «sannsynlighet» benyttes enten eksplisitt (NS 5814) eller implisitt (NS 5832)*
- *Kartlegging av sikringsbarrierer er viktig og inkluderes av alle tilnærmingene enten som et eget trinn i analysen, eller som en del av en sårbarhetsanalyse*
- *Alle tilnærmingene legger vekt på en systematisk fremgangsmåte og har i stor grad de samme hovedprosessdelene (systembeskrivelse/verdivurdering, trusselvurdering, sårbarhetsvurdering, risikovurdering, risikoreduserende tiltak)*

FFI mener at de to tilnærmingene har mange likhetstrekk, og at prosessdelene og vurderingene ikke skiller seg vesentlig fra hverandre. Hovedforskjellen ligger i hvorvidt sannsynlighetsvurderingen beskrives eksplisitt, som i NS 5814, eller implisitt som i NS 5832.

FFI gir noen anbefalinger i rapporten angående gjennomføring av risikovurderinger[9]:

- *Kunnskap og metodeforståelse er viktigere enn valg av metode og tilnærming*
- *Unngå en homogen ekspertgruppe; etterstreb en tverrfaglig sammensetning der representantene har ulike perspektiver, kompetanse og bakgrunn*
- *Etterstreb enkel og forståelig formidling*
- *Synliggjør og beskriv usikkerhet*
- *Gjør rede for arbeidsprosessen, samt valg og bruk av metode og tilnærming*

Sannsynlighet?

Sannsynlighet er et sentralt begrep i risikoanalyser, men blir ofte benyttet uten at det blir klart definert hva som menes med begrepet.[10] Vi benytter en kunnskapsbasert sannsynlighetsvurdering fordi tilsiktede, uønskede hendelser er lavfrekvente hendelser. Det lar seg derfor sjelden gjøre å beregne en matematisk sannsynlighet for tilsiktede uønskede handlinger. Det er med andre ord en stor utfordring kun å benytte historiske data som et grunnlag for å vurdere sannsynlighet. Det er derfor nødvendig å benytte andre datakilder for å vurdere sannsynlighet, herunder kunnskapsbasert sannsynlighet. Hvilke datakilder som benyttes som et grunnlag for å vurdere sannsynlighet, går vi nærmere inn på under risikovurdering og fastsettelse av risikonivå.

Planlegging av risikoanalysen

Ethvert prosjekt bør ha en planleggingsfase. Denne fasen av prosjektet innebærer å avklare behov, sikre forankring hos ledelsen, lære opp nøkkelpersonell og etablere prosjektgrupper med relevante personer.

Det er viktig at det settes av tilstrekkelig tid til planlegging av risikoanalysen. Planleggings-

7
Det er i dag mange ulike tilnærminger til gjennomføring av risikoanalyse. En bidragsyter er NSM, som i 2016 utga håndboken «Risikovurdering for sikring»

8
FFI (2015) Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger

9, 10
FFI (2015) Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger

fasen blir ofte nedprioritert, noe som kan føre til at de økonomiske og tidsmessige rammene som er satt for prosjektet, overskrides. I det følgende går vi gjennom noen av de mest sentrale delene i en planleggingsfase.

Metode for risikoanalyse – grovanalyse

Formålet med risikoanalysene kan variere, og avhengig av formål vil ulike metoder være hensiktsmessig å benytte. Enkelte analysemetoder er godt egnet for visse typer problemstillinger, og mindre egnet for andre. Det er ikke hensiktsmessig å presentere alle de ulike metodene for risikovurderinger i denne sammenheng, da det er mange metoder som sjelden benyttes. Grovanalyse er den metoden som er mest vanlig når risikovurdering av sikring av bygg skal utføres. Vi skal derfor kort presentere hovedtrekkene ved en grovanalyse.

Begrepet grovanalyse benyttes ofte om kvalitative risikovurderingsmetoder som kan utføres med relativt beskjeden arbeidsinnsats.[11] En grovanalyse er vanlig å gjennomføre i en arbeidsgruppe på 3–10 personer. På en systematisk måte identifiserer og gjennomgår gruppen relevante trusselscenarioer, konsekvenser av disse, og usikkerhet/sannsynlighet knyttet til de uønskede hendelsene. Til slutt i analysen presenteres en liste med risikoreduserende tiltak.

Det kan være hensiktsmessig at arbeidsgruppen benytter en sjekkliste som arbeidsverktøy underveis i prosessen. Men for å forhindre at sjekklisten blir en generisk «oppskrift» som man forholder seg ukritisk til, for alle analyseobjekter, bør prosessen starte med en idédugnad med blanke ark. Sjekklisten kan senere benyttes for å kontrollere at alle de sentrale elementene blir undersøkt i analysen. Denne må oppdateres og revideres for hvert objekt som undersøkes. Resultatene fra grovanalysen dokumenteres ofte fortløpende til oppdragsgiver/styringsgruppe for hvert delelement.

Målsettinger og forventninger

Risikoanalyser og revideringer av disse er nødvendige ved endringer i virksomhetens ytre omgivelser eller interne forhold: økt trusselnivå, tilegnelse eller bortfall av verdier, flytting av virksomheten etc. Omfanget av risikoanalyse vil variere etter behov, fra små oppdateringer av gjeldende risikoanalyse til utarbeidelse av en omfattende risikoanalyse der alle sider ved virksomheten gjennomgås, og analysearbeidet strekker seg over flere måneder.

Virksomheten bør starte planleggingen med å avklare hvem som har ansvaret for å gjennomføre risikoanalysene, hvilke ressurser som skal avsettes til arbeidet, start- og sluttdato for prosjektet og avgrensningen av arbeidet. Det kan være en fordel å utarbeide en prosjektplan med datoer for prosjektstart, prosjektslutt og milepæler underveis.

Videre bør det avklares og konkretiseres hva som er målsettingen med analysen. Det er viktig at både prosjektdeltakerne og ledelsen er omforente om hva som skal være gjenstand for oppmerksomhet i analysen. Målsettingene og forventningene bør nedfelles i et skriftlig dokument i form av en avtale eller et referat. Partene må godkjenne dette dokumentet før prosjektstart.

Ledelsesforankring

Det er et kriterium for et vellykket resultat at risikoanalysen forankres hos leder på relevant nivå. I dette ligger at ledelsen tar ansvar og eierskap til prosjektet, og følger og støtter prosjektutviklingen. Nødvendige beslutninger skal tas på ledelsesnivå, og forutsetninger og rammer (tidsmessige og økonomiske) skal avklares på et tidlig tidspunkt. Videre er det et lederansvar å sørge for at prosjektet bevilges tilstrekkelige ressurser. God forankring fordrer aktiv deltakelse fra ledelsen, herunder at man tilegner seg en klar forståelse av hvilke verdier virksomheten besitter, bidrar med å identifisere de potensielle truslene mot verdiene og gir sin

11
FFI (2015) Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger

vurdering av hvordan disse verdiene kan være sårbare mot truslene. Spesielt er det viktig at ledelsen er involvert i vurderingen av konsekvensene ved tap av verdier, og at de uttaler seg eksplisitt om fastsettelse av risikokriterier og risikoaksept. Å fastsette risikoaksept er å ta en overveid beslutning om å ta en risiko som man anser som akseptabel, ut fra kriteriene som legges til grunn, og de fordelene det gir å la være å sikre seg fullstendig. Å kjøre bil er for eksempel risikabelt, men vi gjør det allikevel fordi det gir oss fordeler som veier opp for risikoen.

Når rapporten er ferdigstilt fra analysegruppens side, må leder sette av tilstrekkelig tid til å gjøre seg kjent med vurderingene i analysen for å kunne ta beslutninger om og iverksette risikoreduserende tiltak.

Risikokriterier og sikringsmål

Virksomheten bør fastsette hvilke kriterier som skal brukes for å evaluere risiko. Kriteriene bør gjenspeile organisasjonens verdier, målsettinger og ressurser. Det bør også tas hensyn til roller og ansvar for risikostyring i virksomheten. Risikokriteriene bør fastsettes i forkant av risikoanalysen.

Basert på virksomhetens kjerneoppgaver med tilhørende verdier skal det fastsettes mål for sikring av verdiene. Sikringsmål vil være ett av flere risikokriterier som skal tas hensyn til i risikoanalyseprosessen. Sikringsmål defineres som ønsket eller akseptabel tilstand for verdier under eller etter en uønsket hendelse.

Sikringsmål skal settes før analysearbeidet igangsettes, og kan revideres etter at analysearbeidet er avsluttet. Som vi redegjør for i prosjektgjennomføringskapitlet, kan dette nedfelles i et kravdokument. Se ***kapittel 8, Planlegging av sikringstiltak.*** Eksempler på sikringsmål kan være etterfølgelse av lov- og forskrift, beskyttelse mot enkelte trusselaktører og trusselscenarioer og ivaretakelse av viktige verdier for virksomheten.

Når risikokriterier skal fastsettes, bør disse faktorene overveies:

- *Hvilke konsekvenser som kan forekomme, og hvordan disse skal måles*
- *Hvordan sannsynlighet skal fastsettes*
- *Hvilke tidsrammer som gjelder for sannsynlighet og/eller konsekvenser*
- *Hvordan risikonivået skal bestemmes*
- *Hvilke synspunkter interessenter har*
- *Hvilket nivå av risiko som kan aksepteres eller tolereres*
- *Hvorvidt det må tas hensyn til kombinasjoner av flere risikoer, og i så fall hvordan og hvilke kombinasjoner som bør overveies*

Datainnsamling

Det må legges opp til en strukturert metode for innsamling av informasjon. Dette innebærer å sikre etterprøvbarhet i arbeidet, dobbeltsjekke opplysninger med flere personer, benytte ulike typer kilder og dokumentere alt arbeid underveis i prosessen. Eksempler på dokumenter som kan være relevante å innhente tidlig i en risikoanalyseprosess for et eksisterende bygg, kan være (ikke uttømmende liste):

- *Byggtegninger*
- *Grunnlagsdokument for sikkerhet/lokal instruks for sikkerhet*
- *Verdivurdering*
- *Oversikt over relevante lov- og forskriftskrav*
- *Oversikt over dokumenterte avvik*
- *Organisasjonskart*
- *Avtaler om vakt og sikring*
- *Oversikt over etablerte sikringstiltak*
- *Tidligere risikovurderinger og/eller tilsynsrapporter*
- *Trusselvurderinger*
- *Objektplan fra politi ev. Forsvaret*

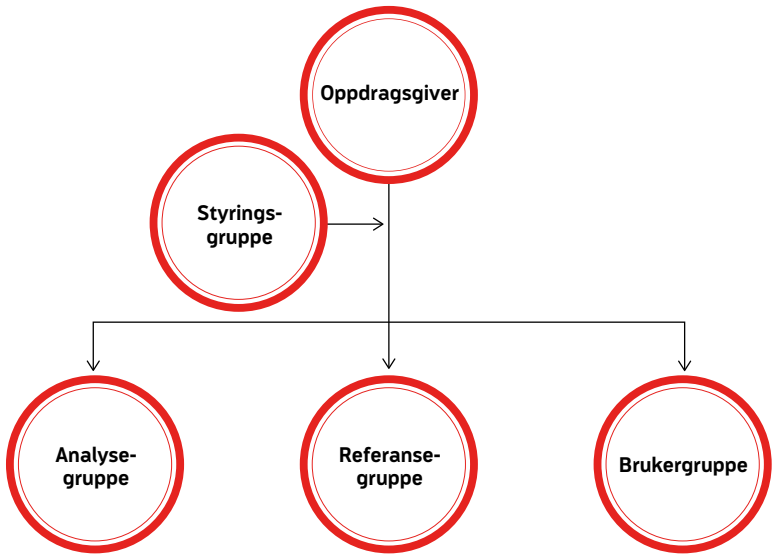
Organisering av prosjektgrupper

I forbindelse med gjennomføringen av risikoanalysen kan det opprettes ulike prosjektgrupper som skal støtte arbeidsgruppen med

SIKRINGSMÅL

Ønsket eller akseptabel tilstand for verdier under eller etter en uønsket hendelse.

Prosjektgrupper



beslutninger og faglige råd. Med mindre det er formålstjenlig å opprette flere grupper, bør man begrense seg til én arbeidsgruppe som består av fagpersoner med kompetanse innenfor risikovurderingsmetodikk og sikkerhetsrådgivning. For mange grupper kan ta unødvendig tid fra analysearbeidet og føre til at prosjektet ikke blir levert i tide. Enkelte prosjekter har imidlertid et formål og et omfang som gjør at det er en klar fordel å opprette flere ulike prosjektgrupper. ***Figuren Prosjektgrupper*** viser et eksempel på en mulig prosjektorganisering. Gruppene har ulike formål og funksjoner:

Styringsgruppe: En formell gruppe som representerer oppdragsgiver, og som fungerer som rådgiver og beslutningstaker.

Referansegruppe: Ressurspersoner som skal bistå prosjektet med faglige råd. Gruppen har ingen formell myndighet i prosjektorganisasjonen.

Brukergruppe: Ressurspersoner tilknyttet analyseobjektet som skal bistå med datainnsamling og informasjon om enkelte avdelinger eller virksomheter som er berørt av prosjektet. Gruppen har ingen formell myndighet i prosjektorganisasjonen.

Analysegruppe: Tverrfaglig sammensatt gruppe av personer som gjennomfører arbeidsoppgavene i prosjektet. Bør ha kompetanse innenfor risikoanalysemetodikk og sikkerhetsrådgivning.

Dokumentasjon

Resultatene fra analysearbeidet bør dokumenteres gjennom referater, skjemaer og avslutningsvis en rapport som dokumenterer analysegruppens vurderinger. Dette sikrer at rapporten kan etterprøves i etterkant av arbeidet.

Objektkartlegging og verdivurdering

Objektkartlegging er en beskrivelse av analyseobjektet, ofte kalt systembeskrivelse. Objektet skal kartlegges, herunder oppdrag, organisasjon, beliggenhet, bygningsmasse, infrastruktur, fysisk og elektronisk sikring og administrative rutiner som er relevant for analysen. En inndeling av objektkartlegging etter lag-på-lag-prinsippet kan være en fordel for en god beskrivelse av objektet med sikringstiltak. Dette vil også være til god hjelp når sårbarhetene senere skal beskrives. Objektkartleggingen bør også gjengi organisering, verdikartlegging og virksomhetens formål. En kartlegging kan med fordel inkludere:

- *Administrative forhold*
- *Sikkerhetsorganisasjon*
- *Verdikartlegging*
- *Sikringsmål*
- *Omkringliggende områder*
- *Bekrivelse av objektet med sikringstiltak*
- *Vakthold og reaksjonsapparat*

Relevante tegninger og kart bør benyttes som grunnlag i planleggingsfasen og ved befaringen. Verdier bør defineres i forkant av befaringen, og bør være utgangspunkt for kartleggingen. Det er en fordel å dokumentere befaringen med bilder og notater som kan benyttes senere i analysearbeidet.

Verdivurdering er en kartlegging av virksomhetens verdier. Verdier defineres som en «ressurs som hvis den blir utsatt for uønsket påvirkning, vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen». [12] Vurderingen utføres av virksomheten selv, fordi det er virksomheten som har best kjennskap til egne oppgaver og målsettinger. Det kan være hensiktsmessig å benytte et skjema for verdivurdering i denne delen av prosessen.

Hensikten med en verdivurdering er å få en oversikt over verdier som bør sikres, hva slags støttesystemer verdiene er avhengig av (f.eks. strøm), samt identifisere konsekvensene av tapte verdier. Verdivurdering er en sentral del av risikoanalysen fordi det på et tidlig tidspunkt i analysearbeidet er viktig å få en god oversikt over det som virksomheten trenger å beskytte. Dette har igjen betydning for objektkartleggingen, utvelgelse av trusselscenarioene og vurderingen av sårbarhetene og risikovurderingen.

Verdiene bør rangeres i en skala etter konsekvensen ved tap av verdien.

Spørsmålene man kan stille seg i forbindelse med en verdivurdering, er:

- *Hvor kritisk er bortfall av verdi X?*
- *Hvilke verdier er virksomheten avhengig av for å kunne utføre sine oppgaver?*
- *Er verdien avhengig av andre verdier for å kunne fungere?*
- *Hvilke verdier kan være attraktive for en trusselaktør?*

For mer informasjon om verdivurdering, se ***kapittel 6, Verdivurdering.***

Trusselvurdering

Trusselvurdering er en kartlegging av det nåværende trusselbildet. Som kilder kan både åpne og graderte trusselvurderinger fra f.eks. Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Etterretningstjenesten (E-tjenesten) benyttes. Det er også relevant å benytte seg av statistikk fra Statistisk sentralbyrå (SSB), tidligere sikkerhetstruende hendelser i virksomheten, samt rapporter om kriminalitet, f.eks. fra KRIPOS. I trusselvurderingen inndeles truslene i fire ulike kategorier: vanlig kriminalitet, etterretning, terror og sabotasje. Innenfor disse kategoriene gis det en generell beskrivelse av den nåværende

12 NS 5830:2012: «Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi»

Klassifisering av verdier

Verdi	Beskrivelse
Lav	Tap eller reduksjon av verdi har små konsekvenser
Moderat	Tap eller reduksjon av verdi kan ha store konsekvenser
Høy	Tap eller reduksjon av verdi har store konsekvenser
Svært høy	Tap eller reduksjon av verdi har umiddelbare og svært alvorlige konsekvenser

trusselsituasjonen, aktuelle aktører og deres modus operandi («arbeidsmetode»).

For mer informasjon om trusselvurdering og utvikling av trusselscenarioer henvises det til ***kapittel 7, Trusselvurdering.***

Sårbarhetsvurdering

En sentral del av risikovurderingen er sårbarhetsvurderingen. Hvor sårbar er virksomheten overfor en uønsket hendelse? Hvilke konsekvenser får det for virksomheten dersom verdier blir borte? Hva skjer med virksomhetens verdier dersom det eksploderer en bombe i gaten rett utenfor?

Sårbarhetsutvalget[13] definerte sårbarhet som et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet vil få med å gjenopprette sin virksomhet etter at hendelsen har inntruffet. Systemet kan i denne sammenheng være en bygning, en militærleir, eller en virksomhet i en bygning.

Det motsatte av sårbarhet er robusthet. Når vi snakker om at et system er sårbart, så mener vi at sårbarheten er vurdert til å være stor, og at det er lite robust overfor ytre påvirkning.[14]

Vi beskriver sårbarheten overfor trusselscenarioet på grunnlag av visse faktorer, for eksempel tilstedeværelse av verdier og eksisterende sikringstiltak.

Når sårbarhetene beskrives, kan det være nyttig med en liste over hvilke sikringstiltak virksomheten har som kan representere en motstandskraft overfor det aktuelle scenarioet. Det kan også være til hjelp å beskrive sårbarhetene etter hvilke barrierer som er satt

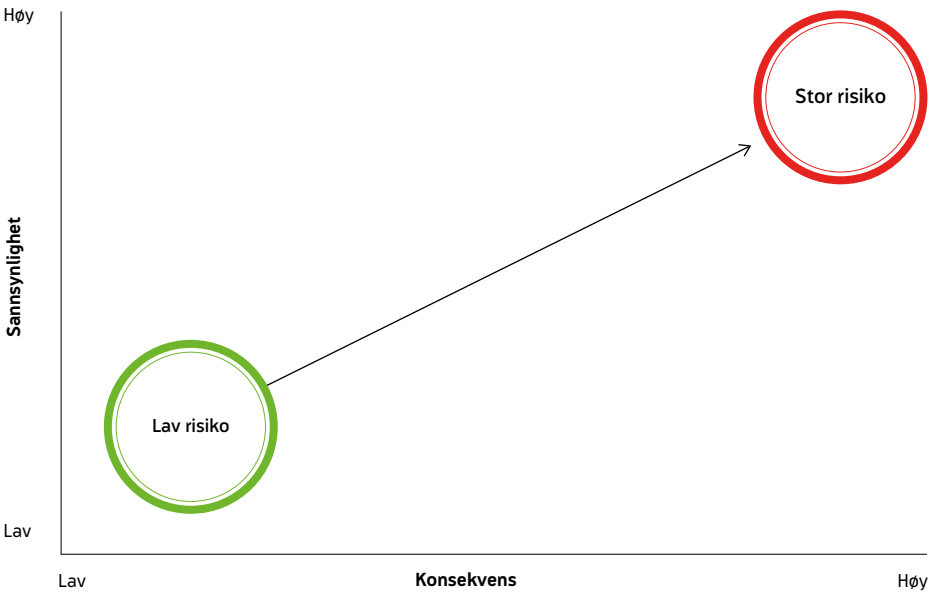
Klassifisering av sårbarheter

Sårbarhet	Beskrivelse
Lav	Eksisterende sikringstiltak adresserer problemet og vil i stor grad motstå en uønsket hendelse
Moderat	Eksisterende sikringstiltak adresserer problemet, men er noe mangelfulle
Høy	Eksisterende sikringstiltak adresserer problemet, men er svært mangelfulle
Svært høy	Det eksisterer ikke sikringstiltak som adresserer problemet

13
Sårbarhetsutvalget (2000)

14
Terje Aven mfl. (2010) Risikoanalyse. Universitetsforlaget: Oslo

Vurdering av sannsynlighet og konsekvens



opp for å forhindre slike type hendelser, hvilke deteksjonsmuligheter som fins, hvordan hendelsen verifiseres, og hvilke rutiner man har for reaksjon når hendelsen inntreffer.

Risikovurdering og fastsettelse av risikonivå

I dette trinnet av analysen sammenstilles resultatene fra verdi-, trussel- og sårbarhetsvurdering. Dette gjøres for alle trusselscenarioene. Risikoen vurderes etter fastsatte kriterier, som vil variere etter hvilken standard som benyttes.

Sannsynlighets- og konsekvensmodellen[15]

Risikoen vurderes som sammenhengen mellom identifiserte konsekvenser (skade/tap av verdier) og sannsynlighet (trusler og sårbarheter). Arbeidsgruppen diskuterer seg frem til samlet

Grad av sannsynlighet

Grad av sannsynlighet	Vurderingskriterier for sannsynligheten
Lav	→ Tilstedeværelse av verdi → Trusselaktørens intensjon og kapasitet → Fravær av aktive sikringstiltak → Fravær av passive sikringstiltak → Historiske data → Trendrapporter
Moderat	
Høy	
Meget høy	
Svært høy	

15 Krav til risikovurderinger. NS 5814, 2008

Boston Square Matrix – Presentasjon av risikobilde

Sannsynlighet							
	Svært høy	5					
	Meget høy	4					
	Høy	3					
	Moderat	2					
	Lav	1					
Risiko	Høy Moderat Lav		1	2	3	4	5
			Ubetydelig	Moderat	Kritisk	Meget kritisk	Svært kritisk
			Konsekvens				

risiko for det enkelte scenario ved å gjøre en kvalitativ vurdering av sannsynlighet og konsekvens etter gitte kriterier.

Risikoen uttrykkes som forholdet mellom sannsynlighet og konsekvens. Det bør benyttes et konsekvensskjema som angir konsekvensen ved tap av verdien. Det bør utarbeides kriterier for vurdering av konsekvens, fordelt på de ulike kategoriene (a) operativ evne/drift, (b) sensitiv/gradert informasjon, (c) liv og helse og (d) økonomiske konsekvenser. For en del virksomheter er det også relevant å vurdere omdømme som egen kategori.

Også i sannsynlighetsvurderingen må det benyttes noen kriterier for å bestemme grad av sannsynlighet for hvert scenario. Dette er en subjektiv vurdering der sannsynlighet vurderes på en skala fra 1 (LAV) til 5 (SVÆRT HØY). Sannsynlighet vurderes etter følgende kriterier:

- *tilstedeværelse av verdi*
- *trusselaktørens intensjon og kapasitet*
- *fravær av aktive og passive sikringstiltak*
- *historiske data*
- *trendrapporter*

Trusselaktørens mulighet til å ødelegge, ta bort eller forringe verdiene som virksomheten ønsker å beskytte, vurderes for hvert enkelt trusselscenario.

Risikoen for de ulike trusselscenarioene presenteres ved hjelp av en risikomatrise, også kjent som Boston Square Matrix. I analysen settes det opp én matrise per konsekvensklasse (liv og helse, operativ evne, økonomi, informasjon).

Trefaktormodellen[16]

I trefaktormodellen beskrives risikoen som forholdet mellom verdi, trussel og sårbarhet. Dette kan illustreres i en «risikotrekant»[17]. Risikoen rangeres etter fastsatte kriterier som er tilpasset virksomhetens egenart, og kan presenteres på forskjellige måter.

NSMs håndbok «Risikovurdering for sikring» gir råd til virksomheter om hvordan denne type risikoanalyse kan planlegges og gjennomføres.

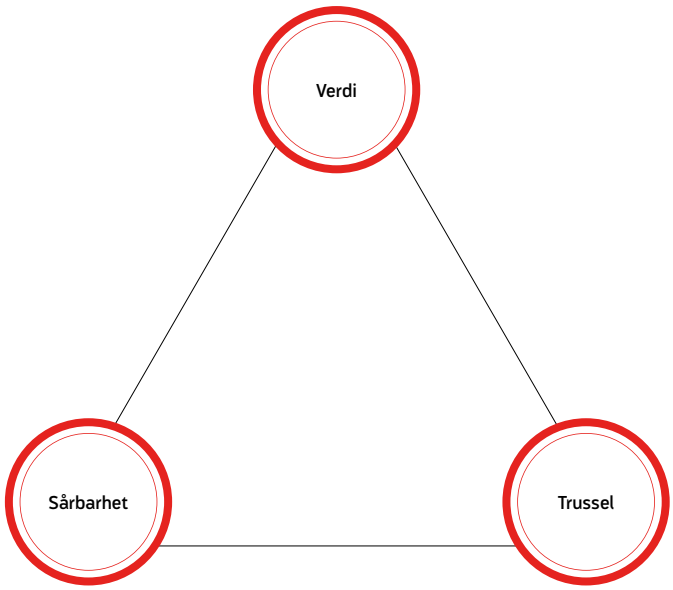
Usikkerhet

Resultatet fra risikoanalysen kan ikke tolkes som et endelig svar; det vil alltid være en viss usikkerhet tilknyttet analyseresultatene. Denne usikkerheten uttrykkes gjennom en vurdering

16 NS 5832:2014 Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse

17 NSM, PST, POD (2016). En veiledning. Sikkerhets- og beredskapstiltak mot terrorhandlinger

Risikotrekanten



av kunnskapsgrunnlaget som analysen bygger på, samt resultatenes følsomhet for endringer i de forutsetninger og antakelser som er gjort i analysene.[18] Dette vil gjelde vurderinger rundt den nåværende trusselsituasjonen, om scenarioene er dekkende, hvor sårbar virksomheten er, og hvor attraktive virksomhetens verdier er for potensielle trusselaktører. Spørsmål vi kan stille oss, er: Har vi presis nok kunnskap om virksomhetens beskyttelsestiltak og hvor effektive disse er overfor identifisert trussel?

En risikovurdering skal ideelt sett være en kvalitativ vurdering foretatt av en arbeidsgruppe med ulik fagkompetanse. Det vil derfor være usikkerhet knyttet til vurderinger foretatt av arbeidsgruppen. Spørsmål som er naturlig å stille seg i denne sammenheng: Har arbeidsgruppen hatt tilgang til tilstrekkelig, relevant og oppdatert datamateriale? Er arbeidsgruppen sammensatt av personer med utfyllende og relevant fagkompetanse, samt erfaring fra arbeid med risikovurderinger?

For å kunne vurdere usikkerheten ved resultatene fra en risikovurdering, må man vite noe om kunnskapen og forutsetningene som analysen bygger på, samt hvilken analysemetode og arbeidsprosess som er benyttet. Forutsetninger som analysen bygger på, bør derfor tydelig fremkomme. Usikkerheten bør videre synliggjøres gjennom en vurdering av selve kunnskapsgrunnlaget som analysegruppen har hatt tilgang til. Videre bør det fremkomme at resultatene er sensitive overfor endringer i forutsetningene. Sensitive resultater er lite generaliserbare. For å vurdere styrken i kunnskapsgrunnlaget kan det benyttes tre indikatorer:[19]

1. *Tilgangen på relevante data og erfaringer*
2. *Forståelsen av hendelsen som analyseres (hvor god er forklaringsmodellen)*
3. *Enighet blant eksperter som deltar i risikovurderingen*

Usikkerhet som er avdekket i forbindelse med analysearbeidet, bør synliggjøres i den endelige

18 DSB (2014) Nasjonalt risikobilde 2014

19 Flage & Aven sitert i DSB (2014) Nasjonalt risikobilde 2014

rapporten. Det avgjørende er at den som har bestilt analysen, får et så godt utgangspunkt som mulig for å ta beslutninger om nødvendige sikringstiltak.

Håndtering av risiko

Når risikonivået er fastsatt, er det nødvendig å vurdere hvordan risikoen skal håndteres. Det er en vanlig fremgangsmåte å se på de fastsatte risikokriterier og vurdere dette opp mot det fastsatte risikonivået for de ulike trusselscenarioene. Deretter er det nødvendig å ta en beslutning på hvordan risikoen skal håndteres.

En forutsetning for god risikoerkjennelse er at det foreligger gode analyser av risiko og sårbarheter. Dette er imidlertid ikke tilstrekkelig. God risikoerkjennelse forutsetter at kunnskapen blir anvendt, og at sårbarhetsreduserende tiltak iverksettes om nødvendig.[20] Det er som tidligere nevnt under ledelsesforankring, avgjørende at ledelsen tar en beslutning på risikoaksept, og deretter vurderer hvilke strategier som er hensiktsmessige for å redusere risikoen.

Det er viktig å være oppmerksom på at ett alternativ innenfor risikohåndtering ikke nødvendigvis utelukker et annet. Alternativene kan ifølge ISO 31000 omfatte følgende:[21]

- *Å unngå risikoen ved å beslutte å ikke begynne eller ikke fortsette med aktiviteten som forårsaker aktiviteten*
- *Å ta eller øke risikoen for å kunne dra nytte av en mulighet*
- *Å fjerne risikokilden*
- *Å endre sannsynligheten*
- *Å endre konsekvensen*
- *Å dele risikoen med en eller flere parter*
- *Å ta risikoen for egen regning etter en veloverveid beslutning*

Det er også en annen kjent risikohåndteringsstrategi som benyttes i mange sikringsmiljøer, ACAT. ACAT står for Avoid, Control, Accept og Transfer. Dersom denne strategien benyttes, kan man utfra ulike risikoer benytte en eller flere strategier for å håndtere risiko:

Unngå (avoid): Aktiviteter som innebærer risiko, unngås av virksomheten. Et eksempel kan være å ikke benytte seg av foreslått tomt for utbygging fordi dette innebærer en for stor risiko.

Redusere (control): Iverksette tiltak for å redusere sannsynligheten eller konsekvensen av en tilsiktet hendelse. Tiltak kan være for eksempel fysiske eller organisatoriske sikringstiltak.

Aksept (acceptance): Akseptere tapet som en følge av en tilsiktet hendelse. Dette inkluderer tilsiktede hendelser som har katastrofale konsekvenser, men der man anser muligheten for at dette skal skje, som meget lav. Da vil man kunne vurdere at kost-nytte tilsier at det ikke er økonomisk forsvarlig å sikre seg mot alle tenkelige tilsiktede hendelser.

Overføring (transfer): Overføre risikoen til en annen virksomhet, annen lokasjon eller en annen avdeling. Dette kan for eksempel være en verdi som kan flyttes til en annen lokasjon med bedre grunnsikring.

Det å velge det best egnede alternativet for risikohåndering innebærer å balansere kostnadene og arbeidet forbundet med iverksettingen, mot fordelen med risikohåndteringen, sett opp mot de fastsatte risikokriteriene inkludert sikringsmålene. For tilsiktede hendelser kan risikohåndtering av dette innebære en vesentlig kostnad. Dette må derfor vurderes opp mot lov- og forskriftskrav og nødvendig beskyttelse av samfunnskritiske objekter.

20
Meld. St. 21. (2012–2013). Terrorberedskap

21
ISO 31000:2009. Risikostyring – Prinsipper og retningslinjer

Tiltak og funksjonskrav

Siste trinn i analysen er å angi funksjonskrav og anbefale risikoreduserende tiltak. Forståelsen av sårbarheter er spesielt viktig her og kan være nøkkelen til kostnadseffektiv risikoreduksjon når trusselbildet er usikkert. Tiltakene må ses i sammenheng med hverandre, og ett tiltak vil sannsynligvis redusere risikoen forbundet med flere av scenarioene. Funksjonskrav eller tiltak angir hvordan risikoen kan reduseres ved hjelp av elektroniske, fysiske og administrative tiltak.

De risikoreduserende tiltak som foreslås, er basert på grunnprinsippene innen sikring, og formuleres på en måte som ikke utelukker alternative løsninger senere i prosjekteringen. Ved denne tilnærmingen er det mulig til slutt å oppnå en helhetlig tilnærming. For mer informasjon om grunnprinsipper innenfor sikring, se ***kapittel 2, Sikringsteori.***

Foreslåtte tiltak varierer fra konkrete enkle tiltak som lett kan iverksettes, til overordnede tiltak formet som råd og en rettesnor for sikkerhetsplanleggingen ved objektet. En detaljert prosjektering av fysiske og elektroniske tiltak vil imidlertid måtte gjennomføres før sikringstiltakene implementeres. I praksis kan det være at objekteier velger å la være å iverksette noen av de foreslåtte tiltakene, for eksempel av økonomiske årsaker. Det bør i så fall vurderes om en enklere versjon av tiltaket bør velges i stedet. Alle tiltak skal være en del av et balansert sikringskonsept, og det er viktig å ha fokus på helheten og lukke sårbarhetene tilstrekkelig for hvert enkelt scenario. Anbefalte risikoreduserende tiltak bør prioriteres. For mer detaljert informasjon om ulike sikringstiltak, se ***del 3, Metoder for sikring***.

Restrisiko

Uavhengig av hvordan risikoen håndteres, er det en erkjennelse at det ikke er mulig å eliminere risiko for tilsiktede hendelser for alle typer trusler. For tilsiktede hendelser må virksomhetene for eksempel ha risikoaksept for at det kan oppstå tilsiktede hendelser som ikke har blitt vurdert, eller akseptere risiko for hendelser der virksomheten kan akseptere konsekvensene dersom de oppstår.

Enkelte virksomheter vil ha et behov for å vurdere risikoen etter at håndteringen av risikoen er gjennomført. Dette er blant annet for å avdekke om tiltakene fungerer etter hensikten, og om det er organisatoriske forhold som har endret seg siden forrige analyse. Det kan også gjennomføres en vurdering av restrisiko som en del av analysen, der risiko vurderes opp mot de foreslåtte tiltakene og funksjonskravene. Denne vurderingen vil naturlig innebære en del usikkerhet på bakgrunn av at effekten av et sikkerhetstiltak vil innebære flere fremtidige forhold i virksomhetene som ikke nødvendigvis beskrives i analysen.

Risikoanalyse er likevel et godt verktøy for å gi virksomheten en mulighet til å redusere risikoen for tilsiktede handlinger. Uten en risikoanalyse vil det være svært utfordrende for virksomheter å få en god oversikt over risikobildet og implementere tiltak for å redusere risikoen. Det er også et viktig poeng at risikoanalysen er en vurdering av et øyeblikksbilde, og den må derfor jevnlig revideres etter endringer i trusselbildet eller verdier, sikkerhetstruende hendelser i virksomheten, organisasjonsendringer og endrede lov- og forskriftskrav.

Kapittel 6

Verdivurdering

Dette kapitlet beskriver hva som menes med verdier, og forklarer hvordan verdivurdering og skadevurdering kan gjennomføres.

Et av de mest grunnleggende spørsmålene som skal stilles når man setter i gang med sikrings- og sikkerhetsarbeid, er hvilke verdier virksomheten har, og hva som skal sikres. Begrepet verdi kan defineres som «en ressurs som hvis den blir utsatt for uønsket påvirkning, vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen».[1]

Verdier kan være funksjoner, fysiske objekter eller informasjon en virksomhet er avhengig av for å utføre sine kjerneoppgaver. En funksjon kan for eksempel være en nøkkelrolle i virksomhetens sentrale beslutningsprosesser, som administrerende direktør. Et objekt kan være et operasjonsrom med en spesiell utrustning. Informasjon kan være forretningskontrakter med børsrelevant informasjon eller informasjon som er gradert iht. sikkerhetsloven.

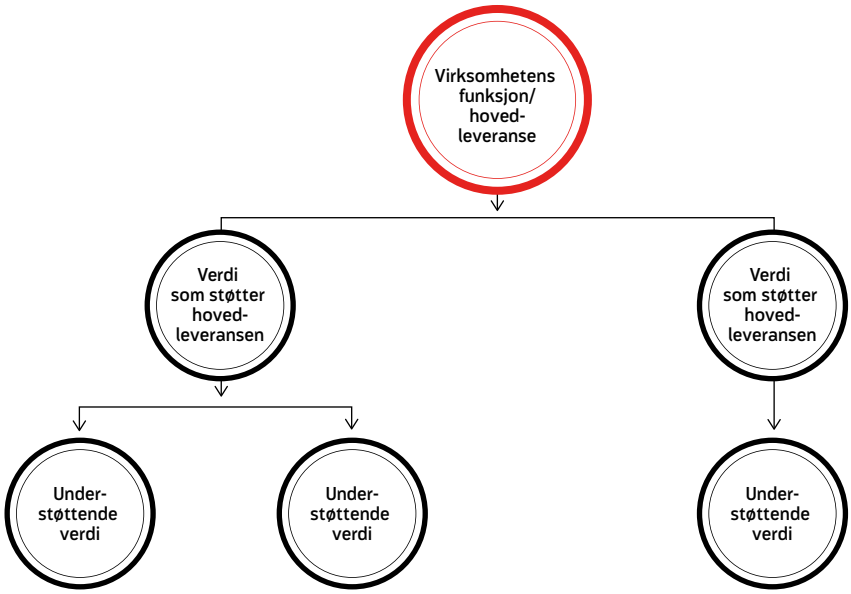
Ulike virksomheter har ulike typer verdier, men følgende verdier er typiske eksempler:

- *Personell*
- *Operasjonsrom*
- *Sikkerhetsgradert eller sensitiv informasjon*
- *Informasjonssystemer*
- *Attraktivt eller lett omsettelig materiell, som for eksempel:*
  - *Kontantbeholdninger*
  - *PC-er, prosjektorer, o.l.*
  - *Legemidler*
  - *Attraktive våpen og ammunisjon (AVA)*
- *Støttesystemer virksomheten er avhengig av for å utøve sine funksjoner, som for eksempel:*
  - *Strømforsyning og reservekraft*
  - *Kommunikasjonsmuligheter og samband (fiber, kabler og antenner, radio)*
  - *Kjøling*
  - *Ventilasjon*
  - *Spesialutstyr*

1 Norsk Standard NS 5830:2012 «Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi», s. 4

Hovedleveranse/virksomhetens funksjon

Sammenheng mellom ulike verdier og nivåer



Verdivurdering

Verdivurdering er en kartlegging og rangering av virksomhetens verdier. Det vil si en prosess for identifisering og rangering av verdier og vurdering av konsekvenser dersom verdiene fjernes, skades eller ødelegges.

Enhver virksomhet må definere og vurdere hvilke leveranser og prosesser som er sentrale for egen drift, og hvilke verdier som understøtter disse leveransene.

Hva som er en virksomhets verdier, vil altså variere etter hvilken type virksomhet det gjelder. Generelt henger verdiens betydning sammen med konsekvensen det vil ha for virksomheten dersom den faller bort. En virksomhet bør også vurdere hvordan og i hvilken grad man selv er avhengig av andre virksomheter.

NSMs veileder i verdivurdering påpeker at når verdiene er definert, bør de rangeres etter viktighet, for eksempel ved at de fordeles på nivåene LAV, MODERAT og HØY.[2] Man kan også rangere verdiene ved å angi tallverdier mellom 1 og 4, der 1 indikerer lavest verdi, og 4 indikerer høyest. En fordel ved å bruke fire i stedet for tre nivåer er at man unngår at det midterste nivået blir et «komfortabelt» utgangsnivå der man plasserer de fleste verdiene uten reell vurdering. Fire nivåer er benyttet både i skadenivå og verdiklassifisering i skjema for ***verdivurdering,*** se vedlegg.

Skjermingsverdige objekter

For virksomheter som er underlagt sikkerhetsloven, er verdier som karakteriseres som skjermingsverdige, de mest sentrale. Skjermingsverdige objekter er eiendom, områder,

2 NSM (2009), «Veiledning i verdivurdering» *www.nsm.stat.no*

Rangering av verdier

Verdi	Konsekvens
Lav	→ Tap eller reduksjon av verdi har små konsekvenser
Moderat	→ Tap eller reduksjon av verdi kan ha store konsekvenser
Høy	→ Tap eller reduksjon av verdi har store konsekvenser
Svært høy	→ Tap eller reduksjon av verdi har umiddelbare og svært alvorlige konsekvenser

bygninger, anlegg, transportmidler, annet materiell, eller deler av slik eiendom som kan skade rikets selvstendighet og sikkerhet ved sikkerhetstruende virksomhet.[3]

Objektsikkerhet var et tema allerede før sikkerhetsloven, men det forelå ikke noen overordnet koordinering av det forebyggende sikkerhetsregelverket på området. Det var opp til den enkelte etat selv å implementere direktiver og bestemmelser. Forarbeidene til sikkerhetsloven beskrev at mens å bygge opp et system for koordinert og faglig kompetent objektsikkerhet antakelig ville være kostnadskrevende på kort sikt, ville mulighetene for koordinering på tvers ha et langsiktig ressurssparingspotensial. Ved å definere og klassifisere skjermingsverdige objekter skulle den forebyggende sikkerhetstjenesten også i en situasjon med lavt trusselnivå kunne forberede og implementere koordinerte sikkerhetstiltak på en hensiktsmessig måte.[4]

Nasjonal sikkerhetsmyndighet (NSM) slår fast at for å oppfylle lovens bestemmelse om å beskytte informasjon og objekter som er skjermingsverdige, må det gjøres vurderinger av hvorfor disse er skjermingsverdige.[5] Dette innebærer i praksis at man gjennomfører verdi- og skadevurderinger, som beskrives i dette kapittelet. Det er for eksempel skadevurderingen som danner grunnlaget for om skjermingsverdige objekter får klassifiseringsgrad VIKTIG, KRITISK eller MEGET KRITISK.

Se ***kapittel 4, Samfunnssikkerhet, lover og regelverk*** for mer informasjon om skjermingsverdige objekter og lovverket som regulerer disse.

Skadevurdering

Verdivurderingen henger i praksis tett sammen med skadevurderingen. Å gjennomføre en skadevurdering innebærer å vurdere konsekvenser ved bortfall eller ødeleggelse av en verdi, og foreta en vurdering av skadepotensialet dersom en verdi blir utsatt for en sikkerhetstruende hendelse. Normalt er derfor skadevurderingen et hjelpemiddel eller en utdypning av konsekvensvurderingene i verdivurderingen.

For virksomheter som ikke er underlagt sikkerhetsloven eller som ikke har skjermingsverdige objekter, kan det tas utgangspunkt i følgende hovedkategorier i vurderingen av konsekvenser ved verdiens bortfall:

Liv og helse
Enten for eget personell eller andre personer som benytter eller er avhengige av virksomhetens leveranser.

3
NSM (2014), «Veileder for objektsikkerhetsforskriften» *www.nsm.stat.no*

4
NSM (2009), «Veiledning i verdivurdering» *www.nsm.stat.no*

5
NSM (2009), «Veiledning i verdivurdering» *www.nsm.stat.no*

Daglig drift og operativ evne
Nedetid for hele virksomheten eller forsinkelser knyttet til viktige leveranser.

Informasjon
Tap eller kompromittering av sensitiv og/eller sikkerhetsgradert informasjon.

Økonomi
Kostnader knyttet til erstatning av ødelagt utstyr, skade på bygninger eller nedetid/forsinkelser av viktige leveranser.

Omdømme
Svekket omdømme eller redusert tillit i befolkningen som følge av en uønsket hendelse. Denne kategorien er ofte nært knyttet til de fire ovenstående, og kan gjerne komme som en konsekvens av disse.

Sikkerhetsloven beskriver skadevurderinger for skjermingsverdige objekter som vurderinger der det spesielt skal tas hensyn til verdienes:

- *Betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket*
- *Betydning for kritiske funksjoner for det sivile samfunn*
- *Symbolverdi*
- *Mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse*

Det skal også vurderes hva som er en akseptabel tidsperiode for funksjonssvikt, mulighet til å gjenopprette funksjonaliteten og objektets betydning for andre objekter.[6]

For å vurdere skadepotensialet ved en verdis bortfall kan det være nyttig å definere terskelnivåer for hvor alvorlige konsekvenser et bortfall vil få i et eget skjema. Se eksempel på skjema i vedlegg. Det er viktig å presisere at nivåene vil variere fra virksomhet til virksomhet.

6
Sikkerhetslovens kapittel 5 «Objektsikkerhet»

Kapittel 7

Trusselvurdering

I dette kapitlet skal vi se nærmere på hvordan vi rent praktisk kan utarbeide en trusselvurdering som er grunnlaget for å få finne ut hva man skal beskytte seg mot.

Begrepet trussel brukes både om kapasitet og intensjon til å gjennomføre uønskede handlinger. I norsk straffelov brukes trusselbegrepet om aggressive ord eller handlinger. Vi definerer trussel som en mulig uønsket handling som gir en negativ konsekvens for en entitets sikkerhet.[1]

Hvilke trusler står vi overfor? Hvem kan i fremtiden tenkes å ville skade/ødelegge vår virksomhet/verdier? Dette er sentrale spørsmål som en trusselvurdering bør belyse og forsøke å gi svar på. Formålet med en trusselvurdering er å kartlegge relevante trusselaktører, deres intensjon, kapasitet og mulige handlemåter. Dette vil gi et godt utgangspunkt for å utvikle relevante trusselscenariorer som vi kan benytte for å vurdere sårbarhet og risiko. Trusselvurderingen inngår som en viktig del av en risikoanalyseprosess.

Generelt

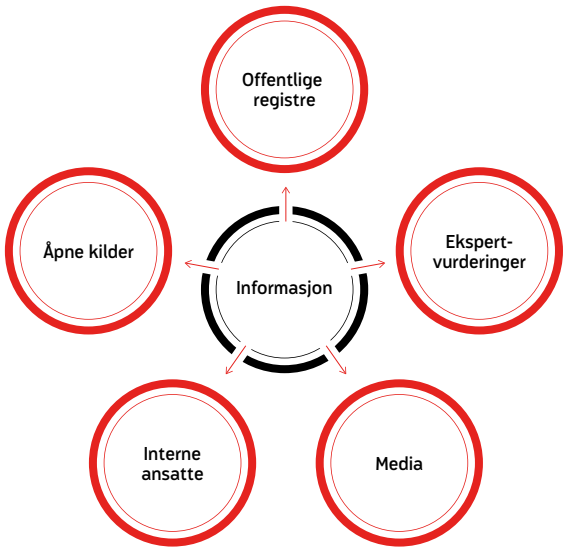
Det er viktig å være oppmerksom på at trusselvurderinger som utgis av ulike myndigheter, i stor grad er ferskvare, det vil si en beskrivelse av den nåværende situasjonen ved utgivelsesdato for rapporten. Hvordan trusselbildet vil utvikle seg i fremtiden, er utfordrende å vurdere. Det er likevel viktig å ta stilling til i trusselvurderingen, slik at vi er bedre rustet til å møte fremtidige utfordringer. Sikringstiltak kan være kostbare, og det er derfor ønskelig at disse også har kapasitet til å gi tilstrekkelig sikring i mange år fremover selv om trusselbildet endrer seg. Derfor er det avgjørende at trusselscenarioer som virksomheten kan bli utsatt for, på litt sikt blir vurdert. Vi ønsker ikke at sikringstiltakene skal være for svake, eller mangelfulle, sett opp mot ulike trusler allerede når de blir implementert. Det er også et poeng å tilrettelegge for å øke sikringen av objektet uten store og kostbare ombygginger.

Det er bare fantasien som setter grenser for hvilke trusselscenarioer som bør settes opp. Det vil imidlertid være viktig å forklare hvordan man har kommet frem til listen med trusselscenarioer, samt hvorfor tilsynelatende aktuelle scenarioer ikke er tatt med.

Kilder for trusselvurderingen i en risikoanalyse kan være både åpne og graderte trusselvurderinger fra f.eks. Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og E-tjenesten. Det er også relevant å benytte seg av statistikk fra Statistisk sentralbyrå (SSB), tidligere sikkerhetstruende hendelser i virksomheten, og rapporter om kriminalitet, f.eks. fra KRIPOS i vurderinger og råd fra organisa-

1
NS 5830:2012 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi

Kilder



TRUSLER

Kategorier
I trusselvurderingen kan det være hensiktsmessig å dele inn truslene i fire ulike kategorier:

- **Terror**
- **Etterretning**
- **Sabotasje**
- **Annen kriminalitet**

sjoner som Næringslivets Sikkerhetsråd. Det er flere internasjonale databaser som fører statistikk over terrorhendelser de siste 20–30 årene, deriblant RAND og University of Maryland, USA.

Innenfor de ulike kategoriene etterretning, terror, sabotasje og kriminalitet gis det en generell beskrivelse av den nåværende trusselsituasjonen, aktuelle aktører og deres modus operandi («fremgangsmåte»).

Vurderinger om fremtidige trusler er en krevende øvelse, med høy grad av usikkerhet. Det er nødvendig å innhente informasjon fra flere kilder for å verifisere vurderingene om aktuelle trusselaktører. Det benyttes i denne sammenheng de samme prinsipper som ved samfunnsvitenskapelig metode for validitet og reliabilitet, med bruk av flere kilder (data) og personer med ulik fagkompetanse. Det vil også for enkelte objekter være nødvendig å innhente kompetanse fra PST og Forsvarets sikkerhetsavdeling (FSA) for å vurdere dette.

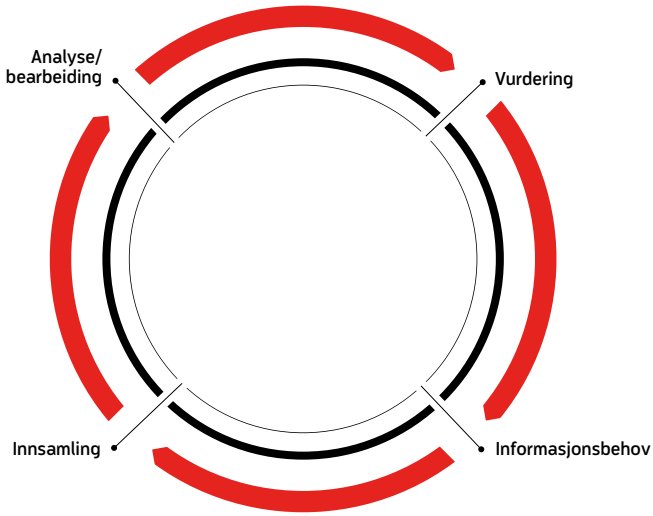
Prosessen frem til beskrivelse av truslene vises gjerne som et etterretningshjul. Prosessen består av en serie delprosesser som skal lede til at en får en best mulig vurdering av mulige trusler basert på tilgjengelig informasjon. Informasjonsdelene settes så sammen til et helhetlig bilde som er tilpasset det aktuelle analyseobjektet.

En trusselvurdering vil aldri kunne fange opp alle relevante forhold som kan ha en betydning for et analyseobjekt. Det er også utfordrende å predikere hvilke trusler som er aktuelle for analyseobjektet. Vurderingen vil derfor være høyst usikker. Det er derfor viktig å ta høyde for denne usikkerheten både ved vurdering av risikoanalysen og ved vurdering av anbefalte sikringstiltak.

TRUSLER VÅPEN-VIRKNING

- **Direkte ild med håndvåpen, rifler, skarpskytterrifler eller rakettvåpen**
- **Indirekte ild med håndgranater, brannbomber, improviserte bombekastere og raketter og droner med eksplosiver**
- **Bærbare enheter med eksempelvis eksplosivladninger eller EMP-kilder**
- **Kjøretøy som bærer av eksplosivladninger og EMP-kilde eller brukt som rambukk**
- **Kjemiske, biologiske og radiologiske trusselstoffer spredt i luft og vann**

Etterretningshjul



Trusselaktører

Trusselvurderingen må innenfor hver aktuelle kategori gi en beskrivelse av trusselaktørene, herunder intensjon, kapasitet og fremgangsmåte. Spørsmål som kan stilles i denne sammenheng:

- → *Hvorfor vil trusselaktøren angripe virksomheten (intensjon)?*
- → *Hvilken fremgangsmåte vil de benytte seg av (modus operandi)?*
- → *Hvilken organisering og tilgjengelige verktøy eller angrepsvåpen kan de benytte (kapasitet)?*

Vi deler trusselaktørene inn i fire ulike kategorier fra ALFA, BRAVO, CHARLIE og DELTA innenfor de fire trusselkategoriene. Tabeller som beskriver disse aktørene, er gjengitt i ***vedlegg Trusselaktører.***

Terror

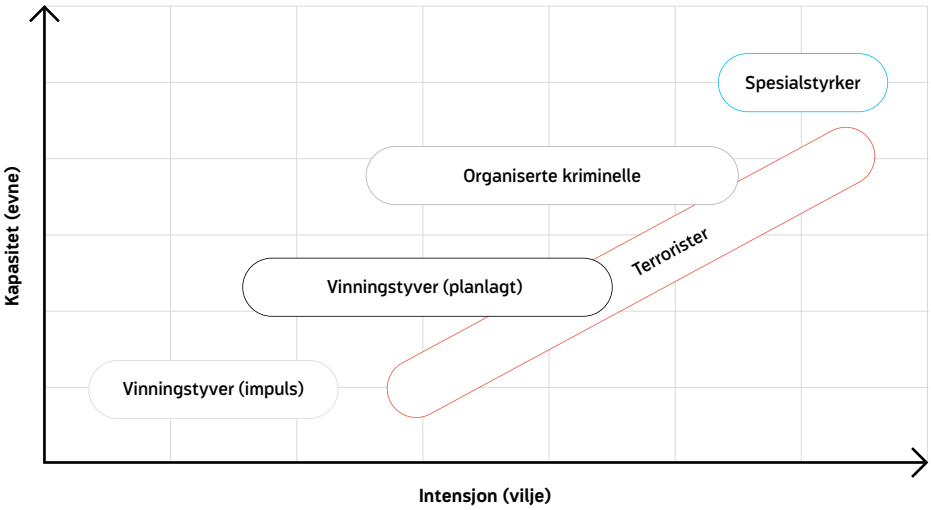
I sikkerhetsloven defineres terrorhandlinger som: «ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer og eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål.»[2] Årsaker til en terrorhendelse kan være at personer eller en organisasjon ønsker å skape oppmerksomhet rundt en sak av nasjonal eller internasjonal interesse. Det som imidlertid er relevant i denne sammenheng, er ikke aktørenes ideologiske eller religiøse overbevisning, men deres evne og vilje til å bruke vold.

Forskning ved Forsvarets forskningsinstitutt (FFI) viser at bruk av bomber har vært, og kommer sannsynligvis til å være, den mest brukte aksjonsformen innenfor terrorisme også i de neste tre til fem årene. Per dags dato omhandler ca. 70 prosent av alle terrorplaner eksplosiver av en eller annen type. FFI fremhever imidlertid at stadig flere aksjoner gjennom-

2
Sikkerhetslovens § 3 pkt. 5

Kapasitet og intensjon

Ulike trusselaktørers evne og vilje til å gjennomføre et angrep



føres med våpen som både er enklere å få fatt i og enklere å bruke enn eksplosiver, som ulike typer håndvåpen.

Terroraksjoner har tradisjonelt blitt gjennomført av flere ulike grupperinger de siste årene, ekstreme islamister, høyreekstremister og venstreekstremister.

Oppsummert har terror blitt gjennomført av flere ulike aktører med ulik erfaringsbakgrunn og motiver, og med flere ulike fremgangsmåter de siste årene:

- *Større bomber (kjøretøybaserte)*
- *Mindre bomber (plassert i bag, vesker)*
- *Selvmordsbombere*
- *Raketter og granater*
- *Håndvåpen*
- *Komplekse angrep (kombinasjon av flere av punktene)*

Det vi ikke har sett så langt, er bruk av såkalt skitten bombe (eksplosiver i kombinasjon med nukleært materiale). I tillegg har det vært relativt få tilfeller av bruk av biologiske eller kjemiske trusselstoffer. Bruk av droner har ikke så langt vært brukt i terrorangrep, men er noe som vi trolig kan se i årene fremover.

Etterretning

Spionasje er i sikkerhetsloven definert som «innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt»[3], og kan i utgangspunktet gjennomføres kun med den hensikt å få tak i informasjon. Her betraktes også etterretning som et ledd i forberedelsesfasen til gjennomføring av kriminelle handlinger, sabotasje eller terroraksjoner. Det antas at aktører vil kunne utføre en viss form for rekognosering, kartlegging eller etterretning før slike handlinger utføres.

Etterretningsaktører har tradisjonelt blitt delt inn i to ulike kategorier: ikke-statlige og statlige aktører. De vil kunne benytte seg av de samme metodene, men intensjonen for etterretningsinnhentingen vil være forskjellig

3 Sikkerhetslovens § 3, første ledd, pkt. 3

mellom de ulike aktørene. De statlige aktørene vil naturlig være interessert i informasjon som kan fremme de nasjonale interessene, mens de ikke-statlige aktørene kan være ute etter informasjon som kan gi fordeler for bedriften, for eksempel innsideinformasjon som f.eks. forskningsresultater og kontraktsinformasjon. I dagens situasjon er informasjon i større grad en handelsvare, og etterretning oftere drevet av en økonomisk interesse.

Uavhengig av hvem som utfører etterretning og hvorfor, er det noen kjennetegn og metoder som går igjen:

- *Kartlegging av åpne kilder som kart, tegninger, rapporter etc. som er offentlig tilgjengelige*
- *Fotografering av omkringliggende områder, bygninger, sikkerhetsrutiner m.m.*
- *Sosial manipulering (social engineering)*
- *Infiltrere ansatte (utro tjener)*
- *Utpressing av ansatte*
- *Hacking (fysisk eller via datanettverket)*
- *Avlytting av møterom, kontorer*
- *Avtitting/avlesning av dokumenter på avstand*
- *Innbrudd*

Spørsmål som en etterretningsaktør naturlig vil stille seg før en aksjon, er bl.a.:

- *Hvor er det verdier? (informasjon, teknologi, våpen, materiell, osv.)*
- *Hvordan er de sikret?*
- *Hvilke verktøy/metoder behøves for å komme til verdiene?*
- *Hvilke rutiner eksisterer på/i målet?*
- *Kan innsidere bestikkes, trues, lures til å gi fra seg opplysninger om målet?*
- *Kan målet infiltreres?*
- *Hvordan kan eventuelle vaktmannskaper eller politiet avledes?*
- *Hvordan komme til og fra målet uten å vekke oppsikt?*

Sabotasje

I sikkerhetsloven defineres sabotasje som «tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet, eller tilsiktet uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering.»[4] Dette omfatter aktører som militære spesialstyrker med spesialutdannelse i alle former for sabotasje, og spesialtrening for oppdraget.[5]

Veiledning for objektsikkerhetsforskriften fremhever at fremmede staters spesialstyrker, som har den aller høyeste kapasiteten, er en aktuell trussel først ved et relativt høyt konfliktnivå av utenrikspolitisk art. Sabotasje av denne typen anses som svært uvanlig i fredstid, og vil normalt bli gjennomført i forkant av en krise/krigssituasjon.

Det vil for mange virksomheter også være relevant å vurdere sabotasje som en handling utført som en reaksjon mot en virksomhet, og ikke som en del av opptakten til en krise/krig.

Sabotasje innebærer tilsiktet skade på mennesker og materiell. Militært er hensikten å påvirke vår militære kapasitet i negativ retning, noe som kan skje både i freds- og krigstid, men også sett i sammenheng med vårt internasjonale engasjement.

Det kan også være mer generelt rettet mot samfunnet, for eksempel i form av aksjoner mot kraft-, olje-, drivstoff- og kommunikasjonsanlegg, samt vann- og næringsmiddelforsyningen. IT-anlegg som styrer ovennevnte, vil være spesielt sårbare.

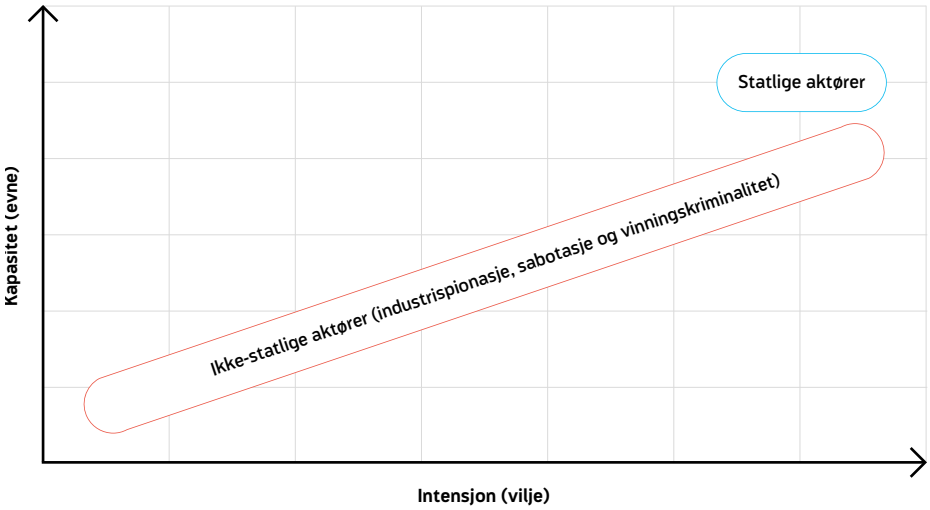
Sabotasjeaksjoner kan forberedes og gjennomføres slik at de ser ut som vanlige ulykker forårsaket av menneskelig feil, slurv og manglende kunnskaper, eller fordekt som ulykker.

4
Sikkerhetslovens § 3, første ledd, pkt. 4

5
Nesser, Petter & Stenersen, Anne (2014): The modus operandi of jihadi terrorists in Europe. Perspectives on terrorism. Volum 8, Issue 6

Etterretning

Ulike trusselaktørers evne og vilje til å gjennomføre etterretning



Annen kriminalitet

Kriminalitet er handlinger som er straffbare i henhold til straffeloven, og utviklingen innenfor kriminalitet følger samfunnsutviklingen som sådan.

Organisert kriminalitet defineres som kriminelle handlinger som utføres av kriminelle grupper eller nettverk som samarbeider, med en form for ledelse, og som over tid opererer med kriminelle handlinger som eneste eller som en dominerende inntektskilde.

Kriminelle aktiviteter motiveres som hovedregel av egen vinning, hovedforskjellen mellom de ulike aktørene innenfor annen kriminalitet er hvilken kapasitet de har til å gjennomføre handlingen. Mer erfarne kriminelle aktører vil gjerne benytte seg av andre metoder sammenlignet med mindre erfarne aktører. Det vil også være ulike verdier de vil være interessert i. Følgende forhold kan være relevant å beskrive i en trusselvurdering av annen kriminalitet:

- *Verdier (attraktive for hvem?)*
- *Lokalisering av verdiene (lett tilgjengelig)*
- *Omfang av verdiene*
- *Bygningens geografiske plassering*
- *Flere tidligere forsøk på innbrudd i nærområdet*
- *Kriminell aktivitet i nærområde (narkotika m.m.)*

Dimensjonerende trussel

Den dimensjonerende trusselen bør beskrives innenfor hver enkelt trusselkategori med angivelse av kapasitet og intensjon. Dette vil igjen gi et utgangspunkt for hvilke trusselscenarioer som skal vurderes i analysearbeidet, og hvilket utgangspunkt prosjektgruppen senere skal ta hensyn til i kravspesifikasjonen. Det er for dem et behov for å ta utgangspunkt i en dimensjonerende ytre påvirkning (trusselnivå) som hele eller deler av et bygg, eller anlegg dimensjoneres for å motstå.

Husk at den dimensjonerende trusselen må ta

utgangspunkt i de fastsatte sikringsmål, se ***kapittel 5, Risikoanalyse*** for mer informasjon om dette.

Trusselscenarioer

Basert på trusselvurderingen og den fastsatte dimensjonerende trusselen, utarbeides trusselscenarioer som eksempler på hva som kan skje. Det skal legges vekt på at scenarioene er tenkelige og representative. I betydningen representativ skal det ikke tolkes dithen at disse scenarioene vurderes som de mest sannsynlige scenarioene, men snarere at beskrivelser, beslutninger og sikringstiltak som man kommer frem til, er basert på resultater fra disse eksemplene, og vil være relevante og dekkende for de fleste andre situasjoner som kan oppstå.

I de fleste risikovurderinger brukes scenarioer for å hjelpe brukeren med å spille ut en uønsket hendelse som kan skje i fremtiden. Direktoratet for samfunnssikkerhet og beredskap (DSB)[6] definerer scenario som: «en detaljert og konkretisert beskrivelse av en uønsket hendelse; en beskrivelse av en framtidig tilstand og den serien av handlinger og/eller hendelser som leder dit». FFI[7] beskriver begrepet scenario som (i) en beskrivelse av et system som i en utgangstilstand, (ii) en tenkt starthendelse. Deretter analyserer man hva som kan komme til å skje ut fra dette utgangspunktet.

En scenariobeskrivelse bør med andre ord inneholde en beskrivelse av hva (hendelseskategori), hvem (trusselaktøren), hvorfor (hensikten) og hvordan (modus operandi).

Sjekklister kan med fordel benyttes som grunnlag for å velge ut scenarioer. Imidlertid er det hensiktsmessig at arbeidsgruppen starter med en idédugnad uten hjelp av sjekklisten, da er sannsynligheten større for at ikke relevante scenarioer for det spesifikke analyseobjektet utelates. Deretter benyttes sjekklisten for å supplere med andre aktuelle scenarioer.

Eksempler på gode trusselscenariobeskrivelser kan være:

- *Vinningskriminell bryter seg inn gjennom vinduet med enkelt innbruddsverktøy med den hensikt å få tak i lett omsettelige verdier.*
- *Fremmed etterretningsaktør avlytter rommet ved hjelp avansert avlyttingsutstyr utenfor bygningen. Hensikten er å få tak i gradert og/eller sensitiv informasjon.*
- *Fremmede spesialstyrker bryter seg inn i virksomheten ved hjelp av innbruddsverktøy. Hensikten er å overta kritiske funksjoner.*
- *Flere terrorister angriper bygningen ved hjelp av flere ulike typer våpen. Hensikten er å skape oppmerksomhet om et politisk/religiøst tema.*

Som trusselscenarioene viser har de ulike trusselaktørene ulik intensjon og kapasitet med handlingene. Dette vil igjen gi føringer for hvordan analyseobjektet skal analyseres. Det vil naturlig være forskjell på hvordan sårbarhet og risiko vurderes overfor en trusselaktør med liten erfaring vs. en med omfattende trening og erfaring.

Trusselscenarioene kan benyttes av virksomhetene i analysearbeidet, men også som et hjelpemiddel på øvelser og i aktiviteter der sikkerhet er tema.

6
FFI (2015) Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger

7
FFI (2015) Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger

Kapittel 8

Planlegging av sikringstiltak

Dette kapitlet beskriver hvordan sikring kan håndteres i de ulike fasene i et byggeprosjekt, slik at riktig sikringsnivå etableres, samtidig som estetiske, funksjonelle og økonomiske forhold ivaretas. Kapitlet tar også opp hvordan ulike leveranser fra risikoanalysen flettes inn i byggeprosessen.

Nøkkelen for et godt prosjekt er å bringe sikkerhet tidlig på dagsordenen, og å få avklart hvilke forventninger og behov bruker har. Sikkerhet er kun et av mange aspekter som skal ivaretas i et prosjekt, og bevisstheten omkring dette hos oppdragsgiver og byggherre, arkitekter og rådgivende ingeniører, helst med sikkerhetsfaglig kompetanse, kan bidra til gode løsninger som forener ulike interesser.

Generelt

I prosjekter der det er behov for å gjennomføre sikringstiltak mot tilsiktede uønskede handlinger, er det anbefalt å utvikle prosjektet gjennom prosjektfaser tilsvarende et tradisjonelt byggeprosjekt. Det henvises i denne sammenheng til norsk standard NS 5834:2016 «Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Planlegging av sikringstiltak i bygg, anlegg og eiendom», som gir veiledning om når og hvordan råd fra sikringsrådgivere bør komme i byggeprosessens faser. Standarden bør benyttes som et verktøy for å få sikringsleveranser med rett detaljeringsgrad på plass til riktig tid i prosjektet.

Foreløpig finnes det i Norge ikke standarder som fastsetter konkrete dimensjoneringskriterier for trusler fra tilsiktede uønskede hendelser. Det kan derfor være vanskelig å fastsette dimensjoneringskriterier for slike trusler, men de grunnleggende forholdene som må tas hensyn til, er:

- *Hva skal sikres? (Verdi)*
- *Hva skal vi sikre mot? (Dimensjonerende trussel)*
- *Hva er sårbarheten?*
- *Hvilke skader/tap/risiko kan aksepteres, og hva anser vi som god nok sikring?*

Når beslutningene knyttet til konsept og systemvalg først er gjort, vil det som regel være kostnadsdrivende å implementere sikringstiltak i ettertid. Sikringstiltak som innføres på et sent stadium, kan også påvirke bygningens visuelle karakter og de planlagte funksjoner i negativ retning.

Sikringstiltak kan implementeres i byggeprosjekter på mange ulike og kombinerte måter:

- *Fortrinnsvis ved å ha sikkerhet med som et premiss allerede i de overordnede valgene; slik som ved tomtevalg, plassering av bygningen i terrenget, kontroll på omkringliggende områder etc.*

- *Videre ved å planlegge for sikkerhet i valg av materialer, konstruksjonsprinsipper og geometri/plassering av funksjoner.*
- *Sikringstiltakene kan også legges utenpå og utenfor selve bygningen, slik at de synliggjøres for en avskrekkende virkning, men dette bør være en villet strategi og ikke en nødløsning eller kompensasjon for mangelfull prosjektering.*

Faser i byggeprosjekt

Navn på faseinndelinger kan variere, men i hovedsak er den overordnede gangen i et byggeprosjekt den samme. Nedenfor blir fasene fra NS 5834 beskrevet og spesielle forhold i tilknytning til sikring omtalt.

Strategisk definisjon
Innledningsvis i et byggeprosjekt kartlegges det overordnede behovet, og prosjektledelse etableres med styrende dokumenter. I denne fasen fastsettes målet og ambisjonene for prosjektet.

Prosjektledelsen legger en strategi for gjennomføring av prosjektet og etablerer en prosjektorganisasjon som typisk består av arkitekt og faglige rådgivere, samt representant(er) fra bruker.

I forbindelse med prosjektetableringen bør det gjøres en første risikovurdering for å avdekke om prosjektet vil kunne få spesielle behov knyttet til sikring (risikoanalyse). Dersom sikring av bygg blir aktuelt, bør arkitekt- og rådgivergruppen inneha eller suppleres med sikringsfaglig kompetanse. Det er fordelaktig om sikkerhetsfaglige rådgivere også har kunnskaper om planlegging og prosjektering av bygninger og anlegg, utover spesialkompetanse innen sikring. Identifisering av verdier og fastsetting av sikringsmål er en forutsetning for riktig sikring senere i prosjektet.

Et annet forhold som bør avklares i forbindelse med prosjektetableringen, er informasjonssikkerhet. Dersom prosjektet inneholder informasjon som er skjermingsverdig, bør det utarbeides en sikkerhetsplan. Sikkerhetsplanen bør si noe om klarering av personell og leverandører, håndtering av dokumentasjon, etablering av prosjektkontor/lokasjon/møterom m.m.

Program- og konseptutvikling
Programfasen består av en rekke utredninger som fastsetter premissene for prosjekteringen. Brukers egne krav utover lov og forskrift bør fremkomme, det gjelder også presiseringer av brukers/rådgivers tolkning av lov- og forskriftskrav. I tillegg til plan- og bygningsloven kan blant annet sikkerhetsloven gjelde for objekter med krav til beskyttelse og sikring.

Det er tidligere forklart at verdier kan være objekter, informasjon eller funksjoner. Verdier som inngår i prosjektet, vil beskrives i rom- og funksjonsprogrammet som utvikles. I prosjekter vil det normalt være krav om å vurdere flere mulige overordnede løsningskonsepter, der alle skal tilfredsstille overordnede sikringsmål for prosjektet. Det er viktig at behovs- og funksjonsanalysen utføres grundig for å kartlegge brukerens reelle behov og krav til sikkerhet.

Grunnlagsdokumenter for sikkerhet og virksomhetens sikringsmål bør være utgangspunkt ved utarbeidelse av kravdokument for sikkerhet.

I prosjekter med spesielle behov for sikring bør det utføres en grundig behovs- og funksjonsanalyse der hensikten er å kartlegge brukernes aktuelle behov og krav til sikkerhet knyttet til sin virksomhet. Oppdragsgivers sikringsmål tas inn i prosjektets kravdokument i en egen del som omhandler sikkerhet. Kravdokumentet og de underliggende krav til sikkerhet vil utvikles gjennom byggeprosjektets faser. I denne prosessen er det svært viktig at bruker er involvert for å få en best mulig beskrivelse av hva som er verdiene som skal beskyttes (verdivurdering),

trusselen som skal legges til grunn (dimensjonerende trussel), og akseptabel sluttilstand om trusselen skulle inntreffe (sikringsnivå).

Kravdokumentet må forankres hos oppdragsgiver/byggherre for at dokumentet skal ha den nødvendige tyngden videre i prosjektet.

Det er viktig at sikringskrav beskrives som funksjonskrav. I senere faser av byggeprogrammet omsettes funksjonskravene i kravdokumentet til ytelsesmål som de prosjekterende vil bruke som grunnlag ved utforming og dimensjonering av løsninger. Ved å formulere kravene som funksjonskrav, og ikke som konkrete løsninger eller produkter, får arkitekt og rådgivere det nødvendige spillerom til å finne frem til de beste tverrfaglige løsningene. Reguleringsforhold avklares og eventuelle konsekvensutredninger iverksettes ved behov. Dersom sikkerhet er en vesentlig premiss i prosjektet, vil det være naturlig at det gjøres en konsekvensutredning med tanke på sikkerhet. Hva vil konsekvensen for området rundt bli dersom det etableres et anlegg med spesielle sikkerhetsutfordringer?

Med kravdokument og andre utredninger på plass kan det gjøres en vurdering av ulike alternative konsepter og forslag til løsning. Dette kan for eksempel være:

- *Ulike tomtevalg og variasjoner over intern plassering av bygg på tomten.*
- *Alternativ infrastruktur, plassering og sikringsbehov.*
- *Nybygg, rehabilitering eller en kombinasjon.*
- *Flere bygninger eller bygge i høyden (alternativ geometri).*
- *Ulike kvaliteter.*
- *Hva skal arkitekturen signalisere? Er ambisjonen åpent og inviterende, eller lukket og avskrekkende?*
- *Hva er mulige sikringsstrategier for de ulike alternativene?*

De alternative løsningskonseptene som prosjektgruppen utarbeider i programfasen, blir utredet, kostnadsberegnet og evaluert med anbefaling om hvilket løsningskonsept virksomheten bør velge for videreføring i et forprosjekt. I hvilken grad løsningskonseptene oppfyller sikringsmålene, bør være med som ett av evalueringskriteriene ved valget av anbefalt løsningskonsept. Evalueringen av sikkerhet gjennomføres for de enkelte konseptene med bakgrunn i kravdokumentet eller verdivurdering og dimensjonerende trussel. For hvert alternativ synliggjøres sårbarhet eller restrisiko slik at alternativene kan rangeres.

Bearbeiding av valgt konsept

Om valgt konsept godkjennes for videreutvikling i et forprosjekt, vil prosjektgruppen videreutvikle konseptet med tegninger, beskrivelse og kostnadsestimat med en detaljgrad som er tilpasset forprosjektfasen. I forprosjektfasen vil også fysiske og elektroniske sikringstiltak planlegges mer detaljert.

Underveis i forprosjektet bør risikoanalysen samt kravdokumentet fra programfasen oppdateres. Når det gjelder sikkerhet bør det gjennomføres en revisjon for å få kontroll på eventuelle svakheter i sikringskonseptet og avvik fra krav. Risikoanalysen bør resultere i en avviksrapport, som prosjekteringsgruppen må håndtere og avvikene lukkes. Om avvik for eksempel er særdeles vanskelig å lukke, eller at kostnader blir urimelig store, kan oppdragsgiver/byggherre revurdere sine krav og akseptere en høyere restrisiko. Etter hvert som prosjektet utvikles, kan det være behov for endringer i kravdokumentet. Nye krav kan komme til og andre falle fra, og således vil kravdokumentet være gjenstand for revisjon i de forskjellige fasene, men like fullt er det viktig med riktig forankring bak hver revisjon.

Detaljprosjektering

Gjennom utviklingen av skisse- og forprosjektet bør sikkerhet være avveid mot andre forhold,

og danne grunnlaget for utvikling av fysiske og tekniske løsninger på detaljnivå. Detaljprosjekt er siste steg i planleggingsfasen, og et detaljert og kvalitetssikret underlag for tilbud og kontrahering av utførende vil i denne fasen bli utarbeidet. Entrepriseformen bør ta hensyn til skjermingsbehov. Eksempelvis kan det være aktuelt å anskaffe sikkerhetsdører/-vinduer som egen entreprise eller direktekjøp for å unngå kobling mellom sikkerhetskrav og plassering, og således unngå unødig spredning av informasjon.

Det skal utarbeides kontrollplaner for sikringsanleggene, som vedlegges anbudsunderlaget. Kontrollplanene bør belyse hva som skal kontrolleres underveis i byggefasen, og på hvilken måte (befaring, foto, osv.).

Før utsendelse av anbudsunderlag og arbeidstegninger bør det gjøres en ny revisjon av risikoanalysen for å avdekke eventuelle svakheter i sikringskonseptet og avvik fra krav. Dette gjøres på samme måte som i forprosjektet for å sikre at eventuelle sårbarheter blir lukket.

Produksjon og leveranser

Under produksjon bør sikkerhetsrådgivere bidra med kontroll i henhold til kontrollplaner og deltakelse ved idriftsetting.

Overlevering og ibruktakelse

Prøvedriften starter når bygget er ferdig og bruker har tatt det i bruk. I prøvedriftsperioden har gjerne entreprenøren ansvar for å drifte anlegget, primært de tekniske anleggene (VVS, el, tele/automatisering, IKT), og besørge eventuelle behov for utbedringer og justeringer. En prøvedriftsperiode varer gjerne ett år, slik at anleggene er testet under alle klimatiske forhold.

Prøvedriftsperioden bør også anvendes for kontroll og testing av anlegget med tanke på beskyttelse og sikring.

Det anbefales at det gjøres en oppdatert sikringsrisikoanalyse der svakheter i sikringskonsept og avvik i prøvedriftsperioden avdekkes. Eventuelle justeringer og tilpasninger kan da utføres så tidlig som mulig.

DEL 3

METODER FOR SIKRING

Del 3 Metoder for sikring gir en bred oversikt over sikringstiltak mot ulike trusler. Kapitlet belyser fagvis aktuelle måter å sikre eiendom, bygg og anlegg på mot uønskede hendelser. Metodene spenner fra arkitektur, konstruksjons-prinsipper, elektronisk sikring og skjerming mot avlytting til vakthold og reaksjonstiltak.

Kapittel 9

Arkitektur og sikkerhet

Dette kapitlet tar for seg hvordan planlegging, arkitektur og formgivning kan brukes som verktøy i sikringsarbeidet, og er primært rettet mot arkitekter, byggtekniske rådgivere, landskapsarkitekter og byplanleggere som har dette som ansvarsområde.

Krav til sikring er et av flere parametere i et byggeprosjekt, og kun gjennom en tverrfaglig tilnærming kan sikringstiltak integreres slik at ulike og av og til motstridende interesser ivaretas. Kapitlet vektlegger særlig sikringstiltak mot eksplosiver, da dette er en trussel med stort skadeomfang på bygg og omgivelser. Mer informasjon om temaet i ***kapittel 16, Beskyttelse mot eksplosiver.***

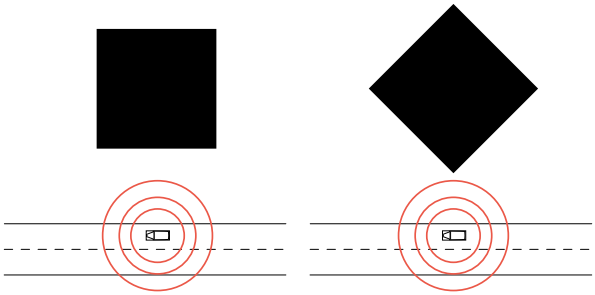
Tradisjonelt sett har arkitekter, planleggere og bygningstekniske rådgivere for liten oppmerksomhet på sikringstiltak mot tilsiktede uønskede hendelser, og sikkerhetsrådgivningen har ofte blitt utøvet av personer med politi-, militær- og sikkerhetsfaglig bakgrunn. Fordi sikringstiltak de siste årene skal svare til en økt trussel, og i tillegg fått stadig større betydning ved større inngrep i bymiljøet, er det viktig at tiltakene utformes med høy kvalitet tilpasset sine omgivelser. Arkitekter, landskapsarkitekter og andre formgivere har derfor en viktig funksjon og et stort faglig ansvar i å ivareta kvalitet i estetikk og funksjonalitet i planlegging og utforming av sikringstiltak. Selv om det for sikringstiltak som oftest foreligger fastsatte krav og dimensjoner, er det likevel store muligheter for å tilpasse utformingen av omgivelser, bygninger og elementer i hvert tilfelle.

En bygnings arkitektoniske uttrykk vil, uavhengig av funksjon, variere etter utforming og materialbruk og kan utformes slik at bygningen fremstår imøtekommende eller avvisende. I sikringssammenheng snakker man også om grad av sikringspreg, og eventuelt hvor avskrekkende et bygg skal være. Utfordringen for arkitekter som jobber med sikringsprosjekter, er å planlegge bygninger og anlegg som både gir et ønsket arkitektonisk uttrykk, har rett funksjonalitet og å samtidig sørge for at sikkerheten er på et akseptabelt nivå. Arkitekter, planleggere og ingeniører som skal planlegge et bygg med behov for sikring, må søke og innhente den nødvendige kompetansen for de sikkerhetsmessige aspektene og benytte seg av denne for å utvikle et godt arkitektonisk svar på oppgaven.

Den beste og mest kostnadseffektive måten å sikre verdier i bygninger mot sikkerhetstruende hendelser på er å sørge for at sikkerhet er med som premiss i planleggingen i en tidlig fase av prosjektet, se ***kapittel 8, Planlegging av sikringstiltak***, samt Norsk Standard NS 5834 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Planlegging av sikringstiltak i bygg, anlegg og eiendom.

Orientering av bygg

i forhold til potensiell eksplosjonskilde



Det vil som regel ved god planlegging være mulig å redusere risikoen radikalt. Det finnes i dag tekniske løsninger som muliggjør dimensjonering av nye bygg og forsterkning av eksisterende for å sikre eller gi skadereduksjon ved for eksempel terroranslag eller trusler som inntrengning og spionasje, se de øvrige ***kapitlene i del 3.***

Tomt

Tomtevalg og plassering på tomt er viktig fordi omgivelsene vil ha stor betydning for hvordan man løser sikringsbehovene. Å etablere avstand er gunstig mot mange typer trusler, og blant annet vil avstand til perimeter være viktig for deteksjonen av et eventuelt inntrengningsforsøk. En trussel med stort skadepotensiale, er bilbomber, og avstand vil være en vesentlig parameter for lastvirkningen, siden eksplosjonslast reduseres meget effektivt med økende avstand mellom eksplosjon og konstruksjon. I tette urbane situasjoner der avstand kan være vanskelig å etablere, vil det kunne bety at kostbare sikringstiltak er nødvendige for å oppfylle ønskede sikringsmål.

Avstand kan også være en premiss for valg av utforming, bæresystem og materialer. Utformingen har betydning for lastvirkninger på fasade og valg av bæresystem, og materialvalg har betydning for byggets kapasitet til å motstå eksplosjonslast.

Bygningens fysiske orientering i terrenget vil ofte bestemmes av tilstøtende bygg og reguleringsplaner, lysforhold og eksisterende infrastruktur. I et sikkerhetsperspektiv vil hensynet til terrengets utforming og fremkommelighet for kjøretøy, offentlige veier og arealer kunne være like viktige.

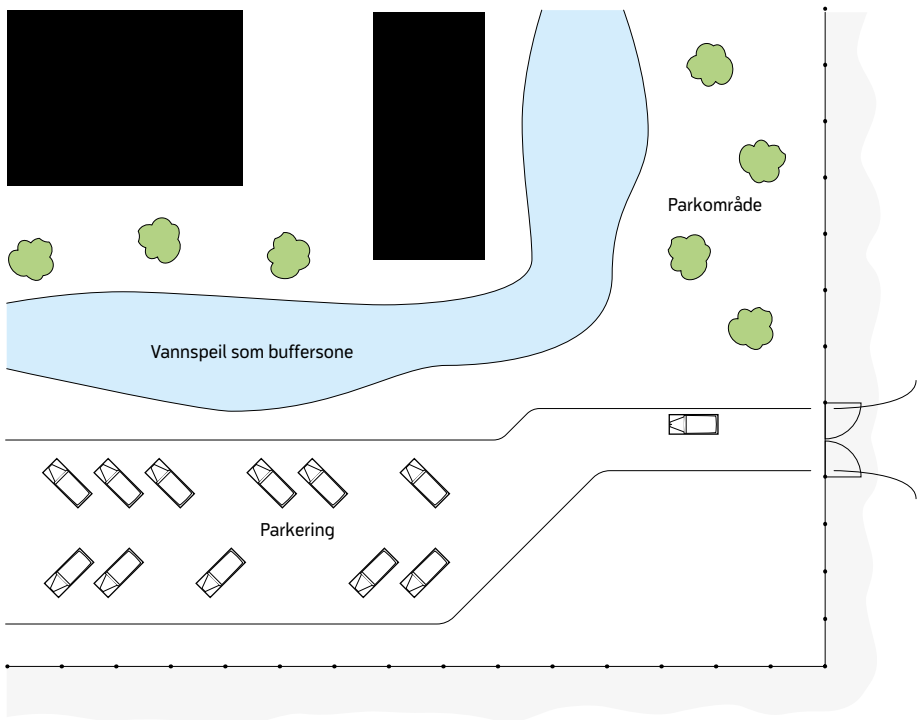
Der tomt er fastlagt, kan man oppnå god sikring ved å vurdere mot trusler:

Eksplosjoner

- → *Byggets avstand til mulig trussel eller angrepspunkt som er det mest effektive tiltaket for å redusere skadene av en eksplosjon*
- → *Orientering og plassering på tomt er faktorer som er viktige med tanke på materialvalg og bæresystem*

Bygning bør orienteres slik at et så lite areal som mulig rettes mot den potensielle eksplosjonskilden.

Landskap som buffersone



Beskytning og spionasje

- → *Nærhet til infrastruktur og omkringliggende bygninger (ekempelvis sårbarheter i andre attraktive mål rett ved tomt)*
- → *Innsyn og sikteavstand fra omkringliggende bygg*

Utomhusarealer og landskapsarkitektur

Ved utforming av utomhusarealer er det store muligheter for god sikring med tanke på å stoppe kjøretøy med eksplosiver ved hjelp av terrengbearbeiding med nivåforskjeller, trapper, vannspeil, grøfter, voller, m.m. Dette gjøres ofte i kombinasjon med mer tradisjonelle elementer som gjerder, murer og pullerter ved områder for inn- og utpassering, og der det er behov for mer fleksible løsninger.

Vurderinger som må gjøres:

- → *Hvilke kjøretøy er aktuelle trusler (lastekapasitet)?*
- → *Hvilken hastighet er det mulig for kjøretøy å oppnå, og i hvilken vinkel vil det treffe sperringene?*
- → *Hvordan skal inn/ut-passeringspunkter fungeres og driftes?*
- → *Kan parkeringsplasser flyttes lenger vekk?*

Tydelig design i uteområdene

Ved planlegging av uteområder rundt bygninger som har behov for sikringstiltak og er plassert i byrom, er det som i andre prosjekter viktig å være tydelig i formgivingen av bevegelsesruter og trafikkavviklingen både for gående, syklende og kjørende. I tillegg til å sikre trygg ferdsel er dette spesielt viktig i sikringsprosjekter for både å ivareta en god oversikt i området,

og ikke skape rom der publikum selv står fritt til å definere bruken av området. Eksempelvis kan tilfeldig beplantning oppfordre til gjemmesteder, skjulte og inntrukne fasader kan skape rom for kriminelle handlinger osv.

Ved å skille trafikken mellom gående, syklende og kjørende gir dette ikke bare en større sikkerhet for myke trafikanter, men også et mer oversiktlig landskap. Visuell kontakt skaper tryggere byrom og vil være like gjeldende for øvrig byplanlegging som ved planleggingen av områder omkring sikringsprosjekter.

Gang- og sykkelstier skal være belyst og ha en visuell kontakt med omgivelser. Vegetasjonen langs disse bør være av en slik art at den ikke kan brukes som skjulested.

Sikringstiltak og bymiljø

Det vil i mange tilfeller være en utfordring å sikre bygg i tette bymiljøer, der det sivile, dagligdagse livet skal forenes med kravene til sikringstiltak rundt utpekte bygg og områder. Spillerommet er også ulikt for offentlige bygg og de kommersielle virksomhetene som ønsker å sikre sine verdier. Uavhengig av hvilket sikringsregime som velges, vil de ha til felles at det er publikum og brukere som skal forholde seg til gitte bevegelsesmønstre, rutiner og praksis på daglig basis. For ethvert prosjekt som involverer implementeringen av sikringstiltak, kreves det både kunnskap om faktiske løsninger og ambisjoner om et godt resultat. Det vil si at det innenfor rammene av angitte sikringsmål finnes rom for kreativitet og muligheter for kombinerte effekter, slik som at en barriere kan ha form som eksempelvis en trapp eller amfi, sitteplass eller vannspeil. Avveiningen her er da om man ønsker en akkumulasjon av mennesker på gitte steder eller ikke, og således ikke legge til rette for det.

Fysiske sikringstiltak kan legges i landskapsbearbeiding der det areal nok, eller integrert i elementer og bygg, mens det også andre ganger vil være riktig å ha et større sikringspreg i og omkring et bygg. Dette er noe som må avklares og avstemmes tidlig i prosessen. Se også her ***kapittel 5, Risikoanalyse*** og ***kapittel 8, Planlegging av sikringstiltak.***

Kjøretøysperrer

Felles for kjøretøysperrer er at uansett utførelse og utforming skal de motstå en gitt trussel. De skal ha en dimensjonering som tar hensyn til minimums- og maksimumshøyder og deres avstand innbyrdes. Montering og forankring vil være viktige betraktninger, da man ikke alle steder kan gå langt ned i bakken, og heller må søke grunnere løsninger både med og uten forankring i hverandre. Dette avsnittet tar for seg noen av de vanligste former for kjøretøysperrer.

Pullerter, både aktive og passive, er gode, testede løsninger for å hindre adgang for uønskede kjøretøyer, og kan være et fornuftig tiltak på steder der det er knapt med areal, som for eksempel utenfor eksisterende bygning som ligger tett på gateløp.

Dersom de derimot er satt opp som repeterende elementer rundt, eller langs større byrom, er de imidlertid ikke alltid det beste formsvar sett fra et publikumperspektiv. Eksemplet er fra King's Cross St. Pancras, London og viser et byrom delt i to av en langstrakt monoton rekke av pullerter.

Det vil i de fleste tilfeller gi en bedre løsning å vurdere et bredere spekter av elementer, eksempelvis gatemøbler og installasjoner med integrert sikring, ramper og lavere murer etc. dersom landskapsgrep ikke er innenfor rammene av sikringsprosjektet.

Sikringstiltak som berører større områder, spesielt i byrom, krever omfattende planlegging for å skape et visuelt ryddig uttrykk. Eksempelvis kan det være hensiktsmessig å vurdere sten-

Pullerter og elementer
Eksempler fra Kvadraturen i Oslo hvor pullerter og elementer er kombinert med kunstneriske uttrykk, som også gir en publikums-opplevelse.

FOTO Forsvarsbygg

Pullerter som kjøretøysperrer
King's Cross St. Pancras.

FOTO Forsvarsbygg

ging av en vei fremfor å perimetersikre en hel park eller større offentlige plasser med etablering av lengre strekninger med pullerter.

Kjøretøysperrer i form av forsterkede murer i ulike høyder kan integreres som sitteplasser, spesialprosjekterte trapper, massive plantekasser/blomsterbed med integrert sikring, eller som en del av et vannspeil eller avrenningssystem.

Se ***kapittel 10, Perimeter- og områdesikring*** for generell dimensjonering av de enkelte fysiske sikringstiltak som er beskrevet i dette avsnittet.

Midlertidige sikringstiltak

Denne betegnelsen gjelder tiltak som etableres inntil grunnsikringen er på plass. Tiden det tar før de mer permanente tiltakene med forhøyet kvalitet blir implementert, kan i praksis strekke seg over flere år, og det er derfor også her viktig å planlegge for og organisere at disse ivaretar et bymiljø den tiden de er i bruk.

Bæresystem

Det er tekniske forskrifter til plan- og bygningsloven med underliggende prosjekteringsstandarder som stiller krav til konstruksjonssikkerhet for bygninger i Norge. Generelt er det krav om at konstruksjoner i Norge skal prosjekteres og utføres slik at konstruksjonen ikke vil bli skadet ved ulike hendelser i et omfang som ikke står i forhold til den opprinnelige årsaken. Det er vanlig å omtale dette som at bygning eller konstruksjon skal ha tilstrekkelig robusthet mot progressiv kollaps.

Ved å følge norske prosjekteringsstandarder oppnår konstruktøren tilstrekkelig robusthet og konstruksjonssikkerhet for alle lastpåvirkninger som standarden krever at norske bygg dimensjoneres for. Standardene dekker ugunstige lastkombinasjoner av egenlast, nyttelast, snø, vind osv., samt geotekniske laster og jordskjelvslaster og ulykkelaster.

Det er viktig å være klar over at norsk standard og eurokoder ikke dekker ulykkessituasjoner forårsaket av utvendige eksplosjoner, krigs-

Pullerter
Bruk av pullerter omkring et maktbygg som kan tenkes ønsket å inneha et eksplisitt sikringspreg. Bildet er fra Kvadraturen i Oslo, der byggene ligger relativt tett på gateløp.

FOTO Forsvarsbygg

Pullerter
Gatemøbler som i skala harmoniserer. Utført i kombinasjon med plantekasser og integrert sikring.

FOTO Forsvarsbygg

og terrorhandling. Dette betyr at det ikke er tilstrekkelig alene å følge prosjekteringsstandardene for å dokumentere tilstrekkelig sikring og konstruksjonssikkerhet for beskyttelse av mennesker og/eller prioriterte verdier og funksjoner, mot trusselscenarioer med bilbomber eller mindre bomber tett inntil eller inne i bygningen.

Selv om en bygning er dimensjonert for å tåle en viss jordskjelvsbelastning, vil en eksplosjonslast fra detonasjon av eksplosiver kunne gi en betydelig kraftigere og lokalisert lastvirkning på konstruksjonen.

Detonasjon av eksplosiver på utsiden av en bygning vil kunne knuse bærekomponenter

Pullerter som kjøretøysperrer
Sikringstiltak som berører større områder, spesielt i byrom, krever omfattende planlegging for å skape et visuelt ryddig uttrykk. Eksempelvis kan det være hensiktsmessig å vurdere stenging av en vei fremfor å perimetersikre en hel park eller plass med etablering av lengre strekninger med pullerter.

FOTO Forsvarsbygg

Kjøretøyshindre
Kjøretøyshindre i form av forsterkede murer i ulike høyder kan integreres som sitteplasser, spesialprosjekterte trapper, massive plantekasser/blomsterbed med integrert sikring, eller som en del av et vannspeil eller avrenningssystem.

FOTO Forsvarsbygg

som er i nærheten av ladningen. Dette kan medføre at deler av bygningen kollapser, selv om bygningen har en viss robusthet mot progressiv kollaps. Luftsjokket fra en bilbombe vil også kunne knuse fasadekomponenter og trenge inn i bygningen. Inntrengning av luftsjokk vil typisk gi løft av dekker, og vegger blir presset utover. Vanlige bæresystemer er normalt konstruert for å tåle store vertikale laster fra egenlast, nyttelast og snølast. Luftsjokket påfører bæresystemet i bygget derfor store belastninger som virker i andre retninger enn det bæresystemet er dimensjonert for.

Ved prosjektering av nye bygninger som skal sikres mot eksplosjonsvirkninger, er det derfor essensielt å velge bæresystem og materiale som er robust mot eksplosjonslast. Et bæresystem av plasstøpt armert betong med sterke forbindelser mellom komponenter i bæresystemet, vil gi potensial for betydelig større motstandsevne mot eksplosjonslastvirkninger, enn et elementbygg med svake forbindelser mellom dekker og vegger dimensjonert for minimumskravene til robusthet i norsk standard. Et elementbygg kan litt forenklet sammenlignes med et «korthus» med svake forbindelser mellom dekker og vegger. Det finnes en rekke enkle lite kostnadskrevende tiltak som kan gjøres i prosjekteringen for å øke en bygnings robusthet for å motstå eksplosjonslaster. Det er derfor viktig at både arkitekter,

Midlertidige løsninger
Eksempler fra London og Oslo, der begge sikringstiltakene har fungert over tid.

FOTO Forsvarsbygg

bygningstekniske og sikringsrådgivere samarbeider om plassering og utforming av bygning og bæresystemer i en tidlig fase av prosjektet.

For mer detaljer om eksplosivlaster, se ***kapittel 16, Beskyttelse mot eksplosjoner. For mer informasjon om lovverk,*** se ***kapittel 4, Samfunnssikkerhet, lover og regelverk.***

Fasader og materialvalg

Byggets ytre skall representerer gjerne den første bygningsmessige barrieren en trusselaktør må forsere for å komme inn til verdiene, og normalt utføres derfor skallsikringstiltak for fasader som inkluderer sikring av dører og vinduer.

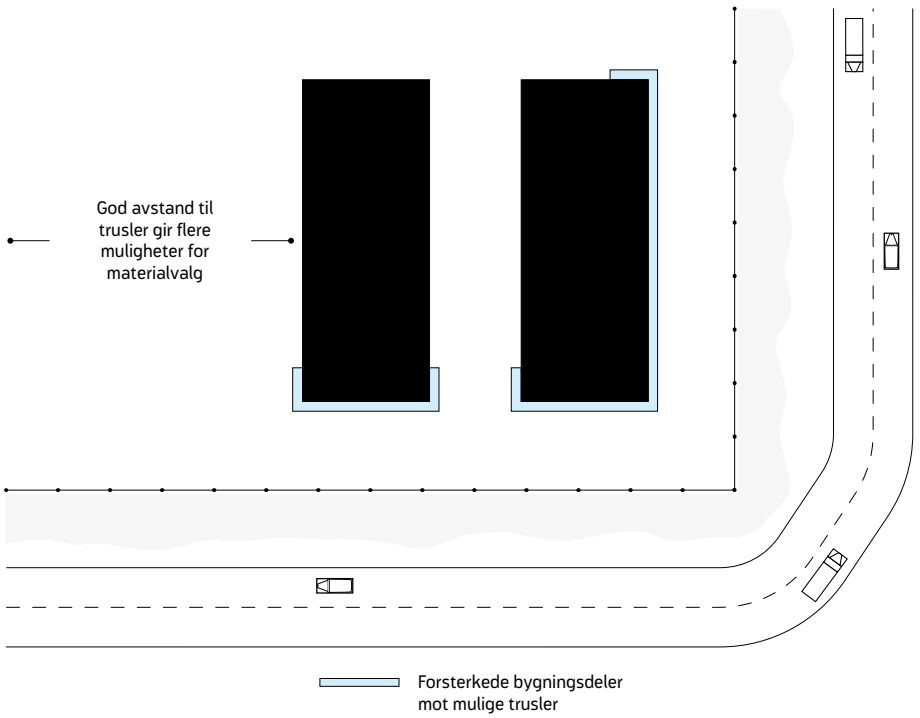
I prosjekter der det er behov for å sikre mennesker og/eller prioritere verdier og funksjoner mot utvendige eksplosjonstrusler, representerer fasaden en kritisk barriere mellom bomben og menneskene på innsiden i bygget. Fasader på et bygg er sårbare for utvendig eksplosjonslast, fordi de representerer den del av bygningen som er plassert nærmest trusselen. Store fasadefelt med glass, vanlige vinduer og dører eller svake yttervegger i sprø materialer som tegl/mur, er også sårbare komponenter for utvendig eksplosjonslast. Om fasade utsettes for luftsjokk fra en bilbombe, vil de svake bygningselementene typisk fragmentere og kastes inn i bygningskroppen med stor hastighet som kan påføre mennesker alvorlige skader. Luftsjokk og fragmenter som trenger inn i bygget, vil også kunne medføre store materielle ødeleggelser.

Det kan derfor være aktuelt å prosjektere fasader og tak slik at de representer en fysisk barriere mellom eksplosjonstrusselen og menneskene og verdiene på innsiden av bygget. Barrieren skal gi beskyttelse eller gi skadereduserende effekt for eksplosjonsvirkningene, slik at det oppnås tilfredsstillende sikkerhet for mennesker og akseptabel sikring av prioriterte verdier og funksjoner.

Fasadeutforming byr på mange valgmuligheter for arkitektonisk utrykk og tekniske løsninger. Det finnes klassifiserte sikkerhetsprodukter for fasadeglass, vinduer og dører som er utviklet med stor motstandsevne mot eksplosjonsbelastning og samtidig normalt kan tilpasses arkitektens planlagte utforming for fasaden. Sikkerhetsproduktene kan også leveres klassifisert med motstand mot inntrengning og/eller beskytning. Det finnes også sikkerhetsprodukter som forsterkningsduker eller spesielle kompositttplater som kan brukes for å forsterke yttervegger, slik at disse oppnår stor motstandsevne mot eksplosjonslast. Byggherrer bør imidlertid være klar over at slike sikkerhetsprodukter gjerne er svært kostbare, og at det i sikkerhetsplanleggingen må være en klar strategi på hvordan bygget skal sikres mot eksplosjonstrusler med kostnadseffektive tiltak.

Om bygningen er plassert i et bysentrum, kan det i praksis være vanskelig å få etablert

Materialvalg og avstander



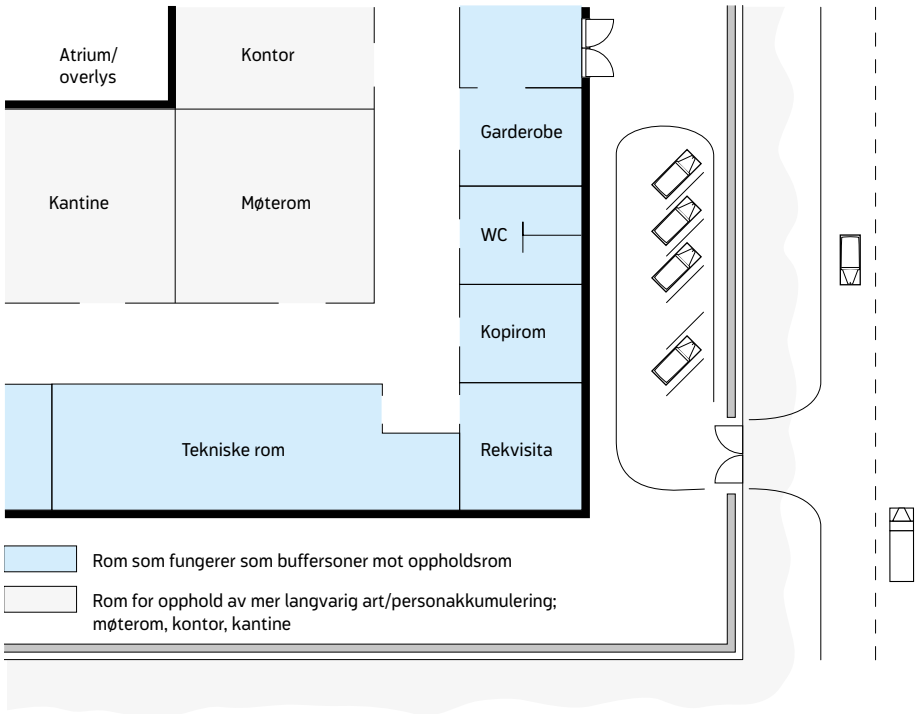
ønsket avstand mellom bygget som skal sikres, og en bilbombetrussel i trafikkert gate. Kort avstand til trussel utløser behov for kostbare sikringstiltak for å gi fasader en akseptabel eksplosjonsmotstandsevne, samtidig som byggherren i tillegg må akseptere risiko knyttet til lokal ødeleggelse av fasadeareal i området nærmest detonasjonsstedet for bomben. Avstand er derfor en kritisk parameter for eksplosjonsvirkningene av en bombe. I tillegg til avstandsskapende tiltak er det viktig å planlegge utformingen av bygget med en geometri som er med på å redusere eksplosjonsbelastningen på fasader og unngår å generere farlige fragmenter. Se ***avsnitt om geometri.***

Med et dimensjonerende trusselscenario med bilbombe foretas beregninger eller simuleringer for å bestemme eksplosjonslasten som virker på fasader og tak. Det er da bestemt en dimensjonerende eksplosjonslast som fasaden skal dimensjoneres mot. Arkitekt og byggeteknisk rådgiver står da overfor et strategisk valg om fasaden skal utformes med «hard» eller «myk» konstruksjonsmessig utforming.

En fasade som utføres med vegger i armert plasstøpt betong, kan dimensjoneres for å motstå store eksplosjonslaster. Yttervegg av armert betong vil være en relativt stiv fasadeløsning som overfører relativt store krefter inn på byggets bæresystem. Valg av «hard» konstruksjonsmessig fasadeløsning krever derfor at det kontrolleres at hovedbæresystemet har kapasitet til å ta opp kreftene som overføres.

Et godt alternativ er å velge en «myk» konstruksjonsmessig utforming, der fasade er

Soneinndeling. Buffersone mot yttervegg



spesielt utformet med duktile elementer. Slike elementer kan være konstruert slik at energien fra eksplosjonslasten kan bli tatt opp i materialet eller innfestingen, og de kan gjennomgå store plastiske deformasjoner uten å gå til brudd. I dette tilfelle vil størrelsen på kreftene som føres inn på bæresystemet, være mye mindre enn i tilfelle med den harde eller stive fasadeløsningen.

En bevisst strategi ved myk dimensjonering er bruk av offerarealer, der fasaden med et ytre bæresystem er konstruert for å dissipere eksplosjonsenergien gjennom lokale ødeleggelser i buffersonen, slik at indre bæresystem og indre sone med viktige arealer er beskyttet mot eksplosjonsvirkningene. Se ***figur Soneinndeling*** med eksempel på løsning med buffersone mot yttervegg.

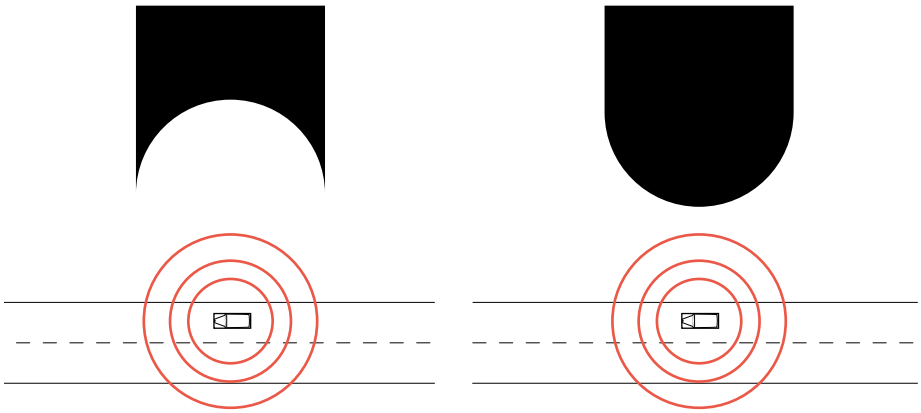
Glass i vindu og fasade

Vanlige vindusglass er sårbare for eksplosjonslaster og vil ved brudd produsere en mengde farlige fragmenter som kan påføre stor skade. Bruk av glass i bygninger bør vurderes nøye.

I nye bygg med sikringskrav må dimensjonering av glassfasader og vinduer gjøres på bakgrunn av en estimert trussel, avstand til trusselen og et akseptert risikonivå.

Funksjonelle krav til fasadens opptreden ved eksplosjonslast bør fastsettes basert på forventet eksponering av personell på innsiden av fasaden. Gangarealer er for eksempel mye mindre frekventert enn oppholdsrom, kontorer og forsamlingsrom, noe som gir ulike krav.

Byggets geometri



Viktig å huske på

- *Det finnes en rekke produkter som er klassifiserte for å motstå både inntrengning, beskytning og eksplosjoner*
- *Det finnes ulike beskyttelsesløsninger for å fange opp vinduer ved innkast*
- *Sett riktige krav til vindu mot eksplosjon, beskytning og innbrudd*
- *Det kan være vanskelig å oppnå tilfredsstillende U-verdi i sikkerhetsglass*

Estetikk

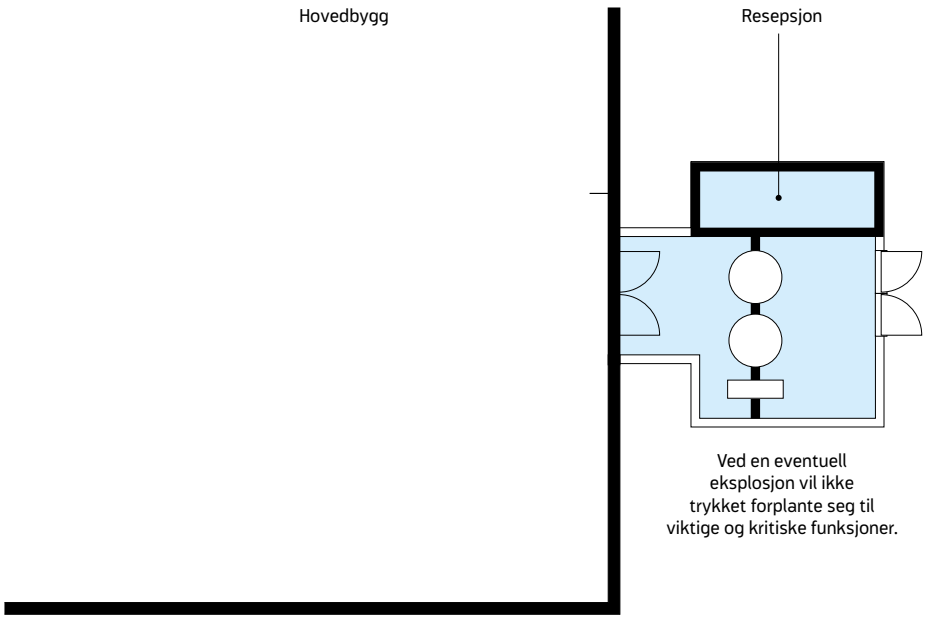
- *Det kan være en utfordring med slanke profiler ved bruk av sikkerhetsvinduer*
- *Det kan ikke være for store vindusfelt i glassfasade, og det må forventes at sprosser må benyttes. Krever spesialprosjektering og beregninger*
- *Ved å benytte jernfattige sikkerhetsglass kan man unngå grønnskjær i glass*
- *Det er mulig å montere innvendig varevindu bak historiske vinduer dersom disse ikke ønskes endret. Dette kan også være en måte å tilfredsstille energikrav på*

Geometri

Byggets geometri kan påvirke skadebildet ved en eventuell eksplosjon.

- *Enkel geometri er mest gunstig*
- *Unngå innvendige hjørner i fasade*
- *Konveks form er mer gunstig enn konkav*
- *Utforming av bygning som ikke skaper økt trykk pga. trykkrefleksjoner*
- *Lite ornamentering, som ved eksplosjonsbelastning kan løsrives og bli skadelige sekundærfragmenter. Eventuelle ornamenter bør lages med lettere materialer, som treverk fremfor mur eller metall*
- *Sprø materialer bør unngås i ytre bygningsskall*
- *En konveks frontvegg kan være et bra tiltak for å redusere eksplosjonslast på fasade*

Resepsjonsområde



Plassering av rom og funksjoner

Rom- og funksjonsplassering i bygg er av stor betydning for hvilket nivå av sikkerhet man klarer å oppnå.

Eksempler på tiltak:

- → *Lave bygg med stort grunnareal sprer folk og verdifulle installasjoner ut over et større areal og reduserer risikoen ved hendelser med utvendige bomber.*
- → *Arealer der folk oppholder seg over tid, slik som møterom, auditorier, kantiner etc. orienteres vekk fra yttervegger som vender mot offentlig tilgjengelige veier og gater. Rom for kortvarig opphold (kopirom, rekvisita, lager, toaletter, tekniske rom og andre støttefunksjoner) kan benyttes som offerarealer*
- → *Unngå overheng og hulrom i fasader, også med tanke på bårne eksplosiver.*
- → *Korridorer mot yttervegger gir buffersone for rom for varig opphold som plasseres lenger inn i bygningen. Naturlig belysning kan likevel oppnås ved at disse rommene plasseres mot sikrede områder som f.eks. atriumsløsninger.*
- → *Unngå parkering i eller under bygningen.*
- → *Varemottak, postmottak og områder for mottak av gjester kan med fordel planlegges som egne konstruksjoner, slik at eventuelle eksplosjoner her ikke får store skadelige konsekvenser for resten av bygget. Se **kapittel 21, Post- og varemottak** for mer informasjon.*
- → *Mot andre trusler, som inntrengning, vil i tillegg soneprinsippet gjelde, se **kapittel 2, Sikringsteori.***

Dersom resepsjon inkorporeres i bygg, kan et stort volum være et lastreduserende grep for

å absorbere en del trykk ved innvendig eksplosjon. Man må merke seg av vinduer og glassflater da vil blåses ut, og således representere en annen fare enn om det var prosjektert for å stå mot en utvendig eksplosjon.

Tekniske installasjoner
Det vil ofte være krav til sikring av tekniske installasjoner. Dette gjelder for eksempel krafttilførsel, ventilasjonsanlegg og IKT-installasjoner. I tillegg er det ofte behov for redundante installasjoner, dvs. at man har to tilsvarende anlegg som driftes parallelt for å gi ønsket driftssikkerhet. En naturlig konsekvens av dette er et økt arealbehov for tekniske installasjoner, på grunn av lengre føringsveier og større sjaktarealer.

Interiør
Innvendig materialbruk har stor betydning for nivået av sikkerhet. Dette gjelder spesielt for himlinger. Disse kan gjøre stor skade ved en eventuell eksplosjon dersom valgt løsning er løse plater som faller ned pga. svak innfesting.

Forsterking av eksisterende bygg

Ved rehabilitering eller ved akutte behov som følge av et endret trusselbilde, kan eksisterende bygninger forsterkes for å tåle større eksplosjonslaster. Dette vil normalt sett være svært kostbart og krevende med varierende effekt.

Dersom hele fasaden må forsterkes, blir det ofte et spørsmål om å bytte vinduer og forsterke yttervegg. Nye vinduer betyr også nye karmer og forsterking av innfesting i vegg. Selve fasadesjiktet der dette er mulig, kan forsterkes ved å bygge en ekstra vegg av stålprofiler eller korrugerte stålplater på innsiden. Denne forankres i gulvdekkene og kles deretter med innvendige bygningsplater. Vinduer kan forsterkes gjennom påmontering av fragmenthindrende film. Dette vil bidra til å redusere fragmentmengden, men vil raskt innebære at hele vindusflaten utgjør en trussel når den kastes inn ved eksplosjon. Et hurtig tiltak som også er relativt billig, er å utruste vinduene med fragmentgardiner. Disse hindrer utsyn da de må henge ned foran vinduene for å være effektive. Disse gardinene fanger opp fragmenter fra glasset og hindrer at de kastes inn i rommet. Se avsnitt om glass og fasader vedrørende bruk av varevindu ved forsterkning av bygg med historisk verdi/antikvariske restriksjoner.

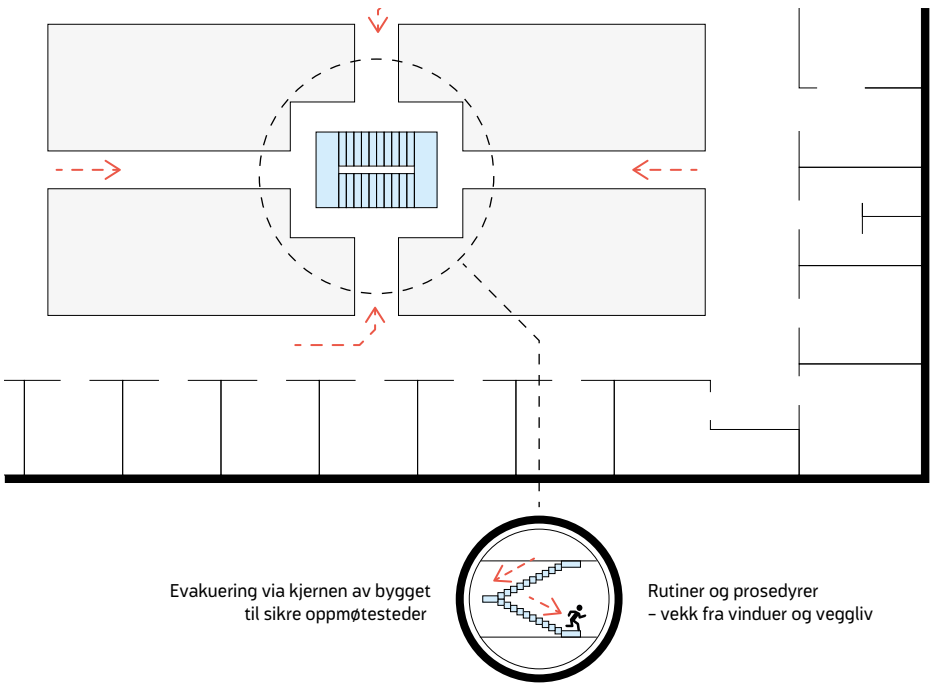
Når sikringstiltak tilføres en eksisterende bygningsmasse, er muligheten for å utforme de grunnleggende sikringsstrategiene begrenset. Hovedutfordringen i slike situasjoner er også ofte å fremskaffe oppdatert tegningsmateriale, og det er viktig å danne seg et beslutningsgrunnlag basert på korrekt dokumentasjon av de gitte forutsetningene. Gamle tegninger av bygget kan være mangelfulle og tidligere rehabiliteringer kan skjule både mulige styrker og svakheter i konstruksjonen. Grundige registreringer og befaringer vil derfor være nødvendig.

Rømning

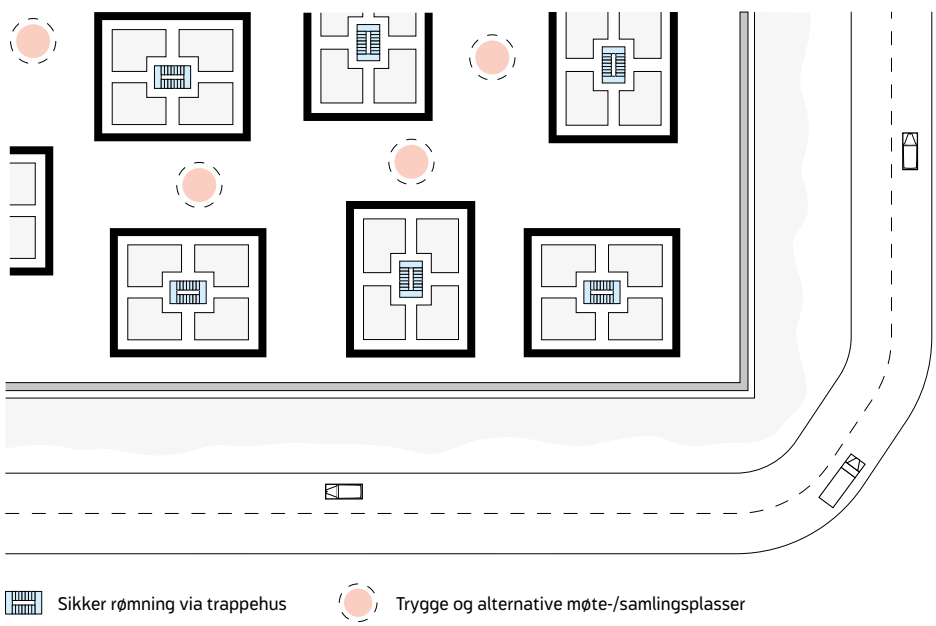
Utover offentlige krav til brannsikkerhet av bygninger, skal alle virksomheter ha et system for varsling og evakuering. Ved en akutt situasjon skal personell få hurtig varsling for så å evakuere gjennom sikre rømningsveier.

I et sikringsperspektiv er rømningsveiene ofte forsterkede kjerner. Disse bør ikke plasseres mot yttervegg, men heller ligge sentralt i byggene. Samlingsplassene skal være trygge og ueksponerte, og de bør være flere i antall for å kunne variere oppmøtested for å unngå fataliteter ved et eventuelt målrettet sekundæranslag. Personell skal til enhver tid vite hvordan de skal forholde seg i en krisesituasjon for å unngå tap av menneskeliv. Se for øvrig ***kapittel 3, Sikkerhetskultur.***

Sikker rømning



Trygge og alternative samlingsplasser



Kapittel 10

Perimeter- og områdesikring

Dette kapitlet omhandler sikring av utendørsareal ved hjelp av blant annet personellhinder (gjerder), kjøretøysperrer og -hinder, deteksjons- og verifikasjonssystemer, tilhørende adkomstområder, samt sikring av områdene innenfor.

Perimeter- og områdesikring spiller en viktig rolle i beskyttelsen av bygg, anlegg, installasjoner eller en leir. I tillegg til å fungere som en klar administrativ og juridisk grense mot omverdenen kan perimetersikringen bidra til å skape sikring i dybden. Slik sikring vil som oftest være både hensiktsmessig og kosteffektiv, og innebærer at det etableres flere lag av fysiske barrierer og deteksjonssoner rundt verdiene som skal sikres. Ved sikring i dybden vil perimeter- og områdesikringen utgjøre de første lagene med barrierer som en trusselaktør må forsere for å ta seg inn til verdiene. En godt utformet perimeter- og områdesikring vil derfor kunne bidra til å vinne tid og samtidig skape forutsetninger for egne, aktive mottiltak. Det er imidlertid viktig å være oppmerksom på at fysiske sikringstiltak i perimeteret ofte har en svært begrenset tidsforsinkende effekt for en kompetent angriper.

Elektroniske sikringstiltak i perimeteret for å detektere og verifisere et angrep, og avslutningsvis et reaksjonsapparat som kan avverge angrepet, er derfor viktig.[1]

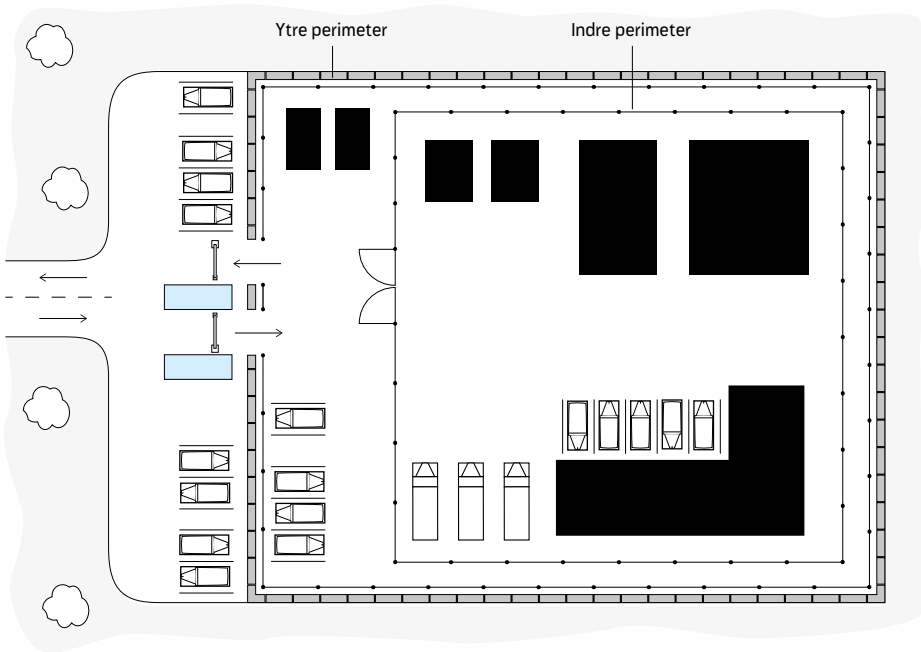
Dersom det er mulig, bør man forsøke å etablere avstand, se ***figuren Perimeter- og områdesikring***, mellom den ytre perimeteret og den eller de verdier som man ønsker å sikre. Ved å etablere avstand kan man oppnå at inntrengeren blir eksponert over et større område, over lengre tid, og det kan være langt enklere å gjøre en sikker verifisering i motsetning til de anlegg der ytre og indre perimeter ligger så tett at en inntrenger kan bevege seg delvis skjult og forsere raskt mellom perimetrene.

Det mest vanlige er å etablere ytre perimeter i tilknytning til eiendomsgrensen, slik at perimeteret markerer tydelig hvor den juridiske grensen går. Det kan være kostbart å etablere et perimeter langs en stor eiendomsgrense, og i mange tilfeller vil det ikke være nødvendig dersom verdiene som skal sikres, er konsentrert innenfor et avgrenset område på eiendommen. I så fall kan det være mer hensiktsmessig å komme frem til en form for avgrensning i en fornuftig avstand i forhold til verdiene. Dersom det skal etableres kjøretøysperrer og kjøretøyhindre for å unngå at uautoriserte kjøretøy slipper inn på eiendommen, vil dette ha konsekvenser for hvor perimetersikringen bør plasseres.

Hvilke sikringstiltak perimetersikringen skal omfatte, vil være en konsekvens av hvilke trusler man står overfor, hvilket reaksjonsapparat som er tilgjengelig, og hvilken reaksjonstid

1
Elektroniske sikringstiltak beskrives i et eget kapittel og blir kun overordnet beskrevet her der det er relevant

Perimeter- og områdesikring



som må beregnes. Det kan være ett eller flere elementer, som f.eks. gjerde, utforming av inn- og utpasseringsområder, sensor- og alarmsystemer, adgangskontroll, kameraovervåkning, belysning, kjøretøyhinder. De fleste av disse elementene er beskrevet nærmere i egne avsnitt i dette kapitlet.

Gjerder og murer

Gjerder og murer vil først og fremst bidra til å signalisere et sikkerhetspreg. Gjerder holder normalt kun ærlige individer ute og er derfor best egnet til å markere en juridisk grense, med mindre det dimensjoneres mot forsering. Murer kan i tillegg til å markere hvor eiendommens grenser går, også gi noe beskyttelse og vil i mange tilfeller være et mer utfordrende hinder å forsere enn et flettverksgjerde.

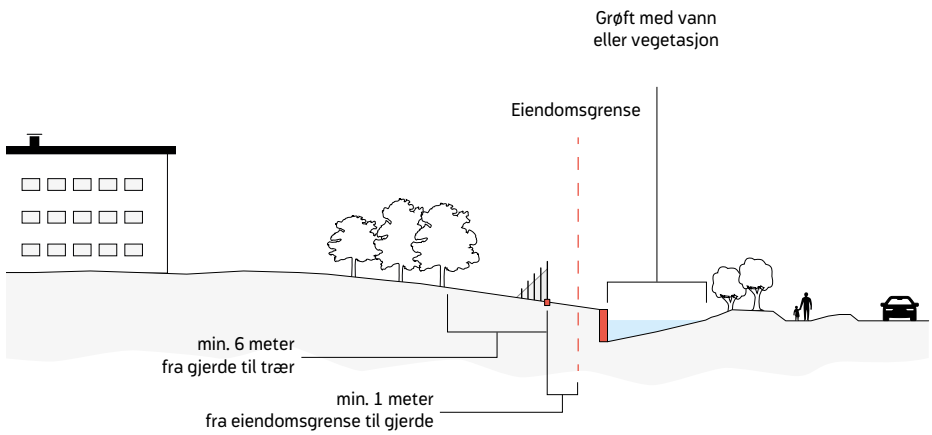
Gjerder og murer vil også ha andre fordeler i tilknytning til den øvrige beskyttelsen av anlegget, fordi de blant annet:

- → *gjør det mulig med bruk av alarmsystemer i tilknytning til perimeteret*
- → *beskytter vaktpersonell mot overraskelsesangrep*
- → *kan fungere som en barriere mot kjøretøy*
- → *gjør det mulig med bruk av vakthunder*
- → *hindrer innsyn*
- → *murer kan gi en effekt ved en eksplosjon ved at fragmenter kan stoppes*

Utforming og kvalitet

Gjerdets utforming og kvalitet gir et signal om hvilken prioritet sikring har på det aktuelle objektet gjerdet omgir. Gjerder og murer vil i de aller fleste tilfeller kun utgjøre en tidsfor-

Avstander gjerde/eiendomsgrenser



sinkelse for en inntrenger. Generelt kan man si at høyden på gjerdet, maskestørrelsen og materialdimensjonene i sum gjør det mer eller mindre vanskelig å ta seg over eller å klippe seg gjennom gjerdet.

Med god tilgang på batteri- eller motordrevne verktøy kan det være enkelt å skjære seg gjennom de fleste typer av gjerder. Et perimeterbarriere som har til formål å forsinke eller avskrekke en inntrenger, bør derfor kombinere gjerde (eller mur) med sikkerhetsbelysning eller elektronisk overvåkning m.m. som for eksempel alarmsensorer (AIA) og kameraovervåkning (TVO). Sjansen for å bli oppdaget vil være stor, og terskelen for å ta seg forbi perimeteret blir følgelig høyere.

Forsterkning av gjerder og murer med piggtråd eller lignende produkter vil gjøre det vanskeligere å klatre over gjerdet. Vanligvis benyttes tre-tråds piggtråd på gjerder, men det finnes også andre produkter til dette formålet. Et sveiset stålgjerde vil bedre kunne motstå gjennomtrengning og forsering, avhengig av maskestørrelsen på nettet, samt dimensjonen og kvaliteten på de enkelte delene av gjerdet. Et høysikkerhets gjerdesystem, bestående av et dobbelt gjerde med et deteksjons- og overvåkningssystem, vil kunne representere en vesentlig hindring for en inntrenger.

Gjerdet må plasseres og monteres i forhold til terrenget slik at det ikke er mulig å krype under gjerdet, og bør ikke plasseres på eiendomsgrensen, men heller trekkes minst en meter inn på tomten. Gjerdelinjen bør inspiseres regelmessig.

Ved planlegging av gjerder gjelder plan: og bygningsloven og lov om nabogjerder, i tillegg til forskrifter, som i hovedsak regulerer gjerdesaker.

Sikringsklasser gjerder

Sikringsklasse	Beskrivelse/krav
1	→ Et hvilket som helst gjerde. → Ingen krav til materialer eller utforming. → Angir visuelt og juridisk en eiendomsgrense. → Har kun en regulerende effekt – ingen tidshindrende effekt.
2	→ Et tradisjonelt flettverksgjerde montert på T-jern som er slått ned i bakken. → Gjerdehøyden skal være minimum 2 meter. → Stolpeavstand maks 2,5 meter. Trådtykkelse min. 2,5 mm. Maskestørrelse maks. 50x50 mm. Min. hver 3. stolpe settes i betong. → Bør forsterkes med tre eller flere piggtrådrader på toppen, kan forsterkes med kveilehindre m.m. → Gjerdet har i hovedsak en regulerende effekt.
3	→ Sikkerhetsgjerde, minimum 2,5 meter høyt. → Gjerdet bør være testet etter en innbruddsstandard, f.eks. den britiske LPS 1175. → Løsningen bør vurderes av spesialist i forhold til trusselen. Vanligvis sveiset gittergjerde, panelgjerder eller sveiset palisandergjerde med hensiktsmessig maskestørrelse, spiletykkelse og -avstand. → Kan forsterkes med piggtrådrader på toppen, kveilehindre m.m.
4	→ Et dobbelt gjerde med minimum et klasse 2-gjerde som ytterste gjerde, og et klasse 3-gjerde som innerste gjerde. → Mellom gjerdene bør det være et deteksjons- og overvåkningssystem. → Begge gjerdene bør utstyres med minst tre rader piggtråd på toppen.

Ved montering av gjerder med piggtråd bør man følge lokale bestemmelser i tiknytning til eventuell gjerdelov.

Planlegging av gjerde

Før man bestemmer seg for hva slags type gjerde som skal settes opp og hvor det skal stå, bør man ha klart for seg hva en ønsker å oppnå:

- → *Er det en generell juridisk eiendoms-markering, eller skal det forhindre noen å passere?*
- → *Hvem ønsker man i så fall at det skal forhindre/forsinke?*
- → *Skal perimeteret integreres med noen form av alarmsensorer?*
- → *Skal gjerdet være til hinder for at gjenstander kan kastes inn på det sikrede området?*
- → *Skal det kunne observeres fra ett eller flere steder innenfor sikret område?*
- → *Skal perimeteret hindre innsyn?*

Dersom et elektronisk deteksjonssystem skal benyttes i forbindelse med gjerdet, kan det være ulike forhold som kan være avgjørende for valg av deteksjonssystem.

Gjerdet kan fungere som bærer for visse typer deteksjonssystemer, men det mest vanlige er at alarm legges innenfor gjerdet. Rent generelt er det ikke å anbefale at man benytter gjerde-

Skilt

stolpene til å feste kamera, belysning eller deteksjonssensorer. Om mulig bør det settes av plass med tanke på å etablere en egen sikringssone på innsiden. I sikringssonen kan det være patruljevei, deteksjonssystem, kameraovervåkning, belysning og lignende.

Det er viktig å være bevisst på mulig skadeverk i forbindelse med at det kastes gjenstander, brannbomber eller eventuelle sprenglegemer over gjerdet.

Skilting

I forbindelse med perimetersikring bør det brukes skilt som beskriver restriksjoner i området.

De fleste vil oppfatte at et gjerde er et hinder som ikke uten videre skal forseres, men ved å benytte skilt forsterkes det strafferettslige vernet. Skiltene bør derfor monteres både ved inngangsportene og langs gjerdet slik at det ikke senere kan reises tvil om at ferdsel på inngjerdet område, parkering inntil gjerdet og bruk av film-/fotoutstyr er uønsket.

Skilt bør tekstes på både norsk og engelsk.

Benyttes det tv-overvåkning for sikring av perimeteret skal dette angis ved egne skilt iht. kravene fra Datatilsynet.

Inn- og utpasseringsområde (adkomstområdet)

Inn- og utpassering vil i de fleste tilfeller utgjøre den mest sårbare delen av perimetersikringen. For så vel militære som sivile installasjoner ser vi i økende grad at det tas i bruk systemer for å avsøke både kjøretøy og personer. Det utføres id-sjekk og i mange tilfeller autoriseres besøkende etter spesielle prosedyrer. For enkelte installasjoner har man også tatt i bruk egne løsninger for post- og varemottak, og det benyttes ofte særskilt trenede, uniformerte personer til å ivareta sikkerheten i selve adkomstsonen. Les mer om ***post- og varemottak i kapittel 21.***

For å oppnå en løsning som kan fungere under ulike trusselnivåer, bør selve adkomstområdet planlegges slik at man ved relativt enkle grep kan endre kjøremønster, skille gående og kjørende, kunne avvise kjøretøy uten at det skaper trafikale problemer, og samtidig ta hensyn til at man skal kunne oppbemanne adkomstsonen dersom de sikkerhetsmessige forhold tilsier dette.

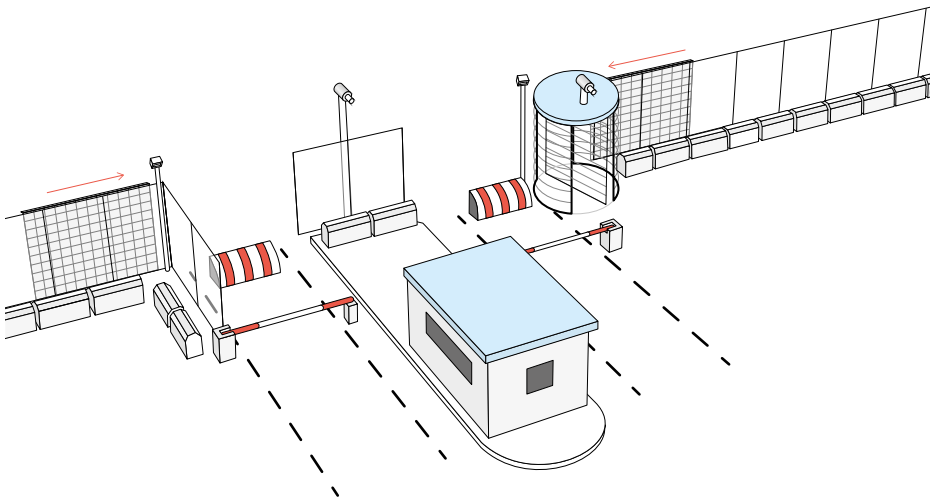
Sikringsløsninger i forbindelse med inn-/og utpasseringsområdet til en virksomhet er i mange tilfeller omfattende og kompliserte, og bør derfor planlegges for å kunne ivareta ulike situasjoner. Det anbefales at bruker(e) setter

opp en detaljert kravspesifikasjon hvor funksjonaliteten til det totale adkomstsystemet beskrives, og det vil være en fordel for både bruker, vaktmannskap/selskap og entreprenør at man forsøker å ivareta alt fra de enkle nedskalerte brukerkravene som vil gjelde under rolige, normale forhold, til de mest ekstreme trusselsituasjoner som adkomstområdet er ment å kunne håndtere.

Følgende forhold bør tas i betraktning:

- → *Hva skal inn-/utpasseringsområdet omfatte, og hva med sekundære løsninger til hovedadkomsten?*
- → *Hvilke ulike nivå på sikring ønskes i forbindelse med innpassering av personell til fots og kjøretøy (inkludert sykler)?*
- → *Hvilket sikkerhetspreg ønsker man å uttrykke?*
  - *Både design og materialvalg har stor betydning for hvilket sikkerhetspreg både perimeteret og adkomstsystemet etterlater seg. Planlegges tiltakene for både normalsituasjon og for økt beredskap godt fra starten av, så kan man i stor grad skjule og bygge inn sikkerhet i de ulike løsningene man velger. Tiltak som må gjennomføres som «hastetiltak», vil gjerne gi et mye kraftigere og mer «uniformert» inntrykk enn tilsvarende løsninger ville gjort dersom de var planlagt i god tid.*
- → *Skal gående og kjøretøy sjekkes, hvilke sjekkrutiner skal benyttes, og hva skal eventuelt iverksettes dersom man under en kontroll enten har mistanke om eller kan verifisere funn av f.eks. en eksplosivladning?*
  - *Ved forhøyning av beredskapsnivået kan det være ønskelig å skille mellom gående og kjørende, tunge vs. lette kjøretøy, da kontrollrutinene kan være svært forskjellige for disse kjøretøygruppene.*
  - *Det kan være flere fordeler ved å skille mellom inn- og utgående trafikk, skille mellom inn- og utpassering av personer og legge til rette for sjekkrutiner av alle innpasserende på et sikkert sted.*
  - *Systemer for at gjester trygt kan legge igjen/deponere mobil- og kommunikasjonsutstyr som ikke er autorisert til bruk i anlegget.*
- → *Hvor mange kjøretøy eller personell skal normalt passere inn og ut, og over hvilke tidsrom?*
- → *Hvilke typer kjøretøy dreier det seg om?*
- → *Er det muligheter for å etablere en sikker, utvendig parkering for å redusere antall kjøretøy under et forhøyet beredskapsnivå?*
- → *Er det muligheter for å legge til rette for håndtering av ulike forsyninger som f.eks. post, pakker, vann, drivstoff, renovasjon og annet uten at man må bringe større kjøretøy inn i anlegget?*
- → *Hvilke fysiske muligheter og begrensninger finnes på det stedet adkomsten ønskes plassert?*
- → *HMS-forhold: Skilting, belysning, betjening og praktiske løsninger som må ivaretas for å unngå mulig skade på personer, men også for å sikre en effektiv avvikling av alle typer bevegelse igjennom adkomstsonen.*
- → *Forhold vedrørende drifts- og vedlikehold må analyseres opp mot valget av utstyr, materiell og ulike løsninger. Hva er akseptabel nedetid for ulike funksjoner, hvilke krav settes til feilretting, skal man ha alternative løsninger som settes i drift ved tekniske feil, utforming av serviceavtaler og responstider, klimatiske forhold (snørydding, is, m.m.), lysforhold, behov for lokal lagring av slitedeler, kritiske deler m.m.*

Bommer, kjøretøysperrer og porter



Gjerder

Gjerder som overstiger 1,5 meter høyde, må byggemeldes. Konferer alltid med lokale bygningsmyndigheter om hva som gjelder av lover og regler.

For at man enklere skal kunne ha kontroll på perimeteret rundt eiendommen, bør gjerdet plasseres minimum 1 meter inn på egen tomt.

Unngå at det lagres elementer langs utsiden av gjerdet som kan gi mulighet for å klatre inn.

Vegetasjon i sonen på utsiden av gjerdet skal holdes nede, da den kan forhindre eller vanskeliggjør inspeksjon, i tillegg til å være et potensielt hjelpemiddel for å klatre inn.

Det anbefales en sone på minimum 6 meter innenfor gjerdet. Denne skal vær fri for bygninger, lagring, parkering, vegetasjon, m.m. Dette område kan benyttes til deteksjonssone, patruljering og eventuelle beredskapstiltak.

Ved å gå ned på maskestørrelsen vil det bli vanskeligere å klatre og klippe i. Dette er først og fremst aktuelt når det gjelder sveisede stålgjerder.

Et gjerde med tilstøtende område må vedlikeholdes. Skader på gjerdet bør utbedres så snart som mulig.

Porter, grinder og bommer

I adkomstpartiet vil det være nødvendig med porter og bommer for å kunne etablere inn- og utpasseringsmuligheter for personell og kjøretøy. Portene må utformes slik at de representerer en minst like stor tidsmessig hindring for en trusselaktør som hva gjerdet eller muren som portene står i, gjør.

I tillegg er det også andre krav til porter. De skal kunne åpnes og lukkes for å slippe inn autorisert trafikk og personell på en tilfredsstillende måte, og det vil i mange tilfeller stilles spesielle krav til materialvalg og utforming. Portene

Høye rotasjonsporter

med kortleser, callinganlegg og kameraovervåkning

må utformes slik at det ikke er mulig å krype under dem.

Låsmekanismen for porter velges ut fra en vurdering av portens styrke, slik at et angrep på låsmekanismen medfører et minst tilsvarende tidstap for en innbryter som et angrep på selve porten. Ved bruk av hengelås bør minimum FG klasse 3 benyttes.

Portløsninger

Portene er enten mekaniske og åpnes og lukkes manuelt, eller de er motoriserte. Motoriserte porter gir mulighet til fjernstyring av portene. En slik styring kan for eksempel være åpning med et automatisk adgangskontrollsystem (AAK), en tidsstyring, radiostyring slik vi kjenner fra garasjeport-åpnere eller en åpne- og lukkeimpuls fra et panel. Motoriserte porter har en rekke feilmuligheter (teknisk feil, strømstans, påkjørsel, m.m.) som kan medføre at porten ikke er operativ. Planer for å håndtere dette må utarbeides.

Alle porter skal tilfredsstille maskinforskriften, som sier hva som kreves av klemsikringer, styringer og sikkerhetsinstallasjoner, for at portene ikke skal gjøre skade på personell og materiell.

Fjernstyrte porter utstyres ofte med magnetsløyfer i bakken for automatisk åpning av porter/bommer ved utpassering av kjøretøy. Det kan være enkelt å manipulere slike løsninger for å oppnå adgang utenifra. Magnetsløyfer med automatisk åpning bør derfor ikke benyttes sammen med høysikkerhetsløsninger.

Det finnes et stort utvalg av forskjellige porttyper og -utførelser. Følgende typer er de vanligste:

- → *Slagporter (personell og kjøretøy, kan være både én- og to-fløyede)*
- → *Skyveporter (større åpninger, kjøretøy etc., er som regel én-fløyede)*
- → *Rotasjonsporter (personell)*

SÅRBARHETER

Kan man omgå sikringstiltakene eller utnytte mangel i sikringen? For eksempel passere inn sammen med autorisert person/kjøretøy?

Kan man lure seg inn ved forskjellige former for social engeneering?

Kan man true seg til adgang? Enten ved trusler mot vaktpersonellet eller true personell med legitim adgang til å gi adgang?

Kan verdiene trues fra yttersiden av perimetersikringen? Eksempel: bilbombe ved ytre perimeter, beskytning, innsyn, avlytting, kartlegging av rutiner.

Kan man trenge gjennom sikringstiltakene?

Utvendige rotasjonsporter

Rotasjonsporter benyttes for å kunne føre kontroll med inn- og utpassering av personell. Ved høysikkerhetsløsninger benyttes gjerne dette i inn- og utpasseringsområdet.

Utvendig benyttes rotasjonsporter oftest som en del av perimetersikringen, enten sammen med en kjøreport i hovedporten, eller som sekundær adkomst i forbindelse med en gangvei fra en parkeringsplass eller lignende. Gjerdet ved rotasjonsporten bør ha en utforming som gjenspeiler portens utforming og kvalitet. En utvendig rotasjonsport signaliserer et sterkt og tydelig sikkerhetspreg. Fordi portene ofte står utsatt for vær og vind, bør de ha tak, lys og gjerne varmekabler i fundamentet.

Rotasjonsportene styres normalt av kortlesere, som integreres i portløsningen. For kommunikasjon med en resepsjon eller vakt bør utvendige porter ha en porttelefon kombinert med kameraovervåkning. Dette gjør at en vakt kan kommunisere med eventuelle besøkende, egne ansatte som har glemt sitt adgangskort, eller ikke får kortet til å virke og så videre, slik at porten eventuelt kan fjernåpnes.

Portene krever en relativt kraftig fundamentering, og til denne må det fremlegges kabler for elkraft og signalkabler for styring, adgangskontroll, kameraovervåkning, porttelefon og lignende.

Materialvalg og overflatebehandling er viktig for portens funksjon. Portene kan leveres i en rekke utførelser. Den mest robuste utførelsen vil være i varmgalvanisert stål, men andre utførelser kan være aktuelle basert på krav til design. Porten må kunne tåle de miljømessige forhold den blir utsatt for, og skal fortrinnsvis fremstå med en design som passer til omgivelsene.

Ved etablering av ulike portløsninger bør det vurderes å etablere en serviceavtale med leverandøren slik at man har en garanti for at porten vil beholde sine funksjonelle og driftsmessige egenskaper, herunder utseende, ved bruk over lengre tid (5–10 år), basert på de lokale miljø- og driftsforhold.

Bommer

Bommer kan være manuelle eller motordrevet, og benyttes vanligvis til å regulere kjøretøytrafikk inn til et område. Bommer har ingen tidshindrende effekt når det gjelder personell til fots, og må derfor overvåkes dersom man ønsker å unngå uautorisert innpassering.

Bommer benyttes oftest i tillegg til porter. Til tider hvor det er stor trafikk av kjøretøy, kan for eksempel en skyveport settes i åpen stilling, mens kjøretøy stanses av en bom for kontroll.

Bommer leveres i mange utførelser, med forskjellige drivmekanismer og forskjellige armlengder. Bommer som benyttes som kjøretøysperre, må ha den nødvendige styrke i forhold til de kjøretøy den er ment å kunne stoppe. For kjøretøysperrer av denne typen vil riktig plassering og innfesting være helt avgjørende. I sammenheng med at det etableres kjøretøysperre(r), kan det også være behov for å etablere en sjikane/et innkjøringsmønster som vil bidra til å redusere hastigheten på kjøretøyene før de kommer frem til bom/kjøretøysperre.

Både bommer og porter er svært utsatt for påkjørsler. Dette kan medføre skader, driftsstans og ventetid for nødvendige reparasjoner. Ved etablering av bommer, porter og kjøretøysperrer bør det vurderes om det kan være behov for et lokalt lager av enkelte slitedeler eller deler som kan være kritiske for operasjonell drift.

Sikringsklasser elektronisk perimetersikring

Sikringsklasse	Beskrivelse/krav
1	→ System som varsler brudd på perimeteret → Skal kunne indikere hvor/hvilken sone det er foretatt uautorisert adgang → Lokal monitorering
2	→ System som varsler brudd på perimeteret → Skal kunne indikere hvor/hvilken sone det er foretatt uautorisert adgang → Lokal monitorering → Har mulighet for overføring til vakt/alarmstasjon
3	→ System som varsler brudd på perimeteret → Skal kunne indikere hvor/hvilken sone det er foretatt uautorisert adgang → Lokal monitorering → Har mulighet for overføring til vakt/alarmstasjon → Skal kunne samhandle med AIA- og AAK-anlegg → TVO-verifikasjon → Alle sentralkomponenter skal være tilkoplet UPS
4	→ System som varsler brudd på perimeteret → Skal kunne indikere hvor/hvilken sone det er foretatt uautorisert adgang → Minimum to forskjellige teknologier på perimeteret → Lokal monitorering → Har mulighet for overføring til vakt/alarmstasjon → Skal kunne samhandle med AIA- og AAK-anlegg → TVO-verifikasjon → Har billedoverføring til godkjent alarmstasjon ved alarmsituasjon eller på kommando, som kan lagre video → Skal ha mekanismer som kan hindre en avansert trusselaktør i å sabotere anlegget (krav til plassering av komponenter, skjerming av kabler, etc.) → Alle komponenter skal være tilkoplet nødstrøm og UPS

Lokale for portvakt

Selv om behovet for bemanning i selve adkomstsonen er begrenset, bør man vurdere å etablere et vaktlokale som kan benyttes i en situasjon der man ønsker å høyne beredskapen.

Lokalet for vakten bør planlegges som en integrert del av inn- og utkjøringsområdet til anlegget, og vil kunne fylle flere funksjoner som blant annet:

→ *Vær- og klimabeskyttelse for vaktpersonell*
→ *Dekningsrom*
→ *Inspeksjonsareal for personell*

Benyttes det en egen hovedvaktstyrke (utrykningsstyrken), bør denne ikke forlegges i inn- og utpasseringsområdet. Ved nyetableringer skal hovedvaktstyrken plasseres inne i anlegget og ikke med direkte tilknytning til ytre perimeter.

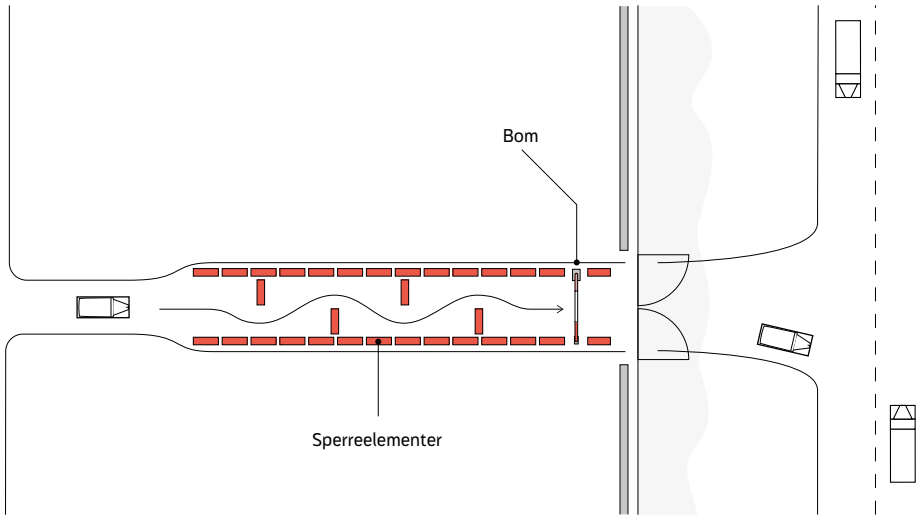
For mer utførlig beskrivelse av vaktfunksjoner og utforming av vaktlokaler, vises det til ***kapittel 13, Vakthold og reaksjonstiltak.***

ADKOMST-OMRÅDE

For å oppnå en løsning som kan fungere under ulike trusselnivåer, bør selve adkomstområdet planlegges slik at man ved relativt enkle grep kan endre kjøremønster, skille gående og kjørende og kunne avvise kjøretøy uten at det skaper trafikale problemer.

Etablering av sperringer (eksempel)

Innkjøring til en virksomhet



Elektronisk perimetersikring

Siden gjerder i begrenset grad vil utgjøre en hindring for en målbevisst og kompetent trusselaktør, anbefales det at hvor anlegget har behov for spesielle sikringsbehov, bør det vurderes å benytte spesialisert deteksjonsutstyr ved den ytre perimeteret, samt effektiv bruk av belysning og overvåkning av både den ytre perimeteret og området innenfor.

Det finnes en rekke ulike systemer, og svært mange er utviklet i og produsert for bruk i land med en helt annen geografi og klima enn det vi har i Norge. Bruk av systemer som ikke takler de lokale forhold, vil kunne forårsake mange unødige feilalarmer, eller i noen tilfeller ikke gi korrekt varsel. Kun et mindre antall av tilgjengelige systemer er tilpasset bruk i våre klimatiske forhold.

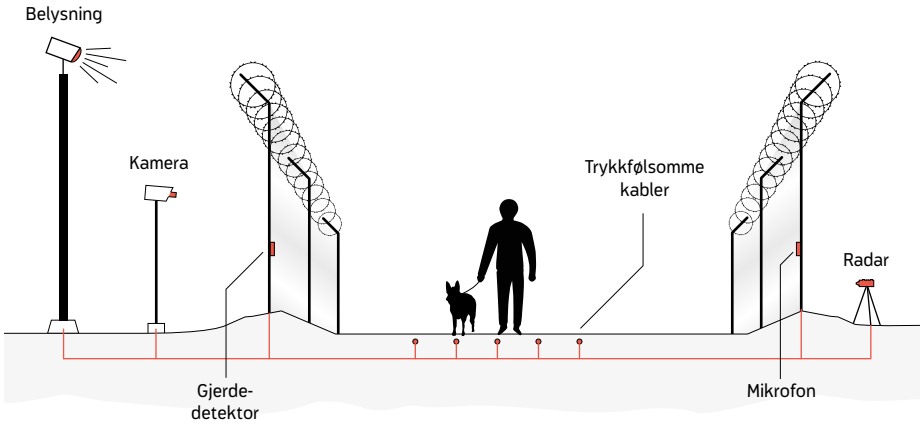
Perimetersikringssystemer består som regel av ulike typer systemer, men uavhengig av teknologi er det en del fellesnevnere mellom dem. Sikringssystemer for perimetersikring bør være sonebasert. Dette gir muligheter for raskt å kunne verifisere hendelsen og sikre korrekt reaksjon. Dekker perimetersikringen et større område, vil grafisk presentasjon og integrasjon med TVO-system være en viktig faktor for å få et fungerende varslingssystem.

Deteksjonssystemer kan bestå av følgende hoveddeler:

Selve deteksjonssystemet kan være enkeltvis eller kombinasjon av f.eks. kamera, linjedetektorer, radar, lekkasjekabel, trykk-kabel, geodetektor/-mikrofon, gjerdedeteksjon, mikrofon og lys, mikrobølgedetektor, seismisk detektor, PIR-detektor, kombinert detektor (f.eks. mikrobølge og PIR) i tillegg til belysning.

I ***kapittel 12, Elektronisk sikring*** vil de ulike deteksjons-, alarm- og overvåkningssystemene beskrives mer utførlig.

Elektronisk perimetersikring



Skissen viser flere ulike sensorer og teknikker som kan anvendes ved etablering av perimetersikring. Tiltakene må planlegges og prosjekteres særskilt.

Sikkerhetsbelysning

Sikkerhetsbelysning kan være en viktig del av sikringen, men kan også hjelpe en angriper hvis det brukes feil.

Ideelt sett skal sikkerhetsbelysningen:

- *Hindre inntrenging ved å skape en følelse av usikkerhet, eller i det minste redusere en inntrengers handlefrihet*
- *Medvirke til oppdagelse av en inntrenger enten ved direkte syn eller ved TVO*
- *Unngå skygger som kan gi en angriper skjul*

I tillegg kan man trenge lys for å:

- *Skjule vaktposter*
- *Assistere ved visuelle observasjoner*
- *Støtte andre deteksjonssystemer, som TVO*

Hensikten med sikkerhetsbelysning er at observasjon/overvåkning av forhåndsdefinerte områder skal være mulig. Det er nødvendig med kunstig belysning i de perioder av døgnet eller årstider når det ikke er nok naturlig lys. Type belysning og plassering av lyset i forhold til hva som skal observeres, er viktig. Feil type belysning eller plassering kan virke mot sin hensikt. Det finnes mange forskjellige typer lyskilder, armaturer og avskjerminger. Disse må velges for det enkelte formål og tilpasses bruksmåter og omgivelser.

Planlegging

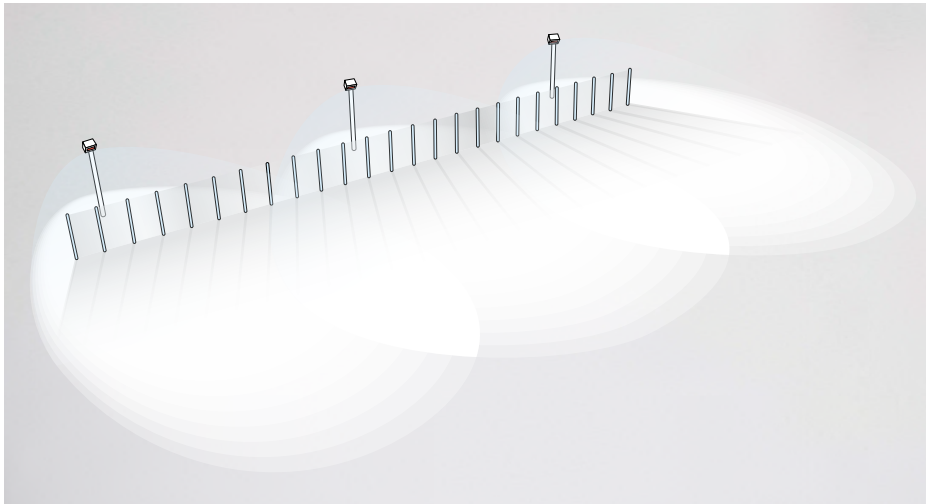
I byggeprosjekter er belysning som regel en del av elektrokonsulentens/-leverandørens ansvar. Brukere bør i samarbeid med sikkerhetsrådgiver spesifisere hva som ønskes oppnådd med belysningen, herunder:

- *hva som skal overvåkes*
- *hvilke belysningsplaner ønskes*
- *når (hele eller deler av døgnet)*
- *skal det samspille med TVO-kameraer og annet deteksjonsutstyr*
- *hvordan skal lyset styres av/på*
- *andre viktige faktorer som kan spille inn, er f.eks. regn, snø, tåke, vegetasjon, vind etc.*

Definisjoner og begreper

Definisjoner og begreper som går igjen i belysningsmiljøene:

Sikkerhetsbelysning



Overlapping ved plassering av lyskastere hindrer blindsoner

- *Lamper = «lyspære» (dagligtale)*
- *Armatur = selve lyskasteren*
- *Lyskilde = lampe og armatur utgjør en lyskilde*
- *Lumen = lampens lysytelse*
- *Candela = intensiteten fra en lyskilde innenfor en gitt romvinkel*
- *Lux = lumen/m² (lysstyrke)*

Det elektromagnetiske spekteret dekker grovt sett radiobølger i den ene enden, til gammastråling (radioaktivt) i den andre. Det synlige lysspekteret går fra 400 nanometer (blått lys) til 700 nanometer (rødt lys). Spekteret ligger mellom ultrafiolett (UV) og infrarødt (IR), der brytningsindeksen er høyere for UV enn for IR. Dette betyr at lys med mye blått i seg, bryter mest når det f.eks. møter vannpartikler i form av regn og tåke. IR-lys trenger lenger gjennom disse værfenomenene. Natrium høytrykklamper har relativt lite blått lys, og fungerer derfor relativt godt i regn og tåke.

Lamper

Det finnes en rekke ulike typer lamper med forskjellige egenskaper, og dermed muligheter og begrensninger i forhold til hva de bør/kan brukes til.

Valg av lamper og detaljløsninger bør overlates til spesialister, som også benytter forskjellige tekniske hjelpemidler for å beregne lysbehovet. Noen grunnleggende tekniske forhold bør man allikevel være klar over:

- *Noen typer lamper lyser maksimalt med en gang, eller meget raskt, mens andre må varmes opp. Gatelys for eksempel tar lang tid å starte opp.*
- *Levetiden på forskjellige typer lamper varierer betydelig.*
- *Forskjellig lys har forskjellige egenskaper avhengig av værforholdene; eksempelvis virker gult lys bra i tåke.*

LED-belysning

LED (Light-Emitting Diode) er en lysemitterende diode som har evnen til å sende ut lys når den stimuleres elektrisk.

Vanlig LED-belysning avgir hverken ultrafiolett eller infrarød stråling. Lyskilden passer derfor godt i miljøer der man ønsker å unngå UV- eller IR-stråling. En fordel med lysdioder er at de ikke inneholder bevegelige eller skjøre deler. Riktig konstruerte LED-armaturer er robuste og motstår vibrasjoner og andre mekaniske påkjenninger meget godt. LED lyser opp meget raskt og er ideelle for belysning som slås av/på svært ofte. LED svikter vanligvis over tid ved redusert lys i stedet for plutselig tap som i andre lyskilder. En LED-armatur kan ha svært lang levetid hvis den består av komponenter av høy kvalitet i en godt planlagt konstruksjon.

LED-belysning har en høyere investeringskostnad enn tradisjonell belysning. En utfordring med LED-belysning er at elektronikken krever stor avkjøling, enten innebygd i armaturet eller i lyskilden, for ikke å overopphete diodene og drastisk redusere levetiden. LED er også spenningssensitiv og må ha riktig polaritet. Feil bruk av LED-farge/spekter vil medføre «feil» lyskvalitet. Usertifisert LED-belysning kan gi støy på radiosignaler.

IR-lys

IR-lys (infrarødt lys) ligger ikke innenfor den synlige delen av lysspekteret, og brukes derfor i situasjoner hvor det ikke er ønskelig med synlig lys. IR-lys må brukes sammen med kameraer som arbeider innenfor IR-spekteret.

IR-lyskastere basert på LED-teknologi kan nyttes på avstander opp til ca. 170–200 meter. Det kan være aktuelt å bruke denne løsningen på steder der man ikke ønsker å sjenere nabolaget (miljø). I tillegg kan løsningen benyttes for å unngå blending av eget personell, eller for å skjule at man har sikringsanlegg i området.

Vær oppmerksom på at IR-lys kan ødelegge for siktemidler og lysforsterkningsutstyr, brukerne må derfor konsulteres.

Armaturer

Veglysarmatur

Veglysarmatur gir et kontinuerlig dekningsfelt i et gitt område. Bruksområdet på denne typen armaturer er langs veger, langs gjerder, etc. Avstanden mellom armaturene er normalt på 5 x høyden på lysmasten. Det finnes spesialreflektorer for enkelte anleggstyper, som kan gi opp til ca. 10 x montasjehøyden/mastehøyden. Disse typene kan være egnet for å belyse gjerder etc.

Lyskastere

Små lyskastere egner seg godt til å opplyse områder som ikke dekkes av den tradisjonelle utebelysningen. Små lyskastere har en rekkevidde på 2,5 til 3 x lyskasterens montasjehøyde. Dekning i bredden er tilnærmet den samme som dekningen i dybden.

Lyskastere finnes i tre hovedtyper:

- → *Rotasjonssymmetrisk – rund reflektor som sender lys i en kjegle fra lyskilden (eks. lommelykt)*
- → *Symmetrisk – reflektor med form som en takrenne og belysning i et rektangulært område*
- → *Asymmetrisk – lyset sendes rett ned og fremover i en gitt vinkel*

Belysningsplaner

Før belysningen vurderes, må operative krav innhentes. Hvilket lys er nødvendig/ønskelig? I tillegg til sikkerhetskrav må HMS-messige forhold vurderes.

Perimeterets belysning

Ideelt sett bør belysningen plasseres slik at området rett utenfor gjerdet er tilstrekkelig opplyst, men slik at innsiden av gjerdet ikke er opplyst. Eventuelle master for lys bør stå minst 3 meter innenfor gjerdet for å unngå at en inntrenger kan benytte de til å passere barrieren eller unngå alarmsystemer, og slik at vakt og sikring har tilstrekkelig patruljeringsområde innenfor gjerdet.

SIKRINGS-BELYSNING

Hvis belysningen er en viktig del av sikringstiltakene, må denne også sikres i henhold til dette.

Sikringstiltak som bør vurderes

- **Fysisk og/eller elektronisk sikring av belysningskomponenter mot sabotasje. Herunder: lyskilde, strømkurs, kabler, koblingspunkter, sikringsskap og lignende**
- **Nødstrøm**
- **Alarm ved feil på belysningen**
- **Rutiner for feilretting**
- **Beredskapstiltak hvis belysningen ikke er tilgjengelig**

Det er viktig at vaktstyrken har mulighet til å styre belysning av/på.

Blendende belysning
Blendende belysning har en sterk avskrekkende effekt. Størst effekt oppnås når lyset kommer omtrent i inntrengerens siktelinje.

I tillegg til den avskrekkende effekten vil belysningen skjule vakter og sikringstiltak bak lyset. Patruljerende vakter vil lettere oppdage en inntrenger som nærmer seg. Belysningen bør plasseres i 1–1,5 meters høyde, og med 6–7 meters avstand.

Områdebelysning
Med dette mener man belysning av området rundt bygninger med beskyttet område. Minimumbelysning 3,0 LUX hvis områdebelysning velges.

Belysning av verdier
Det vil si kraftig belysning på fasaden til viktige bygg. Vanligvis vertikalt lys, som blant annet vil få en inntrenger til å fremstå i silhuett. Sikkerhetsmessig er det tilstrekkelig med lys i 2–3 meters høyde. Denne belysningen anses ofte som estetisk riktig og vil derfor ikke fremstå like mye som et sikringstiltak.

Kjøretøysperrer

Kjøretøysperrer utformes og settes opp for å stoppe eller avvise kjøretøy som forsøker å trenge seg gjennom en grense. Kjøretøysperrer kan være passive eller aktive.

Det kan være flere årsaker til å installere kjøretøysperrer, men en av de største truslene som krever mest oppmerksomhet, er å forhindre at et kjøretøy med eksplosiver skal kunne komme tett på verdien. Ved en eksplosjon er avstand helt avgjørende for skadeomfanget, og det vil derfor være å anbefale at selve kjøretøysperren plasseres så langt som mulig fra verdier og objekter som skal sikres. Det må avklares hvilken dimensjonerende trussel det skal sikres mot, slik som type kjøretøy og angrepsretning, samt at det må beregnes hvilken hastighet kjøretøyet kan oppnå på stedet.

Passive kjøretøysperrer benyttes der kjøretøy ikke skal kunne passere. Typisk er grøfter eller voller i tilknytning til ytre perimeter av sikringsobjektet, eller det kan være pullertrekker rundt en bygning.

Det beste tiltaket mot trusselen fra kjøretøy er passive kjøretøysperrer rundt hele objektet, men vanligvis må det etableres inn-/og utpasseringsområde(r) med aktive kjøretøysperrer. Det er viktig at de passive og aktive kjøretøysperrene danner en helhetlig sikring rundt objektet.

Aktive kjøretøysperrer benyttes der autoriserte kjøretøy skal kunne passere. Slike må ikke vurderes isolert, men som en del av en integrert sikkerhetsløsning som kan omfatte supplerende porter og bommer, skilting og omkringliggende perimetersikring.

Valg av aktive og passive kjøretøysperrer vil være situasjonsavhengig og må baseres på risikovurderinger[2].

Plasseres kjøretøysperren tett innpå en bygning som skal beskyttes, kan det være helt avgjørende at kjøretøyet stoppes omgående, og det må velges en sperre som kan stoppe kjøretøyet på stedet. Hvilken trussel det skal sikres mot; en personbil på 1500 kg eller en trailer på 32 tonn, og hvilken hastighet kjøretøyet kan treffe sperren med, er selvfølgelig også avgjørende for valg av løsning.

Vi anbefaler at man ved anskaffelse av kjøretøysperrer benytter seg av testet og godkjent utstyr. I Norge anbefales det å benytte produkter som er testet og godkjent i henhold til den britiske standarden «PAS 68»[3] ved nyetableringer.

Passive kjøretøysperrer
Passive kjøretøysperrer benyttes der kjøretøy ikke skal kunne passere, og kan grupperes i:

2
Se kapittel 5, Risikoanalyse, for metodikk knyttet til risikovurderinger

3
PAS 68: 2013 Impact test specifications for vehicle security barriers (eventuelt IWA 14-1, som bygger på PAS 68)

Kjøretøysperre

Kjøretøysperrer
Kjøretøysperre som forsterket mur i forbindelse med landskapsbearbeiding. Minimumsmål = 60 cm. Her vist i kombinasjon med passive og aktive pullerter.

FOTO Forsvarsbygg

Kjøretøysperrer
Skulpturelle innslag, London.

FOTO Forsvarsbygg

KJØRETØY-SPERRER

Valgmuligheter
Kun løsninger og produkter som er testet og godkjent i henhold til en internasjonal standard, defineres som kjøretøysperre.

Løsninger som ikke er testet, betegnes som kjøretøyhindringer.

Aktiv kjøretøysperre

- → *Naturlige hindringer*
  - *Voller og grøfter*
  - *Naturlige skjæringer i terrenget*
  - *Enkle tilpasninger av terrenget*
- → *Plassbyggede kjøretøysperrer*
  - *Faste pullerter*
  - *Murer*
  - *Gjerder og wireløsninger*
- → *Utplasserte hindringer*[4]

Typiske passive kjøretøysperrer er pullertrekker langs bygninger og grøfter eller voller i tilknytning til ytre perimeter av sikringsobjektet, men det finnes også andre løsninger som kan benyttes over lange avstander. Grøfter og voller må dimensjoneres og utformes spesielt, og det må være stor oppmerksomhet på problematikk med snø og is.

Murer må være spesielt dimensjonert og fundamentert for å fungere som en kjøretøysperre.

Utplasserte hindringer kan være flyttbare passive kjøretøyshindre som bruker sin vekt og evne til å deformere og absorbere energi som middel for å hindre et kjøretøys fremdrift. De er vanligvis uegnet for å forandre retning på et kjøretøy, med mindre de er sammenkoblet. De varierer betydelig i vekt og utforming.

Det er mulig å benytte frittstående elementer som er dimensjonert for formålet. Disse kan utformes som gatemøbler, plantekasser eller integrert i andre elementer, og dermed skjult. Det er viktig å unngå brudd i kjeden, at alle elementer har lik styrke og at minimum/maksimummål følges.

Det skal være mindre enn 1,2 m mellom elementene (pullerter, blomsterkasser, gatemøbler, etc). Dersom sikringen blir kledd inn og skjult av et svakere materiale, skal det fremdeles ikke være mindre enn 1,2 m mellom de reelle fysiske sikringselementene.

4
Det engelske begrepet som ofte benyttes, er planters

Kjøretøyklasser

Forslag til dimensjonerende eksplosivmengde

Motorsykkel	Personbil	Varebil	Lastebil	Stor lastebil
50 kg TNT	400 kg TNT	1500 kg TNT	4000 kg TNT	> 4000 kg TNT

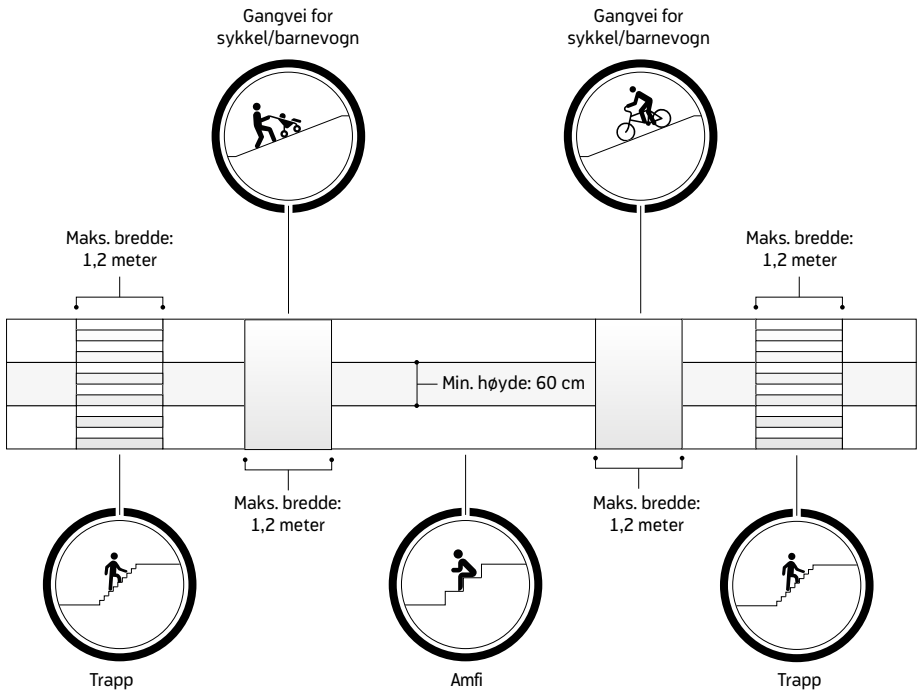
Sikringsklasser for kjøretøysperrer

Sikringsklasse	Beskrivelse/krav
1	→ En kjøretøyhindring som er etablert ved bruk av sperremateriell som kråkeføtter, betongklosser eller lignende. → Avskrekkende effekt. → Vil ofte kunne stoppe mindre kjøretøy i lave hastigheter, men dette kan ikke garanteres.
2	→ En enkel linje med passive og aktive kjøretøysperrer dimensjonert for å stoppe trusselkjøretøyet i en definert hastighet. Det må besluttes hvilket kjøretøy som skal stoppes (personbil, liten lastebil, m.m.), og hvilken hastighet kjøretøyet kan oppnå (50, 60, 80 km/t). → (Single line of Vehicle Security Barriers (VSBs))
3	→ En enkel linje med passive kjøretøysperrer og de aktive kjøretøysperrer suppleres med en sluseløsning. → En adgangskontroll i form av bom eller lignende før man kommer frem til den aktive kjøretøysperren. → (Final denial VSBs)
4	→ En enkel linje med passive kjøretøysperrer og sluseløsninger med aktive og passive kjøretøysperrer. → (Interlocked VSBs)

HMS ved bruk av aktive kjøretøysperrer
En aktiv kjøretøysperre skal respekteres og behandles som en installasjon i stand til å avgi dødelig kraft. Den kan nødstenges meget hurtig og er sterk nok til å løfte en lastebil.

Personellet som skal betjene kjøretøysperren eller har oppgaver i tilknytning til denne, må ha nødvendig opplæring. Merking av kjøretøysperren med nødvendige varselskilt, lys, lydsignal og farger må vurderes for å ivareta personellsikkerhet. Fotgjengere skal ledes unna og helst holdes adskilt fra kjøretøysperren. Når det gjelder HMS-aspektet, bør følgende vurderinger gjøres:

Kjøretøysperring integrert i trapper og amfi



Avstanden i forserbare partier skal som en tommelfingerregel maksimum være 1,2 meter i bredden (trapp og sykkelstier), og en minimumshøyde på 60 cm på trinn/sitteplass i amfi.

- → *Er kjøretøysperren godt nok merket?*
- → *Hva skjer når strømmen går?*
- → *Er det nødstoppknapp?*
- → *Er belysningen tilstrekkelig?*
- → *Er forskjellige sikkerhetsløsninger («safety») tilgjengelig fra leverandøren?*
- → *Hvordan er nødstengingsfunksjonen?*

Diverse typer aktive kjøretøysperrer

Bommer

Veiledning for tilvirkning, installasjon og drift, samt detaljerte plantegninger er tilgjengelig.

Det finnes en rekke produsenter, og bommer fås både manuelle og motordrevede. For å oppnå godkjenning i høye klasser krever det vanligvis dyp fundamentering.

Veisperrer «Road blockers»

Veisperrer er effektive og avskrekkende. De er vanligvis mekaniske/hydrauliske, og betjenes manuelt via betjeningspanel av vakter, eller automatisk ifm. AAK.

De dimensjoneres etter trusselen, og skal tåle gjentatte belastninger. 0,6–0,7 m er vanlig høyde.

De er mulig å få med meget grunt fundament.

Veisperre benyttet i internasjonale operasjoner

Enkel veisperre som kan bygges lokalt. En modifisert utgave av den avbildede er testet.

Betong- og stålfundament med en konstruksjon i firkantstål forsterket med to stålvaiere festet i et eget fundament.

Produktblad med byggebeskrivelse er tilgjengelig.

Mobile veisperrer

Det finnes flere mobile veisperrer på markedet, hovedsakelig i de lavere sikkerhetsklassene.

De er hydraulisk eller manuelt opererte og kan gjøres operative på kort tid (ca. 15 minutter).

Pullerter «Bollards»

Pullerter er kraftige stolper som forankres i et fundament i bakken.

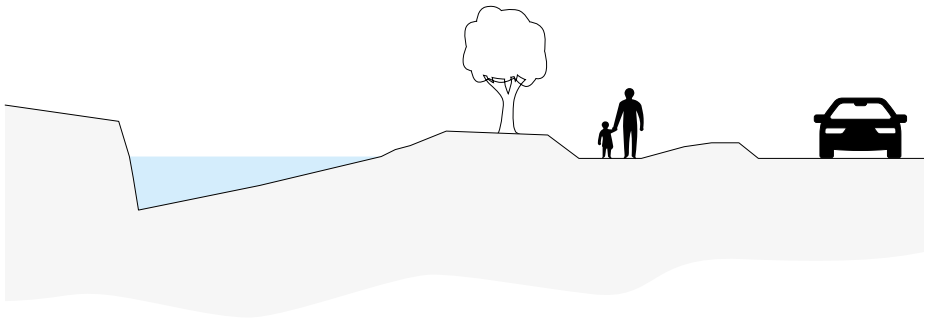
De leveres i utallige utforminger og sikringsklasser. De er gjerne elektro-hydraulisk hev-/senkbare.

Skyveporter

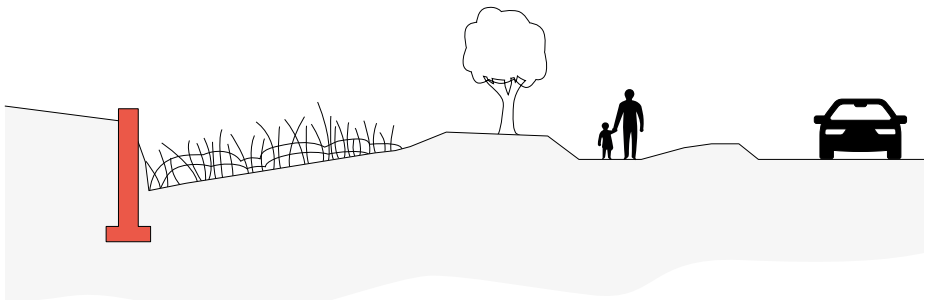
Finnes i alle klasser. De bruker vanligvis relativt lang tid på å åpnes/lukkes. Lukkehastighet på 30 cm/s er vanligst.

Skyveporter er også sårbare for treff mens de er delvis åpne.

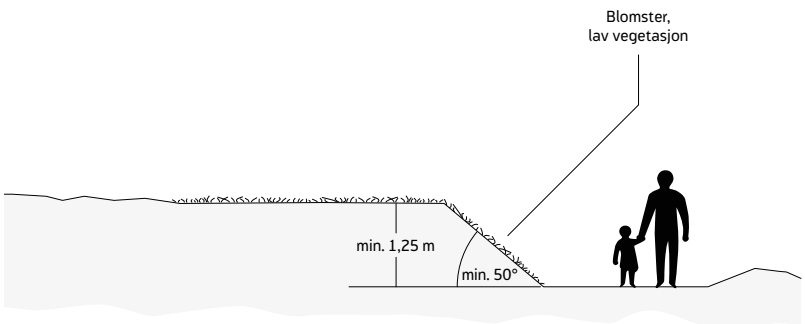
Kjøretøysperre som vannspeil



Kjøretøysperre som forsterket mur



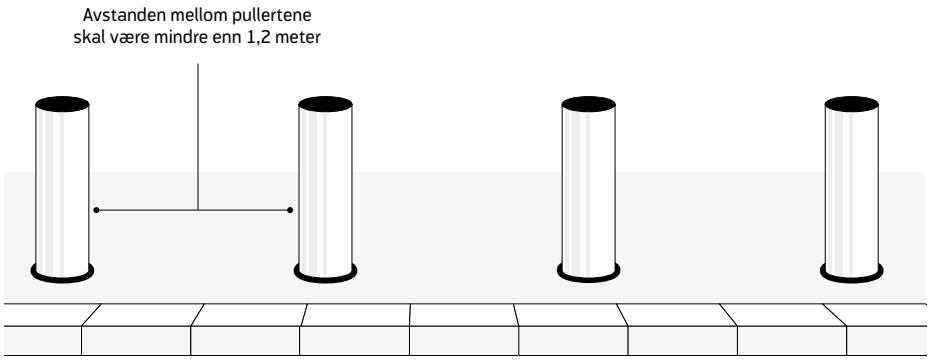
Kjøretøysperre som voll



Aktive og passive kjøretøysperrer

Serie av aktive og integrerte passive kjøretøysperrer i form av gatebelysning, pullerter, benker og plantekasser.

Pullerter



Det er ikke å anbefale pullerter med den oppgitte minimumshøyden på 60 cm, grunnet hms-hensyn. De kan ha dårlig synlighet, og vil være uheldig med tanke på universell utforming.

Sikring fra sjøsiden

I en del tilfeller vil ytre perimeter også bestå av en sjøside. Tradisjonelt har sikring fra denne siden bestått av forbudsskilt og eventuelt økt vakthold ved spesielle situasjoner.

Det er også mulig å sikre sjøsiden med fysiske og elektroniske sikringstiltak.

Under annen verdenskrig brukte man lenser og ubåtnett, undersjøiske barrikader (steinjete) og minefelt for å beskytte viktige marinebaser. Det var liten utvikling på området i mange år, men i senere tid, spesielt etter selvmordsbomben som ble levert med et hurtiggående fartøy, mot fregatten USS «Cole» i 2000, har det dukket opp mange produkter på markedet. Det er nå vanlig med inngjerding av marine- og cruisehavner også til sjøs i en rekke land.

Prinsippløsningen er et gjerde som er plassert på et flytende fundament. Gjerdet kan utformes som ønsket, og utstyres med piggtråd, skilt og eventuelt forlenges under vann. Et gjerde vil naturlig også kreve en inn- og utpasseringsmulighet. Deteksjonssystemer både over og under vann kan etableres i forbindelse med

gjerdet. Dersom det etableres sikringstiltak til sjøs, bør man også ha et reaksjonsapparat som står i forhold til dette.

Områdesikring

Områdesikring er sikringstiltak som etableres mellom perimeteret og sikringen av bygninger. Det er viktig at teknisk utstyr og materiell som befinner seg i uteområdet, også tas med i en verdivurdering og sikres tilsvarende.

Aktuelle sikringstiltak er inngjerding, avlåsing, elektronisk sikring (innbruddsalarm, kameraovervåkning og automatisk adgangskontroll) sikkerhetsbelysning og høyttaleranlegg.

For mer utførlig beskrivelse av funksjoner og teknisk beskrivelse viser vi til kapitlet for Elektronisk Sikring.

Verdier som kan kreve sikring, omfatter: traseer med kabelføring (inkl. kumlokk), koblings- og fordelingsskap, antenner, master, trafoer, utvendige kjølevifter, kjøretøy, beredskapsmateriell, m.m., herunder spesifisert:

Antenner
Antenner kommer i mange typer og former, og kan plasseres på forskjellige måter. Det kan ofte være praktisk å plassere enkelte typer av antenner mellom den ytre og indre perimeteret, og da bør særskilt inngjerding av antennen vurderes.

Tanker
Tanker kan utsettes for sabotasje eller ødeleggelse. Viktigheten av systemet tanken drifter bør avgjøre om den skal plasseres nedgravd, i egne bygg eller fritt på bakken. Om tanken kan ha sikkerhetsmessige konsekvenser for annen virksomhet, vil også ha betydning, for eksempel dersom tanken medfører eksplosjonsfare. Det kan vurderes å gjerde inn frittstående og eventuelt nedgravde tanker. Påfyllingsflenser må sikres.

Materiell som er plassert ute i området
Typisk materiell plassert ute, kan være: kjøretøy, mindre båter, kabelruller, containere med utstyr, hengere, beredskapsmateriell og diverse utstyr som mellomlagres.

Utstyret kan være attraktivt for en vinningsforbryter. Følgende betraktninger knyttet til sikkerhet bør derfor gjøres:

- *Er det forsvarlig at utstyret står ute?*
- *Bør ett eller flere områder inngjerdes?*
- *Er det gjenstander eller områder som bør alarmbelegges?*
- *Bør område(r) eller enkeltobjekter ha kameraovervåkning?*
- *Bør kjøretøyhengere med utstyr på, låses fast?*

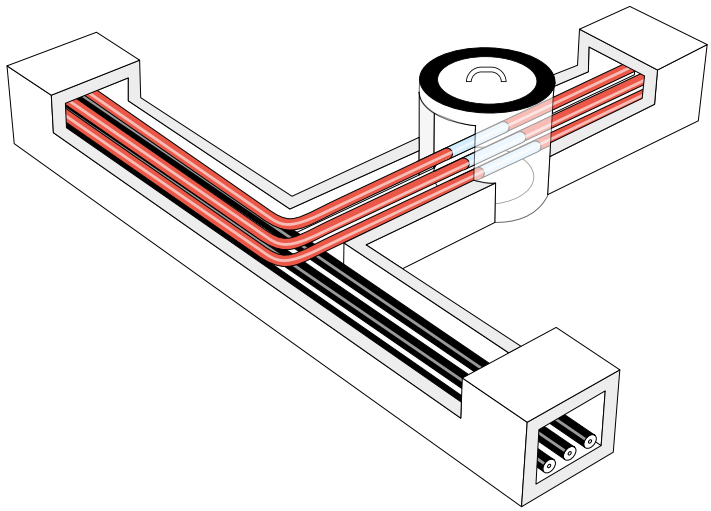
Utvendige kjølevifter og tørrkjølere ved viktige funksjoner bør enten plasseres utilgjengelige eller sikres ved inngjerding og elektronisk sikring.

Sikring av utendørs kabelføringer
Kabler for kommunikasjon og strømforsyning er en viktig del av kritisk infrastruktur. En feil på en kabel vil kunne ramme viktige funksjoner. Funksjonalitet etter skade på denne type installasjoner kan også ta lang tid å reetablere. Det vil i dette perspektivet derfor være naturlig å gi kablene sikring og beskyttelse, fordi kablene kan bli utsatt for tilsiktede sikkerhetstruende hendelser.

Verdien og avhengigheten på det som går i kablene, avgjør hvilket sikringsnivå kabelføringene må ha. Kabelen med størst viktighet i en kabeltrasé blir derfor dimensjonerende for sikringen i kabelgrøften.

Det er viktig å identifisere hvorvidt det er krav til at systemer skal opprettholde sin funksjonalitet etter sikkerhetstruende handlinger, samt hvilken sikkerhetsgradering systemet (eventuelt systemene) skal ha dersom man også må ta hensyn til krav i henhold til sikkerhetsloven.

Utvendig kabelføring



Kabelføringer og kulverter skal sikres slik at de som et minimum tilfredsstiller informasjonssystemets graderingsnivå.

Kommunikasjonskabel som overfører gradert informasjon, må sikres i henhold til kravene i sikkerhetsloven med forskrifter. Det vil si at de skal ligge i rør og trekke- eller koblingspunkter skal være avlåst.

Utenfor kontrollert område skal disse punktene ha innbruddsalarm (AIA). I kontrollert og beskyttet område skal AIA vurderes.

I tillegg til kommunikasjonskabler må det vurderes om strømkabler og kabler til elektronisk sikring (AIA, AAK og TVO) skal sikres fysisk og elektronisk.

Beskyttelse mot EMP/HPM er nærmere beskrevet i ***kapittel 19, Elektromagnetiske effekter***.

Sikringsløsninger for kabelføringer
For kummer er det utarbeidet flere lokk- og låseanordninger. Disse bør være testet og verifisert i forhold til behovet. Avlåsningen skjer enten med en tverrstang avlåst med hengelås over kumlokket, eller et eget underlokk avlåst med hengelås.

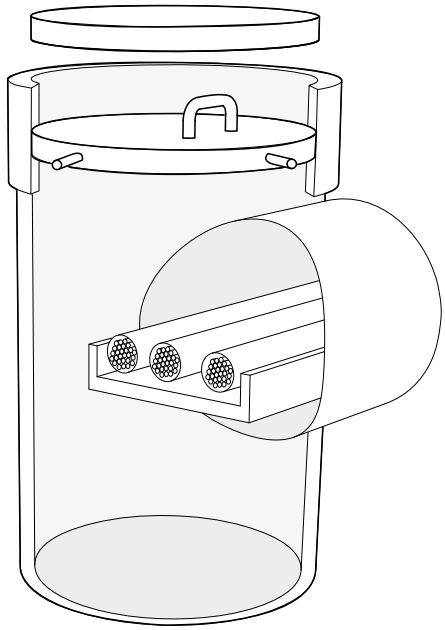
Ingen av disse løsningene kan motstå innbruddsforsøk med verktøy særlig lenge.

Sikkerhetslokket bør sikres med alarm.

For kumlokk som gir tilgang til kabler som er vitale for virksomheten eller inneholder høyt sikkerhetsgradert informasjon, bør det i tillegg vurderes å etablere kameraovervåkning. Sikringsklasse på det elektroniske sikringsanlegget bestemmes av viktigheten av det som går i kablene.

Viktige kabler bør ligge i egne trekkerør.

Kum med dobbelt sikringslokk



Låser vil være utsatt for ytre påkjenninger og må derfor ha ettersyn og vedlikehold.

Virksomheten bør ha et kabelkart, som gir opplysninger om kabeltraseer, plassering av omformere, tilkoblingsutstyr, tilkoblingspunkter, plassering av kummer og skap og overganger mellom ute- og inneområder. Kabelkartet skal graderes etter sitt innhold.

For sikkerhetsgraderte systemer finnes det ytterligere detaljer i «Veiledning til forskrift om informasjonssikkerhet – nærmere bestemmelser om Tempest sikkerhet». Denne er sikkerhetsgradert BEGRENSET og forvaltes av NSM.

Høyttaleranlegg (PA-anlegg)
Som et supplement til annet reaksjonsapparat kan et utendørs høyttaleranlegg være aktuelt. Man vil da ha mulighet til å tilsnakke og gi direktiver til en uvedkommende fra et vakt- eller operasjonsrom. Omfanget av et høyttaleranlegg vil kunne variere kraftig; fra kun en høyttaler rettet mot et «problemområde», til høyttalere i forbindelse med ytre perimeter, eller et omfattende høyttaleranlegg for hele området. Det er også mulig å forhåndsinnspille en standardmelding som kan kobles til for eksempel utløsing av en alarm.

Et høyttaleranlegg gir også andre muligheter til å gi viktig informasjon til personell som befinner seg i aktuelt område, som for eksempel ved en evakuering.

Beredskapsplaner og -tiltak

En innøvd beredskapsplan[5] bør være en integrert del av en virksomhets grunnsikring og beskrive hvilke tiltak virksomheten vil kunne iverksette for å forsterke de faste sikringstiltakene. Ved etablering av permanente sikringstiltak bør derfor behov og muligheter for beredskapsmessige forsterkninger vurderes.

Det er mange spørsmål som bør besvares: Nye eller forsterkede sikringstiltak? Hvor plasseres de? Hvordan utformes de? Hvem skal etablere de? Hvilket materiell er tilgjengelig? Er det planlagt og tilrettelagt for bruk av materiellet? Kan beredskapsmateriell benyttes ved øvelser eller må det anskaffes eget øvingsmateriell?

Eksempler på beredskapsmessig forsterkning av eksisterende sikring:

→ *Forsterkning av adgangskontrollen*
- *Bruk av vakter – innleide eller egne*
- *Ekstra kortlesere/AAK som kan aktiviseres*
- *Gjennomgang av og innstramning i adgangsrettigheter. Kode hele døgnet på all AAK*
- *Er det tilrettelagt for patruljering av ytre perimeter (utvendig eller innvendig)?*

→ *Forsterket perimetersikring*
- *Midlertidig gjerde*
- *Strengere kontroll av kjøretøy – kjøretøysperrer og sjikaner for kjøretøy (speil, eventuelt bruk av betongelementer, kråkeføtter, m.m.)*

Medfører behov for mer plass til kontrollområde, avvisning og parkering

- *Skilting*
- *Observasjonsstillinger*

→ *Styringsmulighet for sikkerhetsbelysningen «av/på» på en enkel måte*

→ *Nytt utstyr*
- *lyskastere*
- *mobile detektorer etc.*
- *Skannere for å oppdage eksplosiver*

→ *Tilrettelegging for sikringsstyrker. Gjelder spesielt skjermingsverdige objekter iht. sikkerhetsloven.*[6]
- *Plassering av kontrollpunkter eller -stillinger. Skal for eksempel sambandslinjer etableres permanent?*
- *Ildstillinger og -felt*

5
I forbindelse med beredskapsarbeid nyttes ofte ulike begreper som katastrofeplan, kriseplan, beredskapsplan, «business continuity»-plan og kontinuitetsplan om hverandre. I dette dokument benyttes begrepet beredskapsplan.

6
Ref. § 3-5. Objekteier plikter å legge til rette for at sikringsstyrker kan forberede, øve og gjennomføre tiltak på og ved objektet for å beskytte dette.

Kapittel 11

Fysisk sikring mot inntrengning

Dette kapitlet beskriver de mest sentrale temaene knyttet til fysisk sikring mot inntrengning. Sikring i dybden benyttes for å oppnå flere fysiske og elektroniske barrierer mellom usikret område og områder med verdier.

I en bygning vil fysiske barrierer være vegger, tak, etasjeskiller, dører og vinduer etc., mens elektroniske sikringstiltak er tiltak for å detektere, varsle eller overvåke uautorisert tilgang.

Begrepet skallsikring benytter vi om sikringstiltak i et skall omkring virksomheten, og vil normalt være byggets fasader og tak inklusive ytterdører, vinduer og åpninger i skallet. Hensikten med skallsikring er å etablere en ytre sikkerhetsbarriere som skal gjøre det vanskeligere for en trusselaktør å ta seg inn til verdien, eller redusere eller forhindre skade på verdier som følge av en uønsket handling.

I skallsikringen bør alle elementer som inngår i skallet, ha tilnærmet lik fysisk styrke mot definerte trusler. Det er for eksempel lite hensiktsmessig å installere en høysikkerhetsdør i en svak vegg med liten innbruddsmotstand. Det er også viktig å være oppmerksom på at åpninger for ventilasjon, kabel- og rørgjennomføringer, kulverter og lignende kan gi adgang gjennom skallet. Slike åpninger må derfor sikres i henhold til kravet for resten av skallet.

I byggeprosjekter vil det være en rekke bruker- og funksjonskrav som skal ivaretas i prosjekterte løsninger. Det kan derfor forventes at det for en fysisk barriere vil være andre krav utover spesifikke sikringskrav. Om vi stiller krav til innbruddsikkerhet for en yttervegg, skal sikringskravene komplementere andre funksjonskrav til aktuell yttervegg. Andre krav til ytterveggen kan være krav til varmeisolasjonsevne, lydisolasjon, brannmotstand etc. Noen ganger kan det være konflikt mellom høye sikringskrav og andre krav. Eksempler på dette kan være at høysikkerhetsvinduer i fasaden må leveres med noe mer redusert varmeisolasjonsevne enn det som er mulig å oppnå uten sikkerhetskrav. Det kan være konflikt mellom ønskede krav til rømning ved brann og sikringskrav mot inntrengning. I disse tilfellene kan det være nødvendig at brannsikkerheten må løses på annen måte, eller med kompenserende tiltak. Brannrådgiver som planlegger brannkonseptet, trenger derfor kjennskap til sikringskrav som skal hensyntas.

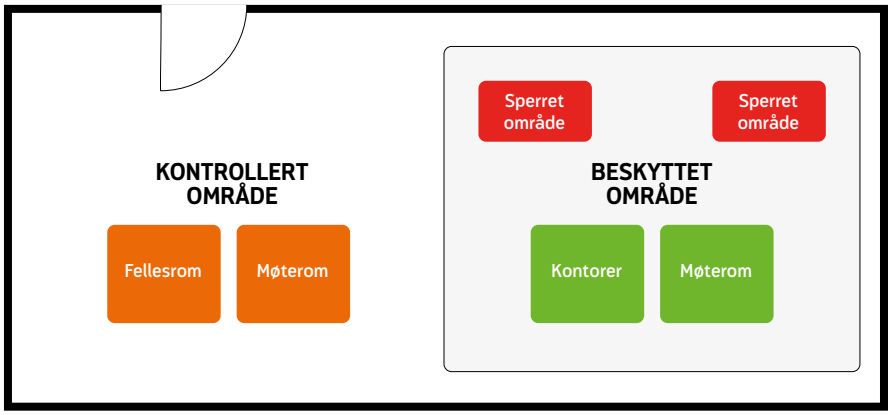
Sikring i dybden

Alle virksomheter som oppbevarer eller tilvirker sikkerhetsgradert informasjon og utstyr, plikter etter forskrift om informasjonssikkerhet[1] fysisk å dele opp sine lokaler i avgrensede områder. Sikringen kan deles inn i tre områder, som danner hvert sitt lag rundt verdiene.[2] Ytterst ligger kontrollert område, deretter kommer man inn i beskyttet område og til slutt sperret område.

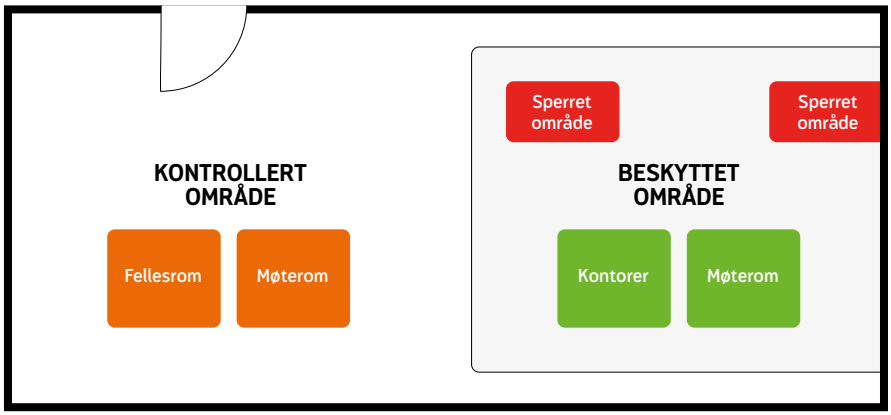
1
Jf. informasjonssikkerhetsforskriften § 6-8 og NSMs Veiledning til forskrift om informasjonssikkerhet

2
Se også NSMs veiledning «Fysisk sikring mot ulovlig inntrengning», se www.nsm.stat.no Veiledningen beskriver blant annet ulike krav til sikring for oppbevaring av gradert materiell i områder som er definert sperret BEGRENSET, sperret KONFIDENSIELT, sperret HEMMELIG og sperret STRENGT HEMMELIG

Eksempel på soneinndeling



Eksempel på soneinndeling, i en idealsituasjon.



Eksempel på soneinndeling – med en praktisk utfordring: Veggen til et sperret område er yttervegg, og er således ikke beskyttet av lag på lag med barrierer.

Sikringsnivået bestemmes av hvilke verdier som befinner seg i området.[3] Det anbefales at alle virksomheter organiserer sitt område etter disse prinsippene. Se for øvrig ***kapittel 10, Perimeter- og områdesikring.***

Virksomheter som er underlagt sikkerhetsloven og tilhørende forskrifter, må forholde seg til kravene som stilles i disse. Det understrekes at disse angir minimumskrav. Det er også beskrevet i lovverket at virksomheter plikter å vurdere om ytterligere sikring er nødvendig for å sikre egne verdier på en tilfredsstillende måte.

Under gis en kort beskrivelse av hvert enkelt område, med eksempler på hvilken type sikring som vil kunne benyttes her.

Kontrollert område er et område som normalt omgir beskyttet eller sperret område, og skal etableres slik at virksomheten kan kontrollere aktiviteten og bortvise uvedkommende. Området kan være både ute- og inneområder som virksomheten eier eller benytter. Adgangen til området kan kontrolleres utenfor bygget, for eksempel ved bruk av gjerde som markerer en klar juridisk grense. Skal objektet ha et høyt sikringsnivå mot en inntrengningstrussel, bør

3 Kravene som beskrives i NSMs veiledning «Fysisk sikring mot ulovlig inntrengning», danner grunnlaget for dette avsnittet.

perimeter rundt kontrollert område sikres både med fysiske og elektroniske sikringstiltak. Elektroniske sikringstiltak kan være automatisk innbruddsalarm (AIA) for deteksjon av angrep, kombinert med (TVO) tiltak for å overvåke og dokumentere hendelsen.

Hvis det kontrollerte området ikke er fysisk avgrenset med etablert adgangskontroll, vil dette medføre større behov for kontroll med beskyttet område.

Beskyttet område skal være fysisk avgrenset, og denne avgrensningen skal være hel. Det skal ikke være mulig å ta seg inn i dette området uten at det oppdages, og det skal ikke være mulig å fjerne en del av denne avgrensningen og sette den tilbake uten at det setter visuelle spor. Virksomheten skal ha etablert kontroll med adgangen. Behovet for kontrolltiltak vil variere etter virksomhetens størrelse og type, men det er vanlig å benytte vakt, resepsjon, adgangskontrollanlegg med kort/PIN-kode eller en kombinasjon av dette. Hovedsaken er at tiltakene skal hindre at uvedkommende får adgang uten at det oppdages. En rettesnor her bør være at de som gis permanent adgang – det vil si de som har egen nøkkel eller adgangskort og kan ferdes fritt alene – bør ha tjenstlig behov for adgang på området.

Området skal sikres i henhold til krav for de verdiene som befinner seg på området, og generelt sett anbefales det å installere automatisk innbruddsalarm (AIA) som en del av skallsikringen. I tillegg bør det installeres automatisk adgangskontroll (AAK) for å ivareta autorisasjonsskillet. Det stilles krav om at adgangskort og besøkskort skal benyttes og bæres synlig i beskyttet område. Dette kravet kan imidlertid fravikes dersom den aktuelle virksomheten er så liten at alle med permanent adgang kjenner hverandre godt av utseende.

Hvis det kontrollerte området ikke er fysisk avgrenset med etablert adgangskontroll, vil dette medføre større behov for kontroll med beskyttet område.

Sperret område deles opp etter viktighet eller graderingsnivå,[4] men felles for alle sperrede områder er fysiske og elektroniske sikringstiltak, samt etablert kontroll ved adgangen. Behovet for kontrolltiltak vil variere etter virksomhetens størrelse og type også her. Tiltakene skal hindre at uvedkommende får adgang uten at det oppdages. De som gis permanent adgang, det vil si de som har egen nøkkel eller adgangskort og kan ferdes fritt alene, skal ha gyldig sikkerhetsklarering og autorisasjon, om virksomheten er underlagt sikkerhetsloven. For andre typer virksomheter kan tilsvarende krav gjøre seg gjeldende, som fremlagt vandelsattest eller andre typer godkjenninger. Vedlikeholdspersonell eller rengjøringspersonell skal ikke gis permanent adgang til sperret område, men må utføre sine oppgaver under oppsyn av autorisert personell. Tilgangen for vaktpersonell vurderes i hvert enkelt tilfelle.

Sperret område BEGRENSET, sperret område KONFIDENSIELT, sperret område HEMMELIG og sperret område STRENGT HEMMELIG må etablereres etter kravene i henhold til sikkerhetsloven.

Det eksisterer særskilte krav til rom som skal benyttes til gradert tale. Disse kravene er nærmere omtalt i ***kapittel 14, Avlytting og avlesing.***

Sikringsklasser

Generelt

Sikringshåndboka benytter sikringsklasser for å definere nivåer av motstandsgrad for fysiske barrierer mot trusler. En viktig anvendelse av sikringsklasser er muligheten dette gir for å dokumentere at det er etablert fysiske barrierer som samlet gir tilstrekkelig innbruddssikkerhet for prioritert verdi mot spesifisert trusselnivå.

4 Det vil si sperret BEGRENSET, sperret KONFIDENSIELT, sperret HEMMELIG og sperret STRENGT HEMMELIG

Trusselaktører og verktøygrupper (eksempler)

Trusselnivå	Eksempel på trusselaktører	Verktøygruppe
A	**Tilfeldig inntrenger**	→ Lett mekanisk verktøy. Eksempel: skrutrekker, lite brekkjern, tang, kniv, hammer og lignende
B	**Kriminelle**	→ Tyngre mekanisk verktøy samt forskjellig elektrisk verktøy.
C	**Organiserte kriminelle**	→ Stort utvalg av mekanisk utstyr, alle typer elektrisk, gass- og/eller skjæreverktøy. Kan også ha motorisert bærbart verktøy, samt håndvåpen.
D	**Internasjonale aktører/organisasjoner** med betydelig kapasitet eller fremmed makts styrker	→ Alle typer verktøy med motor, gass- og/eller hydraulisk drevne verktøy, rambukk, etc. Kan også ha verktøy som krever motorisert transport, samt bærbare våpen og sprengstoff.

Sikringstabellene gir innbruddstider for fysiske barrierer av forsterkede konstruksjonselementer for ulike trusselnivå. Dette kan benyttes i et tidsregnskap for å dokumentere balansert sikring. Se avsnittet om ***balansert sikring***.

Trusselnivå relateres til trusselaktørene som rangert etter økende trusselnivå er: Alfa (A), Bravo (B), Charlie (C) og Delta (D). Trusselaktørene har ulik grad av tilgang på effektive angrepsverktøy og ulik grad av kompetanse for gjennomføring av angrep. Trusselaktøren vurderes innenfor kategoriene kriminalitet, spionasje, sabotasje og terror, som beskrevet i ***kapittel 7, Trusselvurdering***. I ***tabellen Trusselaktører og verktøygrupper*** er det vist en oversikt over trusselnivåene i kategorien kriminalitet, med en forenklet beskrivelse av typisk aktør og hvilke verktøygrupper det kan forventes at trusselaktørene behersker. Det legges til grunn at en profesjonell trusselaktør har tilgang til mer avansert verktøy og har mer kunnskap og erfaring i effektiv bruk av verktøyene enn en mindre avansert aktør. En fysisk barriere vil derfor normalt ha kortere innbruddstid for et høyere trusselnivå enn et lavere trusselnivå.

Sikringsklasser er endret i den nye Sikringshåndboka i forhold til tidligere. Dette gjelder både for «motstandsnivåene» som sikringsklassene representerer, samt endringer for innbruddstid.

I ny sikringstabell er sikringsklasser opp til og med sikringsklasse SK6 tilordnet nivåene RC1 til RC6 i NS-EN 1627. Høyere sikringsklasser enn SK6 relateres til hvelvklasser iht. NS-EN 1143-1, da NS-EN 1630 ikke spesifiserer innbruddstester for trusselnivå Charlie og Delta.

Tilordningen av motstandsnivåer for sikrings-

Motstandsklasser i NS-EN 1627

Forenklet kan vi si at det er følgende relasjon mellom motstandsklasser i NS-EN 1627 og sikringsklasse og trusselnivå i sikringstabellen

Motstandsklasse iht. NS-EN 1627	Sikringsklasse og trusselnivå i Sikringshåndboka
RC3	SK3 /Alfa
RC4	SK4/Bravo
RC5	SK5/Bravo
RC6	SK6/Bravo

Sikringsklasser med innbruddstider – fysisk sikring

2016	Trusselaktør				Sikringsklasser i Sikringshåndboka 2005
	A	B	C	D	
1	5 minutter*	1 minutt*	1 minutt*	Oppgis ikke	–
2	10 minutter	5 minutter	3 minutter	Oppgis ikke	–
3	15 minutter	10 minutter	5 minutter	Oppgis ikke	1
4	30 minutter	20 minutter	15 minutter	Oppgis ikke	2
5	90 minutter	30 minutter	20 minutter	Oppgis ikke	3
6	**	50 minutter	Oppgis ikke	Oppgis ikke	4 og 5
7	**	Oppgis ikke	Oppgis ikke	Oppgis ikke	6 og 7
8	**	**	Oppgis ikke	Oppgis ikke	8

* Det er svært korte innbruddstider for sikringsklasse 1, og det er vanskelig å definere noen eksakt tid.
** Det er lite trolig at en inntrenger i denne kategorien med verktøy som beskrevet for aktuell kategori, vil klare å forsere sikringstiltakene innen rimelig tid.

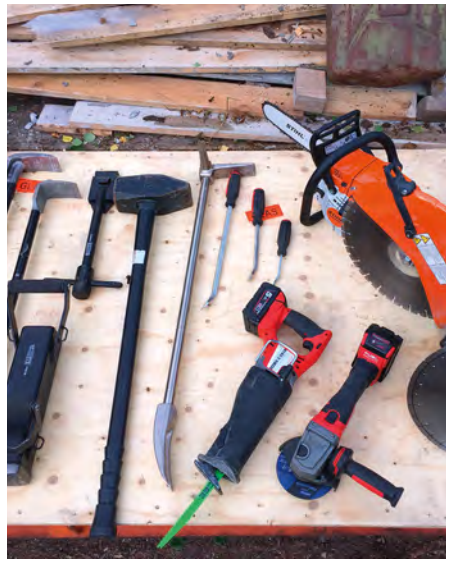
klassene mot klasser i innbruddstandarder, gjør det enklere å anskaffe sikkerhetsprodukter med ønsket motstandsnivå. Sikringsklassen som barrieren skal tilfredsstille, forteller direkte hvilken motstandsklasse produktet skal være klassifisert med. Det er fornuftig å stille krav om at sikkerhetsprodukter skal være klassifisert i ønsket motstandsklasse iht. NS-EN 1627, for å ha kontroll på at produktet som leveres i prosjektet, vil representere en fysisk barriere som gir forventet motstandstid ved inntrengningsforsøk. Klassifisering av sikkerhetsprodukt etter NS-EN 1627 innebærer at produktet er underlagt prøvningsmetodene i serien NS-EN 1628, NS-EN 1629 og NS-EN 1630. De to førstnevnte prøvningsstandardene spesifiserer prøvningsmetoder for henholdsvis bestemmelse av motstand under statisk belastning og dynamisk belastning. NS-EN 1630 spesifiserer prøvningsmetode for bestemmelse av motstand mot manuelle innbruddsforsøk.

For plassbygde konstruksjonskomponenter som ikke kan kjøpes som klassifiserte produkter, gir sikringstabellene til Sikringshåndboka preaksepterte løsninger for de ulike sikringsklassene.

Innbruddstider

Innbruddstid og holdetid angis i minutter, og viser til antall minutter det tar for en definert trusselaktør å trenge seg gjennom en barriere, det være seg vegger, dører, gulv og så videre. Ved manuelle innbruddsforsøk etter NS-EN 1630 måles innbruddstid både som motstandstid (effektiv verktøytid) og angrepstid,[5] som representerer tiden det tar fra angrepet starter, til trusselaktøren har tatt seg gjennom barrieren.

I Sikringshåndboka vurderer vi både verktøytid og angrepstid for trusselnivåer til sikringsklassene. Dette er endret fra forrige utgave av Sikringshåndboka, som benyttet rene verktøytider. For nivå Alfa og Bravo ligger innbruddstiden nærmere angrepstid enn verktøytid. Når det gjelder nivå Charlie og Delta, er de estimerte tidene i tabellen nærmere verktøytid. Et argument for å benytte angrepstider i et tidsregnskap for samlet innbruddstid er at aktørene skilles fra hverandre også når det gjelder kapasitet utover spesifisert verktøy. Sikringstabellen ***Sikringsklasser med innbruddstider*** viser estimerte angrepstider for kombinasjon av sikringsklasse og trusselnivå.



Innbruddsverktøy brukt under testing utført av Forsvarsbygg for å bestemme realistiske innbruddstider for komponentene som testes.

FOTO Forsvarsbygg

Innbruddstesting

Forsvarsbygg utfører manuelle inntrengningsforsøk på forsterkede bygningskomponenter og sertifiserte sikkerhetsprodukter, for å bestemme realistiske innbruddstider relatert til alle kombinasjoner av sikringsklasse og trusselnivå. Innbruddsforsøkene som gjennomføres av Forsvarsbygg, er realistiske uten de samme begrensninger som man kan finne i prøvningsstandarder for innbruddsikkerhet.[6] Forsvarsbygg gjør også andre vurderinger relatert til sikringsklasse og trusselnivå som tas hensyn til i innbruddstidene. For høyere trusselnivå benytter Forsvarsbygg et utvidet sett av innbruddsverktøy for å fastsette innbruddstider.

5

Maksimal total prøvetid i NS-EN 1630 er definert som summen av motstandstid, hviletid, tid brukt på verktøybytte og observasjonstid

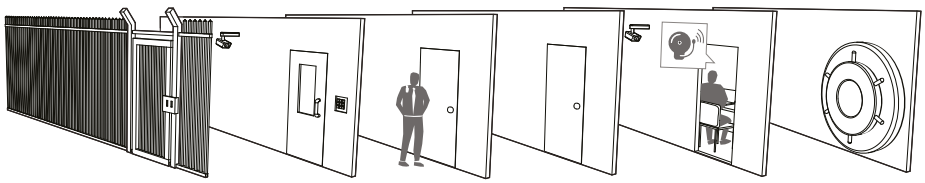
6

Eksempler: Innbruddsprøvning av et P6B etter NS-EN 356 skjer med f.eks. en øksemaskin for å teste innbruddssikkerhet. Forsvarsbygg vil teste glasset med en helt annen metode for å bestemme innbruddstid. Et annet eksempel kan være at Forsvarsbygg tillater bruk av diamantblad på vinkelsliper i en innbruddstest, selv om dette ikke tillates ved innbruddsforsøk etter NS-EN 1630

Test av dører utført av Forsvarsbygg for å bestemme realistiske innbruddstider.

FOTO Forsvarsbygg

Flere typer sikringsdører i kombinasjon



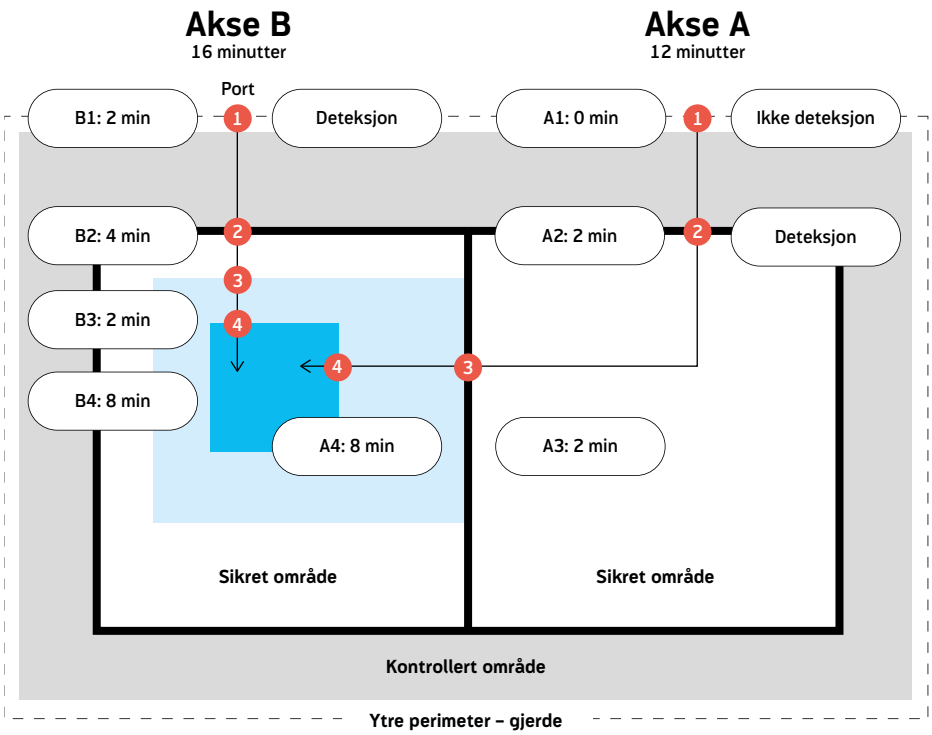
En sammenligning av maksimale totale prøvningstider i NS-EN 1627 for RC3 til og med RC6 og estimerte angrepstider for tilsvarende kombinasjon av sikringsklasse og trusselnivå, viser at Sikringshåndbokas estimerte angrepstider er noe kortere. Dette kan forklares ved at Forsvarsbygg har åpnet for mer variasjon i innbruddsverktøy.

Bildene viser verktøy og manuell innbruddstesting som utføres av Forsvarsbygg for å bestemme realistiske innbruddstider for komponentene som testes.

Balansert sikring

Sikringsklasser beskriver kun kvaliteten på den enkelte barriere. Det er summen av alle barrierene som eventuelt gir balansert sikring. Effektiviteten av de eksisterende sikringstiltakene

Holdetid for to ulike akser inn til samme verdi



HOLDETID A:

A-1	0 (mindre enn 1 min.)
A-2 (Deteksjon)	2 min.
A-3	2 min.
A-4	8 min.
Sum innbruddstid	12 min.
Sum reaksjonstid	10 min.

HOLDETID B:

B-1 (Deteksjon)	2 min.
B-2	4 min.
B-3	2 min.
B-4	8 min.
Sum innbruddstid	16 min.
Sum reaksjonstid	14 min.

kan vurderes ved hjelp av et tidsregnskap, som beskrevet i ***kapittel 2, Sikringsteori.***

Det optimale er å ha flere ulike barrierer mellom ytre perimeter og verdien som skal beskyttes. Når tidsregnskapet skal settes opp, vil både antallet barrierer og hvilke sikringsklasser de tilhører, ha betydning for resultatet. Dette innebærer at flere lag med lavere sikringsklasser kan gi samme resultat i et tidsregnskap som én barriere med høyere sikringsklasse.

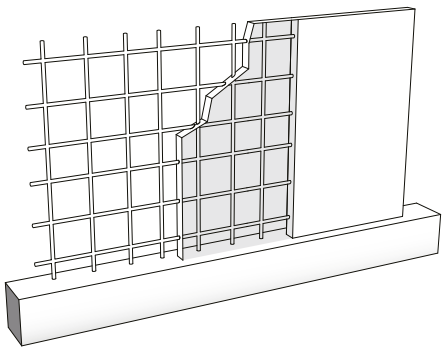
I en bygning vil det ofte være flere veier (akser) inn til verdien. Den samlede holdetiden til de fysiske barrierene i hver av aksene inn til verdien skal beregnes. Tidsregnskapet bør vurderes årlig, slik at eventuelle endringer i barrierer og motstandskraft kan fanges opp.

Vegger, gulv, etasjeskiller og tak

Bygningens yttervegg representerer den første bygningsmessige barrieren en trusselaktør må forsere for å komme inn til verdiene. Typiske *yttervegger* kan for eksempel bestå av stenderverk, betong, lettklinker (Leca), sandwichelementer, eller andre typer konstruksjoner med tre-, tegl- eller metallkledning. Innendørs skiller man i hovedsak mellom *lette innervegger* som modulbaserte kontorvegger og plassbyggede gipsvegger, og *tunge innervegger* som ulike typer betongvegger, lecavegger og teglsteinsvegger.

Sikringsvegger er vegger som er konstruert for å motstå en gitt trussel eller uønsket handling. Disse kan enten være massive vegger av betong, lettklinker eller teglstein, eller såkalte

Vegg utført i armert betong

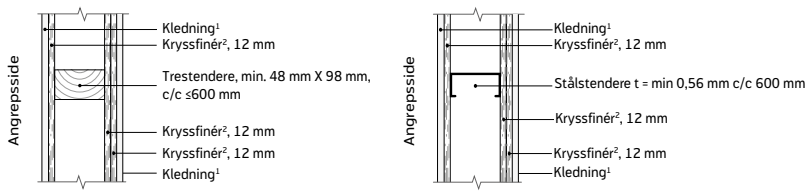
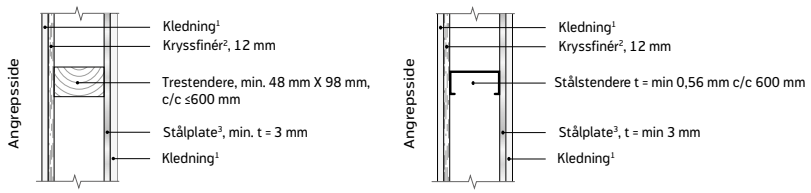
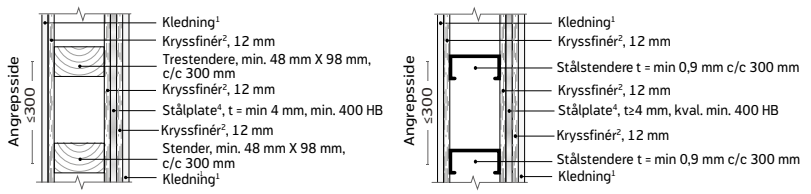
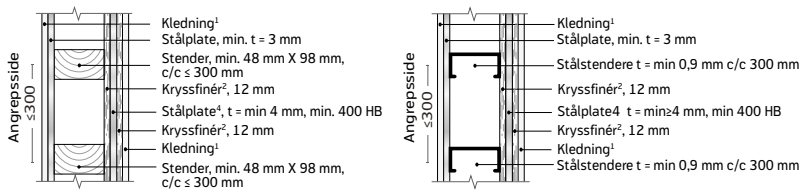


Sikringsklasser for massive vegger, tak/gulv

Sikringsklasse	Massive vegger	Tak/gulv/etasjeskiller
1	→ Udefinert yttervegg	→ Tak, gulv, dekker, etasjeskiller skal ha minst samme innbruddsmotstand som vegger. Det er vanligvis minst like god motstandskraft i ordinære etasjeskiller som i veggene opp til klasse 3 (med mindre det er snakk om et trehus). Fra klasse 4 og oppover bør man vurdere forsterkning også av etasjeskiller.
2	→ 150 mm massiv lettklinker utført og armert etter produsentens anvisning.	
3	→ 250 mm lettklinker utført og armert etter produsentens anvisning.	
4	→ 150 mm enkeltarmert*	
5	→ 180 mm dobbeltarmert*	
6	→ 200 mm dobbeltarmert betong*	
7	→ 300 mm dobbeltarmert betong*	
8	→ 500 mm dobbeltarmert betong*	

* Min. betongkvalitet B30, maks. 150 mm senteravstand for armering.

Sikringsklasser for sammensatte vegger

Sikringsklasse	Sammensatte vegger	Tak/gulv/etasje-skiller
1	→ Ikke spesifisert. SK 3 kan benyttes.	Tak, gulv, dekker, etasjeskiller skal ha minst samme innbruddsmotstand som vegger.
2	→ Ikke spesifisert. SK 3 kan benyttes.	
3		
4		
5		
6		
7	→ Ikke spesifisert. Prosjekteres særskilt.	
8	→ Ikke spesifisert. Prosjekteres særskilt.	

1. F.eks. 12 mm gips eller sponplate. Innfestet iht. Byggforsk/produsentens anvisning
2. Innfestet iht. Byggforsk/produsentens anvisning
3. Innfestet med min. 4 mm skruer c/c t ≤ 200 mm
4. Innfestet med min. 4 mm skruer c/c t ≤ 200 mm i både tre- og stålstendere
5. Samlet tykkelse, f.eks. 22 mm + 12 mm

Test av sikkerhetsglass.

FOTO Forsvarsbygg

sammensatte vegger. Sammensatte vegger består av flere sjikt med forskjellig evne til å motstå gjennomtrengning. Slike vegger kan bestå av en rekke ulike materialer, for eksempel stenderverk, kryssfinerflater, plastmaterialer, stålplater, høyfaste stålplater, eller aluminium.

Ved etablering av sikringstiltak i eksisterende lokaler må man først og fremst vurdere kvaliteten på vegger, etasjeskiller og takkonstruksjoner. Deretter kan man enten rive eksisterende konstruksjoner og sette opp nytt eller forsterke det eksisterende fra inn- eller utsiden.

Tabell Sikringsklasser massive vegger viser sikringsklasser for vegger, gulv og tak. Ofte skal en og samme konstruksjon ivareta krav til bæreevne, varmeisolasjon, akustikk, brann og byggbarhet i tillegg til innbruddskrav. I slike tilfeller må konstruksjonen prosjekteres særskilt for å oppfylle samtlige krav på en mest mulig kosteffektiv måte.

Rom for oppbevaring av KONFIDENSIELL informasjon etableres innenfor beskyttet område, og det stilles krav til utførelse av vegger, dører, vinduer, åpninger og dekker (minimum SK 3-4). Rom for oppbevaring av HEMMELIG informasjon utføres som hvelv i minimum klasse 2 i henhold til NS-EN 1143-1, alternativt plassbygde vegger i form av armert betong eller ulike typer sammensatte vegger (minimum SK 5).[7]

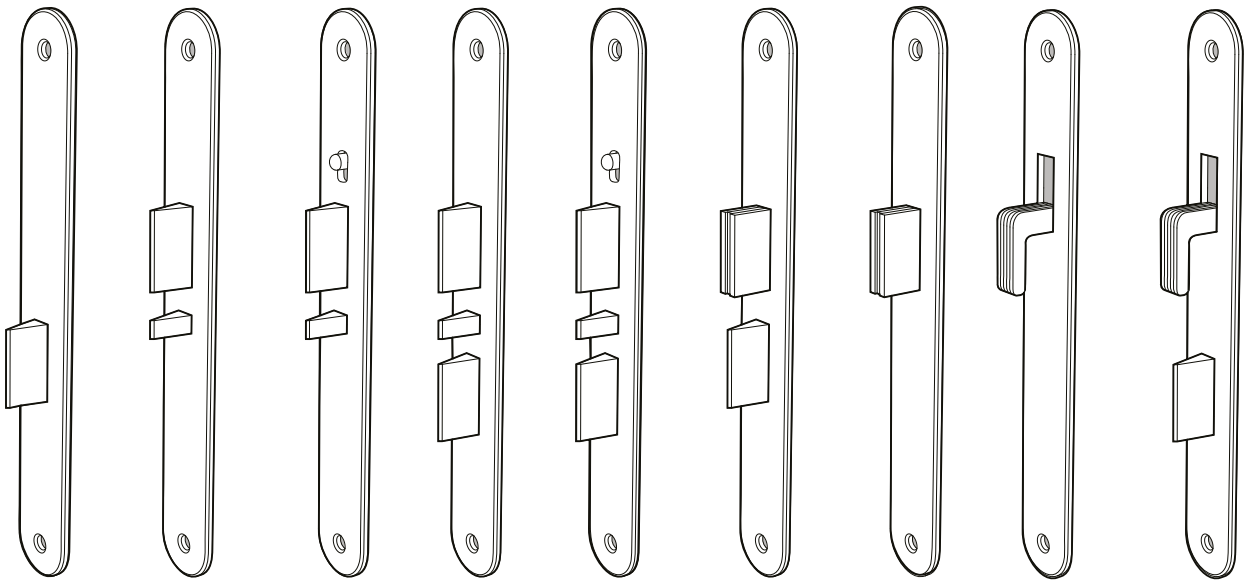
Dører og dørmiljø

Et *dørmiljø* er en fellesbetegnelse på «alt som har med døren å gjøre». Dette inkluderer dørblad, karm, innfesting, lås og beslag, samt eventuell styring i form av dørautomatikk – herunder adgangskontroll og alarmsystemer. Fra et sikringsperspektiv er det viktig å betrakte dørmiljøet samlet og helhetlig.

Det er viktig å være klar over at ett dørprodukt ikke vil tilfredsstille alle typer barrierefunksjoner. Det kan derfor være hensiktsmessig å bruke flere typer sikkerhetsdører i kombinasjon

7 Jf. informasjonssikkerhetsforskriften §6-8 og NSMs Veiledning til forskrift om informasjonssikkerhet

Ulike låstyper



1 Lås med vriderfalle

2 Fallelås med vrider og sylinderfalle

3 Fallelås med vrider, sylinderfalle og oppestillingsbryter

4 Tofallelås med sylinder og vriderfalle

5 Tofallelås med vrider, sylinderfalle og oppestillingsbryter

6 Reilelås med falle

7 Reilelås

8 Hakereilelås

9 Hakereilelås med falle

for å ivareta alle nødvendige barrierefunksjoner i skall- og dybdesikringen.

Eksempel på egenskaper som krever dokumentasjon av funksjon og ytelseskrav, er: brannmotstand, røyktetthet, rømningsfunksjon, lydisolasjon, isolasjonsverdi, innbruddsmotstand, eksplosjonsmotstand, gasstetting, beskytningsmotstand og brukervennlighet.

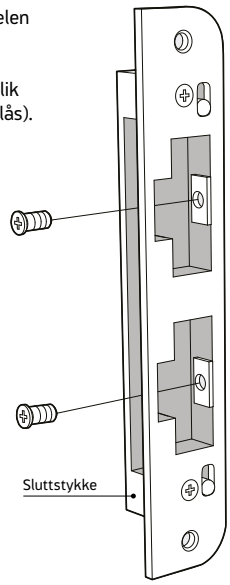
Innsetting av sikkerhetsdører i høye sikringsklasser vil gjerne kreve bruk av konstruksjonsstål eller tilsvarende forsterkning for innfestning av karmer. Slagretningen på dører må være i henhold til dørens godkjenning. Materialer, innfestning, veggen rundt og innfestingsmargin er viktige elementer for dører som skal dimensjoneres for eksplosjonslaster. For øvrig henvises det til produsentenes monteringsanvisning.

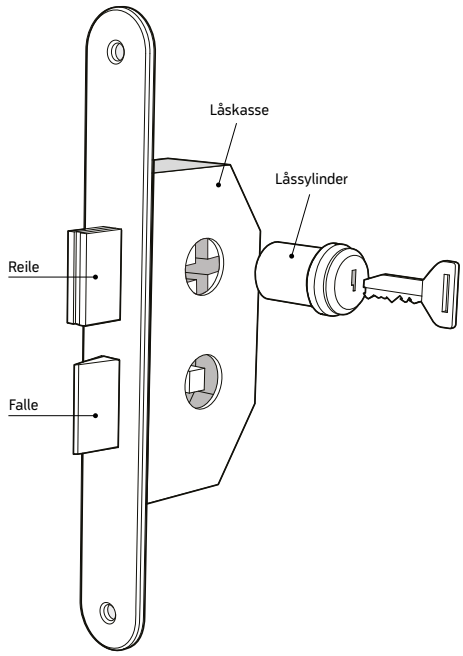
I en byggesak skal det dokumenteres at de tekniske løsningene som er valgt, tilfredsstiller de funksjons- og ytelsesklasser som er forutsatt. Sikkerhetsdører kan ha flere barrierefunksjoner, og det må dokumenteres at produktet er testet og godkjent for alle de aktuelle funksjons- og ytelsesklassene iht. relevante standarder.

Det er viktig å være bevisst på at lyddører og andre sikkerhetsdører krever forsterkninger av veggen rundt døråpningen. Dersom det monteres relativt tunge dører i en lett vegg uten forsterkning, fører dette til vibrasjon av veggen hver gang døren åpnes og lukkes. Dette med-

Låsenhet

Reilelås med falle.
Reile: rettvinklet fremkant som nøkkelen fører ut av stolpen.
Falle: Fjærbelastet med skrå fremkant (lik gammeldags smekklås).





fører igjen problemer med at låser ikke går i lås, utløsning av døralarm, hyppig behov for vedlikehold, misfornøyde leietagere osv. Det er også viktig å være oppmerksom på utfordringer når sikkerhetsdører kombineres med andre krav, slik som krav om lyddemping, varmeisolasjon, brann mv.

Det vil ofte være enkelt å forsere *ordinære dører* for trusselaktører selv på det minst avanserte nivået. Tradisjonelle tredører finnes som massive dører, fyllingsdører og lette dører. Massive tredører vil kunne yte noe motstand i selve dørbladet, men mangler ofte både bakkantsikring og sikkerhetslås. Ordinære ståldører består vanligvis av tynt falset stål, og er som regel isolert. Standarddører kan også være laget av aluminium og plast.

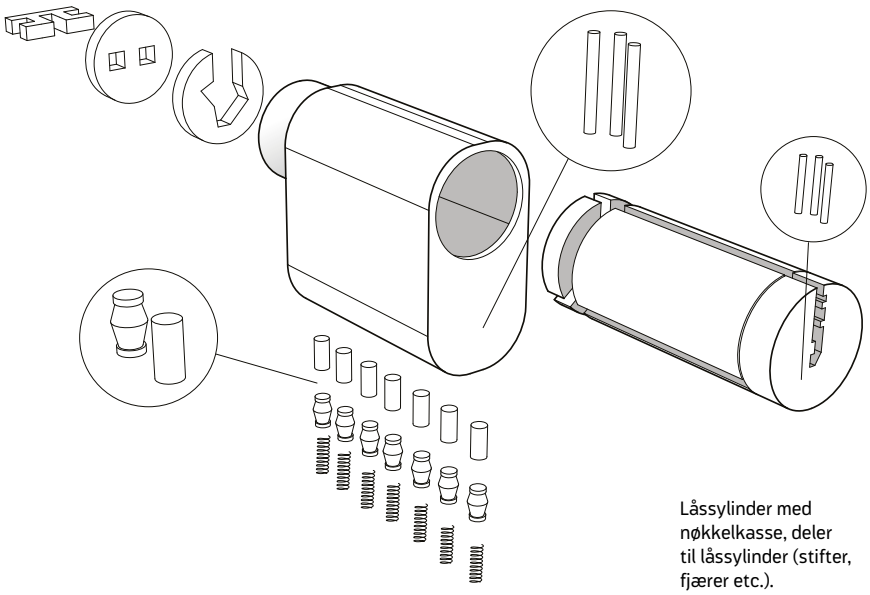
Dører av høy kvalitet kan ha egenskaper som gjør det mulig å oppgradere/forsterke dem slik at de kan kategoriseres som sikringsdører med lav motstand/lav sikringsklasse. Det finnes ulike tiltak som kan gjennomføres for å oppgradere en ordinær dør til sikringsklasse 1 eller 2, men husk at forsterkning av dører skal vurderes av kvalifisert personell. Som tidligere nevnt må døren betraktes som en enhet; innfesting og innfestingsmaterialet er like viktig som dørelementene selv.

Følgende elementer kan benyttes:

- → *Bakkantbeslag*
- → *Hengsler*
- → *Bommer og slåer*
- → *Ulike typer beslag*
- → *Låsenheter*
- → *Oppkiling/forsterkning av karmer*
- → *Forsterkning av dørblad, for eksempel med stålplater, kryssfiner etc.*

Kommersielt tilgjengelige sikringsdører er produsert og godkjent gjennom standarder.

Låssylinder



Låssylinder med nøkkelkasse, deler til låssylinder (stifter, fjærer etc.).

Den gjeldende standarden for sikringsdører er NS-EN 1627:2011. I tillegg finnes den eldre standarden NS 3170, men denne ble tilbaketrukket i 2011. Videre finnes mer spesialiserte standarder, som NS-EN 1143-1 for hvelvdører og NS-EN 356 for sikkerhetsglass.

Sikringsdører kan være uhensiktsmessige i hverdagen på grunn av tyngden, antall låser eller type låser. Disse elementene kan representere en utfordring når det gjelder å tilfredsstille krav til rømningsveier. I bygg med særlig tunge sikkerhetsdører skal det vurderes bruk av egne dagdører og klassifisering av disse. Dagdører er lettdører som kan plasseres innen- eller utenfor en sikkerhetsdør. Eksempelvis kan sikkerhetsdøren stå åpen når det er ansatte til stede, mens dagdøren fungerer som adgangskontroll med AAK og forsterket lås.

Ved bruk av sikkerhetsdører i kombinasjon med AAK vil det ofte være et krav til elektromekaniske låser av typen motorlåser eller motorsluttstykker. Noen av disse låsene kan åpnes noe tregere enn vanlige låser, men vil ikke gi mer enn ett sekunds forsinkelse ved dørpassering. Disse låstypene er i tillegg relativt utsatt for slitasje, og bør derfor ikke benyttes ved hyppig bruk. Et alternativ kan være å installere en egen daglås i døren.

Det skal ikke være bruk av glass i dører hvor det kreves sikringsklasse 5 eller høyere. Der det er krav til sikringsdører, skal dører velges i henhold til klassifisering og godkjenning. Oppgradering av eksisterende dører for å tilfredsstille høyere sikringskrav anbefales ikke, da ettermontering ofte vil svekke opprinnelig konstruksjon. Ettermontering av lås og beslag skal utføres på en slik måte at døren ikke svekkes i forhold til den klassen døra er godkjent i.

Sikringsklasser for dører

Direkte sammenligning av standarder er vanskelig da det benyttes ulike testmeto-

Sikringsklasser for dører og glass i dører

Sikringsklasse	NS-EN 1627: 2011 Gjeldende standard	NS-EN 3170: 1992 Utgått standard	NS-EN 1143-1:2012 Gjeldende standard	NS-EN 1627: 2011 Gjeldende standard
1	1	–	–	P6B
2	2	1	–	P7B
3	3	2	–	P8B
4	4	3	–	
5	5	4	I–II	–
6	6	–	II–IV	–
7	–	–	V–VI	–
8	–	–	VII	–

Merk at det er her er stilt strengere krav til klasse på glasset enn det som følger av standarden NS-EN 1627. Dette er begrunnet i tester gjennomført av Forsvarsbygg.

der og krav i de ulike standardene. ***Tabellen Sikringsklasser for dører og glass i dører*** viser sikringsklasser for dører og glass i henhold til de ulike standardene som er nevnt over.

Branndører er definert i plan- og bygningsloven som dør som etter klassifisering er offentlig godkjent som tilfredsstillende i henhold til branntekniske krav. Slike dører finnes i mange materialer.

Moderne branndører angis med tall og bokstaver. Tallene angir hvor mange minutter døren står mot gjennombrenning. Bokstavene neden-

Låsdeler og funksjoner

Låsdel	Funksjon
Stengeanordning (SA)	→ Bevegelig anordning som går gjennom stolpen og inn i sluttstykket.
Stolpe	→ Feste- og styreplate i fremkant av låskassen med hull for SA.
Låskasse	→ Kasse eller plate med låsdeler, deksel og stolpe montert.
Sluttstykke	→ Tilbehør (beslag) med hull for stengeanordning. Er låskassen montert på døren, monteres tilhørende sluttstykke på karmen.
Reile	→ En stengeanordning med rettvinklet fremkant som nøkkelen fører ut av stolpen.
Falle	→ Fjærbelastet stengeanordning med skrå fremkant (ref. gammeldags smekklås).
Hakereile	→ Reile formet som en krok som dreies ut av stolpen og hekter seg på et mothold i sluttstykket.
Skilt	→ Plate som beskytter vrider og låsetøy.
Sikkerhetsskilt	→ Som skilt, men spesifikke krav til kvalitet og montering gjelder.
Knappvrider	→ Åpner døren fra innsiden uten bruk av nøkkel. Kan erstatte betjening med nøkkel fra innsiden.
Låsenhet	→ Består av låskasse, sluttstykke, sylindre, sylinderskilt med bolter, alt av definert godkjent kvalitet.

for brukes om konstruksjonen og har følgende betydning:

- → **E** *for evnen til å tåle brann (Integritet). I integritet ligger det at bygningsdelen må være så tett at brann ikke smitter gjennom*
- → **I** *for varmeisolasjonen. Isolasjon betyr at brannen ikke skal kunne overføres til baksiden ved varmegjennomgang*
- → **C** *for selvlukkende effekt (en tilleggs-betegnelse dersom døren har selvlukkende utstyr)*
- → **S** *for røyktett konstruksjon (dersom døren har røyktettende listverk)*
- → **W** *for motstand mot varmestråling (kun helt spesielle dører)*
- → ***HENVISNING:*** *Henvisning til definisjon av disse bokstavene EN 13501-2*

Eldre utgaver er merket på karmsiden av dørbladet med et rødt merke med en kode med bokstavene A eller B og et tall. Bokstavene angir om døren er laget av ubrennbart (A) eller brennbart (B) materiale. Bokstaven F angir at det er glassfelt i døren.

Lyddempende dører er merket med gult på kanten av dørbladet mot hengselsiden. Mer-

Utvalgte låstyper med definisjon

Låstype	Definisjon
Lås	→ Stengeinnretning med én eller flere stengeanordninger. Minst én stengeanordning skal manøvreres med nøkkel eller annen anordning.
Symmetrisk lås	→ Låsen betjenes fra begge sider med samme nøkkel. Kan også bety låskasse som er beregnet for symmetrisk utfresing i dør.
Usymmetrisk lås	→ Låsen betjenes ensidig, eller fra begge sider med forskjellige nøkler.
Tilholderlås	→ Nøkkelen må manøvrere plater (tilholdere) i låsen under omdreining. Nøkkelen likner en avansert utgave av en vanlig innendørslås.
Sylinderlås	→ Nøkkelen vrir en sylinder inne i låsen når den dreies om. Sylinderen sperres av små stifter, plater eller skiver som nøkkelen må bevege.
Kodelås	→ Dreibare skiver må dreies med en tallskive til en spesiell stilling (mekanisk kodelås). Finnes også i elektronisk versjon.
Kortlås	→ Kortet som betjener låsen, kan være elektronisk, magnetisk, ha hull eller informasjon som er trykket eller preget. Nøkkel skal kunne anvendes.
HENGELÅS	→ Låsen har en bøyle som skal kunne åpnes og lukkes i låsfestet.

kingen er gul og angir Rw-tallet, som betegner demping av laboratoriemålt luftlyd. Du kan få enkeltdører med demping opp til 45 dB. Slike dører er som regel tunge og tette.

EMP-dempende dører er som regel metalliske og demper stråling fra mange kilder og bølgelengder. Dette er svært spesialiserte dører. Betegnelsene varierer etter behovet.

Skuddhemmende dører er dører med motstand mot beskytning. Disse klassifiseres og prøves i henhold til NS-EN 1522. Standarden spesifiserer syv motstandsklasser som betegnes fra FB1 til FB7. For mer om våpenvirkning på dører se ***kapittel 16, Beskyttelse mot eksplosjoner*** og ***kapittel 17, Beskytning.***

Gasstette dører betegnes som GD og finnes i mange tykkelser. Dette er som regel tradisjonelle tilfluktsromsdører produsert etter norm fra Sivilforsvaret eller Direktoratet for samfunnssikkerhet og beredskap (DSB). I tillegg kan enkelte laboratoriedører produseres som gasstette.

Tilfluktsromsdører er i utgangspunktet ikke egnet som sikringsdører, men kan oppgraderes. Med tanke på redningsoperasjoner er disse dørene konstruert for å kunne åpnes fra utsiden ved hjelp av jekk, spett eller lignende. Skal slike dører ha en sikringsfunksjon, må de modifiseres slik at enkel åpning utenfra ikke er mulig. Kvalifisert personell kan vurdere om en slik dør tilfredsstiller en sikringsklasse.

Sikringsklasser for låsenheter

Sikringsklasse	Låser
0	→ Ingen krav til godkjente låsenheter.
1	→ FG-godkjent låsenhet. (Alle komponenter minimum FG-klasse 3)*
2	→ Godkjente låsenheter i FG-klasse 3 eller høyere.
3-8	→ Normalt krav knyttet til dør låsen skal stå i. Minimum låsenheter i FG-klasse 3.

* FG-310:1 (1.9.2012)

Sikringsklasser for innbruddshemmende vinduer

Sikringsklasse	NS-EN 1627: 2011 Gjeldende standard (minimumskrav)	NS-EN 356: 1999 Sikkerhetsglass (minimumskrav)
1	1	→ P6B
2	2	→ P7B
3	3	→ P8B
4	4	
5	5	→ Glass skal ikke benyttes i sikringsklasse 5–8
6	6	

For at vindu skal oppnå respektiv sikringsklasse, skal både minimumskrav i tabellen til RC-klasse iht. NS-EN 1627 og minimum klasse iht. NS-EN 356 for glass som oppgitt i tabellen, oppfylles. Merk at det er her stilt strengere krav til klasse på glasset enn det som følger av standarden NS-EN 1627. Dette er begrunnet i tester gjennomført av Forsvarsbygg.

Lås og hengelås

Det finnes et svært stort utvalg av låser og et enda større utvalg av beslag til ulike låser. Selv om det kan være utfordrende å skaffe oversikt over de ulike produktene i markedet, må virksomheten ha kunnskap om hvilke typer låser og beslag en har på dører i skallet og i andre dører med spesielle krav til sikring. Et velrenommert låsfirma kan befare virksomheten og utarbeide en tilstandsrapport over status på låser og beslag.

Ut fra et sikringsperspektiv finnes det to hovedtyper av låser: FG-godkjente låser og alle andre låser. FG[8] godkjenner låser etter omforente standarder i samarbeid med tilsvarende nordiske og europeiske organisasjoner. De godkjente låsene skal tilfredsstille visse fysiske krav til styrke og motstandsevne mot angrep fra en innbryter. En låsenhet som er sammensatt av komponenter som består av klasse 3 eller høyere iht FG-310:1,[9] skal omtales som FG-godkjent låsenhet. NSM er godkjenningsmyndighet for låser og hengelåser i henhold til sikkerhetsloven.

Sikkerhetsloven setter minimumskrav til bruk av låser. I tillegg kan ulike sektorer og virksomheter ha egne krav. Forsvarsbygg anbefaler generelt at alle dører i skallet og andre dører med spesielle krav til sikring skal ha minimum FG-godkjent låseanordning. En låsenhet består av flere deler, og ved FG-godkjenning omfatter vurderingen alle deler av låsenheten, og enkeltdeler kan ikke skiftes ut med deler som ikke er FG-godkjent. For å tilfredsstille FGs krav til avlåsning av en dør skal alle sikkerhetsdører ha bakkantbeslag. Bakkantbeslagene forhindrer at døra kan brytes opp ved å skjære over eller bryte opp hengslene.

Fallelåser er ikke FG-godkjent, men benyttes sammen med elektriske sluttstykker. Disse kan ikke benyttes der det er krav til låsenheten.

Reilelåser kan være FG-godkjent og benyttes for eksempel sammen med motorsluttstykker.

Hakereilelåser kan være FG-godkjent, og er vanligvis meget solide. På grunn av sin utforming blir låskassa sammenkoplet til sluttstykket, noe som vanskeliggjør oppbrytning.

Det kan være vanskelig å identifisere en FG-godkjent låsenhet uten god kunnskap om forskjellige låser og låsutstyr. Låskassen kan imidlertid identifiseres ved hjelp av et nummer som er preget inn i låskassens stolpe. På FGs nettsider finnes det liste over FG-godkjente låsekasser.

I dører hvor det ikke er en FG-godkjent lås, eller hvor det er krav til to godkjente låsenheter, kan en tilleggslås monteres. Tilleggslåsen skal monteres minst 40 cm over eller under hovedlåsen. Tilleggslåsen bør være en annen type lås enn hovedlåsen, i tråd med prinsippet om kombinasjon av sikringstiltak. Målet er å forsinke trusselaktøren ved at denne må ha økt kunnskap og benytte ulike verktøy for å forsere barrieren. Til sperret område HEMMELIG eller STRENGT HEMMELIG kreves to godkjente låsenheter, hvorav den ene kan være en FG-godkjent låsenhet, og den andre skal være en godkjent kombinasjonslås.[10]

Låser må fra tid til annen oppgraderes eller skiftes ut. Når man skal skifte låsetøy i en dør, bør det foretas en kvalifisert vurdering av døras sikkerhetsmessige egnethet etter utskiftingen. Dersom nye låser krever en ytterligere utfresing i døra og/eller karmen, kan det medføre en svekkelse i konstruksjonen. Det bør derfor vurderes å skifte hele døra. Ettermontering av låser vil kunne medføre svekkelser av døren og må derfor utføres av kvalifisert personell. Kombinasjonslås bør monteres på fabrikken når døren produseres.[11]

Sylinderlåser er den mest anvendte låstypen, og de kan være svært avanserte. En sylinderlås har normalt en stiftrekke med 6–7 stiftkamre.

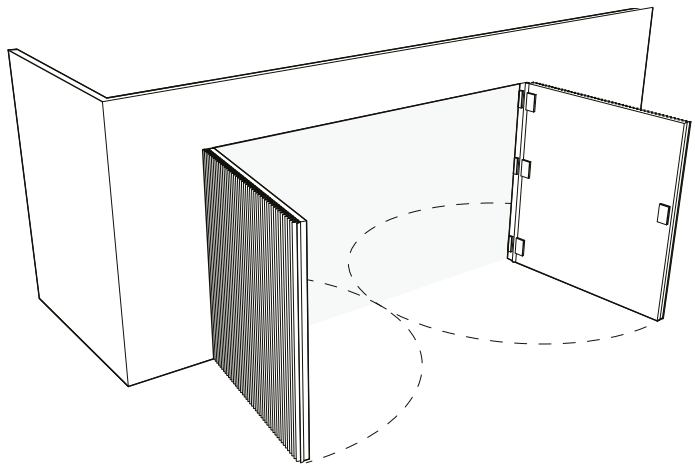
8
Se FGs nettsider for regler for FG-godkjent lås og beslag
www.fg.no

9
Se FGs nettsider for regler for FG-godkjent lås og beslag
www.fg.no

10
For mer informasjon se NSMs veiledning i «Fysisk sikring mot ulovlig inntrengning»
www.nms.no

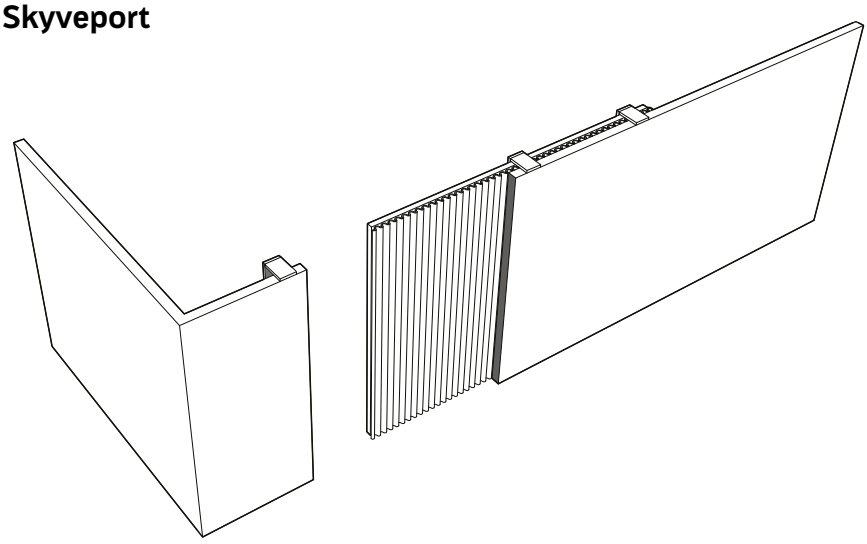
11
Se NSMs Veiledning til forskrift om informasjonssikkerhet kapittel 6: «Fysisk sikring mot ulovlig inntrenging» på
www.nms.stat.no

Slagport



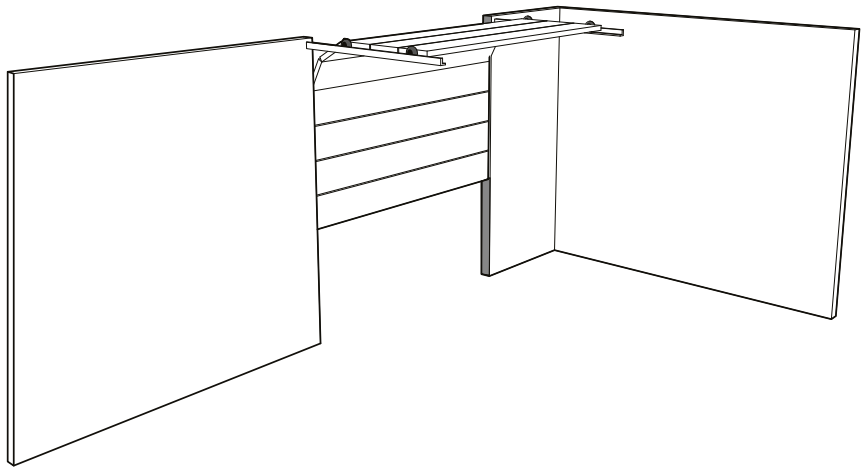
Slagporter kan være både kjøretøysporter og gangporter. Slagporter er hengslet på én side, og åpnes ved å svinge porten om sidehengsler. Portens konstruksjon og portstolpenes fundamentering bestemmer hvor lang en slagport kan være. De fleste leverandører kan levere porter opp til ca. 4-5 meters bredde. For kjøretøysporter vil det ofte være mest praktisk å benytte en to-fløyet port for å oppnå ønsket bredde på åpningen. Portbladet er vanligvis bygd opp av varmeforsinkede stålprofiler med platekledning på hver side. Mellomrommet kan være isolert med mineralull eller polyuretanskum. Slagporter leveres også som kjøretøysperrer.

Skyveport



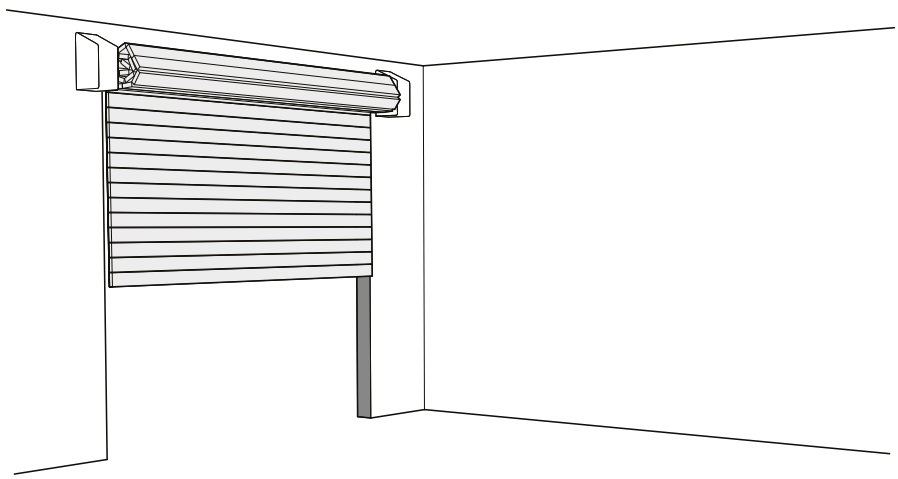
Skyveporter kan som slagportene være rent mekaniske eller motoriserte, men de åpnes ved at portdøren føres parallelt med gjerdet i stedet for å svinge ut eller inn. Dette gjør skyveporter mer anvendelige på steder hvor det er lite plass på inn- eller utsiden av porten. Skyveportene er oftest frittbærende, det vil si at de ikke har noen kontakt med underlaget i selve portåpningen, men de kan også føres langs en skinne nedfelt i bakken. Skyveporter leveres også som kjøretøysperrer.

Leddheiseport



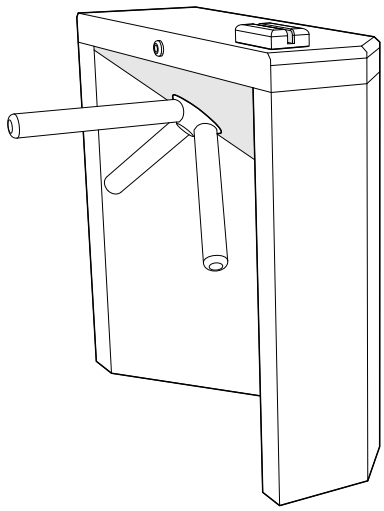
Leddheiseporter forbindes med tradisjonelle porter til garasje og lager, og kan åpnes både manuelt eller med motorstyring. Portene leveres ofte i lette materialer som aluminium, og har gjerne glass for å slippe inn lys. Portene kan låses med hengelås fra innsiden eller ved hjelp av en reile som føres inn i skinnene. Vinduene er innfelt med gummilist rundt og kan lett vippes ut. Som tilleggssikring kan det benyttes rullegitter og kjøretøysperre. Det kan være vanskelig å få tak i porter som er godkjent over NS-EN 1627 klasse 4.

Rulleport



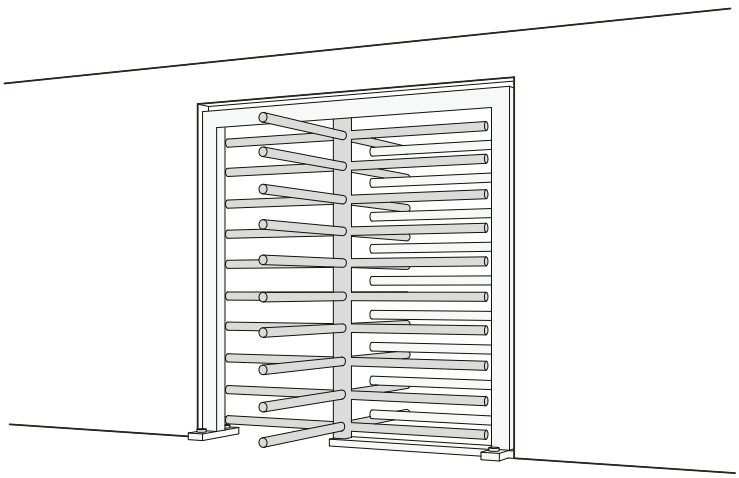
Rulleporter er vanligvis bygget opp av stålprofiler og har samme konstruksjon som rullegitter (se egen seksjon om gitter), men kan også leveres i dukmateriale. Rulleporter benyttes vanligvis der hvor leddheiseporter tar for mye plass. Som tilleggssikring kan det benyttes rullegitter og kjøretøysperre. Det finnes få slike porter som er testet etter NS-EN 1627.

Lav rotasjonsport



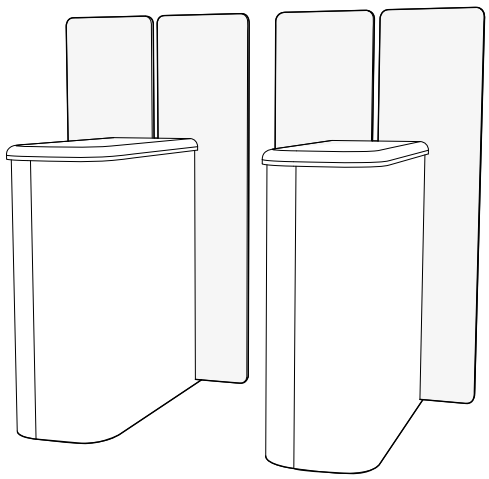
Lave rotasjonsporter eller dreiesperrer består vanligvis av tre glassvinger eller stålbommer som er montert symmetrisk på en roterende midtstolpe. I normalposisjon vil det alltid være en vinge/bom som sperrer for adgangen. Ved bruk av adgangskort og/eller -kode frigjøres porten/bommer og dreier slik at den slipper autorisert personell gjennom. Rundt glassvingene er det sperreanordninger som forhindrer passering.

Høy rotasjonsport



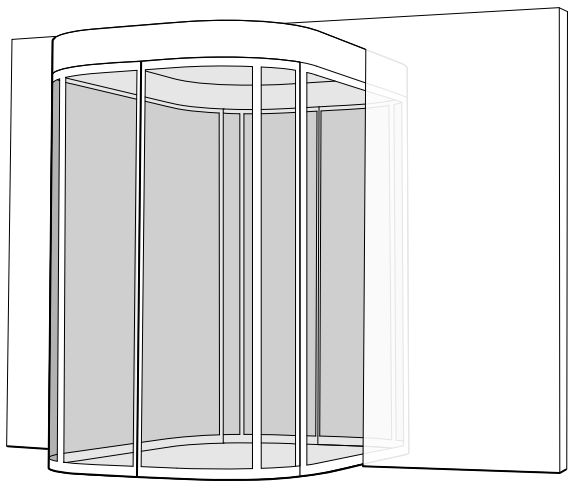
Med høye rotasjonsporter menes sperreanordninger som dekker hele åpningen mellom gulv og tak. Slike anordninger har en kontrollerende effekt, og kan normalt benyttes uten overvåkning. De høye rotasjonsportene består vanligvis av tre eller fire vinger som er montert symmetrisk på en roterende midtstolpe. Vingene kan bestå av en hel glassflate, spiler av pleksiglass, stålbommer eller lignende. I normalposisjon er det alltid en vinge som sperrer for adgangen.

Hurtigdør



Hurtigdører er normalt to glassdører. Ved bruk av adgangskort og/eller -kode vil døras mekanisme trekke dørene til siden, og slippe autorisert personell gjennom, før de igjen lukker seg bak vedkommende som passerer inn.

Sikkerhetssluse



Sikkerhetssluser har en unik egenskap som adgangskontroll: en dør må alltid være lukket før neste åpnes. Inngangsdøren åpnes med adgangskort og/eller -kode, slik at en person kan gå inn i slusen. Slike anordninger har i likhet med høye rotasjonsporter en god kontrollerende effekt.

De mest avanserte kan ha to rader, gjerne plassert i vinkel på hverandre. Noen er kombinert med elektroniske innretninger, men de omtales ikke her. Bruken av flere stifter i samme stiftkammer kan gjøre det mulig for forskjellige nøkler å betjene samme sylinderen. Dette utnyttes i følgende systemer:

Hovednøkkel: Vakten kommer inn på alle de 10 kontorene,

Gruppenøkkel: mens de to gruppesjefene bare kommer inn på sine 5 kontorer.

Individuell nøkkel: og kontoristene bare har nøkkel til eget kontor.

Nøkkeladministrasjon er avgjørende for sikkerheten og å ha god kontroll på låssystemet.[12] En nøkkel er en verdigjenstand på lik linje med verdiene den låser inn/ned.

Følgende regler kan brukes som et utgangspunkt for virksomhetens nøkkeladministrasjon:

- *Nøkler skal ikke settes igjen i nøkkelhull, eller ligge ubevoktet*
- *Nøkler, adgangskort og -koder som gir adgang til verdier utover de regulert av sikkerhetsloven med tilhørende forskrifter og veiledninger, skal gis samme grad av beskyttelse som kreves for verdiene de gir tilgang til*
- *Alle avdelingens nøkkelsystemer skal føres i et nøkkelregnskap, som viser antall produserte, eventuelt antall overtatte nøkler av hver type, beholdning på lager og en bok med utkvittering for hver enkelt utlevert nøkkel*
- *Nøkkelforvaltere/systemansvarlige er ansvarlige for ajourhold av låseplaner*
- *Ethvert utlån av nøkler utover fast tildeling skal føres i en egen nøkkelprotokoll*
- *Nøkler til viktige verdier eller funksjoner bør ha individuell nummerering*
- *Adgangskort til elektronisk adgangskontroll er å oppfatte som en nøkkel, og må av brukerne behandles på samme måte med hensyn til sikring og kontroll.*[13]
- *Nøkler skal til enhver tid være i ihendehavers varetekt*
- *Individuelt utleverte nøkler, adgangskort og -koder kan oppbevares under personlig kontroll. Avlåst privat bolig i bruk anses som under personlig kontroll. Det forutsettes imidlertid at nøkler og koder ikke er merket slik at verdioppbevaringsenheter eller steder kan identifiseres. Oppbevaring i kjøretøy eller lignende anses ikke som å være under personlig kontroll*

Hengelåser benyttes når det ikke er hensiktsmessig eller mulig med dørlåser. Bruksområdet for hengelåser er stort, og de benyttes med tilhørende beslag i samme klasse. Leverandørens beskrevne festemåter skal benyttes.

Vanlige bruksområder for hengelåser kan f.eks. være som ekstralås på dører, og ved avlåsing av kumlokk, lemmer og luker, forskjellige typer gitter osv. En hengelås kan brytes med skjære-, klippe- eller slagverktøy. For å oppnå tilstrekkelig motstandsdyktighet mot innbruddsverktøyene skal det benyttes beslag som dekker eller hindrer adkomst til hengelåsen. En hengelås skal leveres med tilhørende anbefalt beslag.

Porter

Porter i forbindelse med perimetersikring er omtalt i ***kapittel 10, Perimeter- og områdesikring***, mens dette kapitlet forholder seg hovedsakelig til porter som er en del av skallsikringen. Ved valg av porter er det flere forhold som må avklares. Det må blant annet tas hensyn til portenes funksjon, behov for sikring, portstyring, låsemuligheter og praktisk monterbarhet.[14] Porter kan spesiallages for å gi beskyttelse mot innbrudd, innsyn, eksplosjoner og beskytning. Det kan imidlertid være vanskelig å kombinere motstand mot f.eks. eksplosjoner og innbrudd, da materialvalg og

12 For mer informasjon se NSMs veiledning i «Fysisk sikring mot ulovlig inntrengning», nsm.stat.no

13 Jf. også kapittel om elektronisk sikring

14 For generelle valg av porter henvises det til byggforskblad 533.301 Valg av porter og portsystemer

Test av inntrengning gjennom skuddsikkert glass.

FOTO Forsvarsbygg

konstruksjon kan være forskjellig. Store, tette porter i solid stål som er riktig montert, kan imidlertid gi beskyttelse mot flere former for angrep.

For beskyttelse mot flertrinnsangrep er det nødvendig med både sikring i dybden og kombinasjon av ulike sikringstiltak. For eksempel kan man installere flere lag med porter som har forskjellige egenskaper. Noen porter leveres med glass for å slippe inn lys. Dette utgjør en sårbarhet, fordi de fleste vinduer kan knuses eller rett og slett vippes ut av listen de er montert i. Det er viktig å være klar over at porter ikke nødvendigvis har stor motstandsevne mot inntrengning. De må derfor kombineres med flere barrierer og eventuelt kjøretøysperrer for å oppnå hindrende effekt. De fleste porter kan leveres med motorstyring, og kan låses av med elektrisk lås, mekanisk lås, hengelås eller en kombinasjon av disse. Det er viktig å følge monteringsanvisning fra leverandør og sørge for skikkelig forankring av porten. Sikringsklasser for porter følger samme standard og krav som for dører.

Rotasjonsporter, dreiesperrer, hurtigdører og lignende er elektromekaniske innretninger konstruert for å regulere eller kontrollere adgangen slik at kun én person slipper inn av gangen. Portenes utforming, høyde og øvrig funksjonalitet avgjør i hvilken grad de har en regulerende

effekt, eller om de også har en kontrollerende effekt. Med regulerende effekt menes her at «folk flest» vil forholde seg til de restriksjonene som sperringen gir, mens det er fullt mulig å omgå reguleringen ved å forsere sperringen. Med kontrollerende effekt menes her at sperringen gjør det vanskelig å ta seg gjennom denne uten autorisasjon.

Rotasjonsporter, i særdeleshet de høye, vil kunne bidra til å gi et godt sikkerhetspreg. Lavere porttyper bør kun benyttes der de kan overvåkes av en resepsjonist, vakt eller lignende, og hvor det ikke er avgjørende viktig at uautorisert personell ikke slipper inn.

Ofte plasseres rotasjonsporter i et resepsjonsområde, innenfor selve resepsjonen. Plassering og funksjonene rundt rotasjonsportene må kartlegges og planlegges nøye. I spesielt sensitive områder inne i bygningen kan det installeres rotasjonsporter for å sikre kun autorisert adgang. Slike områder kan for eksempel være sperrede områder (i henhold til sikkerhetsloven). For noen virksomheter er adgangskontroll i inngangspartiet ikke mulig. I slike tilfeller kan det være formålstjenlig å etablere rotasjonsporter i et skille mellom åpen og kontrollert sone.

Bruk av rotasjonsporter er relativt uvanlig i Norge sammenlignet med resten av Europa. Det er derfor viktig å be potensielle leverandører om referanser på norske leveranser de har gjennomført. En rotasjonsport vil alltid være avhengig av regelmessig service, så leverandørens kompetanse, og ikke minst kapasitet, er av stor betydning.

Rotasjonsporter styres normalt av et adgangskontrollanlegg. For å sikre mest mulig problemfri drift og vedlikehold er det en stor fordel at samme leverandør har ansvar for AAK-anlegget og rotasjonsportene. På den måten unngår man uklarheter rundt ansvar for eventuelle driftsproblemer.

Det er viktig å kartlegge bruksmønster før detaljprosjektering av rotasjonsportene, slik at det anskaffes det antall og type porter som er nødvendig for god drift. Dette kan gjøres ved å telle antall inn- og utpasseringer om morgenen og på ettermiddagen, og i de tidsrommene med mest trafikk. Resultatet av tellingene bør være dimensjonerende for antall porter.

Vinduer og glass

Vinduer er ofte en mer sammensatt sikringsutfordring enn man antar, og alle elementer i vindusmiljøet må vurderes for å nå det sikringsnivået man ønsker. Dette inkluderer:

- → *Glasset*
- → *Ramme*
- → *Glassets innfesting til ramme*
- → *Karm*
- → *Hengsler, hasper o.l.*
- → *Karmens innfesting til vegg*
- → *Veggen rundt vinduet*

Vinduer, med alle de ovennevnte elementene, må vurderes som en enhet. Hele vindusmiljøet godkjennes iht. NS-EN 1627, og selve glasset godkjennes iht. NS-EN 356. Det kan være forvirrende at det ikke er samsvar mellom sikringsklassene i nevnte standarder. Vinduer iht. NS-EN 1627 klasse 1, skal ha glass iht. NS-EN 356 klasse P5A, vinduer i klasse 2 skal ha glass P6B, klasse 3 P7B og klasse 4 P8B. Det finnes en rekke produsenter av sikkerhetsglass. Glasset skal produseres etter standarden NS-EN 356 «Bygningsglass – Sikkerhetsruter – Prøving og klassifisering av motstand mot innbrudd og hærverk». Selv ved bruk av sikkerhetsglass i en fasade utgjør fremdeles vinduet det svakeste elementet i skallet. Derfor anbefales at det ikke brukes glass overhodet i sikringsklasse 5 og høyere.

En trusselaktør kan forsøke å fjerne glasset fra rammen eller bryte rammen fra karmen. For nye vinduer bør det derfor spesifiseres innbrudds-

Sikringsklasser for gitter

Sikringsklasse	Gitter
3	→ Alternativ 1: I henhold til EN 1627, klasse 3 → Alternativ 2: Maskevidde maks. 6 x 6 cm, minimum 10 mm rundjern eller tilsvarende. Skjøter skal være sveisede.
4	→ Alternativ 1: I henhold til EN 1627, klasse 4
5	→ I henhold til EN 1627, klasse 5
6	→ I henhold til EN 1627, klasse 6

klasse til vinduskomponenten iht. NS-EN 1627, og innfesting i vegg må gjøres etter vindusprodusentens anvisninger. Hvis innfestingen ikke er god nok, vil det være mulig å fjerne hele vinduet ved å sage av innfestingsboltene. For at vinduer og dører skal ha akseptabel sikring, er det viktig at innfestingsbolter tildekkes slik at de ikke er tilgjengelige fra utsiden. Innfesting kun ved hjelp av bygningsskum tillates ikke. Veggen rundt vinduet må ha samme motstandskraft som selve vinduet. Vær oppmerksom på at festet i veggen kan være et problemområde – spesielt i mur og betong.

Til syvende og sist er det viktig å ta det komplette vindussystemet i betraktning, og ikke enkeltproduktene hver for seg. Når et objekt skal sikres mot flere ulike typer trusler, må også vinduene være dimensjonert for å motstå de samme truslene (f.eks. innbrudd, beskytning, eksplosjon osv.).

Ordinære vinduer uten noen form for sikring representerer liten eller ingen innbruddshindring. De svakeste elementene i ordinære vinduer er hasper, kroker og andre beslag. For ordinære vinduer er det som regel ikke selve glasset som er mest sårbart, fordi en gjerningsmann ofte vil unngå å knuse det: Innbrudd gjennom glass kan bety mulig utløsing av alarm, inntrengerne kan skjære seg på glassplinter, og støy fra glassbrudd kan avsløre innbruddet. Å fjerne karmen kan dessuten være en enklere løsning dersom vinduet er festet dårlig inn i veggen. Er gjerningsmannen opptatt av ikke å etterlate spor, installerer han vinduet i veggen etter gjennomført innbrudd.

Det anbefales høyere standard på glass enn hva som anses tilstrekkelig etter NS-EN 1627 når det kommer til innbruddshemmende vinduer. Det betyr at mens EN 1627 tillater bruk av glass klasse P5A i sikringsklasse 2, anbefales det at glasset får klasse P7B på dette nivået.

Glass bestilles med tilleggskrav i henhold til ***Tabell Sikringsklasser for innbruddshemmende vinduer***.

Innbruddshemmende vinduer gis følgende kvaliteter i NS-EN 1627:

Det kan være flere årsaker til at man ikke ønsker å skifte ut vinduene i et bygg som skal sikres; kanskje er vinduene relativt nye eller bygningen har verneverdig status, eller kanskje er økonomien for trang. Da er alternativet (i tillegg til deteksjon og varsling) å forsterke de eksisterende vinduene mot utvalgte trusler:

- *Vinduet kan påføres innbruddshemmende film. En slik film gir imidlertid liten beskyttelse mot inntrengning, selv ved bruk av enkle verktøy. Mest aktuelt er det derfor å benytte denne typen film for å sikre seg mot vandalisme.*
- *Polykarbonat er et materiale som kan brukes i stedet for glass, som har egenskaper som gir en vis motstandsdyktighet overfor mekaniske belastninger. Polykarbonat alene er imidlertid ikke egnet som erstatning for glass i vinduer, og gir liten beskyttelse mot inntrengning, selv ved bruk av enkle verktøy. Polykarbonat er ikke ripebestandig (det kan altså lages riper i «glasset») og påvirkes av værforhold som fukt og lys. Polykarbonat kan brukes i tillegg til glass som en forsterkning på innsiden. Produktet brukes for øvrig som sjikt i noen typer laminatglass. Polykarbonat må ikke forveksles med pleksiglass.*
- *Gitter på innsiden av glasset gir god forsinkelse av innbruddstiden. Gitter brukes vanligvis på innsiden av glass som ikke har egen innbruddssikring.*[15]
- *Skodder montert på utsiden kan medføre en liten forsinkelse og kan derfor ha en viss verdi som innbruddssikring. Med riktig kvalitet og festemetode vil imidlertid skodder montert på innsiden ha best effekt.*

Gitter

Gitter[16] kommer i forskjellige varianter, som for eksempel utstanset i stålplate/aluminium, smijern, med runde eller firkantede stålprofiler, stående og liggende. Gitter vil generelt ha god motstandsevne mot enkelt innbruddsverktøy og mindre slagverktøy. Ved montering av gitter er det er viktig at monteringsanvisningen fra leverandør blir fulgt, slik at egenskapene til gitteret ikke svekkes på grunn av feilmontering eller «raske og lettvinte» løsninger.

Sikkerhetsgitter skal fortrinnsvis monteres på innsiden av vinduet. Dette for å forhindre at gitteret kan demonteres uten at vinduet knuses. Gitter har størst effekt dersom det kombineres med innbruddsalarm. Det må vurderes om åpne-/lukkemekanisme for ulike gittertyper skal være motorstyrt eller med manuell åpning. Det kan benyttes både kortleser og nøkkel for styring av motorisert åpningsmekanisme. For optimal sikkerhet bør åpningsstyring være på innsiden, og sjalusiet bør kunne låses med mekanisk lås på innsiden.

Tabellen ***Sikringsklasser for gitter*** viser en enkel beskrivelse av gitter tilpasset sikringsklassene. Gitter testes i henhold til NS-EN 1627. Spesialgitter kan produseres på bestilling. Forsvarsbygg kan kontaktes i slike tilfeller.

Det finnes fast gitter som er godkjent av FG for innvendig montering på vinduer. Fast gitter kan benyttes til sikring av åpninger der hvor det ikke er hensiktsmessig med porter eller rullegitter (f.eks. av estetiske hensyn). Dersom gitter monteres på utsiden av vinduer, bør det benyttes enveisskruer eller bolter som vanskeliggjør demontering.

Bevegelig gitter skal ikke ha bredde over 3 meter, og innfesting og låsenheter må være iht. FG-krav.

Rulle- og saksegitter finnes som FG- godkjente

15 Se for øvrig beskrivelse i eget avsnitt

16 Se forskriften Innbruddssikring for næringslivet (FG-112:6) for nærmere beskrivelse av krav til gitter og sjalusier

produkter. Saksegitter kan monteres både utvendig og innvendig og er fleksible ved at de kan foldes sammen og hengsles slik at de kan svinges til side. Rullegitter kan monteres både utvendig og innvendig. Avlåsing kan skje med mekanisk eller elektrisk lås, eller en kombinasjon av disse.

Rullesjalusier kan brukes både innvendig og utvendig og gir beskyttelse mot innsyn og innbrudd. Det finnes sjalusier som er godkjent av FG og som gir god sikring mot enkelt innbruddsverktøy og mindre slagverktøy.

Gitterporter benyttes for avstengning av åpninger der man for eksempel av estetiske og arkitektoniske hensyn ikke ønsker verken rullegitter, sjalusi eller saksegitter. De vanligste gitterporter og -dører er laget i smijern eller galvanisert stål, men kan leveres i flere varianter. Gitterport eller -dør kan med fordel monteres som tilleggssikring av en eksisterende port eller dør.

Luker og tekniske gjennomføringer

Luker og tekniske gjennomføringer er et av de områdene der sikringen ofte blir utelatt. Luker og tekniske gjennomføringer etableres i de fleste bygg i forbindelse med ventilasjonsanlegg etc. En tommelfingerregel er at åpninger i form av luker, gitter eller lignende ikke skal være større enn 600 cm^2.[17]

Mindre åpninger skal også sikres dersom de gir lett tilgang til verdier. Selv om det ikke finnes så mange godkjente produkter for å sikre åpninger, bør en søke å sikre dem tilsvarende sikringsnivået i skallet for øvrig.

Det kan være nødvendig med flere lag av gitter og andre typer barrierer for å oppnå god nok innbruddsmotstand. Det bør benyttes solide enveisskruer eller gjennomgående bolter for å forhindre at gitter enkelt kan demonteres. Dersom det benyttes luke med utvendige hengsler, må luken ha bakkantsikring. Luker kan være godkjent etter NS-EN1627-standarden, men kan også produseres til en gitt sikringsklasse.

Det er mulig for en trusselaktør å forurense et bygg eller objekt med kjemiske, biologiske eller radiologiske stridsmidler via byggets ventilasjonsinntak eller lignende. Dette dekkes i ***kapittel 18, Trusselstoffer***.

17
Størrelse refererer til åpning som er stort nok til at en person kan ta seg gjennom

Kapittel 12

Elektronisk sikring

Dette kapitlet tar for seg elektronisk sikring. Med elektronisk sikring menes elektroniske systemer som benyttes for å detektere, overvåke og varsle uønskede hendelser, slik at det kan iverksettes mottiltak.

Kapitlet beskriver bruk av automatiske innbruddsalarmanlegg (AIA)[1], automatiske adgangskontrollanlegg (AAK)[1] og TV-overvåkningsanlegg (TVO)[1] med tilhørende IKT-infrastruktur, og hvordan disse systemene kan integreres sammen.

Generelt om elektronisk sikring

Elektronisk sikring har en tydelig rolle i konsept om helhetlig sikring og blir benyttet til å detektere, verifisere, forsinke og varsle samt at det har en preventiv effekt. Dersom en inntrenger ikke detekteres, vil heller ingen kunne reagere. Dersom alarmen ikke overføres, er det ikke sikkert at noen vil reagere på alarmen. For å verne personell og verdier kan elektronisk sikring benyttes til:

- *Perimetersikring*
- *Skallsikring*
- *Romsikring*
- *Objektsikring*
- *Personellsikring*
- *Overføring til alarmmottak/vakt*

Planlegging av elektroniske sikringstiltak

Et elektronisk sikringssystem vil kunne detektere og varsle om en uønsket hendelse er i ferd med å skje, men elektroniske hjelpemidler vil alene ikke kunne stanse en inntrenger. Til det må det etableres fysiske barrierer i form av sikre vegger, dører, vinduer og andre bygningsmessige hindre som det vil ta tid for en trusselaktør å forsere.

Målet med sikringstiltakene er at en trusselaktør ikke skal kunne ta seg frem til verdiene som skal beskyttes, og da vil en kombinasjon av varsling (alarm), fysisk sikring og reaksjonstid gjøre at trusselaktøren ikke når frem til verdiene før en reaksjonsstyrke er på plass og kan avverge hendelsen,[2] se ***figur Tidsregnskap*** i ***kapittel 2, Sikringsteori.***

Under planleggingen bør det benyttes tegninger over sikringsobjektet, og objektet bør befares. Sikkerhetsutfordringer, bruksmønster og eventuelle lokale tilpasninger avdekkes slik at systemet tilpasses lokasjonen.

Dette bidrar til at behov for overvåkning, soneinndeling av adgang- og alarmområder, betjeningsmuligheter, antall brukere, utvi-

1 Videre i kapitlet vil for enkelhets skyld forkortelsene AIA, AAK og TVO benyttes der det er hensiktsmessig

2 For enkelte objekter er det krav til at tidsregnskapet er positivt, og reaksjonsstyrke skal kunne motstå definert trusselaktør

ELEKTRONISK SIKRING

Relevante lover, regelverk og standarder

NEK EN 50131
Alarmsystemer
Innbrudds- og overfallsalarmsystemer

NEK EN 50132
Alarmsystemer
TV-overvåkning for bruk
i sikkerhetsapplikasjoner

NEK EN 50133
Alarmsystemer
Adgangskontrollsystemer for
bruk i sikkerhetsapplikasjoner

NEK EN 50136
Alarmsystemer
Alarmoverføringssystemer og utstyr

NEK EN 62676
Video overvåkningssystemer
til bruk i sikkerhetsapplikasjoner

NEK EN 50518
Monitoring and alarm receiving
centre (for alarmstasjon)
FG-200:2 FG-regler for automatiske
innbrudds- og overfallsalarmsystemer
(FGs regelverk for innbruddsalarm)

FG-240:1
Krav til elektroniske låsesystemer
(FGs krav til elektronisk låssystem)

Personopplysningsloven*
Stiller krav til omfang og bruk av
TVO og AAK. TVO er registreringspliktig
iht. personopplysningsloven.

Sikkerhetsloven
Objektsikkerhetsforskriften

* For krav i personopplysningsloven, se *www.datatilsynet.no*

delsesbehov og lignende kan ivaretas, og at disse forholdene inkluderes ved prosjekteringen av anlegget. Dette er en av nøkkelfaktorene for at sikringssystemene skal fungere optimalt.

Etter befaring og kartlegging av brukerens behov er man i gang med detaljprosjektering av anlegget, og i denne sammenheng gjøres en vurdering av hvilke ulike typer elektronisk sikring som vil egne seg best til å løse de brukerspesifikke oppgavene.

Noen av betraktningene som bør gjøres før og under detaljprosjektering starter, kan være:

- *Detektorer, kortlesere, overvåkningskameraer (antall, plasseringer, bruk)?*
- *Antall alarmområder/soneinndeling brukergrupper*
- *Sikring av adkomstområder, alternativ adkomst, behov for belysning, overvåkning?*
- *Betjeningstype og plassering*
- *Plassering av sentralutrustning og annet teknisk utstyr*
- *Sabotasjesikring*
- *Kommunikasjon internt og eksternt*
- *Redundans og krav til kapasitet og oppetid på sentralutrustning*
- *Systemintegrasjon mellom AIA, AAK, TVO og/eller andre systemer*
- *Alarm- og varslingsrutiner*
- *Hvor skal alarmer overføres til, og hvem skal verifisere alarmen?*
- *Hvilken reaksjonsstyrke finnes, og hvor lang tid bruker reaksjonsstyrken på en utrykning/avverging (tidsregnskap)?*
- *Fremtidig ivaretakelse av endringer og utvidelse*

Systemene bør enkelt kunne heve sikkerhetsnivået eks. ved hevet beredskap. Systemleverandør bør ikke ha koder til administratornivå for å programmere systemet eller systemkoder for adgangskort. Det bør være en autorisert person som er definert som masterbruker

(superbruker) i systemet. Personen har ansvar for den daglige bruken av koder og tilganger AAK, AIA, TVO.

Det kan være avgjørende at de ansatte informeres godt og tas med i planleggingsprosessen før sikkerhetssystemene innføres. Vellykket drift er helt avhengig av brukernes forståelse for behovet for sikring, og de ansattes representanter bør involveres i prosessen.

Et AIA-, AAK- eller TVO-system er ikke, og skal ikke benyttes som et tidregistreringssystem sett opp mot den enkeltes lønns- og arbeidstid.[3]

På siste side i kapitlet finnes en oversikt med symboler som blir benyttet under detaljplanlegging av sikkerhetssystemer, ***Symboler for AIA.***

Automatiske innbruddsalarmanlegg (AIA)

Et automatisk innbruddsalarmanlegg (AIA) er et elektronisk anlegg som overvåker et område, en bygning eller et objekt, og gir alarmmeldinger ved tilstandsendringer. Med tilstandsendringer menes for eksempel:

- *åpning av dør, vindu, luke, port o.l.*
- *bevegelser i områder som skal være avstengt*
- *vibrasjoner, lyd og lys*
- *fjerning av gjenstander*
- *røyk*
- *manuell utløsning av alarm (f.eks. ved ran, overfall o.l.)*

Ved en deteksjon vil alarmen varsle med lyd/lys og overføre alarmsignalet til et alarmmottak som muliggjør reaksjon, men alarmsystemet kan også settes til å gi stille alarmer, dvs. ikke gi synlige lys eller lydvarsel om at alarm er utløst.

Overfallsalarmer skal varsle med stille alarm.

Et AIA kan sies å ha tre hovedfunksjoner – forebygge, varsle og avskrekke:

- *En forebyggende funksjon oppnås ved at en trusselaktør enten vet eller har grunn til å anta at objektet er sikret med alarm, og derfor unnlater å forsøke seg på et innbrudd. Det er anbefalt å sette opp skilt som forteller at objektet er sikret med alarm. Den forebyggende funksjonen er ofte undervurdert og lite utnyttet, men kan være meget effektiv.*
- *Varslingsfunksjonen oppnås ved at AIA sender en alarmmelding til et alarmmottak.[4] De fysiske og elektroniske sikringstiltakene skal primært utformes etter prinsippet om balansert sikring. Dette innebærer at en reaksjonsstyrke kan nå frem til objektet før trusselaktøren rekker å tilegne seg, fjerne, ødelegge eller forringe verdier.*
- *Avskrekkende funksjon oppnås ved at en utløst alarm setter i gang lokal varsling i form av sirener og eventuelt lyssignaler. Varslingen påkaller oppmerksomhet fra nærmiljøet, den forteller trusselaktøren at han er oppdaget, i tillegg til at den overføres til en vaktsentral som vil sørge for utrykning.*

For å ha maksimal effekt skal AIA prosjekteres slik at alarm ved inntrengning utløses så tidlig som mulig, og aller helst ved innbrudd i ytterskallet.

Sikringsklasser AIA

Sikringsklassene (SK) for AIA velges ut ifra kravet man har til sikring. Dersom det ikke foreligger spesielle verdier, konsekvenser eller en trussel, kan følgende tommelfingerregel benyttes:

- *SK1 Bolig*
- *SK2 Virksomheter med lavt risikobilde*
- *SK3 Virksomheter med høyt risikobilde*
- *SK4 Virksomheter med meget høyt risikobilde*

3 Krav i personopplysningsloven

4 Alarmmottaket rekvirerer normalt da en reaksjonsenhet til lokasjonen

Sikringsklasser AIA

Sikringsklassene (SK) for AIA velges ut ifra kravet man har til sikring. Dersom det ikke foreligger spesielle verdier, konsekvenser eller en trussel, kan følgende tommelfingerregel benyttes:

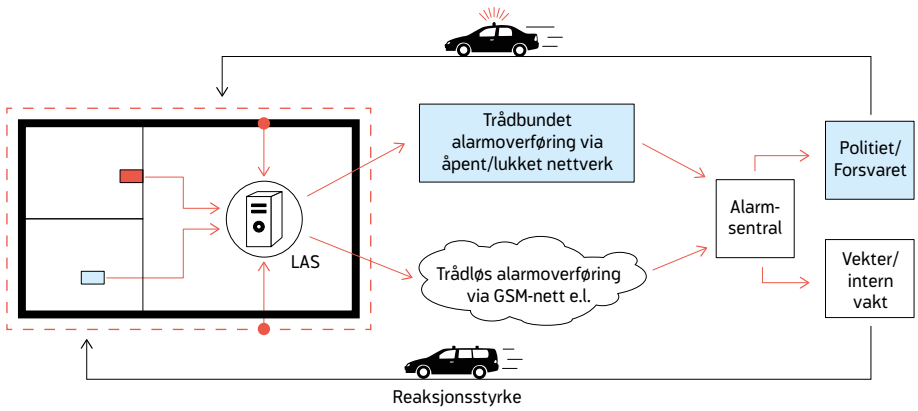
- *SK1 Bolig*
- *SK2 Virksomheter med lavt risikobilde*
- *SK3 Virksomheter med moderat–høyt risikobilde*
- *SK4 Virksomheter med høyt risikobilde*

Sikringsklasse	Beskrivelse/krav
1	→ Minimum NEK EN 50131 Grad 1 → Et system brukt under de premisser hvor potensielle inntrengere har liten kunnskap om alarmsystemer og et begrenset utvalg av lett tilgjengelig verktøy.
2	→ Minimum NEK EN 50131 Grad 2 – ATS 4[2] → Et system som normalt benyttes der et sofistikert angrep ikke er overhengende sannsynlig. Inntrengere er ventet å ha begrenset kunnskap om alarmsystemer, og har kun basisverktøy og bærbare instrumenter. → Det tillates å benytte kortleser tilknyttet AAK (min. SK2) for å styre alarm-områder.
3	→ Minimum NEK EN 50131 Grad 3 – ATS 4[2] → Et system som benyttes når trusselaktør er fortrolig med AIA-systemer og har betydelig mengde verktøy og transportabelt elektronisk utstyr tilgjengelig for å sabotere dem. → Det tillates å benytte kortleser tilknyttet AAK (min. SK3) for å styre alarm-områder[1]. → Systemet etableres med grafisk fremstilling av alarmer på kart/plantegning for å raskere kunne lokalisere alarm, og mulighet for tilknytning i felles presentasjonssystem med AAK og/eller TVO.
4	→ Minimum NEK EN 50131 Grad 3 – ATS 6[2] → Anvendelse for et system hvor sikkerheten er den viktigste faktoren. → Skal sikre mot en inntrenger som har planlagt angrepet i detalj, har meget stor kompetanse og avansert utstyr til sabotasje av AIA. Systemet suppleres med andre omfattende fysiske tiltak og sikkerhetsprosedyrer. Alle utvendige kabler skal legges i stålrør. → Minimum 2 ulike teknologier for overføring av alarm. → Systemet etableres med grafisk fremstilling av alarmer på kart/plantegning for å raskere kunne lokalisere alarm, og mulighet for tilknytning i felles presentasjonssystem med AAK og/eller TVO.

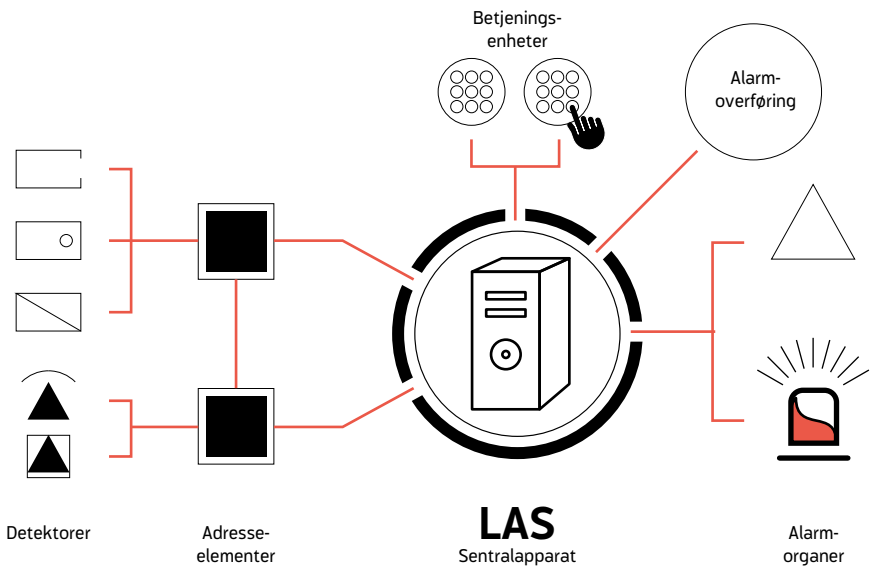
[1]Dersom dette ikke kommer i konflikt med sikkerhetslovens bestemmelser.
[2] ATS = Alarmoverføringssystem (deles i 6 klasser). ATS blir beskrevet som en kombinasjon av 5 parametere:
D: Overføringstid (klasse)
T: Rapporteringsintervall
M: Overføringstid (maksimum)
S: Sikkerhet mot utskiftning
I: Informasjonssikkerhet

Komplett AIA-system

med tilhørende reaksjonsstyrke (eksempel)



Lokal alarmsentral



Betjeningsenheter

Kodepanel for AIA. **FOTO** Forsvarsbygg

Kortleser med værhus. **FOTO** Forsvarsbygg

Beskrivelse av AIA

Et AIA-system består av lokalt alarmanlegg med et alarmoverføringssystem som overfører alarmen til et alarmmottak. Dette avsnittet vil gå noe mer i dybden på enkelte av disse komponentene.

Et komplett AIA-system med tilhørende reaksjonsstyrke kan være som vist i ***figuren Komplett AIA-system*** på forrige side.

Lokal alarmsentral

Lokal alarmsentral (LAS) er sentralenheten med strømforsyning hvor detektorer, betjeningsenheter, alarmorganer og alarmoverføringssystem er knyttet sammen på et eget kabelnett. Sentralen ivaretar en rekke variable funksjoner og styringer, for eksempel:

- *Manuell eller automatisk betjening av hele eller deler av anlegget*
- *Detektere og varsle ved alarm, sabotasje eller andre hendelser*
- *Alarmoverføring*
- *Loggføring av hendelser (alarmlogg og systemlogg)*

Grafisk presentasjon på kart/plantegning på en klient-pc kan med fordel brukes på større anlegg for å gi bedre oversikt og kortere responstid.[5] LAS forsynes normalt med strøm via 230V-nettet, men skal alltid ha reservestrømkapasitet via egne batterier i tilfelle bortfall av 230V.[6]

Lokalt alarmanlegg

Et lokalt alarmanlegg (LAA) er et eller flere frittstående innbruddsalarmsystemer (LAS) med alle nødvendige komponenter.

Eksempelvis kan det være et betjeningspanel som styrer flere alarmsoner som er fordelt over flere områder.

5 Dersom plantegninger eller kart er gradert etter sikkerhetsloven, vil systemet betraktes som gradert, og må sikkerhetsgodkjennes og behandles deretter

6 Iht. FG/NEK EN 50131

PIR-detektor

Passiv infrarød detektor. **FOTO** Forsvarsbygg

Betjeningsenheter

Alarmsystemet betjenes som regel ved hjelp av kodepanel. Det kan også benyttes kortleser for til- og frakopling av deler av AIA, hvis AIA og AAK er integrert. På større systemer kan det med fordel benyttes pc-klient for grafisk presentasjon, men kodepanel skal alltid være tilgjengelig.[7]

Fra ***kodepanelet*** styres LAS. Ved bruk av personlige koder kan autoriserte brukere koble inn og ut hele eller deler av anlegget, sjekke anleggets status og lignende. Enheten består vanligvis av et kodetastatur, et tekstvindu og kontrollamper.

Kortleser kan hos den enkelte bruker benyttes til inn- og utkopling av det aktuelle alarmområdet som brukeren benytter kortleseren for å få adgang til. Dette vil kunne gi et enkelt brukergrensesnitt.

Detektortyper

Det finnes en rekke detektortyper som benyttes i et AIA. I de følgende avsnittene presenteres kort de vanligste formene for detektortyper. I ***kapittel 10, Perimeter- og områdesikring*** og ***kapittel 11, Fysisk sikring mot inntrengning,*** beskrives det hvordan de ulike detektortypene kan benyttes. Dette kapitlet vil forsøke å beskrive hovedtrekkene til de ulike detektorenes virkemåte.

Passive infrarøde detektorer (PIR-detektorer)[8] detekterer refleksjon av varme og gir alarm ved bevegelser i dekningsområdet, og benyttes i hovedsak til innendørs sikring, typisk romsikring.

PIR-detektorer finnes i en rekke forskjellige utgaver[9] med ulike egenskaper og dekningsområder.

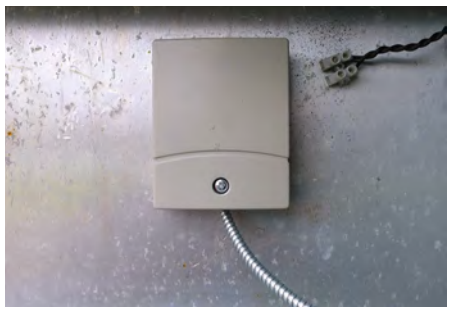
På grunn av at PIR-detektorer detekterer refleksjon av varme har enkelte leverandører utstyrt detektoren med temperatursensor som automatisk justerer detektorens følsomhet i forhold til romtemperatur, slik at detektoren øker følsomheten dersom temperaturen i rommet er lik menneskekroppens utvendige temperatur.

7 Iht. FG/NEK EN 50131

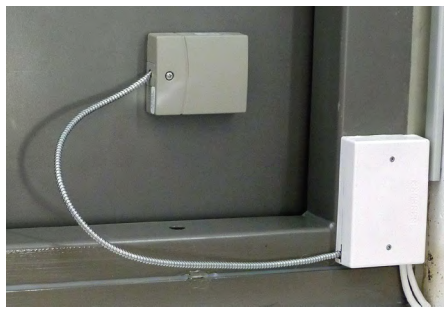
8 Også omtalt som bevegelsesdetektor

9 Både sektor og rekkevidde for PIR-detektoren kan være større eller mindre enn det som er oppgitt ovenfor, avhengig av type

Seismiske detektorer



Seismisk detektor på stålvegg. **FOTO** Forsvarsbygg



Seismisk detektor på hvelvdør. **FOTO** Forsvarsbygg

PIR-detektorer kan leveres med antimaskeringsfunksjon (antimask)[10]. Denne funksjonen gir et varsel dersom detektoren blir tildekket.

Kombinasjonsdetektor vil vanligvis være en detektor med PIR og en eller flere andre deteksjonsteknologier.[11] Bruk av kombinasjonsdetektor minsker feilalarmraten fordi det benyttes to eller flere deteksjonsprinsipper og -givere. Utendørs kombinasjonsdetektorer har gjerne et smalt, men meget langt dekningsfelt.

Magnetkontakter benyttes typisk på dører, porter, vinduer og lignende, og gir alarm ved åpning av for eksempel en dør. De finnes i en rekke utførelser avhengig av bruksområde. Magnetkontakter er en rimelig og stabil detektor, og det anbefales å benytte polariserte/forspente magnetkontakter.

Mikrobryter[12] er en bryter som sitter i selve låsen. Denne sammen med magnetkontakt gir mulighet for status-overvåkning av lukket og låst[13] funksjon på dør.

Seismiske detektorer benyttes på betong- og stålkonstruksjoner, og gir alarm ved forsøk på skjæring, boring og sprenging på konstruksjonen. Typisk bruk er på vegger, gulv, tak og dører i forsterkede rom, på verdiskap og lignende.

Detektorens følsomhet kan ofte justeres, men det kreves god prosjektering og nøyaktig montering for å oppnå et godt resultat. Til bruk på betongvegger og lignende er detektoren mest effektiv dersom den forankres til armeringen, og festes i betongen. Til dette formål finnes egne festeplater og innstøpingsbokser.

Linjedetektorer[14] består av en sender og en mottaker for infrarødt lys. Dersom et objekt kommer mellom sender og mottaker slik at den infrarøde lysstrålen brytes, gir detektoren alarm.

Linjedetektorer benyttes vanligvis utendørs, som skallsikring foran vinduer, på mur, tak eller lignende. Disse krever en god stødig forankring.

Ofte plasseres flere sendere/mottakere over hverandre, slik at de danner en «deteksjonsvegg». Disse har en rekkevidde på inntil 200 m. Linjedetektorer er vanligvis meget pålitelige, og de fungerer godt under de fleste værforhold.

Rans-/overfallskontakt er i sin enkleste form en trykknapp som personellet utløser manuelt dersom de befinner seg i en rans-/overfallssituasjon. Denne typen alarmer finnes det flere typer av, for eksempel nødbryter med glass foran, sparkelist for vegg e.l. Alarmen overføres til et alarmmottak, som iverksetter reaksjon.

Magnetkontakt

for utenpåliggende og innfelt montasje

10
Antimask = funksjon i detektoren som gir sabotasjealarm når detektoren blir tildekket, eller «synsfeltet» til detektoren blir for lite

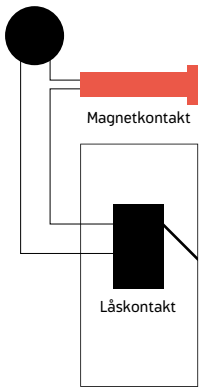
11
Som oftes ultralyd og/eller mikrobølge

12
Også omtalt som låskontakt

13
Lukket og låst-funksjon er en kombinasjon av signal fra magnetkontakt og låskontakt som gir et signal tilbake om døren både er lukket og låst

14
Også omtalt som aktive infrarøde detektorer

Mikrobryter/ låskontakt



Linjedetektorer foran vindu

Rans-/overfalls-kontakt

Laserdetektor

Det kan imidlertid installeres varsellys som varsler personell som befinner seg i samme bygning, slik at disse ikke uforvarende går inn i et område hvor det pågår en trusselsituasjon.

Det finnes også trådløse overfallsalarmer, små sendere som kan bæres i lommen og sender sitt alarmoppkall via lokale mottakere som kan identifisere både hvem det er som sender ut varsel, og til en viss grad også gi en lokalisering av hvor alarmen blir utløst.

Glassbruddetektor gir alarm ved knusing av glass. Det finnes også typer som reagerer på dette sammen med trykkforandringer[15] i rommet. Det brukes i dag stort sett to typer akustiske glassbruddetektorer.

15 Trykkforandringer i form av kraftige lydbølger, som forekommer dersom man eksempelvis slår inn en dør eller vindu

Detektoren gir alarm ved skjæring/knusing av glass. Detektoren dekker gjerne flere vinduer samtidig. Pålimte mekaniske glassbruddetektorer dekker kun ett vindu, og benyttes derfor i hovedsak ikke lenger. Glassbruddetektorer vil ikke være like effektive hvis det er montert film på vinduet.

Optiske røykdetektorer detekterer synlig røyk i luften. Røykdetektorer benyttes vanligvis i brannalarmanlegg, men de kan også benyttes i AIA for å detektere innbruddsforsøk med termiske lanser eller annet skjæreutstyr som produserer røyk.

Laserdetektorer gir alarm ved bevegelser i dekningsområdet, og benyttes til skallsikring, områdesikring, perimetersikring og annen utendørs sikring. Denne detektortypen kan være programmerbar med soner og dekningsområde. Den mest brukte detektoren sender ut ett felt med laserstråler hvor bevegelser i dekningsfeltet gir alarm.

Gjerdedeteksjonskabler finnes i forskjellige varianter (fiber- og mikrofonkabel), men felles for dem er at de festes på et gjerde, og gir alarm ved forsøk på klatring eller klipping i gjerdet. Reagerer på bevegelser/vibrasjoner/endringer i gjerdet. Systemene stiller krav til kvalitet på gjerder porter osv, da det veldig ofte er problem med vind som setter gjerdet eller vegetasjon inntil gjerdet i bevegelse o.l., som skaper alarm. Dersom sensitiviteten justeres for lavt, reagerer ikke systemet på en person som forsiktig klatrer over ved stolper. Systemet kan ha utfordringer i et nordisk klima.

Personellradar kan benyttes til perimetersikring, i tillegg til å fungere godt som et safety-produkt. Enhetene leveres i forskjellige modeller og med forskjellig teknologi[16] og rekkevidde. Personellradar kan detektere objekter i bevegelse over store områder, hvis det ligger geografisk til rette for det. Dette innebærer at området radaren skal detektere i, må være flatt og uten vegetasjon. Det er viktig å merke seg at elektronisk sikringssystem med personellradarer kun detekterer objekter som er i bevegelse, og at systemet slutter å følge et objekt om det er ubevegelig lenge nok.

Mikrobølgedetektor sender ut mikrobølger og gir alarm innenfor dekningsområdet.[17] Detektoren trenger igjennom glass, lettvegger etc. Den benyttes ofte som en kombinasjonsdetektor sammen med PIR, langs fasader eller på innsiden av gjerder. Det benyttes systemer som har sender og mottaker i samme enhet og i separate enheter.

Elektromagnetiske deteksjonskabler graves ned i bakken og måler elektromagnetisk felt over og under bakken. Når en person kommer inn i dette feltet, utløses en alarm. Systemet er avhengig av nøyaktig prosjektering, god drenering og kalibrering over tid. Systemene har mange feilkilder, er lite egnet i det nordiske klimaet og er derfor lite brukt i dag.

Oppsummering

Det er viktig å være oppmerksom på at perimeter deteksjonssystemer ikke er plug and play-systemer; de kan være kostbare å installere og krever en nøyaktig prosjektering. Systemene er ofte avhengig av tilpasninger til de geografiske forhold og at deteksjonssonen er mest mulig «steril», dvs. uten vegetasjon. Perimetersikringssystemer bør alltid kombineres med TVO for å kunne verifisere hva slags alarm det dreier seg om.

Alarmorganer

Med alarmorganer menes sirener, summere, blinklys og lignende. Alarmorganer benyttes dels for å skremme/distrahere trusselaktører, og dels for å varsle omgivelsene. Alle alarmorganer skal være sabotasjesikret slik at det gis alarm ved forsøk på manipulasjon.

Tåkesikring

Tåkegenerator er en form for tidshindring. Dette

16 Det benyttes i hovedsak to typer radarteknologier, som kalles Doppler eller fase-skift

17 Mikrobølgedetektor reagerer på metall og vann, menneskekroppen består av ca. 70 prosent vann

Tåkegenerator

Inntrenger detekteres

Tåkegenerator aktiveres

Rommet fylles med tåke. Det blir vanskelig for inntrengeren å orientere seg.

er en maskin som hurtig sprøyter ut tåke, slik at det blir vanskelig å se og orientere seg. Dette egner seg godt til sikring av materiell-lager, fjellanlegg, større serverrom o.l. Tåkegenerator skal alltid vurderes opp mot brannforskrifter og rømningsveier.

Tåkesystemet skal fylle et volum på minimum 150 m^3 innen 60 sekunder, slik at sikten blir maksimalt én meter. I rom som ikke er ventilert, skal tåkesystemet opprettholde redusert sikt i minimum 10 minutter. Dette kan gi en tidshindrende barriere.

Det kan være en fordel om operatør på alarmmottak kan fjernutløse tåkesikringen etter verifikasjon at trusselen er reell ved bruk av TVO eller lignende. Det forutsetter at alarmmottaket er betjent hele døgnet. Ved utløsning at tåkesikring kan også belysningen kuttes, og strobelys og sirene aktiviseres for å ytterligere desorientere trusselaktøren.

Sabotasjesikring av komponenter innebærer at alle detektorer og komponenter i systemet skal sabotasjesikres. Kabling bør utføres mest mulig som skjult kabling.[18] Hvis det er tilgang til anleggets komponenter for publikum, bør man velge forspente magnetkontakter og PIR-detektorer med antimaskeringsfunksjon[19], slik at disse er overvåket selv om alarmen er avslått.

Alarmoverføringssystem
En alarmsentral skal ha et alarmoverføringssystem som overfører alarmsignaler fra alarmsentralen til alarmmottaket. Alarmoverføring kan skje via nettverk (TCP/IP)[20] eller via overvåket GSM-nett.[21] (Det anbefales ikke å benytte overføring som ikke er overvåket.)

Kravene til alarmoverføring er strengere i EN 50131[22] grad 3 enn i FG-regler grad 3 for automatiske innbrudds- og overfallsalarmsystemer, og en bør derfor etterstrebe å tilfredsstille disse. Det bør benyttes dublert[23] samband for alarmoverføring der forholdene tilsier dette. (FG-regelverket har ikke lenger grad 4.)

Alarmmottak

Et ***alarmmottak***[24] er en sambands- og kommandoplass hvor alarmer mottas og vurderes, og hvor aksjoner blir initiert. Alarmmottaket skal være bemannet døgnkontinuerlig av spesielt utdannet personell. Det skal alltid være minst to personer på vakt, og lokalene skal minst være sikret tilsvarende kravet til sikring av de objektene som alarmmottaket mottar alarmer fra.

På alarmmottaket fremkommer alarmer vanligvis på en monitor, med opplysninger om hvilke eller hvilket objekt det gjelder, detektor som er utløst, hvilken aksjon som skal igangsettes (aksjonsplan) og lignende.

18
Alle konvensjonelle sløyfer skal overvåkes (dobbelbalansert kobling eller lignende godkjent løsning)

19
Antimask er en funksjon i PIR detektoren som gir alarm dersom detektoren blir tildekket

20
TCP/IP (Transmission Control Protocol/Internet Protocol) er en gruppe kommunikasjonsprotokoller som benyttes for å koble sammen enheter (eks. datamaskiner) i nettverk

21
Fortrinnsvis GPRS (General Packet Radio Service), en standard for trådløs dataoverføring med mobilkommunikasjon over GSM-nettet

22
EN 50136

23
Med dublert så menes to ulike overføringsmedier for overføring av alarm, eks. over TCP/IP og GSM

24
EN 50518 Monitoring and alarm receiving centre

Alarmmottak

Alarmer kan også presenteres grafisk. Det vil si at alarmen automatisk presenteres ved å vise utløst detektor eller sone på plantegning og/eller kart på klient-pc. Grafisk fremstilling kan bidra til å redusere reaksjonstiden for vaktstyrken.

For ytterligere beskrivelse av alarmmottak og vaktfunksjoner viser vi til ***kapittel 13, Vakthold og reaksjonstiltak.***

Verifisering av alarmer

For å redusere antall uønskede utrykninger skal det etableres rutiner for verifisering av alarmer. Det er i hovedsak fire måter å verifisere alarmer på:

- *Manuell verifisering betyr at vaktstyrke må sendes ut til sikringsobjektet for å sjekke om alarmen er reell.*
- *Teknisk verifisering gjøres ved hjelp av forskjellige tekniske løsninger. Eksempelvis kan utløsning av to eller flere detektorer til sammen indikere at alarmen er en reell hendelse.*
- *TVO-verifisering betyr at sikringsobjektet er tv-overvåket, og at bilder fra objektet er tilgjengelig på alarmmottaket. En viktig forutsetning her er at TVO-kameraene dekker de områdene der alarmen utløses. Dette er en meget god form for verifisering og gir mulighet for korrekt reaksjon uten at vakt utsetter seg for en eventuell fare.*

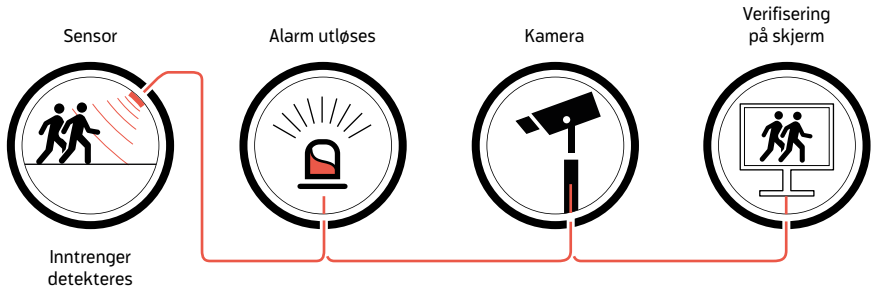
Grafisk fremstilling på kart/plantegning kan med fordel brukes på større anlegg, for å gi økt oversikt og kortere reaksjonstid.

En kombinasjon av ovennevnte vil imidlertid ofte være den mest sikre og kosteffektive løsningen.

Reaksjonsstyrke

Ved mottatt alarm på alarmmottaket varsler operatøren en på forhånd avtalt reaksjonsstyrke. Krav til reaksjonsstyrke må vurderes i forhold til trusselnivå og reaksjonsstyrkens instruks. Reaksjonsstyrken kan bestå av egne vakter, innleid vekterselskap, militære vakter eller politiet.

TVO-verifisering



Automatisk adgangskontroll-anlegg (AAK)

Automatisk adgangskontrollanlegg benyttes for å føre kontroll med adgangen til eiendom, bygg og anlegg på en kosteffektiv måte. Anlegget regulerer hvem som har adgang til å gå hvor og når, og det kan gi alarm ved forsøk på uautorisert adgang. Adgangskontrollanlegget skal slippe inn autoriserte ansatte, gjester og lignende så problemfritt som mulig, men samtidig holde uvedkommende ute. Den mest vanlige bruken i et AAK-system er at man benytter kort og kode i en kortleser for å komme inn, mens man kun trykker på en åpnerknapp for å komme ut. For å heve sikkerhetsnivået kan man benytte kortlesere begge veier slik at vedkommende blir registrert både inn og ut. Det kan være ulike årsaker til bruk av et slikt autorisasjonsskille i dørmiljøet, og i en del tilfeller kan man vurdere å benytte inn- og ut-kortlesere som en del av skallsikringen.

For systemer som baserer seg på bruk av nøkler, kan det ved tap av nøkkel i kritiske situasjoner være nødvendig å bytte hele låssystemet, noe som er meget kostbart. Ved tap av kort er det enkelt å blokkere ett kort i systemet.

Alle viktige komponenter ute i systemet skal varsle ved hendelser, alarmer, sabotasje og/eller kommunikasjonsfeil. Ved forsøk på manipulering av kommunikasjon mellom enheter eller kortleser og adgangskort, skal dette automatisk kunne avdekkes.

AAK-system kan generere ulike alarmer, eller statusendringer. Dette kan være:

- *Registrere passeringer og andre styringer*
  - *Dører som endrer status*
  - *Dør åpen for lenge*
  - *Dør brutt opp*
  - *Feil PIN*
  - *Feil kort/blokkert kort*
  - *Forsøk på manipulasjon av kortleser*
- *Sabotasje på sentral, undersentral, kortleser eller andre komponenter*
- *Kommunikasjonsfeil på sentral, undersentral, kortleser eller andre komponenter*
- *Lavt batteri eller batterifeil på strømforsyning*
- *Databasefeil*
- *Andre programmerbare alarmer og styringer*

Alle hendelser og statusforandringer skal logges.[25]

Universell utforming

Byggteknisk forskrift TEK10 stiller krav til utforming av dørmiljø som for eksempel høydeplassering av kortleser, krav til dørautomatikk, krav til rømning m.m.

25

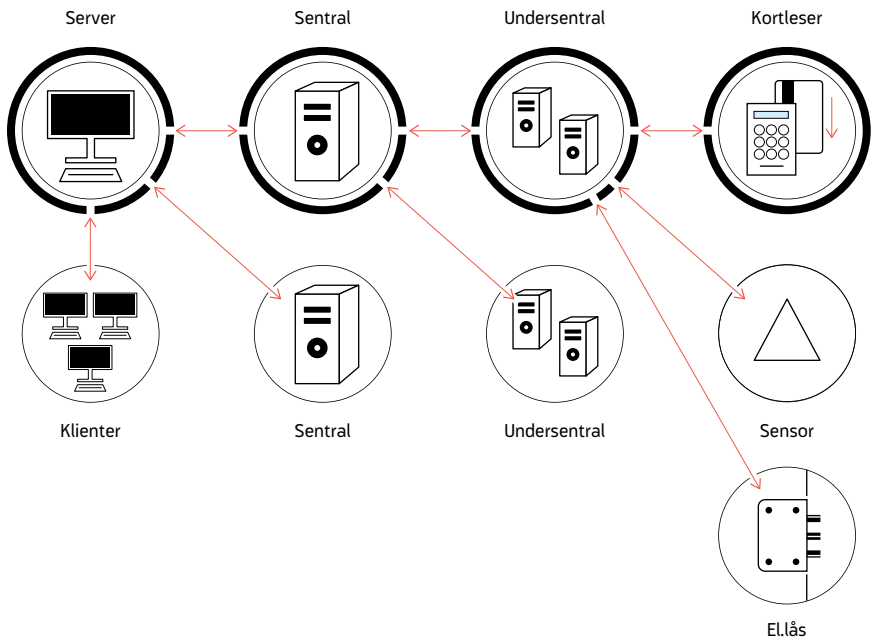
Systemloggen viser hvilke endringer forskjellige operatører har gjort inne på systemet. Dette viser hvilke operatører med navn som har endret oppsettet på AAK, f.eks. åpningstider for kortlesere, styring av alarmer, tilgangsnivå o.l. samt når endringene er foretatt. Hendelseslogg viser hvilke statusforandringer og hendelser som er blitt registrert av komponentene

Sikringsklasser AAK

Sikringsklasse	Beskrivelse/krav
1	**En adgangskontroll basert på elektronisk låst dør:** → Med kodetastatur → Med enkel kortleser (offline)
2	**Et adgangskontrollbasert system som:** → Basert på bruk av adgangskort eller ID-kort med PIN-kode
3	**Et automatisk adgangskontrollanlegg (AAK) som:** → Skal benytte adgangskort med foto og bruk av PIN-kode → Alle sentraler, dørkontroller, koplingsbokser og kortlesere skal ha sabotasjealarm → Har adgangskontroll med hendelses- og systemlogg → Overvåket overføring av alarmer til en sentral enhet → Sentralstyrt database med tilgangs- og nivåstyring → Autonomt uten servertilkopling og lagrer hendelser i eget internt minne Alle loggføringer og databaser har automatisk backup til annen ekstern enhet Systemet skal automatisk overføre alle logger til server når kommunikasjon reetableres Utføres minimum iht. NEK EN 50133
4	**Et automatisk adgangskontrollanlegg (AAK) som:** → Skal benytte adgangskort med foto og bruk av PIN-kode → Alle sentraler, dørkontroller, koplingsbokser og kortlesere skal ha sabotasjealarm → Feil kode på kortleser skal varsles → Har adgangskontroll med hendelses- og systemlogg → Overvåket overføring av alarmer til en sentral enhet som reagerer på alarm → Sentralstyrt database med tilgangs- og nivåstyring → Autonomt uten servertilkopling og lagrer alle hendelser i eget internt minne. Systemet skal automatisk overføre alle logger til server når kommunikasjon reetableres → Alle loggføringer og databaser har automatisk backup til annen ekstern enhet → Servere i clusterløsning[3] e.l. og har redundant intern kommunikasjon → Personellsperre for singel inn- og utpassering Utføres minimum iht. NEK EN 50133

[3] Clusterløsning lar serverdatamaskiner arbeide sammen for å gi økt tilgjengelighet og lav nedetid, der en annen server automatisk vil ta over dersom en server skulle feile.

AAK-system



Rømningskrav
AAK vil kunne komme i konflikt med rømningskrav. I de fleste tilfeller vil det være mulig å forene tekniske og praktiske løsninger som ivaretar både krav til sikkerhet (security) og rømning (safety).

En løsning som ofte frarådes ut fra et sikkerhetsmessig perspektiv, er å koble AAK sammen med brannalarmen på en slik måte at ytterdører, skalldører og dører inn til BESKYTTET[26] eller SPERRET[27] område åpnes/låses opp automatisk ved brannalarm. Daglåsen på sikkerhetsdører kan ev. låses opp slik at en opprettholder kravet rømning, men sikkerhetslåsen (nattlåsen) skal kun låses opp manuelt. Dette må vurderes i hvert enkelt tilfelle, og skal dette benyttes, bør systemet tilkoples døgnbemannet vaktsentral.

Beskrivelse av AAK
Viktige elementer i et AAK-system kan være server/klienter, sentralenhet, undersentral som har til oppgave å styre ett eller flere dørmiljø med kortlesere, elektriske låser og alarmgivere. Strømforsyning bør ha egne batterier, og således være operativt selv under et strømbrudd.

Dette avsnittet vil se litt mer på enkelte av disse komponentene.

Komponenter
Server (maskinvare)
Server/sentral enhet besørger anleggets overordnede drift og kontroll ved hjelp av systemets programvare. På denne sentralen legges brukere og brukerprofiler inn og sentralen henter inn, og lagrer hendelser og endringer i systemet (hendelseslogg og systemlogg).

Vanligvis vil et stort antall hendelser (transaksjoner) lagres i undersentralen, og ved et

26, 27
Sikkerhetsloven

eventuelt brudd i kommunikasjonen mellom sentral og undersentral vil hele transaksjonsloggen lastes opp til server når kommunikasjon reetableres. Server bør plasseres i rack i sikret datarom med kjøling og egen UPS/Nødstrøm for å sikre et godt driftsmiljø.

Klient(er)
Klientene er brukergrensesnittet for operatøren. På klientmaskinen(e) til AAK vil alarmer og statusendringer ute i anlegget presenteres. Fra klienten kan man også gi operatører mulighet for å programmere bruken av systemet. Eksempler er når dører skal være ulåst eller i kort ev. kort og kode, hvem som skal ha tilgang hvor og når, og hvilke hendelser som skal føre til aksjoner som alarm etc. Det vil også være mulig å begrense klienten til kun å fungere som en ren alarmmonitor, dvs. at operatøren ikke gis tilgang til å gjøre endringer, kun betjene løpende hendelser. Alle logger kan vanligvis også hentes ut på klient-pc. På større AAK-systemer kan det være flere operatører på flere klienter. Både sentraler og klienter bør være utstyrt med nødstrøm/UPS-kraft.

Sentralenhet
Sentralenheten håndterer alle tilganger, styringer og hendelser på et lokalt nivå. Det anbefales at nettverket mellom server og undersentraler er et eget dedikert lukket nettverk.

Undersentral/Dørkontroller[28]
Sentralen kommuniserer som regel med de ulike undersentralene/dørkontrollene på en egen «busskommunikasjon». Til undersentralen tilkoples kortleser, magnet/mikrokontakt i dør, elektromekanisk lås, eventuell åpneknapp for utpassering og ev. annet utstyr. Undersentralen bør alltid sabotasjesikres, plasseres i sikker sone og ikke være lett tilgjengelig.

Strømforsyning
Strømforsyning til AAK-anlegget skal ha egen batteri-backup. Det er viktig at denne er tilpasset strømforbruket til alle komponenter som benyttes i systemet. Strømforsyning bør sabotasjesikres og plasseres i sikker sone. Behovet for strømforsyning må vurderes i forhold til sikkerhetsnivå, hvor lang tid det tar å få på plass vakt, og hvor lang tid det tar å reetablere funksjonen, ved bortfall av kraftforsyning. Dersom systemet utvides, må det ovennevnte hensyntas.

Åpneknapp

Kortleser
Kortlesere finnes med og uten tastatur og display, samt med forskjellige kortteknologier.

På kortleseren finnes det en lys/symbolindikasjon eller display som gir brukeren informasjon om døren er åpen eller låst, om det kreves kun kort eller kort og kode for å åpne døra, og lignende. Kortleser benyttes både for inn- og utpassering, men førstnevnte er mer vanlig.

Det bør i hovedsak benyttes kortlesere med tastatur.

Åpneknapp
Det benyttes gjerne en åpneknapp for utpassering. Knappen[29] er en pulsknapp, gjerne med

28
Undersentral behandler alle tilknyttede komponenter i et dørmiljø

et nøkkelsymbol. Det er også mulig å benytte åpneknapp på dagtid, og ut-kortleser for utpassering utenfor kontortiden. (Denne bør sabotasjeovervåkes.)

Magnetkontakt/mikrobryter
Magnetkontakten indikerer at døren er lukket ,og mikrobryteren indikerer at døren er låst. Disse koples sammen for å gi status på at døren er fysisk lukket og låst.

Elektromekaniske låser[30]
Det finnes en rekke forskjellige elektromekaniske låstyper som kan benyttes i AAK-anlegg. En generell regel bør være at den elektromekaniske låsen som benyttes, har en mekanisk styrke som minimum tilsvarer det som ellers ville bli brukt i døra, dersom man ikke hadde AAK. Dette betyr bl.a. at ytterdører bør ha minst en FG-godkjent låsenhet.

Motorlåser tilfredsstiller som regel FGs krav til sikkerhetslåser. Motordriften gjør at de ikke låser opp momentant. Dette bør derfor vurderes der det er stor gjennomgangstrafikk. Motorlåser benyttes som oftest som nattlåser og på dører med spesielle krav til fysisk styrke, for eksempel utvendige dører.

STEP-låser er en fallelås, som låser i dørkarmen, hvor reilen i låskassen i døren alltid er ute. STEP-låser leveres i en rekke kvaliteter, fra kraftig til enklere utgaver. STEP-låser fås i FG-godkjente modeller som da kan benyttes i ytterdører og dører med spesielle krav til fysisk styrke.[31]

Solenoidlåser er fallelåser hvor vriderfunksjonen kobles ut eller inn.

Elektriske sluttstykker leveres i en rekke kvaliteter, fra kraftig til meget enkle utgaver, og er den mest brukte låsetypen.

Magnetlås består av en kraftig elektromagnet som festes i dørens karm, og en metallplate som festes på dørbladet. De kraftigste holdemagnetene har en fysisk styrke tilsvarende FGs krav. Disse er imidlertid ikke FG-godkjent, da de er avhengig av strøm for å holde døren låst.

Magnetlåser har som regel lavere motstandskraft enn øvrige låser.

Pris er ikke alltid ensbetydende med kvalitet, men enkelte av de rimelige låsene på markedet har svært liten fysisk styrke, og kan enkelt manipuleres eller dirkes. De bør derfor ikke benyttes.

Karmoverføring består av to plater med en hul spiralfjær mellom som kabel føres i fra karm til dørblad.

Dørlukker/døautomatikk
AAK-dører bør ha en dørlukker eller en døautomatikk som lukker døra. Dørlukker er det mest vanlige. Dørlukkeren må være tilpasset den aktuelle døra, og den må være justert slik at døra lukkes på en tilfredsstillende måte.[32]

Tilkopling av automatiske dørpumper må forhindre at dørpumpen forsøker å åpne døra før låsen i døra har gått i åpen stilling. All tilkopling skal være på sikker side av dørmiljøet.

Andre styringer for AAK
I tillegg til dører kan AAK styre heiser, rondeller, bommer, porter, kjøretøysperrer og lignende. Denne typen løsninger kan også kombineres med styring av TVO-kameraer, og dette vil spesielt være en fordel ved innpasseringspunkter. Ved sammenkopling av AAK mot slikt utstyr bør en ha klare og gode beskrivelser av grensesnittet mellom de ulike utstyrsleveransene.

Nettverk
AAK er å anse som et informasjonssystem som er knyttet sammen via nettverk.

Server/sentral og klientene er normalt koplet sammen med bruk av samme type teknologi

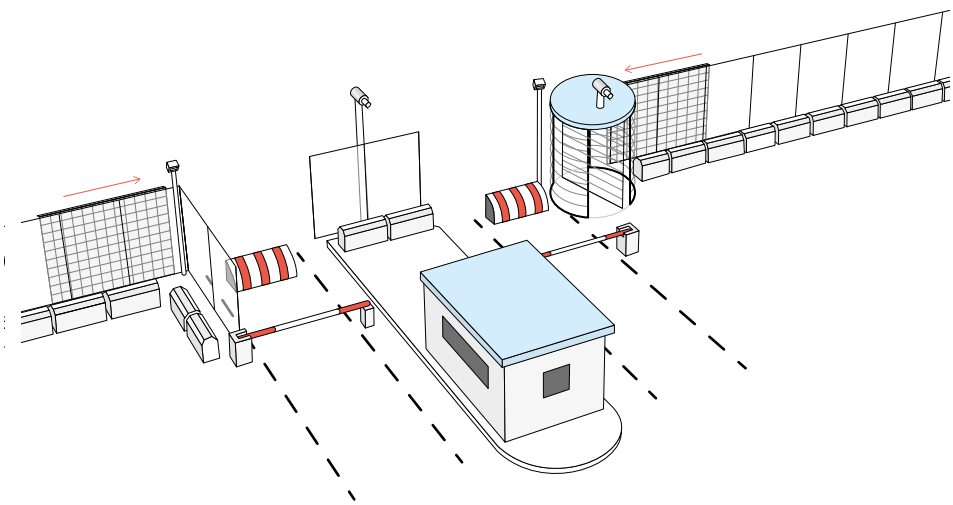
29
Det kan også benyttes fotocelle o.l. for automatisk åpning

30
For låstyper som ikke har mikrobryter innebygget i selve låsen, kan det være enklere å manipulere systemet til å tro at døra er lukket og låst dersom det kun er magnetbryteren som angir status

31
FG-godkjente sluttstykker er kun godkjent når låsen er låst uten spenning (rettvendt)

32
TEK10 stiller krav til dette

Porter, bommer, kjøretøysperrer og lignende



som de fleste andre datanettverk. Vanligvis er det busskommunikasjon (ring- eller stjernenett) som ivaretar informasjonsflyten mellom sentralen, undersentralene og kortleserne. Leverandøren vil i de aller fleste tilfeller ha sine egne anbefalinger om valg av utstyr og kabel til kommunikasjon, men for valg av traseer er det viktig at kommunikasjonen mellom undersentralen og dørmiljøet legges på sikker side av døren.

IKT-ansvarlig i virksomheten involveres i en tidlig startfase av prosjektet for å få kartlagt behov til løsning og krav til nettverkskomponenter som switcher, kabling etc.

Kortproduksjon for adgangskort

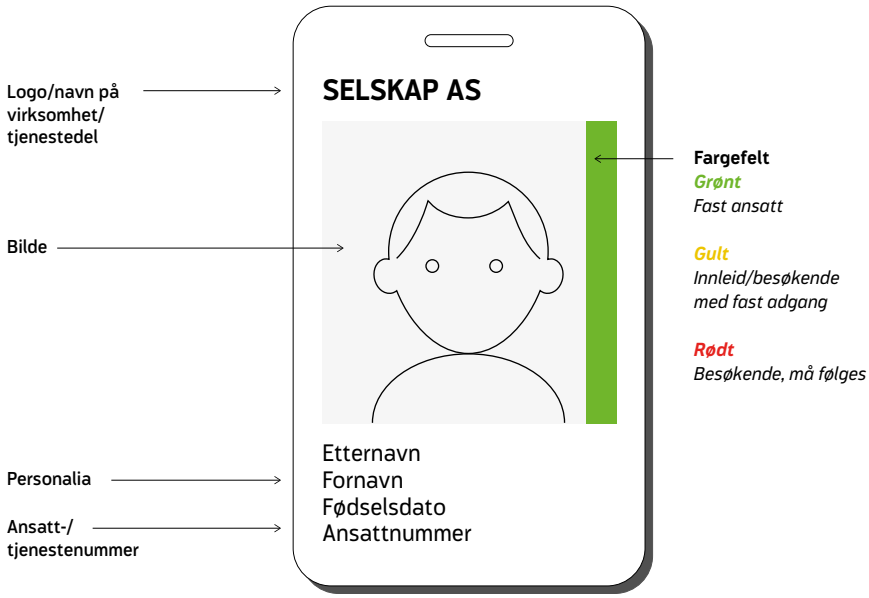
Adgangskontrollkort kan kjøpes ferdigprogrammert, men ut fra et sikkerhetsmessig perspektiv anbefales det at bruker produserer og koder adgangskortene selv. For mindre, enkle systemer med lav risikoprofil kan ferdig programmerte kort være et greit alternativ. Dersom virksomheten har et høyere krav til sikring, bør man kjøpe blanke kort og selv programmere disse. Uavhengig av løsning bør brukeren ha krypteringsnøkkelen for adgangskortene, slik at andre[33] ikke har tilgang til å manipulere systemet.

Mange av utstyrsleverandørene innen AAK kan også levere kortproduksjonsutstyr og i noen tilfeller bør det vurderes om dette skal være en integrert del av AAK-systemet.

Ved bruk av egen kortproduksjon er det spesielt viktig at man tar hensyn til følgende: Bruk kamera med tilstrekkelig god kvalitet for identifisering av person, slik at bildekvaliteten blir så god som mulig.

33 Kortprodusent, systemleverandør, vekter etc.

Adgangskort (eksempel)



Kortteknologi for AAK

Det finnes en rekke forskjellige kortteknologier som benyttes i AAK, hver med fordeler og ulemper. De mest brukte teknologiene for berøringsfrie (RFID) adgangskort i Norge er Mifare og HID. Det er også mulig å kombinere kort, PIN og biometri (fingeravtrykk, iris eller lignende). Adgangskort kan også leveres med smartbrikke med eget dataminne (smartkort). Dette åpner for en rekke nye muligheter som at kortet også benyttes for adgang til IKT-systemer o.l.

Berøringsfrie kort

Det finnes en rekke forskjellige berøringsfrie kortteknologier. Felles for disse kortene er at de har innbakt minnebrikke(r) og antenne, som blir aktivert av kortleserens spenningsfelt.

Proxkort

Disse kommer i hovedsak i to typer, én type der nummersekvensen er programmerbar, og én type som er låst fast. Denne typen teknologi brukes vanligvis ikke på nye anlegg da det er en eldre teknologi.

HID[34]

HID er en teknologi, hvor det er kortleverandør som setter krypteringskoden på adgangskortene.

De mest benyttede typer er:

→ *HID iClass*
→ *HID Mifare*
→ *HID Desfire*

Mifare

Mifare er en teknologi hvor brukeren selv kan sette krypteringskoden på adgangskortene.

34 HID kortteknologi leveres av HID Global

De mest benyttede typer er:

- *Mifare Classic*
- *Mifare DesFire*
- *Mifare DesFire Ev 1 og DesFire EV2*

Magnetstripekort

Denne typen kort var lenge dominerende som kortteknologi i AAK. Det skyldes først og fremst at det var en teknologi som ble benyttet på bankkort o.l. Teknologien består av magnetstripe som programmeres. Magnetstripekort er svært enkle å kopiere og bør ikke anskaffes på nye installasjoner.

Andre teknologier

Det finnes en rekke andre kortteknologier i bruk, magnetmønsterkort, metallbrikkekort, strekkodekort, hullkort, infrarøde kort m.fl. Disse omtales ikke nærmere her, da dette er foreldet teknologi.

Adgangskort

Adgangskortet er et bevis på at bæreren er autorisert for ferdsel i området, og skal bæres synlig. Kortet må utformes slik at det er mulig å raskt sammenligne bilde på kortet med ansiktet på kortbæreren, for eksempel når to personer som er ukjente for hverandre, møtes i en korridor, en døråpning eller lignende. Hologram på adgangskortet kan vurderes dersom det foreligger krav til et høyere sikkerhetsnivå.

Det bør også produseres kort for besøkende, servicepersonell, innleid hjelp, midlertidig lånekort for de ansatte og lignende. Det kan være formålstjenlig å benytte forskjellige fargekoder på kortene for lettere å skille personellgrupper fra hverandre.

Øvrige funksjoner

De fleste systemer har mange ulike tilpassede funksjoner, enkelte er beskrevet her.

Rans-/overfallsalarm

I en trusselsituasjon hvor en autorisert bruker tvinges til å åpne en dør for en ikke-autorisert, kan autorisert bruker taste en egen trusselkode og dermed varsle om situasjonen til vakt uten at trusselaktøren er klar over det (døren vil åpne på normal måte).

Anti passback

Anti passback vil si at kortet kun fungerer inn i et område/en sone ved bruk av en spesifikk kortleser. Kortet vil fungere som normalt inne på området, men kortet vil ikke fungere på andre kortlesere før du har registrert deg ut av området/sonen på en spesifikk kortleser.

Dette gjør det også mulig å holde oversikt over hvem som er inne i det aktuelle området, noe som også kan være svært nyttig hvis det skulle oppstå brann eller andre kritiske hendelser.

Anti passback bør kun benyttes der man har personsluser for inn- og utpassering.

Tailgating er når en person som ikke har autorisert adgang, følger etter en person med autorisert adgang når han/hun benytter adgangskortet for å passere. Dette kan enkelt forebygges ved å benytte personsluser på inn- og utganger.

Logg

Hendelsesloggen viser alle endringer og statuser på anlegget. Om systemet har en god søkemotor innebygget, kan man begrense søk til f.eks. dørmiljø, alarmpunkt, kortinnehaver, kort, bestemte statusendringer, og kombinere disse med tidsperiode.

Systemloggen viser hvem som utfører hvilke endringer (programmeringer) og når på klient og server.

Andre AAK-systemløsninger

Det eksisterer også andre enklere løsninger. Felles for de systemene som presenteres nedenfor, er imidlertid at sikkerheten ved systemene ikke ivaretas i samme grad sam-

menlignet med løsningene som er presentert i forrige avsnitt.

Trådløse kortlesersystemer
Det finnes flere typer fabrikater her. De fleste store leverandørene har dette i sitt segment. Løsningene er forskjellige, med ulike typer kommunikasjonsplattformer og kortteknologier.

Fellesnevneren er at sikkerhetsnivået i hovedsak er lavt. Det dreier seg om online-systemer, delvis online-systemer (kommunikasjonen åpner f.eks. hver time) og rene offline-systemer.

Stand-alone/offline-systemer
Det finnes også ulike typer stand-alone-systemer. Disse er mer å regne som passeringskontrollsystemer enn adgangskontrolsystemer. Fordelen med disse er at de er billigere å anskaffe, og har trådløs teknologi. Ulemper ved slike systemer er imidlertid at sikkerheten ikke er like god, det er ingen varslingsmuligheter ved uregelmessigheter, og man har derfor lav kontrollmulighet.

TV-overvåkningsanlegg (TVO)

Bruk av TVO i en sikringssammenheng kan benyttes til å overvåke kritiske deler av områder eller bygg og til enhver tid følge med på aktivitet i området, eller som et hjelpemiddel for å få god oversikt. TVO kan også benyttes til deteksjon dersom man benytter avansert videoanalyse.

En annen funksjon er at vaktmannskaper kan kontrollere adgangen til porter og dører uten selv å være eksponert for angrep. TVO som verifisering av hendelser gir mulighet for tilpasset reaksjon (for eksempel fra vaktstyrke eller politi) uten å måtte verifisere på stedet. Bilder fra TVO som lagres gir muligheter for bevisførsel av hendelser.[35]

Beskrivelse av TVO

TVO-anlegget består av en rekke enkeltprodukter, som ofte kommer fra forskjellige produsenter. Utstyrsprodusenter benytter forskjellige spesifikasjonsstandarder, noe som gjør det vanskelig å sammenligne utstyret. Førsteklasses utstyr fra forskjellige produsenter gir nødvendigvis ikke et førsteklasses sluttprodukt hvis de ikke er tilpasset hverandre.

Utvikling av kameraer går stadig fremover, og oppløsningen i kameraer økes i takt med den teknologiske utviklingen.

Det bør minimum benyttes optiske kameraer med HD-oppløsning dersom det ikke er forhold som tilsier noe annet. Det er ulike oppfatninger om hva som bør være minimum av oppløsning i forhold til det spesifikke kameraets oppgave. «Live video» er definert til 25 bilder per sekund og digitale kameraer kan vanligvis lagre mellom 0,5 til 30 bilder per sekund.[36] Dette vil kunne bidra til å redusere lagringsmengden fra hvert enkelt kamera vesentlig. Dersom systemet har avansert videodeteksjon, kan systemet ha eks. min. 12 bilder per sekund for at analysen skal fungere.

I ***tabellen Generell oppløsning for ulike typer kameraer*** på side 177 vises oppløsningstabeller for optiske og termiske kameraer. Tabellene viser sammenhengen mellom betegnelsen på kameraet og oppløsningen det har. Lavere oppløsning gir dårligere kvalitet på bildet, mens høyere oppløsning gir bedre bilde, men vil imidlertid kreve mer lys.

Ved prosjektering av TVO er det viktig å vurdere hvilken funksjon de forskjellige kameraene skal ha.

Forhold som kan spille inn, er:
→ *Topografi, lysforhold, kameraplassering, klimatiske forhold og andre omgivelser*

35
Ofte kan det være en forutsetning at TVO-systemet har elektronisk våtmerkestempel for å verifisere ektheten av opptaket

36
Enkelte kameraer lagrer også 60 bilder per sekund eller mer

Sikringsklasser TVO

Sikringsklasse	Beskrivelse/krav
1	**Krav til TV-overvåkningsanlegg (TVO) som:** → Kun har lokal monitorering og lagring
2	**Krav til TV-overvåkningsanlegg (TVO) som:** → Har lokal monitorering og lagring → Har mulighet for overføring til vakt/alarmstasjon Skal minimum tilfredsstille NEK EN 62676
3	**Krav til TV-overvåkningsanlegg (TVO) som:** → Har lokal monitorering og lagring → Lokal lagring på redundant løsning → Skal kunne samhandle med AIA- eller AAK-anlegg → Har videooverføring til alarmstasjon ved alarmsituasjon eller på kommando → Har mulighet for videoanalyse eller integrasjon mot analysesystem → Alle sentralkomponenter er tilkoplet UPS → Kameraer og andre nettverksenheter skal varsle ved feil Skal minimum tilfredsstille NEK EN 62676 og NEK EN 50132. Kravspesifikasjon*
4	**Krav til TV-overvåkningsanlegg (TVO) som:** → Har lokal monitorering og lagring → Har lokal lagring på redundant løsning → Skal kunne samhandle med AIA- eller AAK-anlegg → Har kontinuerlig lagring av opptak på sikringsobjektet → Har videooverføring til godkjent alarmstasjon, kontinuerlig, ved alarmsituasjon eller på kommando, som kan lagre video → Skal ha alle mekanismer som kan hindre en avansert trusselaktør i å sabotere anlegget (krav til plassering av komponenter, skjerming av kabler, etc.) → Har mulighet for videoanalyse eller integrasjon mot analysesystem → Alle komponenter er tilkoplet nødstrøm og UPS → Kameraer og andre nettverksenheter skal varsle ved feil Skal minimum tilfredsstille NEK EN 62676 og NEK EN 50132. Kravspesifikasjon*

* Nasjonalt kompetansesenter for sikring av bygg har utarbeidet egen kravspesifikasjon. Denne er gradert.

→ *Kameratype (optisk/termisk), linse/optikk, krav til oppløsning, bildekvalitet, nettverk, maskinvare servere og klienter*
→ *Type TVO-system programvare (VMS – Video management system)*
→ *Type avansert videoanalyse programvare (VCA – Video content analytics)*
→ *Skjult eller diskret overvåkning*

Det finnes ingen «korrekt» mal, så dette bør vurderes i hvert spesifikke tilfelle for å få et optimalt resultat.

Generell oppløsning for ulike typer kameraer

Betegnelse	Oppløsning i piksler
Generell oppløsningstabell for analoge optiske kameraer	
Analog (4CIF / D1)	704x576 (linjer)
720p (HD ready)	1280x720
1,3 MP	1280x1024
2,0 MP	1600x1200
1080p (HD)	1920x1080
3,1 MP	2048x1536
5,0 MP	2952x1944
2160p 4K (UHD)	3840x2160
10,0 MP	3648x2752
Generell oppløsningstabell termiske kameraer	
Lav oppløsning	160x120
Lav oppløsning	320x240
Standard oppløsning	640x480

Forslag til minimumskrav for ulike kamera

Type	Oppløsning ved objektet
Identifikasjon (Utendørs)	5 piksler per. cm
Verifikasjon	2,5 piksler per. cm
Observasjon	1,25 piksler per. cm
Deteksjon	0,25 piksler per. cm

Deteksjon

Benyttes gjerne for perimetersikring og typiske normer som benyttes, er krysselinje «trip-wire» og områdedeteksjon «forbidden area». Et objekt på 1 x 0,5 meter bør ikke underskride 30 piksler på den maksimale deteksjonsavstanden.

Termisk kamera egner seg meget godt til deteksjon av denne type.

Verifikasjon

Det bør kunne skilles på om objektet er sivilt eller militært, og hvor mange personer og/eller kjøretøyer det dreier seg om.

Typisk verdi vil være at det minimum skal 80 mm pr. piksel.

Identifikasjon

For å identifisere bør man ha 250 piksler i bredden på bildet der man skal identifisere, men dette er avhengig av de forhold som angitt over. Typisk vil være at et tall i et registreringsskilt minimum er 15 piksler høyt. Et ansikt med bredde på 16 cm bør minimum være 40 piksler i bredde.

Termisk kamera kan være uegnet til identifikasjon.

Se også standard NEK EN 62676.

Hoveddeler i et TVO-system

Analoge TVO-system er gjerne eldre type, med analoge kameraer tilkoplet en matrise, og/eller DVR (Digital Video Recorder) lagringsenhet. Ofte med monitorer tilkoplet direkte i DVR-enheten eller med en pc-klient som viser ett eller flere bilder på en eller flere skjermer.

Hybrid TVO-system består ofte av en DVR/NVR/Server[37] som har mulighet for tilkopling av både analoge og digitale IP-kameraer. Analoge kameraer blir koplet rett inn i DVR/NVR eller ved bruk av enkodere.[38] IP-kameraer tilkoples TVO-systemets nettverksstruktur. Enheter i systemet blir som regel tilkoplet via nettverk. Sentralenheten kan ofte tilkoples flere skjermer eller pc-klient med monitor(er).

Digitalt TVO-system består i hovedsak av IP-kameraer[39] tilkoplet en nettverksstruktur. Bilder lagres på server(e), og anlegget betjenes fra en eller flere pc-klienter. Systemene er ofte veldig fleksible, og intelligent videoanalyse kan integreres. Ved etablering av nye TVO-systemer i dag benyttes hovedsakelig kameraer med full HD-oppløsning (1080p /1920x1080), med mindre forhold eller ønsket funksjon tilsier noe annet.

Programvare (Video management system – VMS)

Det leveres i dag mange programmer for TVO-system, fra de enkleste som kun viser ett bilde, til det som har innebygget videoanalyse for ulike problemstillinger, SMS-varsling og distribusjon til smarttelefoner. Det er derfor viktig for brukeren å gjennomføre en egen undersøkelse av krav til funksjonalitet og driftsstabilitet hvor nødvendig support er lett tilgjengelig.

Videodeteksjon

Forskjellige systemer har mer eller mindre avansert deteksjon. Forskjellen ligger i hvor avansert og god signalbehandlingen er, før programmet avgjør hva endringen skyldes, og varsler en alarm.

Videodeteksjon kan deles i to hovedgrupper: System som baserer seg på bevegelsesdeteksjon (motion detection), og system med intelligent videoanalyse (video content analytics).

Bevegelsesdeteksjon

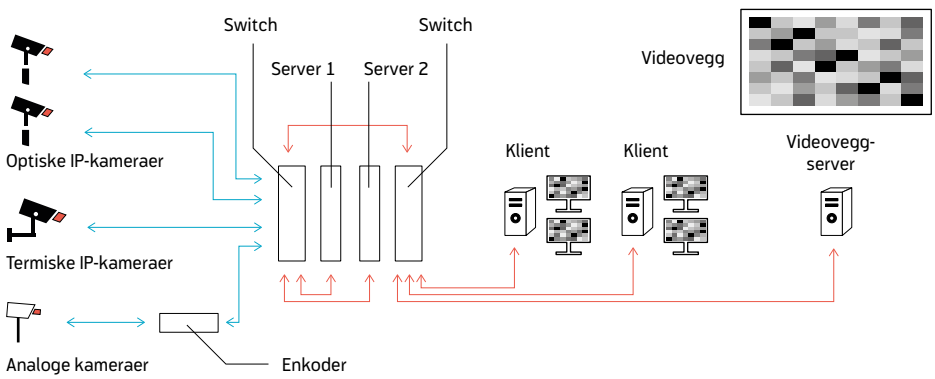
Bevegelsesdeteksjon er i store trekk basert på endringer i bildene som normalt kan leses som lys-/kontrastendringer, eller det som også betegnes som grå-tone-endringer. Normalt defineres det ett eller flere deteksjonsfelt i bildet med en skala på hvor mye bevegelse i feltet som skal endres, og alarm utløses ved beve-

37
DVR: Digital video recorder, NVR: Network video recorder

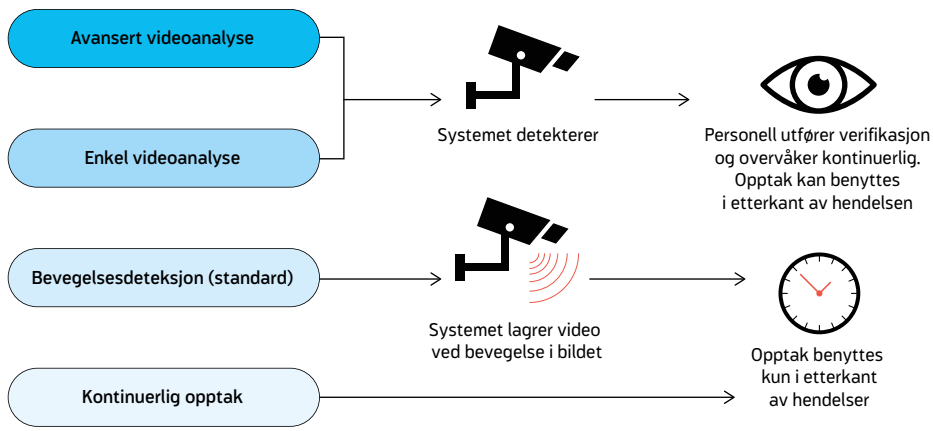
38
Enkoder: Konverterer analogt videosignal til digitalt videosignal (IP)

39
IP-kamera er digitalt overvåkningskamera som koples direkte til en nettverks switch som overfører signalet til server, klient eller andre nettverksenheter

Hoveddeler i et TVO-system



Videodeteksjon



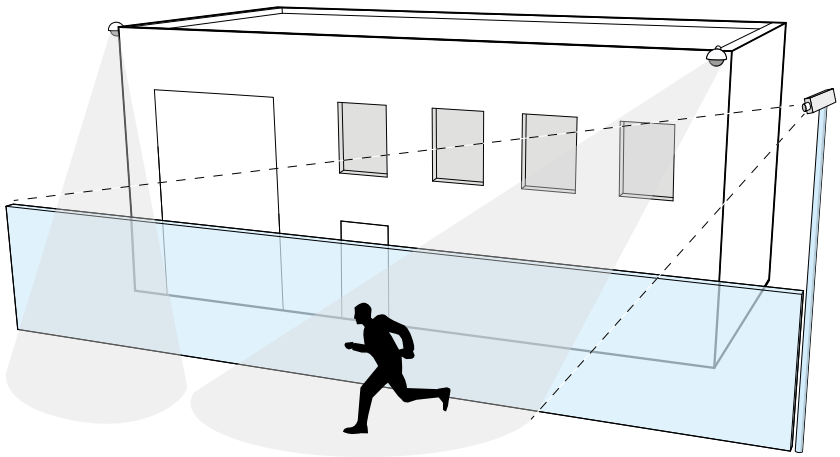
gelse i bildet. Uten korreksjoner vil dette egne seg mindre godt utendørs, fordi det utendørs er en rekke naturgitte forhold som påvirker et videodeteksjonssystem.

Intelligent videoanalyse
(Video content analytics – VCA)
Intelligent videoanalyse er et avansert system som ved avansert programvare kan skille mellom ulike type objekter, som f.eks. mennesker og biler. De fleste systemer beregner størrelsen på objektet, hastighet og retning, sammen med innebygde algoritmer. Dette gir et grunnlag for å avgjøre om dette er et menneske som kryper/går, et kjøretøy, etc. Systemet kan hurtig detektere på ulike hendelser.

Typiske hendelser er:
→ *Kryssing av linje (detekter når noen eller noe krysser en bestemt linje i en bestemt retning)*

Videoanalyse

Videoanalyse med deteksjon ved kryssing av linje



- → *Forbudt område (detekterer når noen eller noe beveger seg inn på et område)*
- → *Telling (teller personer som krysser ett bestemt punkt)*
- → *Bestemt kjøreretning*
- → *Kun kjøretøy tillatt, ikke personer eller omvendt*
- → *Fjerning av objekt (for eksempel maleri etc. Benyttes kun innendørs)*
- → *Gjenglemt objekt (f.eks. koffert etc.). Slike funksjoner fungerer ikke alltid optimalt, spesielt ikke der det er mye bevegelse eller «støy» i bildet.*

Videoserver

En videoserver er en datamaskin med en eller flere harddisker for lagring av video, samt egen harddisk for lagring av konfigurasjonen av TVO-anlegget. Videoserveren bør stå i et eget lukket nettverk tilknyttet klienter og kameraer etc. Alle bilder fra alle kameraer kan lagres kontinuerlig, men for å effektivisere lagringskapasiteten finnes det flere muligheter:

- → *Komprimere video*
- → *Redusere antall bilder per sekund som lagres*
- → *Lagre video når det er aktivitet i bildet (VMD)*
- → *Lagre video ved alarm fra AIA*
- → *Lagre video ved hendelser fra AAK*
- → *Lagre video ved hendelser i videoanalyse (VCA)*
- → *Redusere oppløsningen (lite egnet)*
- → *Kombinasjon av overnevnte*

Den totale lagringskapasitet avhenger altså av flere faktorer. Antall dager med opptak, antall kameraer som tilknyttes, oppløsningen på kameraer i systemet, hvor mange bilder pre sekund som lagres totalt, og hvilken type komprimering det benyttes, er de vanligste faktorene, men det er ikke noen korrekt fasit.

PoE-klasser (Power over Ethernet)

Standard PoE	PoE+	High PoE	PoH
7,5 watt	15 watt	30 watt	60 watt

Det er flere metoder for å komprimere video. Følgende er mest benyttet

- *MJPEG – Meget god billedkvalitet, men krever mye lagringsplass og båndbredde. Egner seg best til «live» videofremvisning*
- *MPEG4 – Eldre komprimeringsmetode, ofte store og plasskrevende filer.*
- *H.264 – God billedkvalitet, komprimerer bildet mer.*

Ulike TVO-systemer har også egne varianter av videreutviklede standarder av overnevnte.

IKT-nettverk

Å designe nettverket korrekt er kritisk viktig for å unngå «flaskehalser». Det bør benyttes kvalitetsutstyr, og med programmerbare switcher. Nettverkskabling skal utføres på godkjent måte i henhold til kravene for EN-50173. Switchene bør være av god kvalitet og ha god over-kapasitet. Flere kameraer som leveres i dag, benytter PoE (Power over Ethernet) for strømforsyning. Dette betyr at det er switchen som overfører signal fra kamera til server/klient og strømforsyner kameraene. Switchene må da ha nok kraft til å forsyne alle kameraer som er tilkoplet. Det er også mulig å benytte en injektor for direkte strømforsyning.

Tabellen PoE-klasser beskriver de ulike PoE-klassene[40] som er mest vanlige for tv-overvåkning.

Klient

Med klient menes pc-en operatøren benytter for å betjene TVO-systemet. Her vil bilder, alarmer og statusendringer ute i anlegget presenteres. Her endres også oppsettet for systemet. Klienter bør ha redundant strømforsyning.

Større systemer har ofte flere klienter som alle har flere monitorer. Siden klienten ofte skal vise store videostrømmer, krever dette betydelig kapasitet av grafikkort o.l., for å imøtekomme krav til oppløsning, tilkopling og håndtering av større mengde data.

Fra klienten kan en operatør velge kameraer for å se «live», styre bevegelige kameraer, hente inn bilder fra flere kameraer vist på en eller flere monitorer eller se og søke i opptak eller hendelser. Operatørrettigheter kan tildeles individuelt, og hver operatør bør logge seg inn med eget passord.

Monitor

Monitorer som leveres til TVO-systemer, er stort sett beregnet for døgnkontinuerlig bruk. Større TVO-systemer kan ha flere monitorer tilkoplet sammen til en videovegg. Størrelse og oppløsning på monitoren(e) bør vurderes tidlig. For å kunne gi optimalt gode bilder, må monitoren være tilpasset oppløsningen i kameraet.

Skal operatøren ivareta et sikkerhetsanlegg, er ikke dette en bifunksjon, men en primærfunksjon, og må utformes deretter. Det innebærer at dersom operatøren har andre arbeidsoppgaver, skal ikke synsvinkelen endres nevneverdig under de ulike operasjonene.

Kamera

Kameraer til TVO leveres i et meget stort utvalg, både med hensyn til pris og kvalitet. Til nye TVO-anlegg leveres i dag stort sett IP-nett-

40
Standarden 802.3af beskriver krav til Standard PoE og Poe+, mens standarden 802.3af beskriver krav til High PoE og PoH

Optisk kamera

Optisk minidome kamera. **FOTO** Forsvarsbygg

Termisk kamera

Termisk bilde av perimetergjerde. Tatt om natten.
FOTO Forsvarsbygg

verkskameraer, men det finnes fortsatt flere analoge modeller. Fordelen med et IP-kamera er nyere teknologi, hovedsakelig bedre oppløsning, flere innebygde muligheter og større fleksibilitet.

Flere kameraer har i dag også inn- og utgang for lyd[41] som kan brukes for å kommunisere et varsel, eller opplyse en trusselaktør som tar seg inn at vedkommende er oppdaget.[42] Andre grunner kan være hvis det er behov for å ha stemmeopptak av trusselaktør eller man har behov for å høre hva som skjer ute på objektet, f.eks. at det benyttes verktøy etc. Det finnes også forskjellige spesialkameraer, for eksempel kameraer med innebygd lysforsterkerutstyr.

Det skilles mellom optiske og termiske kameraer.

Optiske IP-kameraer

Disse kameraene kommer i flere utgaver, og mange er skreddersydde til å løse forskjellige utfordringer. Et IP-kamera er avhengig av nettverkskabel for bildeoverføring, strømtilførsel for kamera og eventuelt varmeelement. Det leveres også IP-kamera som kun krever en nettverkskabel for signaloverføring, strømforsyning og eventuell styremotor (Power over Ethernet, PoE). Switchene i nettverket må da dimensjoneres for å forsyne kameraet med strøm.

Kameraene kan ha inngang/utgang for mikrofon/høyttaler, og I/O-kort for styringer. Det er fordelaktig om kamera leveres med automatisk fokusjustering. Dette gjør at man kan endre fokusfelt på bildet fra kamera i programvaren og ikke ute på selve kamera – noe som ofte koster tid og penger (og er væravhengig på utvendig kamera). Noen kameraer leveres også med styrt fokus og zoom-mulighet fra programvare (DC-styrt objektiv).

Optiske analoge kameraer

Disse leveres i flere utgaver og benytter hovedsakelig coaxialkabel for signaloverføring av video til sentralenhet. De fleste kameraer kommer med automatisk dag/natt-funksjon, og innebygget elektronikk som bearbeider bildet lokalt i kameraet og øker lysømfintlighet. Vanligvis gir kamera med mekanisk dag/natt-filter bedre bilder enn tilsvarende kamera med elektronisk dag/natt-filter. Strømtilførsel til kameraet, varmeelement og eventuelt styremotor bør legges frem til kamerapunktet. Styrbare analoge kameraer krever som regel en egen to-tråds kabel for signaler til styring, men

41
Ved opptak av lyd sammen med video skal det søkes spesielt om dette til Datatilsynet

42
Dette krever at lyd inn- og utgangen er tilkoplet et lydanlegg med mikrofon og høyttaler

de fleste systemene kan overføre signalene via samme kabel som videosignalet.

I perimetersikring bør benyttes termiske kameraer til deteksjon og optiske kameraer til verifikasjon. Det er ikke anbefalt å benytte optiske kameraer til perimeterdeteksjon, grunnet svake prestasjoner i dårlig vær.

Optikk – optiske kamera
Sensorbrikkene leveres i forskjellige størrelser[43], normalt gir større brikke bedre bilde enn mindre brikke, men de krever mer lys. De fleste TVO-kameraer gir fargebilde på dagtid og skifter automatisk til sort/hvitt på natt da dette gir bedre bildekvalitet ved dårlig belysning. Det er her viktig å bruke kameraer med mekanisk nattfilter og ikke elektronisk, da dette vanligvis gir bedre billedkvalitet.

De fleste kameraer fungerer i det infrarøde spekteret. Det betyr at de kan benyttes sammen med IR-belysning.

Fast optikk har et fast synsfelt. Zoom-optikk har et variabelt synsfelt (fra vidvinkel til tele).

Fokuseringen kan innstilles på selve optikken på faste kameraer, mens på zoom-kameraer skjer den automatisk.

Termiske kameraer
Termiske kameraer «ser» den termiske strålingen (varmebølgene) fra for eksempel personer og forskjellige bakgrunner, og produserer et termisk bilde. Termiske kamera har i hovedsak lavere oppløsning enn tradisjonelle IP-kameraer. Faste termiske kameraer kommer med fast optikk, fra nærbilde (vidvinkel) til avstandsbilde (televinkel). Termiske kameraer kan se kroppsvarme fra noen få meter til kilometer, avhengig av modell, optikk, fabrikat og miljø. Termiske kameraer kan med stor effektivitet benyttes i perimetersikring da det ikke påvirkes av lys/mørke, men de kan påvirkes av tett snødrev og tåke, røyk og til dels regn. Kombinasjonen av tett snødrev og billys kan medføre problemer.

Bevegelige kameraer (Pan Tilt Zoom – PTZ)
Dersom det er behov for et bevegelig kamera, kan det benyttes et styrbart domekamera. Med domekamera menes et kosteffektivt kamera som er montert inne i en kuppel. Disse kan styres horisontalt og vertikalt, og har zoommulighet.

Domekameraer kan kun benyttes til enkelte kameratyper, stort sett opp til 36 x optisk zoom for optiske og 140 x zoom for termisk. PTZ-kamera kan ha forhåndsprogrammerte posisjoner, som betyr at de automatisk stiller seg inn på bestemte posisjoner ved signal fra eksterne systemer, f.eks. AIA eller AAK.

Overføring av video til vakt
Overføringssystemer for TVO kan hovedsakelig deles inn i to kategorier:

- *Direkte overføring av video til lokal vaktsentral. Benyttes oftest når TVO automatisk overfører video ved hjelp av alarm fra AIA eller AAK eller intelligent videoanalyse.*
- *Alarm fra AIA overføres til annen vaktlokasjon. Her henter alarmoperatør opp kameraer fra lokasjonen på sin klient for verifisering av hendelsen.*

Dedikerte lyskilder
IR-lysenheter kommer i ulike modeller som belyser forskjellige bredder og lengder, men typen bør være tilpasset kameraet. Kameraer som leveres med innebygd IR-belysning, belyser gjerne et felt opptil 25 meter foran kameraet, men eksterne IR-lyskastere kan belyse felt opp til 200 meter. Det benyttes i dag hovedsakelig IR-LED-lys.

Hvitt lys (konvensjonelt lys)
Hvitt lys-enheter til TVO fungerer på samme måte som en lyskaster, men er designet for å

43
Normal sensorbrikkestørrelser er: 1/2", 1/3", 1/4" og 1/6"

Termisk kamera

Termiske kameraer leveres som regel med fast linse. **FOTO** Forsvarsbygg

gi et jevnere lys i stedet for et kraftig konsentrert lys. Lyskasteren er utformet på en måte som gjør at lyset fordeles jevnt utover en bred flate. Lyset er optimalisert i forhold til kameraets egenskaper.

Det brukes ofte LED-dioder til begge typer lys. Det kan med fordel kombineres med sikringsbelysning.[44]

Lysforhold

Et optisk TVO-kamera er avhengig av lys for å kunne produsere et bilde. Det finnes kameraer som gir gode bilder selv ved meget svak belysning, men kameraene er avhengige av et relativt jevnt lysnivå for å gi gode bilder.

Kameraenes lysømfintlighet oppgis med verdien lux. Det er en enhet for å måle reflektert lys. Når databladet til et kamera oppgir at det gir gode bilder ved for eksempel 1 lux, er dette vanligvis lys målt rett på sensoren, se tabell ***Omtrentlige luxverdier ved ulike belysningsforhold***, neste side.

Som det fremkommer av tabellen, er det snakk om meget store variasjoner, og ingen kameraer kan gi gode bilder under alle lysforhold. Kraftige refleksjoner fra f.eks. sol på snø vil kunne blende et kamera fullstendig. I tabellen på neste side vises ca. refleksjonsverdi på noen objekter.

Integrerte sikringssystemer

Med ***integrerte sikringssystemer*** menes automatiske innbruddsalarmanlegg, automatiske adgangskontrollanlegg og tv-overvåkningsanlegg som i større eller mindre grad er sammenkoplet. Anleggene kan også omfatte brannalarm, porttelefon, portstyring med mer. Graden av sammenkopling kan variere. Definisjonen av integrasjon i sikkerhetssystemer kan være alt fra potensialfrie kontakter til

44 Sikringsbelysning er nærmere beskrevet i kapittel om perimetersikring

Omtrentlige luxverdier ved ulike lysforhold

Lysforhold	Ca. lux verdi
Stearinlys, 20 cm avstand	10
Kraftig lommelykt, 1 m avstand	250
Gatebelysning	20 – 200
Kontormiljø	400 – 800
Sollys gjennom vindu, ettermiddag	3500
Sommerdag i sola	40 000 – 100 000

Omtrentlig refleksjonsverdi for noen objekter

Objekt	Refleksjon
Snø	95 %
Hvit sement	85 %
Betong og grønt gress	40 %
Lys hud	25 %
Asfalt	5 %
Våt asfalt	2 %

avansert integrering med ulike protokoller og databaseintegrasjoner.

Av driftsmessige hensyn skal man gjøre en vurdering av nytten av å sammenkople flere sikringssystemer til et integrert system. Ideelt sett skal det benyttes autonome systemer for AIA, AAK og TVO. Det er imidlertid en viktig integrasjon å kunne presentere de ulike systemene på en enhetlig, ensartet og effektiv måte for operatører som betjener sikkerhetssystemene.

Under følger ulike eksempler på databaseintegrasjoner og styringer.

Eksempel 1: Når dør med AAK blir brutt opp, sendes det et signal til TVO. Kameraet som overvåker korridoren med bevegelsesdeteksjon (motion detection), tar opp hendelsen og viser live video. Dette vil presenteres i vakt på «pop-up»-skjerm med alarm. Hendelser linkes også sammen i database-logg.

Eksempel 2: Det opprettes et perimetersikringssystem. Det blir programmert inn soner for de ulike områdene rundt perimeteren. Ved alarm på et av deteksjonssystemene, f.eks. på sone 2, vil et kamera snu seg mot sone 2, ta opp hendelsen, og 60 sekunder etter at alarmstatus er normal igjen. Dette vil presenteres i

vakt på «pop-up»-skjerm med alarm. Hendelser linkes også sammen i databaselogg.

Nettverk

En generell bemerkning knyttet til elektronisk sikring er at et økende antall av sikringssystemer som leveres i dag, er avhengig av nettverk.[45] Elektroniske sikringssystemer bør av sikkerhetsmessige årsaker alltid legges på eget lukket nettverk med mindre det er forhold som tilsier annet. Dette gjøres for å ivareta sikkerheten og integriteten ved systemet.

Uavhengig av nettverkets størrelse bør alltid bruker, driftsansvarlig og kravstiller (IKT-avdeling o.l.) involveres for å få et best mulig resultat. Det må tas med i betraktningen at dette bør være et lukket nettverk som har full redundans. Spesielt ved TVO-installasjoner bør nettverket beregnes med stor kapasitet og i samarbeid med leverandør av TVO-system.

Det er derfor viktig å involvere riktige parter på nettverkssiden, og å være trygg på at leverandør også har kompetanse på dette. I tillegg bør kjøper ha kunnskap om utstyret og bruken av det.

Det vil, uavhengig av oppbygning og hvor tett nettverket er integrert i sikringssystemene, være viktig at det nettverket som benyttes, er stabilt og designet for å takle de utfordringene som det settes krav til. Det kan være båndbredde, oppetid, fleksibilitet, sikkerhet på selve nettverket med mer.

Det å designe nettverket med korrekt kablingsstruktur og switcher for å unngå «flaskehalser» er kritisk viktig. Videre anbefaler vi å benytte kvalitetsutstyr med programmerbare switcher[46] på større anlegg. Nettverkskabling skal utføres på godkjent måte, beskrevet i kravene for NEK EN-50173.

Det anbefales å skille de ulike fagområdene AIA, AAK og TVO i forskjellige lukkede nettverk. Dette kan gjerne gjøres i virtuelle nettverk, dersom systemene ikke skal sikkerhetsgodkjennes iht. sikkerhetsloven.

Alle porter i switcher bør ha managment, og portene bør logisk låses til faste MAC-adresser.[47] For utvendige IP-kameraer og andre sensorer bør porten på switchen låses logisk og deaktiveres dersom forbindelsen brytes.

Dersom det er kritisk viktig at alle sensorer og alarmsystemer fungerer ved strømbrudd, må også alle switcher, klienter, servere og komponenter ha redundant strømforsyning.

45
TCP/IP (Transmission Control Protocol/Internet Protocol) er en gruppe kommunikasjonsprotokoller som benyttes for å koble sammen enheter (eks. datamaskiner) i nettverk

46
Switcher med management

47
Media Access Control address

Symboler for AIA

SA	Sentralapparat		Mikrofon
	Ranskontakt/Fingertrykk		Låskontakt
	Ranskontakt/Fingertrykk m/lys		Elektrisk dørlås/sluttstykke
	Ranskontakt/Fottrykk		Vann
	Seismisk detektor for hvelv- og safedør		Foto-kamera
	Seismisk detektor for vegger, gulv og tak i hvelv		Kontrollpanel-foto
	Magnetkontaktåpning/Åpningskontakt		TV-kamera
	Lysdetektor	V	Video-opptaker
	Bespinning		Videovelger
S M	Linjedetektor		TV-kamera m/beskyttelseshus
	Ultralyd-detektor		Startknapp-foto
	Mikrobølge-detektor		Monitor
	Passiv infrarød detektor (pir) på vegg venstre, i tak høyre		Sirene
AM AM	Kombinert pir/pir med antimask på vegg venstre, i tak høyre		Summer
	Kombinert pir – ultralyd på vegg venstre, i tak høyre kan også være antimask – se over		Horn
	Kombinert pir – mikrobølge på vegg venstre, i tak høyre kan også være antimask – se over		Alarmklokke
	Glassbrudd detektor		Brannalarmsentral
S M	Alarmtransmisjon sender (venstre) Mottaker (høyre)		Manuell brannmelder
S/M	Alarmtransmisjon sender/mottaker	°C	Varmedetektor
	Tåkesikring		Flammedetektor
	Kortleser m/tastatur		Røykdetektor
	Kortleser u/tastatur	I	Røykdetektor, ione
	Seddelklips/Klype		Røykdetektor, optisk
	Styringsenhet	M K	Røykdetektor, multikriterie
	Forbikopler	L D	Røykdetektor, linjedetektor
	Lysdiodeindikator	ARD	Røykdetektor, aspirasjon
	Varsellampe	I U	Brannteknisk styresignal signal inn (venstre) Signal ut (høyre)


garnisonsforvaltning
VAKT & SIKRING
MILITÆR
VAKT

Kapittel 13

Vakthold og reaksjonstiltak

Dette kapitlet presenterer alternativer for vakthold og reaksjonstiltak. Forskjellige alarmmottak og reaksjonsstyrker beskrives, og ulike begreper gjennomgås.

For noen virksomheter kan det være tilstrekkelig å bemanne inngangen med resepsjonstjenester som utfører inn- og utpasseringskontroll. I andre og mer utsatte virksomheter kan det være nødvendig å dimensjonere mot et mer alvorlig trusselbilde.

Relevante spørsmål som virksomheten bør stille seg, er:

- *Hvilke trusler kan vi bli utsatt for?*
- *Hvilke sikkerhetstiltak vil redusere risikoen for mulige, tilsiktede hendelser?*
- *Hvilken kapasitet har vakten?*
- *Hvilket samarbeid har vi med politi eller andre reaksjonsstyrker?*

Vakt, alarmmottak og reaksjonsstyrke må ses i sammenheng med hvilke behov virksomheten har for sikring av sine verdier, hvilke sikringstiltak som er implementert, og hva slags trussel man har valgt å dimensjonere seg mot.

Det anbefales at det gjennomføres en risikoanalyse før det fastsettes krav til vakt- og reaksjonsstyrke. Sivile virksomheter angir krav til vakt- og resepsjonstjenester i interne sikkerhetsbestemmelser.

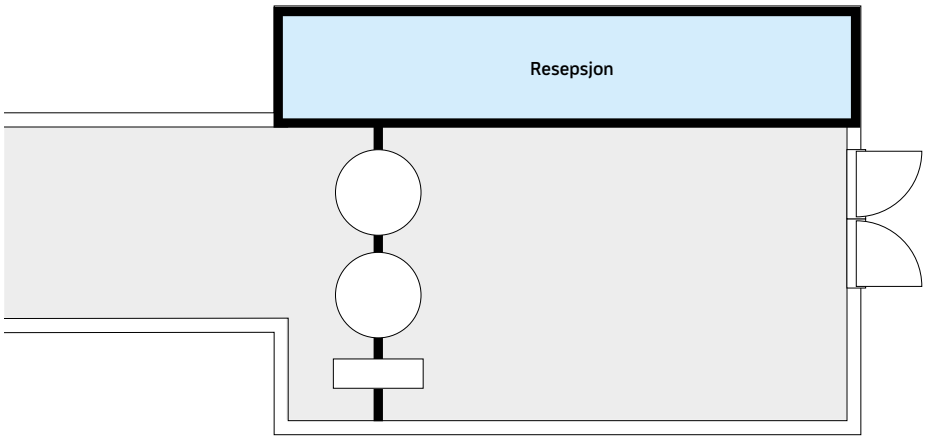
Vakthold

Med begrepet vaktlokale menes alt fra et enkelt skilderhus for værbeskyttelse, en portvakt eller et resepsjonsområde til et eget forsterket rom med sluseløsninger, skuddhemmende glass og andre sikringstiltak. Betjeningen i dette området kan være en resepsjonist, en vekter, portvakt, ordensvakt eller annet personell som også kan inngå som del av et mer omfattende adkomstparti med søkssoner, patruljering, varemottak, skannersystemer, betjening av adgangskort, journalføring av inn- og utpassering m.m.

Vi skiller mellom resepsjonsfunksjonen som en ren servicefunksjon og vaktfunksjonen som del av sikkerhetsinstallasjonene, og vi velger i fortsettelsen av dette kapitlet å bruke begrepet «vaktlokale» som betegnelse på funksjonen der besøkende kan henvende seg i forbindelse med kontroll ved inn- og utpassering.

Vaktfunksjonen bør ha en utforming som tillater bortvisning av ikke-autoriserte besøkende uten at dette forhindrer ordinær inn- og utpassering. Dersom beredskapsnivået heves, må det være mulig med enkle grep å gjøre tilpasninger:

Resepsjon som egen konstruksjon



Ved en eventuell eksplosjon vil ikke trykket forplante seg til viktige og kritiske funksjoner.

- → *Etablere større avstand mellom mulig trussel og definert verdi*
- → *Skille kjørende fra gående*
- → *Etablere egne soner for kontroll av kjøretøy*

En beregning av forventet antall inn- og utpasseringer fordelt over døgnets 24 timer kan gi noen indikasjoner på hvor mye vaktpersonell det bør være, samt hvilke tider av døgnet adkomsten og vaktlokalet eventuelt har behov for økt bemanning. Adkomsten ved et anlegg er ofte den mest utsatte delen av anlegget, og derfor skal man tilstrebe å ha et lavest mulig antall personer med fast opphold her. Ved å skille innpasseringer fra utpasseringer samtidig som man benytter enveis-rotasjonsgrinder for passering, oppnås god oversikt. Dersom man planlegger for å høyne beredskapsnivået i adkomstsonen, bør det også tas hensyn til at antallet vaktmannskaper skal kunne økes uten at dette innebærer ombygginger av selve vaktlokalet.

Vaktmannskapet kan utføre tilleggsfunksjoner som å overvåke fjernbetjente sekundære adkomster, kamerasoner og tekniske alarmer. Dersom disse funksjonene utgjør en vesentlig del av oppgavene, må egne, trenede mannskaper settes til å utøve disse oppgavene.

I enkelte tilfeller kan det for vakten være nødvendig å benytte seg av tvangsmidler (se Reaksjonsstyrke). Ved utformingen av vaktlokalet kan det også være hensiktsmessig å sette av et eget rom for den pågrepne, i påvente av at politiet kommer for å hente personen.

Utformingen av vaktlokalet bør generelt være dimensjonert for å tåle en forhøyet trusselsituasjon. Dette kan innebære:

- → *Resepsjonsløsninger som beskytter mot personangrep og/eller beskytning*
- → *Sikret adkomst til selve vaktlokalet*
- → *Forsterkede vegger i f.eks. betong*
- → *Nok plass til økt bemanning ved forhøyet beredskap*
- → *Systemer for registrering av besøkende*
- → *Sluser som forhindrer inntrengning*
- → *Skuddsikre vinduer eller vinduer forsterket mot eksplosjoner*

VAKTSTYRKE

Benyttes som betegnelse på den faste bemanningen som sikrer adkomsten inn til et anlegg.

Det kan være alt fra en kombinert vakt- og resepsjonsbetjening til en større styrke fordelt på ytre og indre perimeter, portvakter, mannskap som søker av kjøretøy og besøkende, streifvakter og operatører i en vaktsentral.

I militær sammenheng betegnes denne styrken også som Force Protection (FP), og de har til oppgave å beskytte verdiene innenfor sperringene.

Avhengig av virksomhet kan det være ulike behov for adgangskontroll. Registrering av besøkende bør gjøres slik at det ikke hindrer ordinær inn, og utpassering, og blir det behov for å gjennomføre nærmere kontroll av personer eller gjenstander, er det hensiktsmessig å etablere et eget område for dette. Se for øvrig eget kapittel om Post og varemottak.

Reaksjonstiltak

Dersom det varsles eller detekteres at en trusselaktør prøver å trenge seg inn et sted, eller på annen måte skader et objekt eller virksomhet, må det iverksettes tiltak for å forhindre, eller redusere potensiell skadevirkning av angrepet. Reaksjonstiltak skal sikre opprettholdelse av objektets funksjonalitet ved en tilsiktet uønsket hendelse, eller sikre forutsetninger for gjenopprettelse av funksjonalitet etter en slik hendelse. Vesentlige elementer for riktig reaksjon ved en tilsiktet uønsket hendelse er alarmmottak og reaksjonsstyrke.

Adkomstsonen vil ofte være et av de mest sårbare punktene i perimeteret og de fysiske tiltak som iverksettes her, enten de er permanente eller midlertidige, skal være dimensjonert etter en gitt trussel. Helt grunnleggende for sikring av bygg og anlegg er tidsregnskapet. Skulle en hendelse inntreffe, så skal denne detekteres, verifiseres og bistand i form av reaksjonsstyrke skal tilkalles. De tiltak vi har å hjelpe oss med inntil nødvendig hjelp ankommer, vil være de fysiske sperrene som er installert i adkomstsonen, i den ytre perimeteret og i «skallet». Det er derfor viktig å vite hvor lang tid selve reaksjonsstyrken bruker for å komme til unnsetning, og at de fysiske tiltakene er robuste nok til å kunne stå imot inntil hjelpen kommer.

Alarmmottak

Et alarmmottak er et sted hvor alarmer, primært fra elektroniske sikringssystemer, tas imot, presenteres og bearbeides. Oppgaver, bemanning og sikring vil avhenge av den verdien som skal beskyttes. Noen må være gitt et ansvar for behandling av alarmene, men alarmmottak omfatter hele spennet fra en enkel løsning i en resepsjon til et spesielt alarmmottak med omfattende sikringstiltak og dedikert personell. Alarmsentral benyttes om et alarmmottak som er spesielt beskyttet og godkjent for å kunne benyttes til mottak av alarmer. I regelverket til Forsikringsselskapenes Godkjenningsnemnd (FG) settes det krav[1] til en alarmsentral for at den skal være FG-godkjent, og FG benevner den da alarmstasjon. Den skal tilfredsstille en rekke ulike bygningstekniske krav. Forsvaret har egne krav til sine alarmsentraler.

Hensikten med et alarmmottak er at reaksjonsstyrker skal få beskjed raskt, og mest mulig detaljert informasjon om årsaken til at de rykker ut. Alarmmottaket har til oppgave å verifisere selve hendelsen, mens reaksjonsstyrker har til hensikt å sørge for at sikkerheten blir gjenopprettet snarest mulig. For sivile brukere vil reaksjonsstyrken i første omgang normalt være eget personell eller vektertjeneste, eventuelt etterfulgt av politiet dersom hendelsen tilsier det, mens for militære brukere vil det ofte være en egen reaksjonsstyrke som rykker ut. Når man planlegger vaktlokaler, er det viktig å påse at reaksjonsstyrken ikke lokaliseres i selve vaktlokalet, men i egne lokaler adskilt fra vakten.

Alarmsentralen skal kunne håndtere alarmer fra automatiske innbruddsalarmanlegg (AIA), styring/administrasjon av Automatisk adgangskontroll (AAK), og overvåkning via tv-overvåkningsanlegg (TVO). Ved uønskede hendelser er det hensiktsmessig at alarmsentral kan kommunisere direkte med reaksjonsstyrken, da man fra alarmsentral forhåpentligvis har oversikt over situasjonen og kan følge opp hendelser mens de pågår. For å sikre at denne kritiske funksjonen ivaretas ved uønskede hendelser, bør også et alarmmottak plasseres slik at det er tilstrekkelig beskyttet, uavhengig av situasjon.

1
FG-200:1 og EN 50518-1, 2 og 3 vedrørende FG Regler for Alarmstasjoner

Dersom anlegget er utstyrt med et eget, lokalt alarmmottak som også er i besittelse av alt teknisk utstyr og lokalkjent personell, kan det være hensiktsmessig at det er alarmmottaket som holder kontakt med reaksjonsstyrken, iverksetter operasjonsledelse og holder kontakt med alle nødvendige tilstøtende tjenester og sørger for løpende kontakt med overordnet operativ ledelse.

Drift og bemanning

Utforming og bemanning av et lokalt alarmmottak vil i stor grad avgjøres av hvilke ulike systemer som skal betjenes, og i hvilken grad alarmmottaket er ment å understøtte overordnet operativ ledelse. Enkelte alarmmottak har kun begrensede funksjoner, mens andre alarmmottak er sentrale og kan ha funksjoner der man overvåker et større antall installasjoner, bygg eller anlegg, og er derved utformet som alarmsentraler.

Under planlegging av ulike sikringstiltak ser vi ofte et stort fokus på hvordan en best løser de tekniske utfordringene, men tilsvarende lite fokus på de menneskelige faktorene.

Arbeidet i en alarmsentral eller et alarmmottak kan til tider være stressende, og det er derfor viktig at man både rekrutterer til og trener på de oppgavene som skal gjøres. Personellet må også være forberedt på at de vil oppleve situasjoner som ikke har noen klar og forutbestemt rutine, men med tilstrekkelig øvelse og erfaring bør medarbeiderne ha godt nok grunnlag til både å foreslå og iverksette tiltak.

Selve «hjertet» av alle de ulike tekniske løsningene vil en finne i vakt-/alarmsentralen. Utformingen av denne må tilpasses den planlagte bemanningen, men det vil også være behov for å kunne planlegge for både økt bemanning, og plass til ekstern operasjonsledelse.

Det er når betjeningen i alarmsentralen oppdager uregelmessigheter, eller verifiserer en trussel at reaksjonsstyrker tilkalles. Reaksjonsstyrkene er derfor helt avhengig av hva operatøren i alarmsentralen kan melde, hva operatøren har observert, og i sum er alle avhengige av at operatøren har god situasjonsforståelse. Det oppnår man best under forhold som ikke gir for stor arbeidsmengde i forhold til trening og kapasitet. God situasjonsforståelse er også avhengig av at mannskapet er fortrolig med den teknikken de har tilgjengelig, så vel som at operatøren har optimal årvåkenhet i sitt arbeid.

Ulike studier av begrepet «vigilance decrement»[2], som best kan oversettes med fallende årvåkenhet, viser at de som betjener monitorer og signalsystemer, ofte viser seg å ha fallende årvåkenhet etter 20–30 minutter foran skjermene. Dette avhenger noe av arbeidsintensitet, men basert på det vi kjenner til, vil det være et vesentlig bidrag til god situasjonsforståelse at man roterer på denne oppgaven hvert 20 minutt. For døgnbemanning av et alarmmottak vil det normalt være behov for minst to personer til stede til enhver tid. Alarmmottaket bør utformes slik at den hvilende vakten kan trekke seg tilbake fra de tekniske installasjonene til et egnet hvilerom. Alarmmottaket bør i tillegg ha funksjoner som bad/wc, minikjøkken med kjøleskap og kokemuligheter.

Dersom alarmmottaket er utrustet med flere ulike systemer som har behov for uavhengig og samtidig betjening, vil det være hensiktsmessig å påse at de ulike operatørene ikke forstyrres av «nabo-støy». For større sentrale alarmmottak kan det være nødvendig å utforme lokalene slik at man har en egen observasjonsplass (supervisor) i lokalet som kan overvåke samtlige prosesser fra en egnet posisjon. Ved utforming av slike alarmmottak kan det også være hensiktsmessig å legge til rette for at ekstern operasjonsledelse kan ha en egen plass i lokalene.

Når man planlegger plassering av mer avan-

2

Human factors in CCTV control rooms: A best practice guide (CPNI):

Nuechterlein, K.H., Parasuraman R., Jiang Q (1983) «Visual sustained attention, image degradation produces rapid sensitivity decrement over time. Science, 220, 327-9

Nathalie Pattyn, Xavier Neyt, David Hendrickx, Erica Soetens, «Psychophysiological investigation of vigilance decrement: Boredom or cognitive fatigue? (2008) Physiology & Behavior 369-378

Vakt- og alarmmottak

Selve «hjertet» av alle de ulike tekniske løsningene vil en finne i vakt-/alarmsentralen. Utformingen av denne må tilpasses den planlagte bemanningen, men det vil også være behov for å kunne planlegge for både økt bemanning og plass til ekstern operasjonsledelse.

FOTO : Sindre Sørhus/Forsvaret

serte alarmmottak, bør dette være plassert i et bygg eller en installasjon som er sikret tilsvarende de viktigste verdiene som mottaket er ment å overvåke.

Tekniske løsninger ved særlige viktige funksjoner

Alarmmottaket kan ved særlige viktige funksjoner vurderes å også ha et separat ventilasjonsanlegg hvor luftinntaket er beskyttet mot sabotasjeangrep. Alarmmottaket bør være utstyrt med egen nødstrømkilde, som har kapasitet til å holde driften i minst 48 timer inklusive drift av nødsystemer. Alle kabel- og rørføringer inn og ut av alarmmottaket bør være beskyttet mot sabotasje slik at alarmmottaket eller større deler av sensorer og alarmgivere ikke kan settes ut av spill. Det vil også være nødvendig at alarmmottaket utrustes med alternative kommunikasjonskilder for både inn- og utgående meldinger.

Reaksjonsstyrke

Reaksjonsstyrke er personer og enheter som tilkalles for å hindre, avverge eller begrense skadene av en uønsket hendelse. Reaksjonsstyrkens mandat, type og bemanning vil avhenge av verdien som skal beskyttes, og spenner fra egne ansatte og vektere til bevæpnet politi eller militære styrker.

Det er viktig å være bevisst på at reaksjonstiden (tidsregnskapet) til reaksjonsstyrker vil variere, og det er nødvendig å avklare samarbeid og forventet reaksjonstid med det lokale politidistriktet eller lokal vaktstyrke. Reaksjonsstyrkens faktiske styrke er sammensatt av flere vesentlige forhold:

- → *Personellets utdanning og treningsnivå*
- → *Tilgjengelig utstyr*
- → *Planverk for reaksjon*

Virksomheten må avklare hvilken kapasitet reaksjonsstyrken kan forvente å ha ved en

tilsiktet hendelse, og se dette i sammenheng med grunnsikringen til virksomhetene.

Dersom trusselnivået er lavt, eller dersom instruksen tilsier at reaksjonsstyrken kun skal observere og rapportere, kan alle typer reaksjonsstyrke benyttes. For vanlige virksomheter vil det normalt være hensiktsmessig å benytte seg av trenet mannskap fra et vaktselskap som en reaksjonsstyrke.

Dersom trusselnivået er høyt, eller at reaksjonsstyrken i henhold til instruksen skal aksjonere mot eventuelle inntrengere, må reaksjonsstyrken være opplært til, ha myndighet og utrustning til å møte aktuell trussel:

- *I en militær sammenheng er reaksjonsstyrke en egen styrke, spesielt trent og utstyrt for å kunne understøtte vaktmannskapet dersom en tyngre trussel skulle opptre, og den betegnes gjerne som en QRF (Quick Response Force). Styrken skal være dimensjonert og utstyrt slik at den til enhver tid er tilgjengelig med et minimum av tilkallingstid, og den skal være dimensjonert for å håndtere enhver relevant trussel som inngår i objektets trusselbilde. Beredskapssituasjonen avgjør reaksjonsstyrkens størrelse. Reaksjonsstyrken skal ikke ha sitt tilhold i den ordinære vakten/resepsjon, men ha egnede og sikre lokaler.*
- *I en sivil virksomhet vil dette i de aller fleste tilfeller vil være en oppgave for politiet.*

Dersom tiden reaksjonsstyrken trenger for å komme frem til objektet er usikker eller lang, må dette kompenseres ved å forsterke de fysiske tiltakene i adkomstsoner, perimeter og skall slik at man oppnår et positivt tidsregnskap.

For så vel sivile som militære anlegg vil det i fredstid være politi som skal ta hånd om ulovlige inntrengere eller andre som mistenkes for å begå eller ha planer om å begå kriminelle handlinger. Vaktmannskapet har imidlertid anledning til å ta i bruk tre hovedtyper av tvangsmidler:

Pågripelse: Med pågripelse mener vi å holde igjen en person som er mistenkt for en straffbar handling. Straffeprosessloven § 176 gir sivile rett til å pågripe når det er på fersk gjerning eller etter ferske spor. Kravene er at vaktmannskapet er sikker på at det er begått en straffbar handling, og at det er rett gjerningsmann som pågripes. Ved en pågripelse må en ikke bruke mer makt enn nødvendig, og den pågrepne skal straks overleveres til politiet.

Ransaking: Vaktmannskapet vil også ha muligheten til å visitere en person og undersøke det han har med seg, når det er mistanke om en straffbar handling. Som hovedregel er det imidlertid bare politi som kan ransake. Men det finnes noen unntak i straffeprosessloven § 178. Som privatperson eller vakt kan du ta en gjenstand fra en person dersom gjenstanden kan brukes til vold eller benyttes for å unnslippe. Et krav for at vaktmannskapet skal kunne foreta ransakelse, er at man må ha samtykke fra den som blir ransaket.

Beslag: Vaktmannskapet kan ha anledning til å ta beslag, det vil si å ta ting fra en mistenkt, for eksempel tyvegods. Vaktmannskapet kan etter straffeprosessloven § 206 gjennomføre et beslag. Kravet er at den mistenkte påtreffes eller forfølges på fersk gjerning eller etter ferske spor. Det som er beslaglagt, skal straks overleveres til politiet.

Særlige beskyttelsesbehov

For virksomheter med særlige beskyttelsesbehov kan det være nødvendig med en vaktfunksjon i forbindelse med perimeter eller ytterste grense. Personellet som betjener den ytre vakten, må ha mulighet til å stenge av innpasseringsområdet og varsle alarmmottak samt reaksjonsstyrke på en rask og effektiv måte

Veiledende krav til reaksjonsstyrker

Sikringsklasse	Beskrivelse
1	→ Eget eller eksternt personell uten spesiell kompetanse og utstyr
2	→ Vektere med kunnskap og utstyr
3	→ Politi eller militær vakt
4	→ Trenede spesialmannskaper fra politiet eller Forsvaret

dersom dette skulle bli nødvendig. Dette setter krav til trenet personell og tilpassede løsninger. Det vil normalt være politiet som skal håndtere tyngre eller bevæpnede trusselaktører. Eget personell bør derfor trenes spesielt i teknikker for rask og sikker observasjon og sørge for at man har tilgjengelig kommunikasjonsutstyr slik at dette kan bidra til rask tilbakemelding til reaksjonsstyrken.

Den ytre vakten med tilhørende fasiliteter representerer første barriere, og må plasseres i hensiktsmessige lokaler tilpasset forskjellige beredskapstrinn, og bemannes med øvet personell.

Hjelpemidler for trygg og effektiv kontroll av kjøretøy kan for eksempel være:

- → *Sluseløsninger, hvor man skiller lettere og tyngre kjøretøy*
- → *Lommelykt og søkespeil for manuell kontroll*
- → *Automatiske undersøkelsessystemer som kamera og skiltgjenkjenning*
- → *Spesialtrente søkehunder*
- → *Det ytre vaktområdet bør også være utformet med tilstrekkelig snuplass slik at det er mulig å avvise trafikk som ikke har eller får adgang til området.*

For objekter som er klassifisert iht. objektsikkerhetsforskriften, vil det være krav om et sikringskonsept hvor kombinasjonen av barriere, deteksjons-/verifikasjonstiltak og reaksjonsstyrke skal forhindre eller begrense tap av verdier. Det er også krav om tilrettelegging for økt vakthold og sikringsstyrker.

Bestemmelser for vakt og sikring i Forsvaret fastslår blant annet krav til vakt og sikring av Forsvarets installasjoner, informasjonssystemer, personell og materiell.

Sikringsstyrke

Personer og enheter fra politiet eller Forsvaret som har til oppgave å beskytte et objekt mot en mulig eller konkret trussel.[3] Sikkerhetsloven benytter betegnelsen Sikringsstyrke om en

3
Fra Lovdata: «Instruks om sikring og beskyttelse av objekter», 2012

kapasitet som blir tilkalt ved fare for kompromittering av verdier som er skjermingsverdige, jf. sikkerhetsloven. Sikringen kan utføres på ulike måter, men som objekteier av et skjermingsverdig objekt er man pliktig til å legge til rette for bruk av sikringsstyrker, også under øvelser. En sikringsstyrke kan derfor bestå av enten militære mannskaper, politi eller i andre tilfeller også vaktmannskap og vektere. I Sikringshåndboka er det også benyttet betegnelsen reaksjonsstyrke om denne kapasiteten.

Livvaktstyrke

På bakgrunn av egne analyser som utføres av PST, plasseres VIP i ulike risikogrupper. Risikogruppene inneholder definerte sikkerhets- og beskyttelsestiltak. Eksempelvis vil noen VIP ha kontinuerlig nærsikring av bevæpnede livvakter og benytte pansret kjøretøy, mens andre kun har elektroniske varslingstiltak. Det er PST som til enhver tid avgjør hvem som er en VIP, og hvilken type sikring som skal iverksettes for hvert unike «objekt.» Det er en egen spesialtrent livvaktstyrke som ivaretar disse funksjonene. I ulike sammenheng betegnes dette også som en sikringsstyrke, men som det fremgår ovenfor, definerer sikkerhetsloven en sikringsstyrke noe annerledes.

Forsvaret og VIP

Innen alliansen av ulike NATO-land er det også etablert systemer for hvordan man innenfor militære former håndterer ulike VIP-statuser. Her følger ikke Forsvaret nødvendigvis de samme regler og tiltak som blir benyttet av PST, men det er tradisjon for at høyere rangert befal og andre spesialrådgivere innenfor det militære blir betraktet som VIP. VIP-status i en militær sammenheng vil også indikere hvilke tiltak som skal iverksettes for transport, beboelse, beskyttelse og rent generelt gi en indikasjon av hvilke risiki en VIP kan utsettes for når vedkommende er på besøk i en fremmed base.

Kapittel 14

Avlytting og avlesing

Dette kapitlet omhandler skjerming mot urettmessig ervervelse av informasjon via akustisk, visuell og/eller elektromagnetisk registrering.

Vår tids informasjonssamfunn bygger i stor grad på tilgang og deling av informasjon, noe som gir oss mange kjente fordeler. Det er samtidig slik at dagens informasjonsteknologi og delingskultur kan utgjøre en sikkerhetsrisiko. Sensitive opplysninger kan gi alvorlige skadefølger dersom de blir kjent for uvedkommende, og det er derfor viktigere i dag enn noen gang med en høy grad av bevissthet i forbindelse med informasjonsformidling.

Det store omfanget av utstyr med sendere og mottagere vi omgir oss med, som mobiltelefonene vi bærer med oss, utgjør en stor usikkerhet knyttet til hvem som får tilgang til informasjon.

Urettmessig ervervelse av formidlet informasjon kan deles inn i tre kategorier:

Akustisk avlytting handler om uønsket registrering av lyd. Dette kan være direkte avlytting, eller indirekte avlytting via strukturer som er i kontakt med lydkilden, slik som dører, vegger og gulv samt rør og kanaler. For eksempel vil en radiator kunne fange opp lyd og lede informasjon videre via sitt tilkoblede rørsystem. Indirekte avlytting kan også skje via utstyr med mikrofoner som er plassert i nærheten av kilden.

Visuell avlesing handler om uønsket registrering av lys, eller det som er synlig. Dette kan være direkte visuell registrering som gjennom utvendige og innvendige vinduer, men også indirekte fjernavlesning ved hjelp av for eksempel laser. Kikkerter og kameraer med zoom er fortsatt effektive virkemidler og kan være enda mer effektive dersom de er montert på en drone.

Elektromagnetisk registrering (Tempest) handler om uønsket registrering av elektromagnetiske signaler. Dette er aktuelt der informasjonen formidles via utstyr som avgir elektromagnetiske signaler, som f.eks. datamaskiner og VTC-utstyr. Informasjonen i disse systemene kan overføres til nærliggende kabler, men også kanaler og andre bygningsdeler, for så å bli spredd videre. Mer informasjon om Tempest følger i slutten av kapitlet.

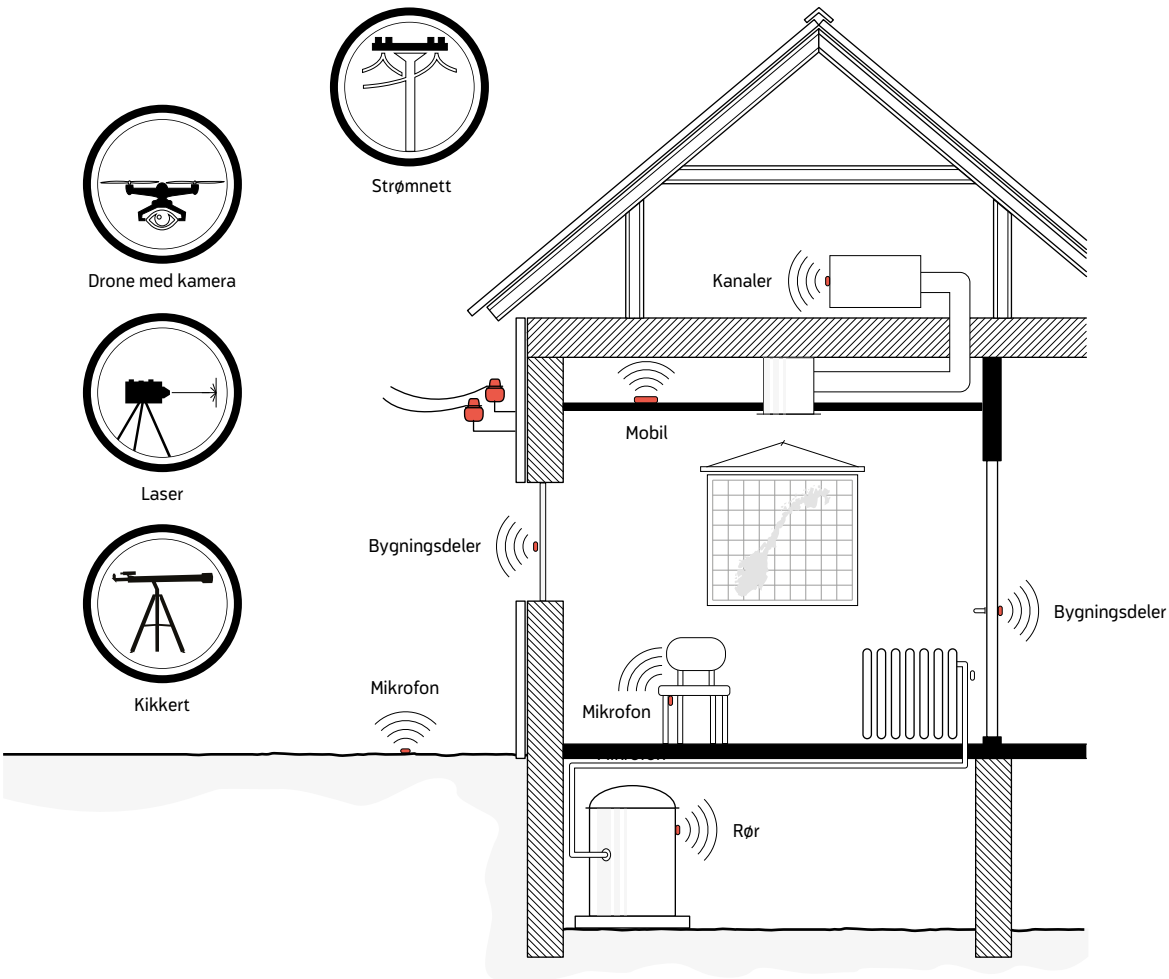
Skjerming av informasjon

Skjermingsbehov

For at sensitiv informasjon ikke skal komme på avveie, kan det være nødvendig å skjerme informasjonen mot urettmessig registrering. For å finne det rette skjermingsbehovet legges følgende faktorer til grunn:

→ *Hva er verdien vi skal skjerme?*
→ *Hva er trusselen vi skal skjerme oss mot?*

Eksempler på kilder til registrering av informasjon



For virksomheter underlagt sikkerhetsloven vil skjermingsbehovet være gitt ut fra informasjonens aktuelle graderingsnivå.

→ *Hva er skjermingsbehovet?*
→ *Hvilken restrisiko kan vi akseptere, og hva anser vi som god nok skjerming?*

Skjermingsnivå
Skjermingsnivået beskriver den samlede ytelsen for virksomme skjermingstiltak.

For å finne det mest hensiktsmessige skjermingsnivået må vi vite følgende:

I ***tabellen Skjermingsnivå*** er det definert fire nivåer for skjerming, som i denne sammenhengen samsvarer godt med nivåene for sikkerhetsgradert informasjon. Det er samtidig slik at skjermingsnivået og graderingsnivået ikke henger direkte sammen, og at det i enkelte tilfeller kan være hensiktsmessig med et avvikende

Skjermingsnivå for sensitiv informasjon

Nivå	Beskrivelse
1	→ Lav grad av skjerming
2	→ Middels grad av skjerming
3	→ Høy grad av skjerming
4	→ Svært høy grad av skjerming

skjermingsnivå, på bakgrunn av lokale forhold. Skjermingsnivåene er særlig anvendbare for virksomheter som ikke er underlagt sikkerhetsloven, men har tilsvarende skjermingsbehov.

Skjermingstiltak

Overordnet bør alle som befatter seg med sensitiv informasjon, sørge for at uvedkommende ikke får kjennskap til informasjonen. Noen ganger kan det være tilstrekkelig å trekke for gardinene, eller snu pc-skjermen, men ofte vil det være behov for mer omfattende tiltak, avhengig av ønsket skjermingsnivå. I oversiktene som følger nedenfor er det listet opp anbefalte tiltak for hvert skjermingsnivå. Tiltakene er gruppert i tre kategorier:

Forutsetninger: Plassering og organisering i forhold til omkringliggende faktorer som naboer, andre funksjoner, uteområder m.m.

Fysiske tiltak: Bygningsdelers egenskaper for bl.a. lydreduksjon, begrensinger for tekniske føringer, innsynsskjerming, fysisk og elektronisk sikring m.m.

Administrative tiltak som godkjenning av rom, adgangskontroll, protokollføring av besøkende, instrukser/rutiner for bruk m.m.

Skjermingstiltakene skal samlet yte det rette nivået for skjerming, og for å unngå overdimensjonering av enkelte deler eller «huller» i skjermingen er det nødvendig med en helhetlig tilnærming ved etablering av lokaler for formidling av sensitiv informasjon. De anbefalte tiltakene er basert på minstekravene for gradert informasjon på nivå HEMMELIG med VTC. funksjon gitt i sikkerhetsloven[1] med forskrift[2] og veiledere. Disse kravene, med supplerinnger, er å finne igjen i «Skjermingsnivå 3» og har vært utgangspunktet for en konkretisering av anbefalte tiltak for de andre nivåene.

Det understrekes at virksomheter underlagt sikkerhetsloven alltid er pliktet å følge de til enhver tid gjeldende krav som stilles i aktuelle lover og forskrifter. Anbefalingene her er ment som et supplement og forslag til konkretisering av tiltak for å imøtekomme disse.

1
Lov om forebyggende sikkerhetstjeneste, kapittel 4. Informasjonssikkerhet

2
Forskrift om informasjonssikkerhet, kapittel 9. Sikring av konferanserom med mer mot uønsket avlytting og innsyn

Anbefalte ytelser

Skjermingsnivå	
1	→ Benyttes normalt dersom **det i noen grad kan medfølge skade om informasjonen blir kjent for uvedkommende.** → **For virksomheter underlagt sikkerhetsloven vil dette nivået typisk gjelde for permanente lokaler i Norge, hvor det skal formidles gradert informasjon i kategorien** BEGRENSET. → **Generelt gjelder normal byggeteknisk utførelse, med noen ekstra krav til bruk.**
Forutsetninger	
Plassering	→ Rommet skal plasseres i minimum KONTROLLERT område.
Organisering	→ Det kan etableres både koblede rom og hele soner for denne type bruk.
Bruk	→ Den enkelte bruker er alltid ansvarlig for at informasjonen ikke kommer på avveie. → Rommet kan benyttes til andre formål dersom dette ikke anses å svekke sikkerheten.
Fysiske tiltak	
Lydreduksjon	→ 37 dB. → Lokalet skal være alminnelig fagmessig utført mtp. tetting, slik at lyd ikke trenger ut gjennom åpninger ifm. kabelgjennomføringer, systemvegger etc.
Innsyn	→ Mulighet for innsynsskjerming.
Rør, kanaler og kabler	→ Normal byggeteknisk standard, dog skikkelig utført.
Elektronisk utstyr	→ Ingen spesifikke bygningsmessige krav.
Overflater	→ Ingen spesifikke krav.
Fysisk sikring	→ Låsbar dør.
Administrative tiltak	
Godkjenning	→ Den enkelte bruker kan godkjenne disse lokalene.
Personell	→ Ingen spesifikke krav.
Inventar	→ Ingen spesifikke krav.
Rutiner	→ Ved BEGRENSET eller tilsvarende sensitiv tale skal dører og vinduer lukkes. Ved bruk av skjerm, lerret eller tilsvarende skal det gjøres tiltak mot innsyn. → Det må vurderes i det enkelte tilfelle om utstyr med sender og mottagere bør legges ut av rommet.

Skjermingsnivå	
2	→ **Benyttes normalt dersom det kan medfølge skade, dersom informasjonen blir kjent for uvedkommende.** → **For virksomheter underlagt sikkerhetsloven vil dette nivået typisk gjelde for permanente lokaler i Norge, hvor det skal formidles gradert informasjon i kategorien KONFIDENSIELT.** → **Generelt gjelder god byggeteknisk utførelse, med tilleggskrav til tekniske installasjoner, og bruk.**
Forutsetninger	
Plassering	→ Rommet skal plasseres i BESKYTTET område, men kan ha grense til KONTROLLERT område. → Rommet kan også plasseres mot yttervegg, men da skal arealer utenfor være kontrollerbare, og eventuelle vinduer må sikres særskilt, med tanke på lyd-gjennomgang og innsyn.
Organisering	→ Det kan etableres både koblede rom og hele soner for denne type bruk.
Bruk	→ Den enkelte bruker er alltid ansvarlig for at informasjonen ikke kommer på avveie. → Rommet kan benyttes til andre formål dersom dette anses å ikke svekke sikkerheten.
Fysiske tiltak	
Lydreduksjon	→ 44 dB. → Lokalet skal være godt fagmessig utført med tanke på tetting, slik at lyd ikke trenger ut gjennom åpninger i forbindelse med kabelgjennomføringer etc.
Innsyn	→ Det skal være mulighet for innsynsskjerming ved formidling av sensitiv informasjon.
Rør	→ Rør kan føres iht. øvrige funksjoner, med enkle utbedringer. Radiator, kjøling, sprinkling etc. er OK, forutsatt at det gjennomføres med metalliske brudd i forbindelse med romavgrensingen.
Kanaler	→ Kanaler kan føres iht. bygningens øvrige funksjoner, men det må etableres galvaniske skiller ved gjennomføring til rommet, samt lyd-feller iht dempningskrav (42 dB).
Kabler	→ Nødvendige kabler kan føres iht. bygningens øvrige funksjoner. Overflødige kabler skal tas vekk.
Elektronisk utstyr	→ Lokal skjerming av utstyr og avstand til mulige ledere som kabling, rør og kanaler, bør planlegges iht. instruks for skjerming mot Tempest.
Overflater	→ Alle faste overflater skal være utført på en slik måte at det vil etterlate spor dersom noen har forsøkt å løsne eller på annen måte bearbeide disse.
Fysisk sikring	→ Låsbar dør, og adgangskontroll. Ved behov for forsterkning av bygningsdeler mot inntrengning bør dette tilsvare minimum SK 3.
Administrative tiltak	
Godkjenning	→ Lokalet skal godkjennes av lokal sikkerhetsansvarlig før bruk. → Det stilles ikke krav til lydmåling. Nye lokaler som er prosjektert etter TEK-10 og har fulgt pre-akseptert ytelsesnivå iht. NS 8175 kl. C for møterom, anses som OK. Ved etablering av funksjon i eksisterende lokaler med ukjent oppbygging må det gjøres en kvalifisert byggteknisk vurdering med tanke på lydegenskapene.
Personell	→ Kun særskilt utpekt personell skal ha tilgang til rommet uten følge.
Inventar	→ Det skal kun være nødvendig inventar/utstyr i rommet, og det skal være enkelt å holde oversikt.
Rutiner	→ Rommet skal holdes avlåst. → Det skal foreligge en rutinebeskrivelse tilgjengelig for ansvarlige brukere. → Utstyr med sender og mottagere skal ikke bringes med inn i rommet dersom det skal formidles sensitiv informasjon.

forts. anbefalte ytelser

Skjermingsnivå	
3	→ **Benyttes normalt dersom det kan medføre alvorlig skade om informasjonen blir kjent for uvedkommende.** → **For virksomheter underlagt sikkerhetsloven vil dette nivået typisk gjelde for permanente lokaler i Norge, hvor det skal formidles gradert informasjon i kategorien HEMMELIG.** → **Det vil normalt være behov for spesielle konstruksjoner og produkter for å oppnå akseptabel lyddempning. For etablering i eksisterende bygg vil dette normalt medføre noe ombygging, for å forsterke særlig vegger, dører og eventuelt vinduer, men også legge til rette for kontrollerbare omgivelser.**
Forutsetninger	
Plassering	→ Rommet skal plasseres i BESKYTTET område, og alle omkringliggende volumer med inventar skal være kontrollerbare. Det kan ikke være fastmontert utstyr på tilgrensende overflater. (Rommet kan plasseres mot yttervegg, men da skal arealer utenfor være minimum KONTROLLERT, og eventuelle vinduer må sikres særskilt, med tanke på lyd-gjennomgang, innsyn, innbrudd og fjernavlesing med laser). → Dersom rom må plasseres mot KONTROLLERT område innvendig, må bygningsdelene samlet yte en motstandsevne tilsvarende minimum SK 3.
Organisering	→ Det kan etableres koblede rom, men det kan IKKE etableres soner (større arealer med ulike funksjoner) for denne type bruk.
Bruk	→ Den enkelte bruker er alltid ansvarlig for at informasjonen ikke kommer på avveie. → Rommet kan benyttes til andre formål dersom dette ikke kan svekke sikkerheten, og de gjeldende rutinene følges.
Fysiske tiltak	
Lydreduksjon	→ 52 dB lydreduksjon i omkringliggende konstruksjoner, produkter og installasjoner. For dører vil det for dette nivået være hensiktsmessig med to dører i tandem for å sikre god nok tetting. Det samme gjelder vinduer.
Innsyn	→ Eventuelle vinduer skal ha innvendig lystett skjerming mot innsyn, (f.eks. gardiner), og utvendige skjermingstiltak mot fjernavlesning (f.eks. persienner).
Rør	→ Det skal ikke føres andre rør inn til dette rommet enn det som er strengt nødvendig. Ved behov for rør skal disse isoleres og termineres i rommet, samt utføres med metalliske brudd i forbindelse med romavgrensingen. → Radiatorer er ikke tillatt (kan enkelt erstattes med f.eks. panelovn). Sprinkling kan aksepteres med tiltak nevnt over.
Kanaler	→ Det skal ikke føres andre kanaler til rommet enn det som er strengt nødvendig. Disse skal termineres i rommet og utføres med metalliske brudd i forbindelse med romavgrensningen, samt lydfeller iht dempningskrav (52 dB). → Det skal tas hensyn til Tempest-risiko og kabling med ulikt graderingsnivå skal holdes adskilt i henhold til egen instruks for dette.
Kabler	→ Det skal ikke føres andre kabler til rommet enn det som er strengt nødvendig. Disse skal termineres i rommet og utføres som åpent anlegg. Det skal tas hensyn til Tempest-risiko, og kabling med ulikt graderingsnivå skal holdes adskilt i henhold til egen instruks for dette.
Elektronisk utstyr	→ Lokal skjerming av utstyr og avstand til mulige ledere som kabling, rør og kanaler skal planlegges iht. instruks for skjerming mot Tempest.
Overflater	→ Alle faste overflater skal være utført på en slik måte at det vil etterlate spor dersom noen har forsøkt å løsne eller på annen måte bearbeide disse.

Fysiske tiltak	
Fysisk sikring	→ Låsbar dør med ekstra tilleggs-lås (FG klasse 3, med nøkkel utenfor system. Nøkkelen skal oppbevares i oppbevaringsenhet for minimum KONFIDENSIELT eller tilsvarende). → Dører med utvendig hengsling skal ha bakkantsikring, og eventuelle vinduer skal monteres slik at forsering utenfra lett kan oppdages. → Kanaler og andre åpninger større enn 600 cm^2, må sikres mot inntrengning. Ved behov for forsterkning av bygningsdeler mot inntrengning skal dette tilsvare min. SK 3.
Administrative tiltak	
Godkjenning	→ Dersom rommet etableres for HEMMELIG tale, skal NSM godkjenne dette før det kan tas i bruk. → NSM må vurdere om det er behov for teknisk sikkerhetsundersøkelse (TSU), samt lydmåling.
Personell	→ Kun særskilt utpekt personell skal ha tilgang til rommet uten følge.
Inventar	→ Etter at rommet er godkjent, kan det ikke forekomme supplering eller utskifting/endring av inventar. (Det er f.eks. ikke anledning til å ta med seg en ekstra stol inn i et godkjent rom for SN 3 uten at rommet mister sin godkjenning. Det er derfor viktig å planlegge bruken godt på forhånd.) → Nytt eller ikke allerede godkjent inventar, må sikkerhetsundersøkes før det kan tas inn i rommet.
Rutiner	→ Det skal foreligge en rutinebeskrivelse tilgjengelig for ansvarlige brukere som beskriver rutiner for avlåsing, oppbevaring av nøkler, beskyttelse mot innsyn, drift av ulike systemer, inventarliste og forbud mot å bringe inventar inn eller ut av rommet. → All aktivitet skal loggføres. → Utstyr med sender og mottagere skal ikke bringes med inn i rommet.

forts. anbefalte ytelser

Skjermingsnivå	
4	→ **Benyttes normalt dersom det kan medføre helt avgjørende skade om informasjonen blir kjent for uvedkommende.** → **For virksomheter underlagt sikkerhetsloven vil dette nivået typisk gjelde for permanente lokaler i Norge, hvor det skal formidles gradert informasjon i kategorien STRENGT HEMMELIG. Det vil normalt være behov for spesielle konstruksjoner og produkter for å oppnå akseptabel lyddempning. For etablering i eksisterende bygg vil dette normalt medføre betydelig ombygging.**
Forutsetninger	
Plassering	→ Skal i sin helhet plasseres i BESKYTTET område. → Vinduer er IKKE tillatt.
Organisering	→ Det kan IKKE etableres koblede rom, eller soner (større arealer med ulike funksjoner) for denne type bruk.
Bruk	→ Den enkelte bruker er alltid ansvarlig for at informasjonen ikke kommer på avveie. → Rommet kan IKKE benyttes til andre formål.
Fysiske tiltak	
Lydreduksjon	→ 60 dB lydreduksjon i omkringliggende konstruksjoner, produkter og installasjoner.
Innsyn	→ Det skal ikke være muligheter for innsyn.
Rør	→ For dette nivået vil det ikke være tillatt med rør. Sprinkling kan aksepteres dersom aktuell grein er tørr, isolert og for øvrig gjennomført med metallisk brudd.
Kanaler	→ Det skal ikke føres andre kanaler til rommet enn det som er strengt nødvendig. Disse skal termineres i rommet, og utføres med metalliske brudd i forbindelse med romavgrensingen, samt lydfeller iht. dempningskrav (60 dB).
Kabler	→ Det skal ikke føres andre kabler til rommet enn det som er strengt nødvendig. Disse skal termineres i rommet og utføres som åpent anlegg. Det skal tas hensyn til Tempest-risiko, og kabling med ulikt graderingsnivå skal holdes adskilt i henhold til egen instruks for dette.
Elektronisk utstyr	→ Lokal skjerming av utstyr og avstand til mulige ledere som kabling, rør og kanaler skal planlegges i henhold til instruks for skjerming mot Tempest.
Overflater	→ Alle faste overflater skal være utført på en slik måte at det vil etterlate spor dersom noen har forsøkt å løsne eller på annen måte bearbeide disse.
Fysisk sikring	→ Låsbar dør med ekstra tilleggs-lås (FG klasse 3, med nøkkel utenfor system. Nøkkelen skal oppbevares i oppbevaringsenhet for minimum KONFIDENSIELT eller tilsvarende). → Dører med utvendig hengsling skal ha bakkantsikring, og eventuelle vinduer skal monteres slik at forsering utenfra lett kan oppdages. → Kanaler og andre åpninger større enn 600 cm^2, må sikres mot inntrengning. → Ved behov for forsterkning av bygningsdeler mot inntrengning bør dette tilsvare min. SK 4.
Administrative tiltak	
Godkjenning	→ Ved etablering av rom for STRENGT HEMMELIG tale skal NSM godkjenne dette før det kan tas i bruk. Det vil være behov for TSU, og rommet skal lydmåles.
Personell	→ Kun særskilt utpekt personell skal ha tilgang til rommet.
Inventar	→ Etter at rommet er godkjent, kan det ikke forekomme supplering eller utskifting/endring av inventar. (Det er f.eks. ikke anledning til å ta med seg en ekstra stol inn i et godkjent rom for SN 4 uten at rommet mister sin godkjenning. Det er derfor viktig å planlegge bruken godt på forhånd.) → Nytt eller ikke allerede godkjent inventar må sikkerhetsundersøkes før det kan tas inn i rommet.
Rutiner	→ Det skal foreligge en rutinebeskrivelse tilgjengelig for ansvarlige brukere som beskriver rutiner for avlåsing, oppbevaring av nøkler, beskyttelse mot innsyn, drift av ulike systemer, inventarliste og forbud mot å bringe inventar inn eller ut av rommet. → All aktivitet skal loggføres. → Utstyr med sender og mottagere skal ikke bringes med inn i rommet.

Tempest, skjerming mot elektronisk avlytting

Generelt

Elektrisk/elektronisk utstyr kan sende ut elektromagnetisk stråling. Dette er kjent fra EMI/EMC-problematikk, der man vil unngå at stråling fra elektronisk utstyr skal forstyrre annet elektronisk utstyr.[3] Utstyr som skal selges i Norge, må godkjennes etter å ha blitt testet for utstråling (og immunitet) og har etter godkjenning fått CE-merking. Testingen er ofte gjort på prototyper, og produksjonsmodeller kan ha blitt forandret etter testing. Strålingen fra serieprodusert utstyr kan da i noen tilfeller overgå grensene som er satt.

Strålingen som kommer fra utstyret, kan også ha med seg informasjon fra systemet. På denne måten kan sensitiv informasjon gjøres tilgjengelig for utenforstående. Den som vil få tak i denne informasjonen, vil kunne fange opp langt svakere signal enn det som skal til for å forstyrre.

Noe elektronisk utstyr er bygget med tanke på informasjonssikkerhet og har ekstra lite utstråling. Det vil likevel være nødvendig å ta hensyn ved installasjon når man skal sikre seg mot lekkasje av informasjon. Informasjon kan spres gjennom stråling fra utstyret, eller signaler kan følge kabler eller andre metalliske konstruksjoner.

Beskrivelsene som følger gjelder for virksomheter underlagt sikkerhetsloven, men kan være like aktuelle for andre virksomheter med tilsvarende skjermingsbehov.

Krav til installasjon

Nettverk som skal behandle informasjon gradert KONFIDENSIELT eller høyere, skal bruke fiberoptiske kabler. Dette er også et krav for installasjoner som behandler BEGRENSET i utlandet, men det er også anbefalt i Norge. Kobberkabler på inntil 5 meter kan imidlertid brukes for å koble seg til nettverk og andre komponenter inne på samme kontor.

Signaler kan overføres fra ett system til et annet, både gjennom stråling og via kabling, så graderte og ugraderte systemer skal derfor holdes adskilt. Utstyr med forskjellig graderingsnivå kan imidlertid stå sammen. Graderte og ugraderte systemer kan benytte samme multifiberkabel, men signal på ugradert fiberkabel må da regenereres via elektrisk omformer før den føres ut av kontrollert område. Alle graderte kabler skal holdes innenfor kontrollert område.

Informasjon kan også smitte over på andre systemer hvor det kan bli modulert og spredd videre for eksempel på strømledninger. Bruk av nettfilter kan redusere denne sårbarheten. Dersom gradert informasjon fanges opp av radiosendere, kan signalene spres over store avstander. Mobiltelefoner og andre radiosendere med ladeutstyr skal derfor holdes minimum 1 meter borte fra utstyr som behandler gradert informasjon.

Andre måter signaler kan bli spredt over store avstander på er f.eks. gjennom kabelnett for radio- og tv-signaler. Digital lydbehandling på pc-er er også en kilde til spredning av informasjon elektronisk.

Andre krav

Veiledningen Tempestsikring av IKT-systemer[4] angir mer detaljerte krav til utstyr og installasjon. Kravene er avhengig av graderingsnivå på informasjonen, og hvor stort inspiserbart område man har rundt seg, dvs. område du har kunnskap og kontroll over, og der avlytter ikke kan etablere seg over tid uten å bli oppdaget. Tempest-tiltak for et og samme system kan variere for utstyr som har forskjellig geografisk plassering. Bruk av skjermbur eller skjermende materialer f.eks. i forbindelse med skjerming mot EMP/HPM, kan redusere krav til utstyr og installasjon.

Hjemmel for disse kravene er gitt i sikkerhetslovens forskrift om informasjonssikkerhet § 5.

3
EMI-Electromagnetic Interference (elektromagnetisk interferens), EMC-Electromagnetic Compatibility (elektromagnetisk sameksistens)

4
Dokumentet er sikkerhetsgradert. Autoriserte brukere får tilgang til dette hos Nasjonal sikkerhetsmyndighet

Kapittel 15

Menneskelige og organisatoriske tiltak

Kapitlet gir en oversikt over tiltak som sammen med fysiske og elektroniske sikringstiltak kan bidra til å redusere risikoen for uønskede tilsiktede hendelser.

Organisatoriske sikringstiltak er skriftlige eller muntlige beskrivelser som regulerer prosesser, rutiner, atferd og/eller anvendelse av andre sikringstiltak.[1] Disse kan være:

- *Administrasjon og ledelse: regler, rutiner, prosedyrer, retningslinjer, planverk etc.*
- *Analyse: risikoanalyser, gransking, management-rapporter*
- *Verifikasjon: revisjoner, tester, øvelser*

Menneskelige sikringstiltak er tiltak som påvirker atferd og reell evne til å bruke teknologiske sikringstiltak og følge organisatoriske sikringstiltak, samt menneskelige handlinger som utføres for å hindre en uønsket hendelse.[2]

Viktige faktorer for å øke og styrke ansattes evne til å ta i bruk teknologiske tiltak og følge organisatoriske tiltak er:

- *Kognitive faktorer: holdningsskapende arbeid, læring, beslutningsprosesser etc.*
- *Sosiale faktorer: sikkerhetskultur, gruppetenkning, empati etc.*
- *Biologiske faktorer: søvn, hvile, næring, stress, evne til å fungere*

Hvorfor har ikke de fysiske og elektroniske sikringstiltak den ønskede effekten mot tilsiktede handlinger? Ofte er svaret manglende bevissthet om sikkerhetsrutiner og planverk i organisasjonen. Hvilke krav bør virksomheten sette til organisatoriske og menneskelige sikringstiltak? Hvilke rutiner følges ved sikkerhetsbrudd? Hvem har ansvaret? Har vi beredskapsplanverk? Dette er spørsmål som virksomheter bør stille seg ved gjennomgang av sikkerheten.

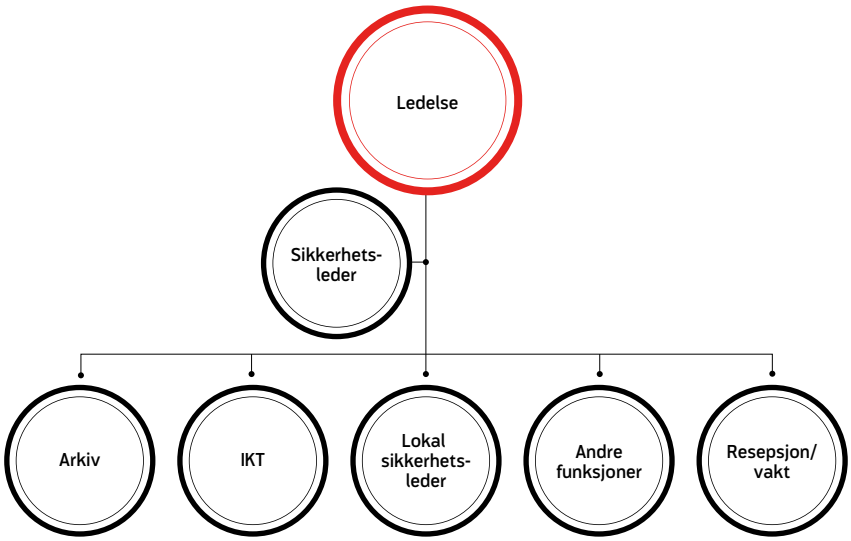
Eksempler på regulerende tiltak er grunnlagsdokument for sikkerhet, beredskapsplaner, lokale instrukser, opplærings- og kursvirksomhet, avvikshåndtering og krisehåndteringsplaner. Organisatoriske tiltak innebærer også plassering av sikkerhetsansvar i organisasjonen, bruk av manuelt vakthold og motivering til en god sikkerhetskultur i organisasjonen. Les mer i ***kapittel 3, Sikkerhetskultur*** og ***kapittel 13, Vakthold og reaksjonstiltak.***

Hvem har ansvaret for sikkerheten i en virksomhet?

Virksomhetens leder har det formelle ansvaret for sikkerheten i virksomheten. Det er lederen som tar de overordnede beslutningene og legger føringer for hvordan sikkerhetsarbeidet skal gjennomføres og organiseres. Ansvaret innbefatter blant annet å:

1, 2
Fra NS-EN 5830:2012. Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Definisjoner

Organisering av sikkerhetsorganisasjon (eksempel)



- *avsette nødvendige ressurser for å ivareta sikkerheten i virksomheten*
- *motivere og bevisstgjøre om behovet for forebyggende sikkerhet*
- *gi veiledning til ansatte, følge opp resultater innen forebyggende sikkerhet etter at mål er fastsatt*
- *evaluere*[3] *sikkerhetstilstanden minst én gang i året*

Utøvende funksjoner kan imidlertid delegeres, for eksempel til en sikkerhetsorganisasjon.

Hva består en sikkerhetsorganisasjon av?

Virksomheter som omfattes av sikkerhetsloven, skal etablere en sikkerhetsorganisasjon. Denne skal bestå av sikkerhetsleder med stedfortreder og et tilstrekkelig antall personer ut ifra virksomhetens sikkerhetsbehov.[4] Det er et krav at utøvende og kontrollerende oppgaver fordeles på forskjellige medarbeidere.[5] Sikkerhetsorganisasjonen kan i sin enkleste form bestå av en virksomhetsleder og en sikkerhetsleder, eller den kan være inndelt i strategiske og utøvende sikkerhetsnivåer med egne ledere og sikkerhetsansvarlige.

Virksomheter som ikke er underlagt sikkerhetsloven, bør også ha en sikkerhetsorganisasjon der roller og ansvar er klart definert. Nasjonal sikkerhetsmyndighets (NSM) veiledning for sikkerhetsstyring[6] gir føringer for hvordan sikkerhet bør organiseres i en virksomhet. I ***figuren Organisering av sikkerhetsorganisasjon*** er det vist et eksempel på hvordan sikkerhet kan organiseres.

Sikkerhetsorganisasjonen med sine sikkerhetsansvarlige skal sørge for at ansatte har tilstrekkelig kompetanse om forebyggende sikkerhet, og at sikkerheten ivaretas i det daglige arbeidet. Sikkerhetskulturen i virksomheten er avgjørende i denne sammenhengen, se ***kapittel 2, Sikringsteori*** og ***kapittel 3, Sikkerhetskultur*** som går nærmere inn på dette.

3
Lovmessige krav gjelder dersom virksomheten er underlagt sikkerhetsloven, se forskrift om sikkerhetsadministrasjon § 4–4

4
Forskrift om sikkerhetsadministrasjon § 2–5

5
Ibid. § 2–4

6
NSM (2015). Veiledning for sikkerhetsstyring. *www.nsm.stat.no*

Kurs og opplæring for ansatte

De ansatte bør ha jevnlig opplæring i sikkerhet. Hensikten med opplæringen er at de ansattes bevissthet om sikkerhetsrelaterte utfordringer styrkes. Relevante temaer kan være:

- *Hva er bedriftens eksisterende og nye sikringstiltak, både fysiske og elektroniske?*
- *Hva er mistenkelig aktivitet, hvordan kan du bli oppmerksom på dette? Hva er normaltilstanden i vår virksomhet, og når bør vi reagere på avvik fra normaltilstanden?*
- *Hvordan skal det rapporteres, og til hvem, hvis man oppdager kartlegging eller forsøk på sosial infiltrasjon?*
- *Hva kan du som ansatt gjøre for å hindre at noen tar kontroll over mobiltelefon eller pc (hacking, phishing[7], installering av ondsinnet programvare)?*
- *Hva skal man være bevisst på ved behandling av sensitiv eller gradert informasjon?*
- *Hva er sensitiv informasjon? Hvilken type informasjon kan deles med andre, legges ut offentlig eller på sosiale medier?*
- *Hva er relevante trusselscenarioer for vår virksomhet?*
- *Hvordan opptre ved en truende hendelse som bombetrussel, angrep, infiltrasjon, CBR[8]-trussel?*

Trening og øvelser

Øvelser er et svært godt egnet virkemiddel for å evaluere og forbedre virksomhetens planverk og rutiner. Både forberedelse av øvelser og gjennomføring av øvelser vil bidra til at svakheter i organisasjonen avdekkes. Medarbeidere som har vært gjennom en øvelse og kjenner til planer og tiltak, vil også kunne reagere som planlagt på en uønsket hendelse. Øvelser gir dermed kunnskaper og ferdigheter på individnivå, så vel som på operativt og strategisk nivå. Eksempler på øvelser som kan gjennomføres:

- ***Skrivebordsøvelser:*** *Teoretiske øvelser der man tar for seg ulike trusselscenarioer og forsøker å finne mottiltak ved hjelp av virksomhetens rutiner og planverk. Slike øvelser involverer vanligvis bare ledelse og stab.*
- ***Spilløvelser:*** *Her øves både kriseledelse og stabsarbeid. Øvelsen krever aktiv handling fra deltakerne, og bruk gjerne kommunikasjonsmidler som telefon og e-post. Deltakerne kan for eksempel kommunisere med responsceller som simulerer relevante aktører. Spilløvelser er godt egnet til å øve ansvars- og rolleforståelse, samordning og koordinering, samt utfordringer knyttet til krisekommunikasjon, informasjonsdeling og etablering av et felles situasjonsbilde.*
- ***Praktiske øvelser*** *der de involverte parter iverksetter tiltak som de ville ha gjort i en reell situasjon, slik at planverk, ansvar og roller blir øvet.*

Utarbeidelse og oppdatering av planverk

Et planverk bør ta for seg arbeidsoppgaver, roller og ansvar ved en normaltilstand, og ved tilsiktede/utilsiktede hendelser. Planverket for fredstid bør være likest mulig planverket som gjelder ved krise og krig. Politiet bruker for eksempel tiltakskort for ulike hendelser, slik at responsen blir mest mulig presis og effektiv. NSM veiledning for sikkerhetsstyring[9] gir flere eksempler på utarbeidelse av planverk.

Sjekklister, rutiner og instrukser

Gode etablerte rutiner styrker sannsynligheten for at minst mulig overlates til den enkeltes skjønnsvurderinger. For at virksomheten skal kunne ha oversikt over hvilke sikkerhetsrutiner som skal følges, kan det være nyttig å utarbeide sjekklister. Eksempler er sjekklister for kontorsikkerhet, vakt-/låserutiner, sikkerhetsrevisjon og opplæring. Enkelte virksomheter har også instrukser som angir krav til de ansatte.

7
Phishing: Digital snoking eller fisking av sensitiv informasjon som blant annet identitet, kredittkortinformasjon og passord

8
CBR: kjemiske (C), biologiske (B) og radiologiske (R) trusselstoffer

9
NSM (2015). Veiledning for sikkerhetsstyring. *www.nsm.stat.no*

Bakgrunnssjekk og sikkerhetsklarering av ansatte

Virksomheter som ikke har befatning med sikkerhetsgradert informasjon, kan også ha behov for å gjøre en bakgrunnssjekk av sine ansatte. For tiltredelse i enkelte stillinger i helse- og omsorgssektoren er det for eksempel påkrevd med (utvidet) politiattest. Private virksomheter kan ha behov for å skjerme informasjon som er sensitiv av forretningsmessige årsaker, og det finnes en rekke veiledninger man kan benytte seg av.

Ansatte som skal jobbe med gradert informasjon må autoriseres, og for å få tilgang til informasjon, gradert KONFIDENSIELT og høyere må de sikkerhetsklareres.[10] På samme måte må virksomheten tilpasse arbeidsplassen slik at de(n) som ikke er sikkerhetsklarert, ikke kan komme i befatning med gradert informasjon. NSMs veiledning for personellsikkerhet gir føringer på hvordan virksomheten bør administrere dette.[11]

Administrering av brukertilganger

De ansattes tjenstlige behov for tilgang til bygninger, etasjer, rom eller datasystemer må avklares. Det er derfor viktig at virksomheten har bestemmelser som angir dette. Tjenstlig behov kan variere etter arbeidsoppgaver og ansvar, og tilganger kan derfor innvilges for en avgrenset periode. Virksomheten bør også ha rutiner for endring eller fjerning av brukertilganger.

Avvikshåndtering

Virksomheten må ha rutiner og instrukser for håndtering av avvik. Avvik og hendelser innen sikkerhet kan potensielt skade eller true verdier. Det bør være klare rutiner for hvordan et avvik eller hendelse rapporteres, slik at dette kan utbedres så snart det lar seg gjøre. Det må videre skilles mellom avvik, feil og mangler. De ansatte må være godt kjent med rutiner for avviksmeldinger, og de må være lett tilgjengelige.

Beredskapsplaner og krisehåndtering

Beredskapsplaner er nødvendig for å kunne håndtere spesielle hendelser og krisesituasjoner på en god måte. Kompetanse i beredskap og krisehåndtering krever systematisk arbeid med planverk, personell og ledelse. Å planlegge håndtering av kriser og katastrofer er et viktig ledd i virksomhetens strategiske og operative arbeid, enten det dreier seg om en offentlig virksomhet, en bedrift eller frivillig organisasjon.

Beredskap defineres som «forberedt evne til på kort varsel å kunne øke et sikkerhetsnivå, håndtere en uønsket hendelse eller tilstand, eller evne til å gjenopprette tilfredsstillende tilstand etter en uønsket hendelse eller tilstand».[12]

«Plans are worthless, but planning is everything»[13] – fundamentet for evnen til å håndtere kriser ligger i forberedelsene: planverk, trening, øvelser, samhandling og tankesett. Når det haster med å handle, blir man sjelden bedre enn forberedelsene tilsier.

Etablering av gode og fungerende beredskapsplaner kan være et omfattende arbeid:

- → *Planverk må utarbeides på grunnlag av oversikt over risiko og sårbarhet i egen virksomhet.*
- → *Beredskapsplanverket bør ha en systematikk som sikrer involvering og forankring i organisasjonen.*
- → *Beredskapsplaner og krisehåndtering må øves[14] og vedlikeholdes.*

Omfanget vil variere fra enkle planer med fokus på varslingsrutiner og krisekommunikasjon til omfattende planverk med kriseorganisering, hendelsesspesifikke tiltakskort og delplaner, plan for personell- og pårørendehåndtering, relevante maler og prosedyrer,

10
Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) av 20. mars 1998 nr. 10 § 19

11
NSM (2012) Veiledning til sikkerhetslovens kapittel 6 og forskrift om personellsikkerhet

12
Fra NS 5830

13
Sitat Dwight D. Eisenhower (tidligere US president)

14
Sikkerhetsloven/Forskrift om sikkerhetsadministrasjon § 3-4 sier at beredskapsplanen skal øves jevnlig og minst en gang i året

kontinuitetsplan, beredskapsmessige sikringstiltak, m.m.

Virksomheter som politiet og Forsvaret har beredskapsplaner som er bygget opp med ulike beredskapsnivåer. Beredskapsnivåene er ment å iverksettes i en tidsbegrenset og ekstraordinær situasjon som følge av endringer i risikobildet. Dette kan også være hensiktsmessig for andre virksomheters beredskapsplan, spesielt i forhold til terrorhandlinger.[15]

Utarbeidelse av beredskapsplaner og omfanget av disse behandles ikke i Sikringshåndboka utover det som kobles mot eiendom, bygg og anlegg.

15

«Terrorsikring. En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger» 2015. NSM, PST og Politidirektoratet

Kapittel 16

Beskyttelse mot eksplosjoner

Dette kapitlet beskriver de grunnleggende effektene ved en eksplosjon og hvilke skader disse effektene kan påføre bygninger. I tillegg beskrives krav, dimensjonering og tiltak for beskyttelse av bygninger og verdier mot eksplosjonsbelastning.

Eksplosiveffekter

Et høyeksplosiv (sprengstoff) er et stoff med stor lagret potensiell energi. Energien er lagret kjemisk og frigjøres ved at eksplosivet utsettes for varme eller støt. Energien i et høyeksplosiv frigjøres ved en detonasjon. En detonasjon er en forbrenning som går raskere enn lydhastigheten i eksplosivet. Hastigheten til en detonasjon kan variere fra 1 000 til 10 000 meter pr. sekund avhengig av typen eksplosiv. Idet en sprengladning detoneres, omformes eksplosivet fra et fast stoff eller væske, til gass med temperatur på 2000º til 5000º celsius og trykk 50 000 til 300 000 ganger høyere enn trykket i atmosfæren. På grunn av det høye trykket og temperaturen vil gassene ekspandere med en voldsom hastighet. Ekspansjonen av gasser resulterer i en sjokkbølge som vil forplante seg utover i den omkringliggende luften og ned i bakken, se foto neste side. En sjokkbølge er en trykkbølge som beveger seg med en hastighet som er høyere enn hastigheten til lyden i det materialet den beveger seg i. Sjokkbølgen som beveger seg i bakke og luft, omtales som henholdsvis grunnsjokk og luftsjokk. Størstedelen av energien vil gå til luftsjokk når eksplosivet er plassert over bakken, som for eksempel i et kjøretøy. Energien som går ned i bakken, vil være med på å forme et krater og skape et grunnsjokk som gir rystelser i omkringliggende installasjoner. Videre i dette kapitlet vil luftsjokket omtales som trykkbølgen.

Det eksisterer et stort utvalg høyeksplosiver med forskjellige egenskaper. Dette er egenskaper som energitetthet, detonasjonshastighet, etterbrenning og gassutvikling. For å kunne sammenligne eksplosiver er det vanlig å beskrive et spesifikt eksplosivs egenskaper i forhold til egenskapene til trinitrotoluen (TNT). Således gjøres TNT til en referanse. Denne omregningsfaktoren omtales som TNT-ekvivalenten.

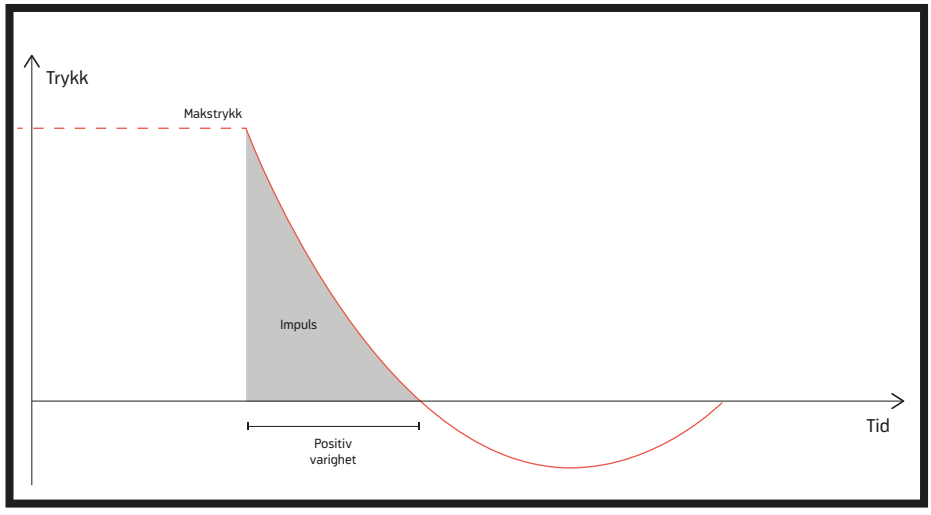
Når en trykkbølge i luft treffer en bygning, vil bygningskomponentene få en momentan og meget kortvarig belastning. For å angi en eksplosjonsbelastning fra trykkbølgen er det vanlig å angi maksimaltrykket, impulsen og positiv varighet, se ***figur Trykkforløp for trykkbølge i luft*** neste side.

Om trykkbølgen treffer på en hindring, som for eksempel en fasade, vil den bli reflektert. Trykket som da oppstår på fasaden, kalles et refleksjonstrykk. Om trykket passerer parallelt med trykkbølgens bevegelsesretning, vil trykket være uforstyrret, og betegnes som sidetrykk. Refleksjonstrykket kan være fra 2 til nesten 20

Detonasjon av et kjøretøy med eksplosiver

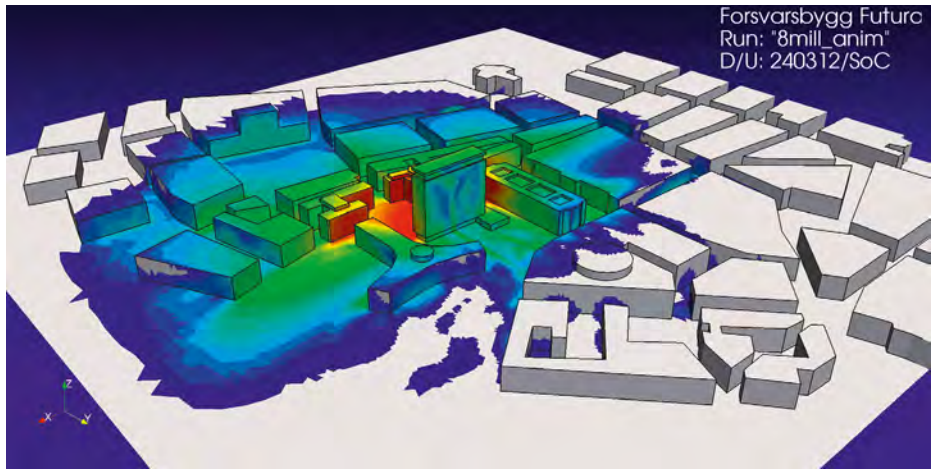
Fotografi som viser detonasjon av et kjøretøy med eksplosiver. Trykkbølgen er synlig som en «glassaktig» halvkule. Den er synlig fordi lyset brytes av det høye trykket. **FOTO** Ole Morten Størseth

Trykkforløp for trykkbølge i luft



Kurven viser trykk/tidsforløpet for et punkt som trykkbølgen passerer.

Luftsjokksimulering



Numerisk simulering av maksimaltrykket fra eksplosjonen i Regjeringskvartalet 2011, hvor «varme farger» angir høyt trykk. **FOTO** Forsvarsbygg

ganger større enn sidetrykket, derfor vil fasader vendt mot et potensielt eksplosjonssted måtte være kraftigere enn resten av fasadene.

For å beregne eksplosjonsbelastningen på et frittstående objekt kan det ofte være tilstrekkelig med empiriske metoder som Kingery og Bulmash-kurvene.[1]

Ved eksplosjoner i tettbygde områder og bymiljø kan utbredelsen av trykkbølgen bli meget kompleks på grunn av refleksjoner fra andre bygg og forsterkende effekter i trange gater. For å beskrive eksplosjonsbelastningen i kompliserte omgivelser kan det derfor være nødvendig å gjennomføre numeriske trykkbølgesimuleringer som vist i ***figuren Luftsjokksimulering***.

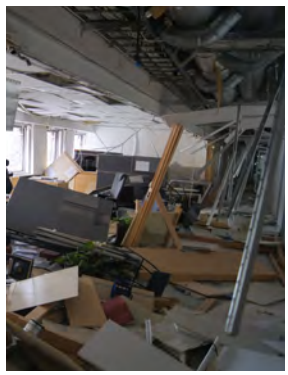
En trykkbølge som treffer bygget, kan føre til at hele eller deler av bygget raser sammen og vinduer kan bli knust over store arealer. Det beste tiltaket mot trykkbølger er å skape størst mulig avstand mellom bygget og potensielt eksplosivsted (engelsk: standoff). Bygningsskadene i Regjeringskvartalet i 2011 var i all hovedsak forårsaket av trykkbølgen i luft, se foto neste side.

Dersom eksplosjonen skjer inne i en bygning, vil trykkbølgen bevege seg mellom vegger og etasjeskiller, og en vil få flere trykkbølgebelastninger. Samtidig vil det også bygge seg opp et langvarig trykk i rommet referert til som et gasstrykk. Gasstrykket vil kunne rive og blåse rommet eller bygget fra hverandre. Størrelsen på gasstrykket er avhengig av eksplosivmengden i rommet, volumet til rommet og hvor store muligheter det er for at gasstrykket kan bli ventilert ut gjennom åpninger i rommet. Områder som kan være spesielt utsatt for innvendige eksplosjoner, er f.eks. resepsjoner, garasjeanlegg og lagre og bygninger hvor det oppbevares eksplosiver, kjemikalier og gass.

Om et eksplosiv har en bøssing eller innkapsling vil det i tillegg til trykkbølgen også bli fragmenter. Fragmenter som stammer fra våpenet

1
Referanse: Kingery, Charles N., and Gerald Bulmash, «Airblast Parameters from TNT Spherical Air Burst and Hemispherical Surface Burst,» U.S. Army Ballistic Research Laboratory Technical Report ARBRL-TR-02555, Aberdeen Proving Ground, MD, April 1984

Skader på bygninger på grunn av luftsjokk



Regjeringskvartalet i Oslo 22. juli 2011 og skader på bygninger på grunn av trykkbølgen i luft. **FOTO** Forsvarsbygg

Skadebilde ved eksplosjoner

Utvendig eksplosjon

Utvendig eksplosjon med en ren 7 kg eksplosivladning på 1 meter avstand mot en betongkonstruksjon.

Innvendig eksplosjon

Innvendig eksplosjon i en betongkonstruksjon fra en ren 7 kg eksplosivladning.

Fragmenterende eksplosjon

Utvendig eksplosjon med en fragmenterende granat med 7 kg eksplosiver på 1 meter avstand. **FOTO** Forsvarsbygg

omtales som primærfragmenter. Hvis eksplosivene er plassert i et kjøretøy, vil det være kjøretøyet som er kilden til primærfragmenter. Trykkbølgen vil når den beveger seg gjennom luften, også kunne ta med seg løse gjenstander eller kunne kaste knust glass fra vinduer inn i bygg. Denne typen fragmenter omtales som sekundærfragmenter. Primærfragmentene fra et kjøretøy med eksplosiver vil normalt ha liten effekt på bygninger sammenlignet med

Testforsøk med overdekning på eksplosivlager

Utkast av fragmenter ved eksplosjon i et eksplosivlager, fra jordoverdekkede forsøk utført på Rena.
FOTO Hans Fredrik Asbjørnsen

FOTO AP / NTB Scanpix (the destroyed building, Khobar Towers, and crater in Dhahran, Saudi Arabia)

trykkbølgen. Men mennesker i nærheten av et kjøretøy med eksplosiver, vil derimot ofte få større skader fra primærfragmentene enn trykkbølgen. For mennesker i bygninger vil det være sekundærfragmenter fra knuste vinduer som representerer den største faren. For militære våpen og stridshoder vil ofte kombinasjon av fragmenter og trykkbølgen kunne gi vesentlig større skade på bygget enn hva trykkbølgen klarer alene.

Skadebildet fra eksplosiver vil være vesentlig forskjellig avhengig av om man har en innvendig, utvendig eller fragmenterende eksplosjon. Dette er illustrert i ***figur Skadebilde ved eksplosjoner*** på forrige side, hvor 7 kg eksplosiver er detonert i ulike konfigurasjoner.

I Saudi-Arabia, ved Khobar Towers, ble det i 1996 detonert en tankbil med flere tonn eksplosiver på ca. 30 meters avstand fra bygget. Tankbilen var plassert ved en støttemur av betong, som ble knust og kastet mot bygget av trykkbølgen. Kombinasjonen av trykkbølgen og sekundærfragmentene påførte bygget større fasadeskader enn hva trykkbølgen alene kunne forårsaket.

I forbindelse med en ulykke i lager hvor det oppbevares store mengder eksplosiver, gass eller kjemikalier, vil en kunne få kombinasjon av effekter på omgivelsene. Utkastet av fragmentene fra lager, utkast fra krater og trykkbølgen i luft vil kunne skade bygninger og mennesker i et stort område. ***Bildeserien over*** viser eksplosjon i et jordoverdekket eksplosivlager optimalisert for å redusere utkast og for å styre trykkbølgen i sikker retning.

I tilfeller hvor en har en eksplosjon i en tunnel, under bakken eller i et eksplosivlager, kan effekten fra luftsjokket og utkastet av fragmenter dempes. Dette kan gjøres ved å ha tilstrekkelig med masser rundt og over tunnelen eller eksplosivlageret. Men når ladningen er under bakken eller har god overdekning, kan grunnsjokket bli den dimensjonerende eksplosjonslasten for bygninger i nærheten av eksplosjonen.

Bygningsskader ved eksplosjoner

Bygningsskade fra eksplosjoner vil ha ulik karakter avhengig av mengde eksplosiver og avstand mellom bygning og eksplosiver. Om eksplosjonen skjer inne i eller i nærheten av bygget, er faren stor for sammenrasning med katastrofale konsekvenser for verdier og personell i bygget, om eksplosjonen derimot skjer på større avstand, er det vinduer som er svakeste element, og som vil kunne representere den største faren for personell.

Det første man vil sikre seg mot når en beskytter bygninger mot eksplosiver, er uforholdsmessig stor sammenrasning. Sammenrasning skjer oftest ved at enkelte bærende bygningskomponenter blir så skadet i en eksplosjon at de mister sin bærende evne, og det resterende bæresystemet ikke har kapasitet til å holde større deler av bygget oppe. Dette kalles progressiv kollaps. Den andre og erfaringsmessig sjeldnere kollapsformen er når den globale eksplosjonsbelastningen på bygget er så stor at bygget skyves over ende. Evnen til å motstå denne effekten kalles global stabilitet.

Stålbygg og betongbygg har ofte god motstandsevne mot progressiv kollaps, fordi armert betong og stål er duktile materialer som tåler relativt store deformasjoner. Mange nyere betongbygg består av bærende prefabrikkerte betongelementer. Dersom forbindelsen mellom disse elementene er svake, vil bygget ha liten evne til å overføre krefter til andre bærende elementer dersom for eksempel en søyle blir ødelagt. Gode forbindelser og duktilt materiale i bæresystemet er altså viktig for å unngå progressiv kollaps.

Bygg som er oppført med bærende teglsteinsvegger, som er et sprøtt materiale, kan være utsatt for progressiv kollaps. Men det er ikke bare materialet som avgjør, bygg med

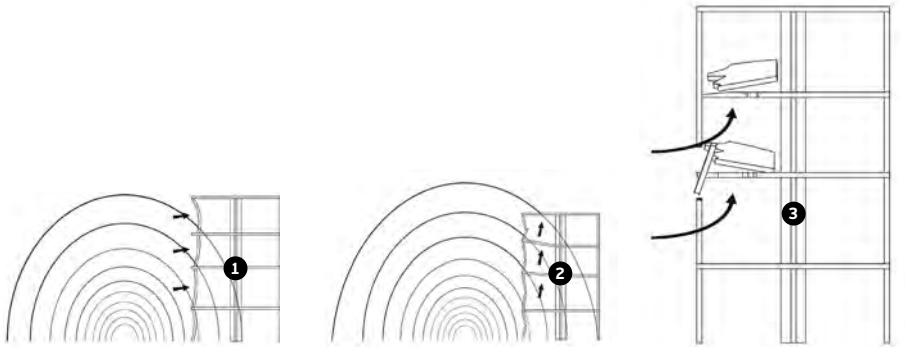
Progressiv kollaps av bygninger

Eksempler på progressiv kollaps av bygninger, henholdsvis Murrah Federal Building i Oklahoma City i USA og USAs ambassade i Beirut i Libanon etter kjøretøy med eksplosiver på utsiden av byggene.
FOTO AP / NTB Scanpix (the American Embassy in Beirut, Lebanon, after a huge bomb blast)og Charles Porter IV / Zuma Press / NTB scanpix (Oklahoma City Bombing)

Sentralbanestasjonen i Bologna i Italia i 1980 etter at en koffert med 23 kg eksplosiver eksploderte inne i bygget, og 85 personer omkom.
FOTO AP / NTB Scanpix (Italy Right Wing Terror, 1980)

Bygningsskader ved eksplosjon

Bygningsskader fra eksplosjoner som kan føre til progressiv kollaps



Trykkbølgen fra eksplosjonen trenger inn i bygningen gjennom vinduene og svake fasadeelementer.

Trykket som trenger inn i bygget, gir oppadrettede krefter på dekkene.

Dekkene løftes og ødelegges, som igjen medfører at dekker og søyler kobles fra hverandre. Resultatet blir tap av stabilitet, som igjen kan medføre progressiv kollaps.*

* FEMA 430: Risk Management Series «Site and Urban Design for Security Guidance Against Potential Terrorist Attacks», Federal Emergency Management Agency (FEMA), December 2007.

slanke teglsteinsvegger er mer utsatt enn murbygning med tykke, bærende vegger.

Normalt er bygninger dimensjonert for å ta opp krefter som følge av tyngdekraften, snølaster og vindlaster. Ved en innvendig eksplosjon eller dersom en trykkbølge fra en utvendig eksplosjon trenger inn i bygget, vil det oppstå krefter som virker i retninger bygget i utgangspunktet ikke var dimensjonert for. Dette kan være oppadrettede krefter på etasjeskillere og -forbindelser og horisontale krefter på bærende vegger.

I tillegg til at en skal unngå progressiv kollaps, må bygget også ha en tilstrekkelig stabilitet til å ta opp den globale eksplosjonsbelastningen. Det gjøres blant annet ved å ha tilstrekkelig med avstivende skiver i bygget. I ***figuren Simulering av global forskyvning til et betongbygg*** er det gjengitt resultater fra en numerisk beregning som illustrerer hvordan et bygg vil svinge som følge av en stor eksplosjonsbelastning.

Når en har sikret seg at byggets bæresystem motstår eksplosjonslasten, vil de svakeste komponentene være vinduer, dører og fasaden. Trykkbølgen vil knuse vinduer og kaste glasset inn som fragmenter. De fleste bygg har store arealer med vinduer som gjør at glassfragmentene vil utgjøre fare for en høy andel av personellet i bygget. Trykkbølgen vil også kunne trenge gjennom de ødelagte vinduene og gjøre skader innover i bygget. Dersom eksplosjonsbelastningen er stor, vil også vegger eller deler av veggene kunne bli kastet inn i bygget.

Hastigheten på glassfragmentene vil avgjøre hvor langt fragmentene kastes inn, og for hvor mange de vil utgjøre en fare. I ***figuren Skadenivå*** er det beskrevet sammenhengen mellom innkastlengde av vinduer og tilhørende faregrad. Dette er definisjoner som benyttes både ved testing av vindusløsninger og ved beskrivelse av skadebilder i forbindelse med skadeanalyser eller sårbarhetsanalyser.

Simulering av global forskyvning i et betongbygg

En utvendig eksplosjon vil kunne sette hele bygget i svingninger. Figuren viser en numerisk beregning hvor kreftene på ulike komponenter i bygget er beregnet. Fargene angir forskyvning. **FOTO** Forsvarsbygg

Det finnes ulike standarder for prøving og klassifisering av vinduers motstandsevne mot eksplosjonsbelastning. I NS-EN 13123-1 er vinduer klassifisert[2] i EPR-klasser (Explosion Pressure Resistance). I ***tabellen Klassifisering av vinduer*** angis maksimalt trykk og impuls fra en eksplosjon som vinduet kan utsettes for, uten at vinduet skal avgi farlige fragmenter. Ved en EPR-klassifisering er kravet at både karm og glassruten skal motstå belastningen. I siste kolonne i tabellen er tilhørende avstand og eksplosivmengde angitt for å oppnå de angitte belastningene.

Glassruten kan forsterkes ved å legge en film[3] på innsiden. Om filmen også er festet til karmen, vil løsningen forsterkes ytteligere. Løsninger med film kan ha kapasitet inntil et EPR1-nivå. Ønskes løsninger med høyere nivå, benyttes vindu med laminert glass. Dette gjøres ved å skifte ut eksisterende vindu eller sette inn et nytt vindu på innsiden av eksisterende vindu. Et laminert glass består av to eller flere glassplater som er limt sammen med plastfolie. Erfaringsmessig har ofte slike vinduer noe dårligere U-verdi (ca. 1.3 W/(m^{2}K)) enn vanlige vinduer. Løsninger kan også i varierende grad medføre farge i glasset. Når en velger å forsterke med film eller nytt laminert vindu, er det viktig at også karmen, rammen og forbindelsen tåler eksplosjonsbelastningen. Et vindu vil ikke være sterkere enn den svakeste komponenten, dette er illustrert i ***Glassrute ved eksplosjon***, hvor glassruten er sterkere enn innfestningen mellom vindusramme og vinduskarm.

Moderne fasadeløsninger er ofte av stål, aluminium eller treverk. Ikke bærende vegger konstrueres gjerne i treverk og isolasjon, eller spesialprofiler og isolasjon. Slike fasadeløsninger har begrenset evne til å tåle eksplosjonslaster. Ikke bærende vegger av betong eller stålprofiler forankret i dekkene og bekledd med tunge materialer har større evne til å tåle eksplosjonslaster.

I ***figuren Bygningsskader*** er ulike beskyttelsesnivåer eller skadenivåer estimert for normale stål og betongbygg. Diagrammet gjelder for bygninger som ikke er designet for å tåle eksplosjonsbelastning. Teglsteinsbygg, med slanke bærende vegger, vil kunne ha vesentlig dårligere kapasitet. Diagrammet kan benyttes for en rask overslagsmessig vurdering av bygget, men det er viktig å være klar over at bygninger kan ha høyere eller lavere motstandsevne mot eksplosjoner enn diagrammet angir.

2
Andre standarder som også benyttes er NS-EN 13123-2 (EXR-klasser), NS-EN 13541 (ER-klasser) og ISO 16934 (EXV- og SB-klasser).

3
Løsninger med film har begrenset levetid i forhold til et klassifisert vindu.

Glassrute ved eksplosjon

Glassrute som knuses og kastes inn i rommet ved en eksplosjon. Fra tester utført av Forsvarsbygg.

Glassrute som knuses og kastes inn i rommet, delvis mot eksplosjonsstedet.

Glassrute som knuses og kastes inn i rommet, fra siden.

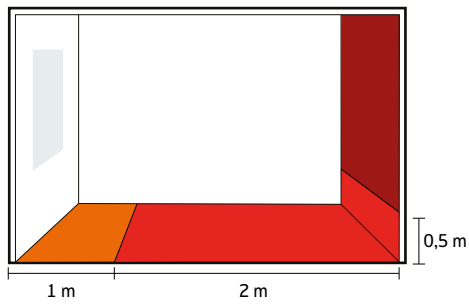
Skadenivå

*Definisjon på skadenivåer for vinduer utsatt for en eksplosjon basert på UK Glazing Hazard Guide**

Beskjedent innkast
(eng. Minimum hazard)
Glasset knuser eller vinduet ødelegges og eventuelle fragmenter fra vinduet faller maksimalt 1 meter inn i rommet. Dvs. liten fare for personskader. Blir også kalt «Break safe».

Svakt innkast
(eng. Low hazard)
Fragmenter fra vinduet blir kastet opp til 3 meter inn i rommet med en maksimalhøyde på ½ meter over gulvet. Fragmentene kan føre til alvorlige personskader, spesielt i nedre del av kroppen.

Kraftig innkast
(eng. High hazard)
Fragmenter kastet kraftig inn i rommet og en får fragmenter som går lengere enn 3 meter fra vinduet med en høyde på over ½ meter. Fragmentene fører ofte til alvorlige personskader, og det er fare for omkomne.



* UK Glazing Hazard Guide, cubicle stand-offs, tables & charts, SAFE/SSG, Explosive Protection, London SSG/EP/4/97, June 1997.

Klassifisering av vinduer etter NS-EN 13123-1

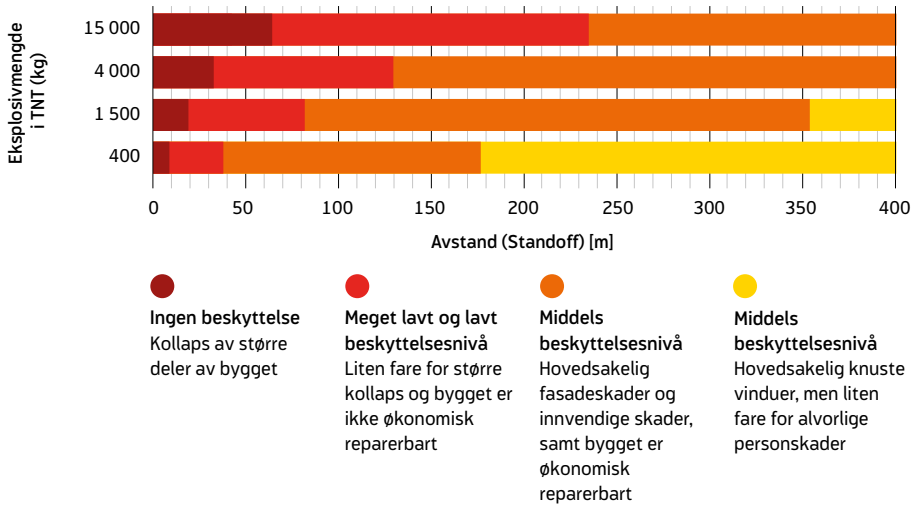
Klasser	Maks. trykk	Maks. impuls	Tilhørende eksplosivmengde og avstand (Reflektert)
EPR 1	50 kPa	370 kPa-ms	ca. 90 kg TNT på 33 meters avstand fra vegg
EPR2	100 kPa	900 kPa-ms	ca. 370 kg TNT på 36 meters avstand fra vegg
EPR3	150 kPa	1500 kPa-ms	ca. 900 kg TNT på 40 meters avstand fra vegg
EPR4	200 kPa	2200 kPa-ms	ca. 2000 kg TNT på 46 meters avstand fra vegg

Vindu ved eksplosjon

Fra tester utført av Forsvarsbygg

Innfestningen av rammen i karmen er svakere enn glasset, og hele vinduet blir kastet inn i rommet.

Bygningsskader



Estimerte skader på normale stål- og betongbygg med meget tykke murvegger, som funksjon av eksplosivmengde og avstand

Krav til beskyttelse

For å kunne dimensjonere beskyttelse av verdier i bygninger mot eksplosjoner, må eier av virksomheten bestemme seg for hvor store skader som kan aksepteres på verdiene dersom en eksplosjon skulle inntreffe. For å oppnå riktig beskyttelse er det en forutsetning at virksomhetseieren kartlegger sine verdier, samt hva som kan være en akseptabel tidsperiode for funksjonssvikt eller bortfall av verdier. Virksomhetens sikringsmål må ligge til grunn for vurderingene. Basert på sikringsmål velges beskyttelsesnivå opp mot definerte trusler.

Beskyttelsesnivået trenger ikke nødvendigvis gjelde hele bygget, men kan variere for forskjellige deler eller funksjoner i bygget. Nasjonalt kompetansesenter for sikring av bygg har definert 5 nivåer for beskyttelse. Ut fra disse beskyttelsesnivåene beskrives konsekvenser for bygningskonstruksjonen og verdier i et bygg.

Dimensjonering mot eksplosivbelastning

Dimensjonering av bygninger mot eksplosivlaster krever at det foreligger en dimensjonerende trussel med et tilhørende kriterie for akseptabel skade. I denne prosessen anbefales det at benyttes beskyttelsesnivå for å beskrive akseptabel skade. Ved å velge et beskyttelsesnivå fra tabellen ***Overordnet beskrivelse av beskyttelsesnivå*** i forhold til den dimensjonerende trussel, kan en finne skadekriterier for de enkelte bygningskomponenter i tabellen ***Beskyttelsesnivå for bygninger og verdier mot eksplosjonslaster***. Beskyttelsesnivåene er basert på beskrivelser i UFC 4-010-01 «DoD Minimum Antiterrorism Standards for Buildings». Videre når dimensjonering skal gjennomføres, finnes mer detaljerte og kvantitative beskrivelser i PDC-TR 06-08 «Single Degree of Freedom Structural Response Limits for Antiterrorism Design».

Tiltak for beskyttelse mot eksplosjonsbelastning

Oppnåelse av beskyttelse mot eksplosivbelastning innebærer en helhetstankegang. Nedenfor er det angitt de mest vanlige tiltakene for beskyttelse mot eksplosjoner. En mer utførlig beskrivelse av enkelte tiltak finnes i ***kapittel 9, Arkitektur og sikkerhet.***

Skape avstand (standoff)

Det tiltaket som ofte vil ha størst effekt på skadeomfanget, er å skape avstand mellom

Overordnet beskrivelse av beskyttelsesnivå

Beskyttelsesnivå				
0 **Ingen beskyttelse**	1 **Meget lav grad av beskyttelse**	2 **Lav grad av beskyttelse**	3 **Middels grad av beskyttelse**	4 **Høy grad av beskyttelse**
Målsetting				
Ingen	Avverge katastrofale konsekvenser	Beskytte liv og helse	Beskytte verdiene	Uabrutt operativ evne
Skadeomfang				
En hendelse medfører alvorlig skade med katastrofale konsekvenser.	En hendelse medfører alvorlig skade, men katastrofale konsekvenser unngås.	En hendelse medfører alvorlig skade, men viktige verdier kan reetableres ved annen lokasjon.	En hendelse medfører skade, men verdier kan reetableres på stedet.	En hendelse medfører kun ubetydelig skade.

Beskyttelsesnivå for bygninger og verdier mot eksplosjonslaster

Beskyttelsesnivå	Skade på bygnings-konstruksjon	Skade på personell	Skade på innhold (materielle verdier)	Operativ drift
0	Fare for global kollaps.	Tap av liv for majoriteten av personell i kollapsede områder.	Fare for tap eller ødeleggelse av innhold.	Fare for tap eller ødeleggelse av funksjon eller tjeneste.
1	Lokal kollaps kan forekomme, men progressiv kollaps forventes ikke. Arealer i og rundt skadeutsatt område kan ikke brukes.	Alvorlige skader på majoriteten av personell i skadeutsatt område, mulig tap av liv. Mindre til moderate skader på personell utenfor skadeutsatt område.	Fare for tap eller ødeleggelse av innhold.	Fare for tap eller ødeleggelse av funksjon eller tjeneste.
2	Liten fare for lokal kollaps, men skadeomfanget er slik at bygningen eller bygningsdelen ikke er økonomisk reparerbar, og må normalt rives.	Mindre til moderate skader på majoriteten av personell i skadeutsatt område, mulig enkelte alvorlige skader. Tap av liv forventes ikke. Mulig mindre til moderate skader på personell utenfor skadeutsatt område.	Innhold forventes å være intakt for uthenting.	Funksjon eller tjeneste må reetableres på ny lokasjon med påfølgende nedetid.
3	Arealer i og rundt skadeutsatt område kan brukes etter opprydding og reparasjoner.	Mulig mindre til moderate skader på personell i skadeutsatt område, tap av liv forventes ikke. Mulig overfladiske skader på personell utenfor skadeutsatt område.	Innhold forventes å være intakt.	Funksjon eller tjeneste kan gjenopptas etter midlertidig evakuering og/eller reparering og opprydding.
4	Hovedsakelig fasadeskader, og skadeomfanget er slik at bygningen eller bygningsdelene er økonomisk reparerbare.	Mulig overfladiske skader på personell.	Overfladiske eller ubetydelig skader på innhold.	Funksjon eller tjeneste er operativ umiddelbart etter en hendelse.

potensielt eksplosivsted og bygning. Dette kan oppnås gjennom:

- → *Ved nybygg, velg tomt som gir mulighet for stor avstand til offentlig tilgjengelig vei, deretter plasser bygget med størst mulig avstand til eksplosivtrussel.*
- → *Verdier plasseres eller flyttes til deler av bygget der trusselen har minst effekt.*
- → *Etabler kjøretøysperrer rundt bygget.*
- → *Plassere kontroll av post og varer utenfor ytre perimeter.*
- → *Differensiere trafikken rundt bygget. Ofte er det vanskelig å få stengt veier,*

for å unngå at kjøretøy kan frakte store mengder eksplosiver nær bygget. Det kan derfor være nyttig å skille ulike kjøretøy for å unngå at de største kjøretøyene kan komme for nær ved å skille mellom større og mindre kjøretøy, egne, ansatte og besøkende, kollektivtrafikk osv. Baksiden ved kjøretøyshinder er at det må tas hensyn til at utrykningskjøretøy skal kunne komme frem til bygget ved behov.

Merk at etablering av kjøretøyssperrer ikke nødvendigvis hindrer at mindre mengder eksplosiver kan bringes frem til bygget.

Unngå innvendige eksplosjoner

Det er viktig å merke seg at innvendige eksplosjoner er spesielt ødeleggende av to årsaker, nemlig at eksplosjonslasten forsterkes i et lukket eller begrenset ventilert volum, og at bygninger ikke er dimensjonert for belastninger i de retninger som innvendige eksplosjoner medfører.

Tiltak for å unngå sammenrasning og kollaps på hovedbygninger:

- *Eksplosjoner i parkeringsanlegg og tunneler vil kunne ha stor effekt på bygninger over. Derfor bør ikke bygg plasseres over eller oppå med mindre man har kontroll på hva som transporteres i kjøretøyene.*
- *Legg til rette for post- og varemottak utenfor bygget, spesielt dersom posten og varene ikke er forhåndskontrollert.*
- *Områder hvor man ikke har kontroll på hva som medbringes av personer, som resepsjonsløsninger og lignende, bør plasseres utenfor bygget eller i tilbygg.*
- *Unngå bruk og lagring av brennbar gass i bygninger som skal beskyttes. Brennbar gass kan føre til forverret skadebilde ved for eksempel brann eller eksplosjon.*

Bruk av trykkbølgebarrierer

Barriere i forkanten av et bygg kan øke sikringen av bygget mot blant annet fysisk inntrenging, innsyn, beskytning og stoppe fragmenter fra eksplosjoner. Barrierer kan også redusere trykkbølgen fra en eksplosjon, men dette er senarioavhengig, i ytterste konsekvens kan en barriere forsterke virkningen. Det vil derfor være nødvendig med beregninger for å vurdere om barrieren gir en ønskelig effekt, samt dimensjonering av barrieren for å unngå at barrieren avgir farlige fragmenter mot bygget.

Bygningsmessige tiltak for å unngå sammenrasning og kollaps

Bygninger som er dimensjonert mot større jordskjelvslaster, vil normalt være utført med konstruksjonsdetaljer som gjør bygningen mer robust også til å motstå eksplosjonsvirkninger. Det kan derfor være hensiktsmessig å følge anbefalinger til utforming av konstruksjonsdetaljer som er gitt i litteratur, for å øke robustheten til konstruksjoner mot jordskjelvlaster. Bygg inn kapasitet til å motstå laster som kan oppstå ved eksplosjonsbelastning, som f.eks. løft av dekker ved luftsjokkinntrengning.

Bæresystem:

- *Velg bygningskonstruksjon med gode forbindelser i bæresystemet ved å sørge for overkapasitet i konstruksjonenes evne til horisontalt og vertikalt lastopptak. Knytt sammen bygningsdeler horisontalt og vertikalt.*
- *Benytt robuste bæresystem som har duktil oppførsel ved overbelastning, og med kapasitet til å spre energi gjennom store plastiske deformasjoner før brudd. Dette er i tråd med vanlig konstruksjonspraksis for konstruksjoner i stål eller plass-støpt armert betong.*
- *Sørg for at de horisontale kreftene på fasadene overføres til dekket og ikke til søylene.*
- *Unngå bruk av elementer i utsatte deler av konstruksjonen.*
- *Ved dimensjonering mot eksplosjonsbelastninger må det tas hensyn til at det*

kan oppstå krefter på bygningsdeler i andre retninger enn det bygningen normalt er dimensjonert mot.

- *Utform bæresystem slik at det er potensial for omfordeling av laster til en sekundær bæreretning om det oppstår en kritisk hendelse, der en primærbærekomponent faller bort.*
- *I eksisterende bygg kan kapasiteten til eksisterende bærende søyler økes ved å kapsle inn søylen med stål eller armert betong.*
- *Begrens spennlengder i bæresystemet både for å unngå at luftsjokkvirkninger påføres store belastningsflater, som igjen medfører store deformasjoner, samt at store spenn gir potensial for at større arealer kollapser enten ved overbelastning eller ved bortfall av bærekomponenter. Begrensning av spennlengder betyr også at etasjehøyde ikke bør være høyere enn det som er nødvendig.*
- *Bruk avstivende skiver med hensyn til global stabilitet.*

Fasadeforsterkning:

- *Det er ofte vanskelig og kostbart å forsterke yttervegger. Ulike duker eller belegg på innsiden av veggen gir relativt liten økning i kapasiteten, mens ekstra vegg på innsiden med god innfestning oppe og nede kan gi vesentlig høyere kapasitet. Uansett forsterkningsløsning er det svært få dokumenterte produkter som motstår eksplosjoner på skalert avstand mindre enn 2 (f.eks. 400 kg på mindre enn 15 meter).*
- *Unngå vinduer i tak og reduser bruken av vinduer generelt, spesielt store vinduer.*
- *Hele vinduet må dimensjoneres mot eksplosjonsbelastning, ikke bare glassruten. Bruk av film på vinduer er en rask og billig løsning, men har begrenset motstandsevne mot eksplosjoner. Det er viktig at filmen er godt festet til karmen, og likeledes må resten av vinduet tåle eksplosjonsbelastningen. Kraftige laminerte vinduer kan være en kostbar løsning, men har god motstandsevne mot eksplosjoner. De totale kostnadene vil ved utskiftning være betydelig høyere enn bare prisen på det enkelte glass/vindu. En stor del av kostnadene er gjerne knyttet til tilrettelegning og montering av vinduene.*
- *Bruk av spesialgardiner som hindrer at vinduet eller deler av vinduet blir kastet inn i rommet, kan øke beskyttelsen, men blir sjelden brukt fordi gardinene reduserer lysforholdet i rommet, utsikten og er ofte lite estetisk pent.*
- *Fasader vendt mot potensielle eksplosjonssteder og i de nederste etasjene bør normalt være kraftigere enn resten av fasadene.*

Møblering, utstyr og innvendige glassvegger:

- *En god møbleringsplan kan redusere faren, eksempelvis kan en begrense antall sitteplasser foran vinduer. Et problem med dette tiltaket er at møbleringen lett kan bli endret i etterkant, når den ansatte finner ut at han eller hun ønsker å sitte ved vinduet.*
- *Ved en eksplosjon vil det kunne oppstå rystelser i bygget, slik at tungt utstyr og inventar faller ned og skader personellet, i tillegg til at utstyret kan bli ødelagt. Fastbolting av utstyr reduserer faren.*
- *Ved en eksplosjon kan trykkbølgen forplante seg innover i bygget. Innervegger av glass kan lett knuse og gi fragmentskader på personell i bygget, samt skade personell ved en evakuering etter hendelsen. Begrens derfor bruken av innervegger av glass eller eventuelt bruk film eller laminert glass.*

Tiltak mot eksplosiver levert med raketter, bombekastere og droner

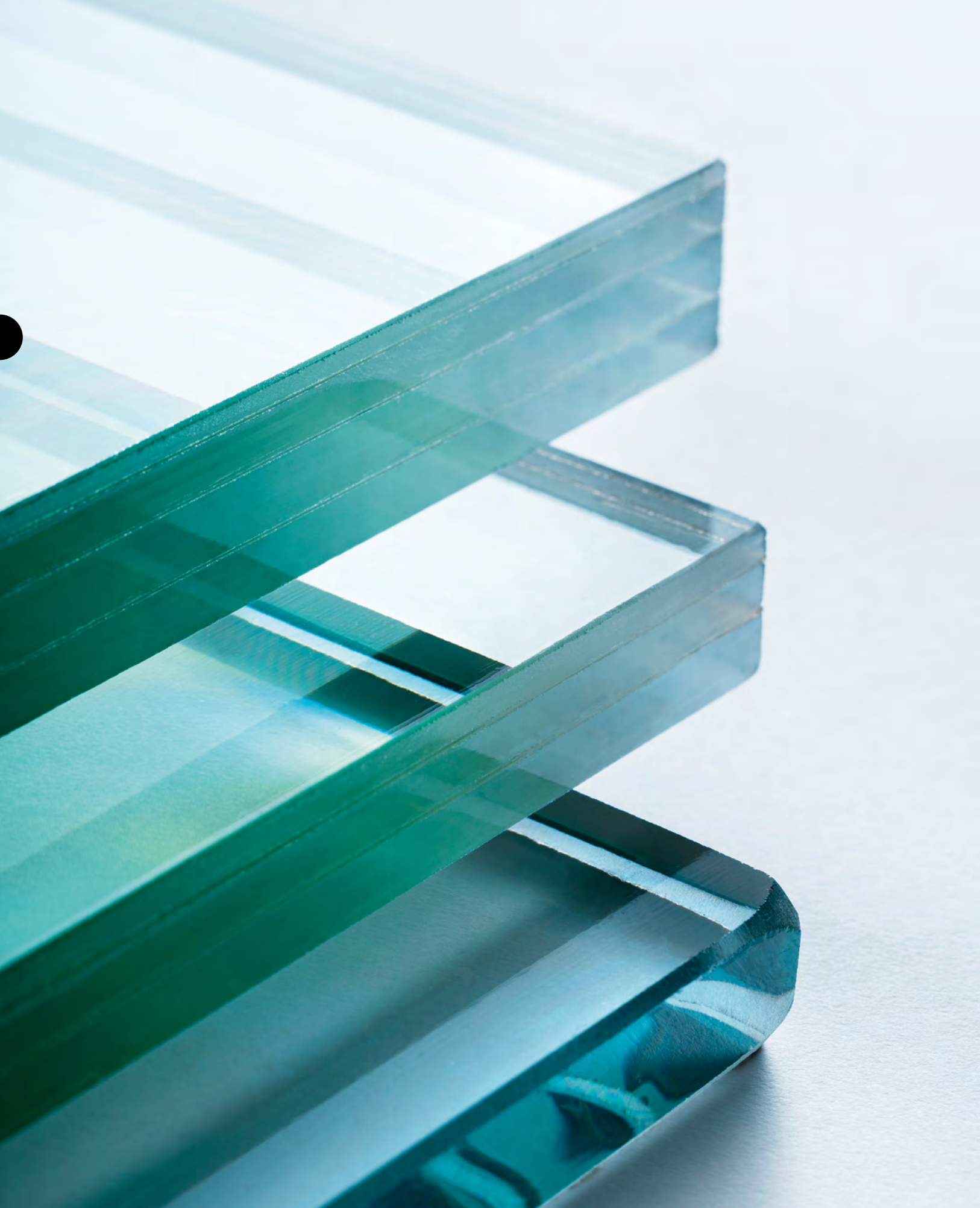
Eksplosiver som detoneres direkte mot vegger, tak og vinduer, kan utgjøre stor fare på bakside. For mange bygninger vil det ikke være mulig å stoppe eksplosiver levert med improviserte raketter, bombekastere eller droner før de treffer bygningskroppen. Den mest kosteffektive løsning for denne typen trusler vil ofte være å skape avstand mellom detonasjon og det beskyttende skallet. Dette gjøres gjennom å bruke to skall. Det første skallet dimensjoneres for å utløse detonasjon av raketter eller granaten, eller stoppe dronen. Det neste skallet plasseres et stykke innenfor og dimensjoneres for å stoppe fragmenter og trykkbølge.

Andre tiltak

Dekningsrom
I enkelte tilfeller vil det være aktuelt å etablere dekningsrom for de ansatte.

Vakthold, varsling, rutiner og evakuering
Tidligst mulig deteksjon av trusselsituasjonen og korrekt varsling til de ansatte er vesentlig ved en eksplosjonstrussel. Alarmer og TVO er viktige hjelpemidler. Vakthold kan være avskrekkende, og er viktig for å oppdage en uønsket handling i tide. Evakueringstid i et bygg vil variere etter antall personer i bygget og bygningsmessige utforminger. Evakueringstiden vurderes ofte å ligge på 3 til 10 minutter. Det er viktig med et varslingssystem som kan styre evakueringen, gode rutiner for de ansatte, samt trygge og alternative evakueringsmuligheter. Det vil for eksempel si samling i trappesjakter i betong som skjermer personellet, og mulighet til å evakuere vekk fra eksplosivladninger.

Beredskapsplan
Virksomhetens beredskapsplanverk er svært viktig ved en eksplosivhendelse. Her bør det beskrives både muligheten til å øke sikkerheten i situasjoner hvor trusselen blir større, hvordan en eksplosivhendelse skal håndteres, og hvordan man kan reagere for å redusere konsekvensene av en hendelse.



Kapittel 17

Beskytning

Dette kapitlet omhandler beskyttelse mot beskytning, med innføring i de mest utbredte våpentyper og hvordan lage løsninger som ivaretar krav til sikring, kan lages.

Beskytning er en angrepsform som kan utføres av trusselaktører med lav kapasitet; uten avansert planlegging, med enkle våpen av enkeltpersoner eller små grupper. Målet kan være å ramme personer som har en maktsymbolikk knyttet til seg, for eksempel myndighetspersoner eller personell tilknyttet politi og forsvar. Studier ved FFI/Terra beskriver hvordan terroraksjoner har gått fra å være store og organiserte og som involverer flere aksjonister, til enkeltmannsterroristen, som opererer med våpen som er lette å anskaffe. Denne typen trusselaksjoner krever lite ressurser i form av planlegging, og personell kan på den ene siden implisere et begrenset skadeomfang, men på den andre siden en svekket mulighet for å varsle og avverge angrepet. Andre typer angrep uten klare politiske eller ideologiske motiver utført med håndvåpen forekommer også med jevne mellomrom.

Vurdering av sikringsnivå

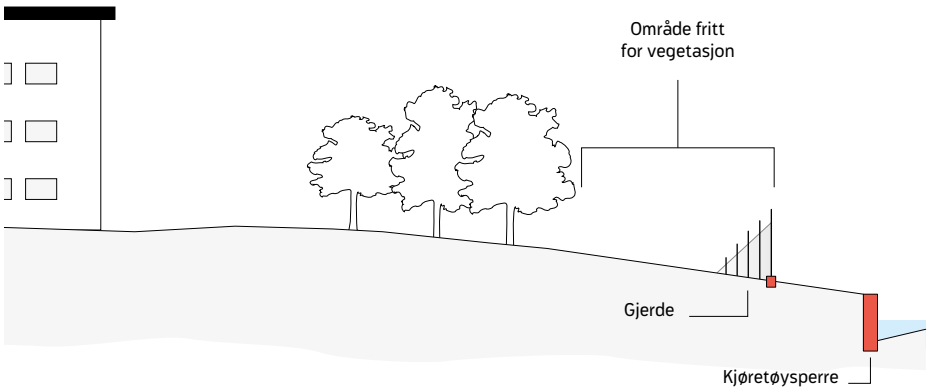
Enkelte bygninger har større behov for beskyttelse på grunn av verdiene som befinner seg der, enten det er snakk om personell, funksjoner eller utstyr. For eksempel er personell i resepsjon og vakt spesielt utsatt. Dersom området rundt objektet er oversiktlig og med fritt innsyn, eller om publikum har fri tilgang, er det enklere for trusselaktøren å observere målet over tid uten å bli oppdaget.

Hva slags sikringsnivå et bygg eller deler av et bygg skal ha, fastsettes i en verdivurdering, se ***kapittel 6, Verdivurdering.*** Hvilke tiltak som bør iverksettes, fastsettes, etter en grundig analyse av trusler og sårbarheter, se ***kapittel 5, Risikoanalyse.***

For et objekt som har et lavt sikringsnivå, kan beskyttelsestiltaket være å blokkere frie siktelinjer eller plassere funksjoner hvor de ikke kan nås med skytevåpen. Ved høyere beskyttelsesbehov skal anleggets evne til å motstå våpeneffekter vurderes. Skuddsikre vinduer og vegger installeres om nødvendig.

I risikoanalysen skal det avdekkes om trusselaktøren har mulighet til å komme tett på objektet. Med økt distanse minsker sannsynligheten for å treffe målet, samtidig som det stilles høyere krav til skytteren. Valg av våpen bestemmes også av avstand til målet; dersom det for eksempel ikke er mulig å komme nærmere enn 50 meter, er det sannsynlig at trusselaktøren velger en skarpskytterrifle med større rekkevidde. Hvis det derimot er mulig å komme tett på objektet, kan trusselaktøren benytte et lettere håndholdt våpen.

Vegetasjon som hindrer innsyn



Å hindre innsyn er et nyttig prinsipp, et så enkelt tiltak som å benytte persienner og gardiner, vil gjøre målet vanskeligere å identifisere. ***Figuren Vegetasjon som hindrer innsyn*** viser et eksempel på hvordan bruk av beplantning eller høydeforskjeller i terrenget kan hindre innsyn til et bygg eller område.

Våpenvirkninger og anslag

Som benevnelse på våpenammunisjon benyttes ofte prosjektiler. Prosjektiler er ammunisjonen brukt i alle typer skytevåpen, og det finnes en rekke ulike typer ammunisjon, også innenfor lik kaliber.

Viktigste parameteren for penetrasjonsprosessen er anslagshastigheten. Andre viktige parametere er:

- *banen og vinkelen til prosjektilet før treff*
- *dynamiske materialegenskaper til både målet og prosjektilet*
- *tykkelsen på målet og randbetingelser*
- *prosjektilets diameter, masse og neseform*
- *masseforholdet mellom målet og prosjektilet*
- *forholdet mellom prosjektildiameter og prosjektillengde*

Finkaliberammunisjon betegner prosjektiler mindre enn 20 mm. Diameteren på prosjektilet i militær og sivil finkaliberammunisjon varierer fra 4-5 mm opp til cirka 13 mm, og vekten spenner fra noen gram opp til ca. 60 gram. Prosjektiler kan bestå av blant annet såkalt ***ball-ammunisjon*** med en myk stål- eller blykule, eller ***panserbrytende prosjektiler,*** AP-ammunisjon (armour piercing), med en hardere stålkjerne. Panserbrytende prosjektiler anvendes om det er spesielt harde mål som skal perforeres, siden disse prosjektilene har større gjennomtrengningsevne enn ball-ammunisjon.

Finkaliberammunisjon er lettere tilgjengelig enn ammunisjon til større våpen. ***Tabellen med våpentyper*** viser eksempler på ulike typer håndvåpen og skarpskytterrifler med tilhørende ammunisjon.

I deler av verden hvor det er konflikter eller i tyngre kriminelle miljøer, er det også tyngre

PENETRASJON

Penetrasjon i våpensammenheng betyr inntrengning av et prosjektil i et materiale.

Dersom et mål perforeres, trenger prosjektilet gjennom materialet og fortsetter med en resthastighet.

Anslag defineres som sammenstøt mellom prosjektilet og målet.

RPG-7 granatkaster.

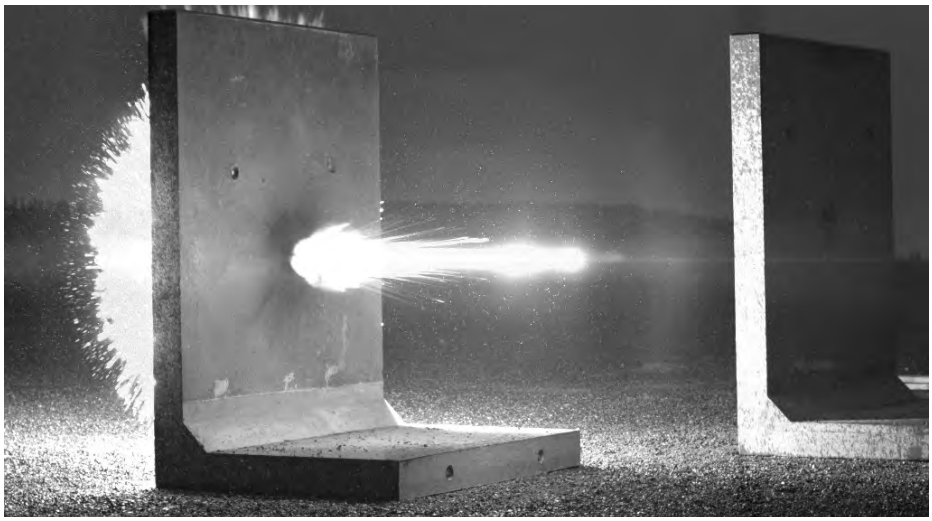
FOTO FFI

våpen i omløp. Kraftigere håndholdte våpen kan være blant annet hulladninger eller såkalte «multi-purpose»-våpen. Hulladninger er en granat med en eksplosivladning med rettet virkning. Et eksempel på en hulladning er en RPG-7 rakettkaster, som vist i bildet ovenfor, med en PG-7 V granat. Granaten er belagt med et tett formbart metall som kobber. Ved anslag settes eksplosivladningen av, og kobberet projiseres ut i en tynn, flytende stråle med en hastighet på rundt 10 000 m/s. Jet-strålen kan penetrere opptil flere meter i ulike materialer. Sjokkbølger fra sprengladningen og innstrømming av varme fra eksplosjonsgasser kan også medføre skade på mennesker eller materiell. Bildet på neste side viser effekten av en PG-7 V granat avfyrt mot en betongvegg. Å få full beskyttelse mot granater med rettet sprengvirkning er svært vanskelig, og konstruksjonen må dimensjoneres spesifikt for denne trusselen.

Multi-purpose-ammunisjon er prosjektiler som kan skade målet på flere ulike måter. Disse prosjektilene bryter lett gjennom mål uansett utforming og bringer med seg brann-, splint- og sprengvirkning inn i målet. Det finnes også målsøkende prosjektiler som navigerer seg mot målet ved hjelp av et innebygget system som

Våpentyper		Ammunisjon	
	Beretta 9 mm*		9 mm, 124 grain FMJ*
	Smith & Wesson .44*		.44 Magnum, 240 grain SWC*
	HK416 Rifle**		.223 cal, 5,56 NATO, 55 grain FMJ*
	HK417 Skarpskytterrifle**		.30 ca., 7.62 NATO, 150 grain FMJ*

* **FOTO** Kripos
** **FOTO** FFI



Effekten av RPG-7 avfyrt mot et betongelement.

FOTO Forsvarsbygg

fanger opp stråling; enten elektromagnetisk eller varmestråling, eller reflekterte radar- eller laserstråler fra målet.

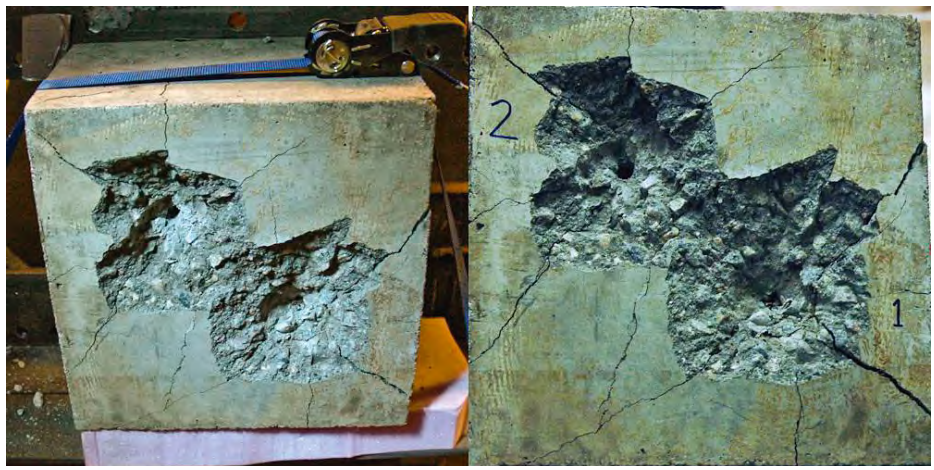
Til tross for at det finnes en rekke kraftigere prosjektiler og missiler, vil det i dette kapitlet fokuseres på beskyttelsestiltak mot finkaliber- og skarpskytterrifler. Disse våpnene er lett tilgjengelige på markedet. Trusselen kan likevel innebære et bredt spekter av våpen med vesentlig forskjellig kapasitet, noe som må tas høyde for når sikringen skal designes.

Utforming av beskyttelseskonstruksjoner

Bygninger kan konstrueres for å motstå beskytning. Før beskyttelseskonstruksjonen designes, må det avgjøres mot hvilke trusler den skal dimensjoneres for. Utfordringen kan være at trusselbildet ofte er komplekst, samt at det finnes et utall ulike våpen og ammunisjonstyper.

Det finnes krav i henhold til norsk lov som brukes ved design av beskyttelseskonstruksjoner. Spesifikke beskytningskrav finnes for glass, vinduer og dører (NS-EN 1063 og NS-EN 1522), men kan også brukes for andre typer materialer og konstruksjoner. Kravene inneholder testprosedyrer som er delt inn i ulike klasser (såkalt BR- eller FB-klasse). Hver klasse inneholder ulike skyteoppsett med gitt ammunisjonstype, anslagshastighet, antall enkeltskudd og avstander testen skal utføres for. Når trusselbildet er definert, er neste steg å velge dimensjoner som tilfredsstiller designkravet. Mer om dette finnes under avsnitt for ***Beskyttelse ved bruk av glass***. Videre er det viktig å være klar over at penetrasjonsproblemet er et ikke-lineært og komplisert materialteknisk problem. Derfor er det påkrevd med enten fullskala forsøk eller avanserte numeriske beregninger for å dimensjonere beskyttelseskonstruksjoner utsatt for beskytning.

Skadene som oppstår i et bygningselement forårsaket av beskytning, vil i de fleste tilfeller være lokale, slik at resten av konstruksjonen forblir upåvirket. Ved anslag kan beskyttelseskonstruksjonen skades ved knusing av fronten eller ved avskalling på baksiden av materialet. Anslagsenergien brukes hovedsakelig til å deformere prosjektilet og forskyve materialet som penetreres. Dette skjer ved veldig høye temperaturer, og mye av energien går over til varme, og penetrasjonsprosessen



Bilde av krater i front på 200 mm tykk betong fra to skudd med 7.62 mm AP. Betydelig skade i platen, men betongen er i stand til å stoppe prosjektilene.

FOTO Forsvarsbygg

er over i løpet av mikrosekunder. Når prosjektilet deformeres, reduseres evnen til å trenge gjennom det resterende veggmaterialet. Formålet med beskyttelseskonstruksjonen er å absorbere energien fra anslaget og redusere hastigheten til prosjektilet. Dette oppnås ved riktig materialvalg, utforming og tykkelse på konstruksjonen. Hovedpoenget er å dimensjonere beskyttelseskonstruksjonen slik at den er tykkere enn den kritiske tykkelsen for valgt materiale og oppsett. Den kritiske tykkelsen er den tykkelsen som kreves for å stoppe for et gitt kaliber.

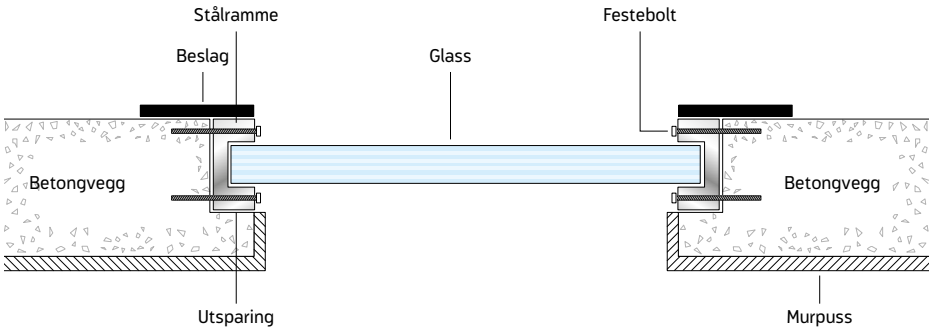
Selv om konstruksjonen ikke er fullstendig perforert, kan det oppstå avskalling på baksiden som følge av trykkbølgen som brer seg gjennom materialet. For slanke konstruksjoner kan det være behov for tilleggsbeskyttelse på baksiden, ettersom fragmenter fra konstruksjonen kan kastes i høy hastighet inn i rommet. Hvor mye konstruksjonen fragmenterer, og hvor stort krateret er på på fremsiden av konstruksjonen, vil være avhengig av tykkelsen og styrken på materialet.

Det kreves ulik beskyttelse mot ulike våpen. ***Panserbrytende prosjektiler*** kan perforere mange millimeter med stål og glass. En tommelfingerregel er at det kreves cirka 10 ganger tykkere betong enn stål, og cirka 10 ganger tykkere sand enn betong. Likeså kreves det omtrent dobbelt så mye stål for beskyttelse mot AP ift. Ball for 7.62 mm kaliber, tross lik anslagsenergi, men dog ulik kjerne. Konstruksjonen blir utsatt for et stort dynamisk støt i et lokalt område, og lasten er mange ganger større enn den statiske lasten konstruksjonen normalt sett er dimensjonert for.

Overganger mellom skuddsikre vegger og vinduer, og mellom skjøter i konstruksjonen ellers, må ha like høy beskyttelse som resten av konstruksjonen. Skuddsikre vinduer leveres ofte med innfestningsløsninger som har minst like høy beskyttelse som resten av vinduet. Når det gjelder skuddsikre glass, må det sørges for at selve skjøten mellom glasset og innfestningen tilfredsstiller samme krav som resten av konstruksjonen. Hull og utsparinger etter for eksempel forskalingsstag i betongvegger må tettes igjen. ***Figuren Enkel innfesting av glass i betong*** på neste side viser eksempel på hvordan skjøter og innfestinger til vinduer kan utføres.

Dersom det er relevant å dimensjonere for større trusler som hulladninger, bør det vurderes å flytte skjermingsverdige objekter eller verdier av stor viktighet til områder av bygget som er mer skjermet. Beskyttelse mot hullad-

Enkel innfesting av glass i betong



Se standarder og veiledninger for ytterligere detaljering. Merk at denne tegning ikke viser alle sjikt.

ninger krever større arealtverrsnitt og er derfor ikke hensiktsmessig i konvensjonelle bygninger. Viktige funksjoner og personell kan i stedet plasseres i de delene av lokalene hvor det ikke er mulig å bli beskutt, enten fordi det ikke er innsyn eller på grunn av store avstander.

Beskyttelse ved bruk av betong og tegl

Bygninger med ordinære dimensjoner på bærende betongvegger vil ofte ha tilstrekkelig penetrasjonsmotstand mot finkaliberprosjektiler. Det er flere egenskaper ved betong som har betydning for hvor motstandsdyktig den er, og tilslagsstørrelse, fasthet og alder på betongen er eksempler på variabler som avgjør penetrasjonsdybden. Armering har derimot liten betydning for penetrasjonsdybden, men kan redusere avskalling og kraterdannelse. Dersom prosjektilet treffer et armeringsjern, vil prosjektilet kunne skifte retning, noe som kan gi hastighetsreduksjon.

Beskyttelse ved bruk av stål

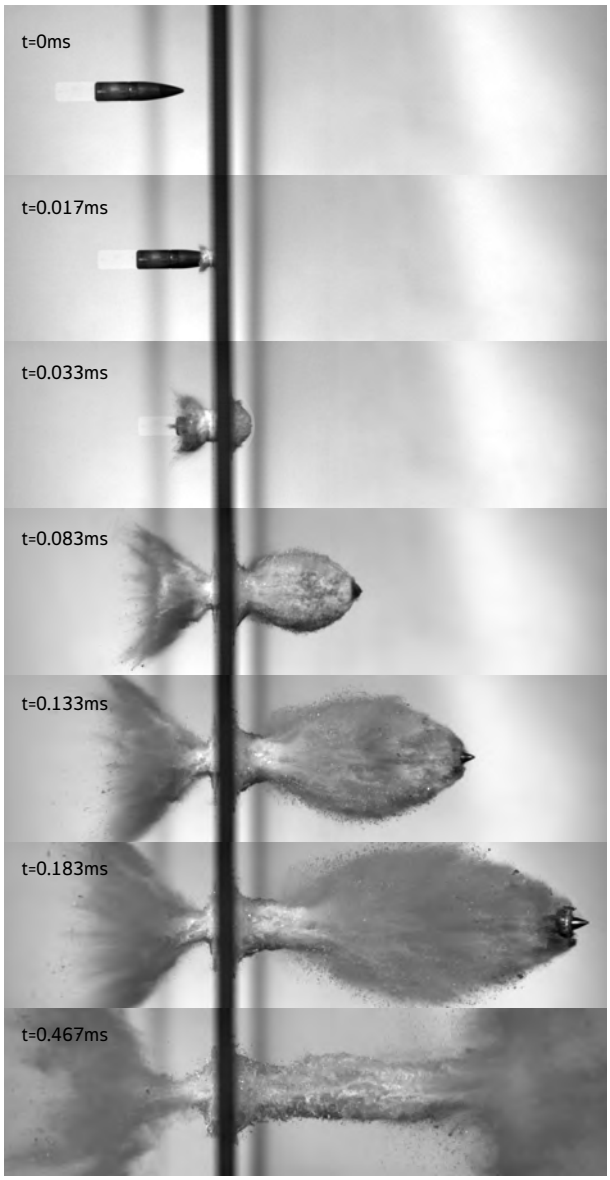
Stål er det materialet som i forhold til tverrsnittareal eller tykkelse gir høyest grad av beskyttelse. I permanente byggverk er det sjelden utfordringer knyttet til selve vekten av beskyttelsen. Stålplater med tilstrekkelig tykkelse er imidlertid tunge, dermed er det en del kostnader knyttet til produksjon og montering. Konstruksjonen stålplatene monteres til, må også kontrolleres for tilleggsvekten fra platene. Stålplater av ulik kvalitet kan benyttes som beskyttelse alene, eller i kombinasjon med for eksempel betong. Stålplater kan for eksempel brukes for å beskytte mot avskalling fra betongvegger. Enda høyere beskyttelsesgrad oppnås ved å benytte panserstål (høyfast stål). Det kreves ikke like tykke stålplater ved bruk av panserstål, men panserstål er mindre duktilt enn vanlig konstruksjonsstål og dyrere ved innkjøp. (Kilde: Modern protective structures Krauthammer)

Beskyttelse ved bruk av lettmetaller

Hvis lav vekt er påkrevd, kan et lettmetall benyttes som beskyttelsesmateriale.

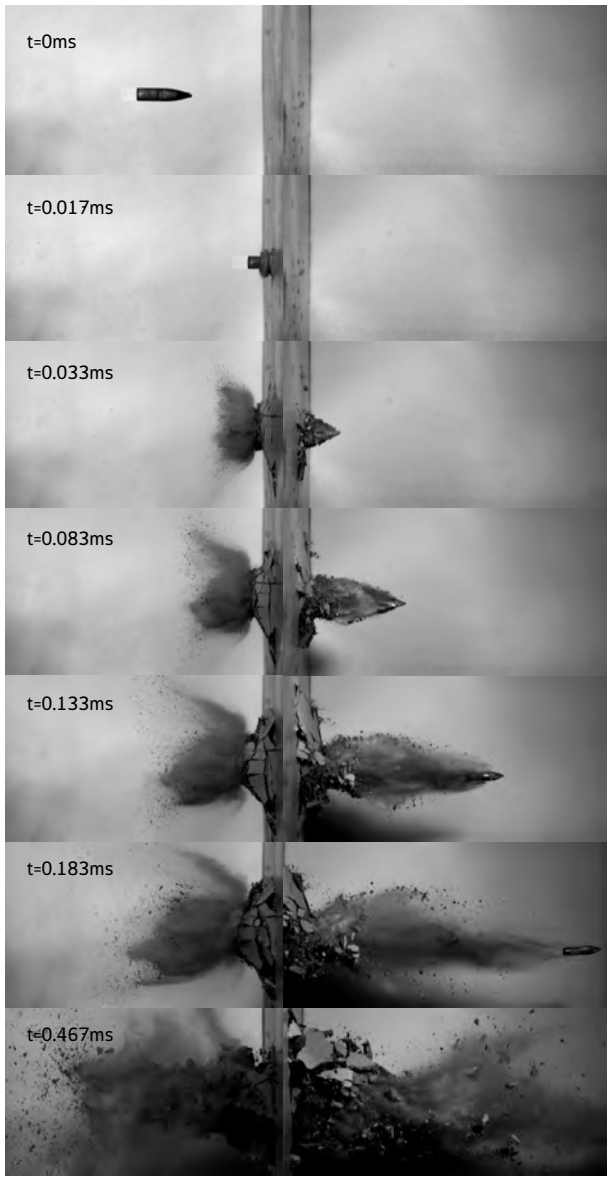
Typiske lettmetaller er aluminium, magnesium og titan. Slike materialer har som regel stor styrke i forhold til vekten, og brukes derfor

Skyteforsøk glass



7.62 mm AP-kule skutt på et laminert sikkerhetsglass bestående av 2x3 mm glass med 1.52 mm PVB imellom. Treffhastighet er ca. 900 m/s, mens uthastighet er ca. 870 m/s. Denne tykkelsen har med andre ord lite penetrasjonsmotstand for valgt ammunisjon.

Skyteforsøk betong



7.62 mm AP-kule skutt på en 50 mm tykk B45 betongplate. Treffhastighet er ca. 710 m/s. Kula går gjennom og får en resthastighet.

Kilde: S. Hallset, J. Haagerud, T. Auestad & T. Børvik; Skyteforsøk mot ulike stål- og betongmaterialer. SIMLab/Department of Structural Engineering, SIMLab/NTNU, 2010

Klassifisering av glass, vinduer, dører, sjalusier o.l.

Iht. NS-EN 1063 og NS-EN 1522

Våpentype	Kaliber	Glass	Vinduer, dører, sjalusier o.l.
Håndvåpen	9 mm	NS-EN 1063, BR 2 (SF)	NS-EN 1522, FB 2
Håndvåpen	.44 Magnum	NS-EN 1063, BR 4 (SF)	NS-EN 1522, FB 4
Rifle	7,62 mm	NS-EN 1063, BR 6 (SF)	NS-EN 1522, FB 6
Rifle	7,62 mm AP	NS-EN 1063, BR 7 (SF)	NS-EN 1522, FB 7

Tykkelse og vekt for et utvalg skuddsikre glass

SF-(splint free)-godkjenning

Klasse	Tykkelse [mm]	Vekt [kg/m2]
BR4	22	ca. 45
BR6	38	ca. 80
BR7	73	ca. 150

ofte som energiabsorbenter i forbindelse med ekstremlaster som støt, eksplosjon og kollisjon. Spesielt aluminium i ulike legeringer er mye brukt i beskyttelseskomponenter innenfor transportsektoren. Sammenlignet med høyfast stål har aluminium lavere styrke og duktilitet, men egenvekten er kun 1/3 av stål. Dermed kan man bruke tykkere plater og samtidig oppnå lavere vekt. Forsøk har vist at kapasiteten til stålplater mot beskytning øker tilnærmet lineært med fastheten. Med andre ord, jo sterkere stål jo bedre beskyttelse. Dette gjelder ikke på samme måte for aluminium, siden høyfast aluminium blir sprø og kan fragmentere ved støtlast. Dette vil kunne redusere kapasiteten til beskyttelsen. Det er derfor viktig å vurdere dette fenomenet hvis høyfaste aluminiumsplater eller tilsvarende lettmetaller brukes som ballistisk beskyttelse.

Alternative lette materialer vil være kompositt-løsninger av ulike typer, men slike materialer benyttes som regel i kombinasjon med andre metaller og/eller keramer. Det er derfor påkrevd å dokumentere kapasiteten hvis denne typen løsninger velges som beskyttelseskomponent.

Beskyttelse ved bruk av granulære masser

Et granulært materiale er en samling av atskilte partikler som mister energi når de kolliderer. Sand, grus og pukk er eksempler på granulære materialer som kan brukes i beskyttelseskonstruksjoner. I granulære materialer bidrar friksjonen mellom partiklene til å redusere energien eller hastigheten til prosjektilet. I mange tilfeller er granulære masser et godt alternativ for å oppnå tilstrekkelig beskyt-

telse, sammenlignet med dyrere materialer. Slike løsninger krever imidlertid mer volum og dermed plass enn for eksempel høyfaste stålplater. Retningsendring av prosjektilet er også en viktig mekanisme til å redusere prosjektilets penetrasjonsevne på. Ved lagvis inndeling av konstruksjonen er det viktig å designe slik at prosjektilet blir ført inn gjennom det første materialet, og gjerne blir knust og deformert på vei inn slik at hastigheten reduseres. Neste lag bør være et materiale som absorberer den resterende energi ved å pakke seg rundt prosjektilet, f.eks. sand, slik at prosjektilet blir fanget inne i konstruksjonen. Eventuelt kan det være et tredje materiale som er sterkt nok til å stoppe prosjektilet for godt. Beskyttelsesløsninger med lagdelte sjikt og granulære masser er plasskrevende og dermed ikke like praktisk i konvensjonelle bygg. (Kilde: Modern protective structures Krauthammer).

Beskyttelse ved bruk av glass

I dag finnes det sikkerhetsglass som er klassifisert mot våpenskudd iht. NS-EN 1063. Det finnes både herdede og laminerte sikkerhetsglass. Laminerte sikkerhetsglass er komponert gjennom en lamineringsprosess der to eller flere glassplater legges lagvis med elastisk plastfolie imellom. Deretter varmes komponenten opp, slik at folien fester seg til glasset. Det er en folie av polyvinyl butyral eller harpiks som gjør det laminerte glasset seigt og vanskelig å trenge gjennom. Glasset sprekker når det overbelastes, men glassplintene henger fast i folien. Laminerte sikkerhetsglass betegnes som SF (splintfri) eller NS (no splint). For herdede sikkerhetsglass fragmenterer glasset i tusenvis av små biter, og fragmenter vil dermed forekomme på innsiden av glasset. Disse betegnes også som splintavgivende glass. Sikkerhetsglass som er klassifisert iht. NS-EN 1063, har mange glassjikt. Når et prosjektil treffer glasset, vil energien fordeles på et gradvis større areal etter hvert som det trenger inn i et nytt glassjikt. Sikkerhetsglass gir også beskyttelse mot fysiske angrep med stumpe eller skarpe gjenstander.

Standard NS-EN 1522 fastsetter kravene og klassifisering for vinduer, dører, skodder og persienner. Disse skal oppfylles ved testing iht. prosedyrene gitt i standarden for testing NS-EN 1523. NS-EN 1063 angir som nevnt krav til beskyttelse og testprosedyre mot beskytning for sikkerhetsglass og laminert glass. Ifølge testprosedyren skal det avfyres en serie innenfor hver klasse, med 3 skudd for en gitt ammunisjon, en gitt anslagshastighet og med en gitt avstand mellom hvert skudd. Avstanden mellom skuddene skal ikke være mer enn 120 mm for våpnene i denne klassen. Utdrag fra klassifisering av glass i NS-EN 1063 og tilsvarende klasser for vinduer og dører i NS-EN 1522 er gitt i ***tabellen Klassifisering av glass, vinduer, dører, sjalusier o.l.*** Eksempler på tykkelse og vekt på skuddsikre glass med SF godkjenning er gitt i ***figuren Tykkelse og vekt for et utvalg skuddsikre glass***.

Sikkerhetsglass er mye tyngre enn vanlig glass. Vekten kan være opp mot 500 kg per vindu, og de må monteres i spesielt designede karmer. Splintavgivende glass har en lettere vekt, og kan derfor være å foretrekke fremfor splintfrie glass. Dersom det skal benyttes sikkerhetsglass eller andre tunge materialer, må konstruksjonens bæreevne kontrolleres. Ved ettermontering av skuddsikre vinduer eller andre tunge materialer må fasader og bæresystemer kontrolleres for de nye lastene. Det er også viktig å sørge for at innfestningene i veggen er kraftige nok til at den ytre belastningen kan fordeles via vinduskarmen og inn i byggets bæresystem. Ved bruk av skuddsikre glass i en yttervegg bør det installeres isolerglass i tillegg, som skal ligge ytterst.

I resepsjoner eller ved vaktposter hvor det foregår ID-kontroll inn til et beskyttet område, bør det monteres vinduer med sikkerhetsglass.

Kapittel 18

Trusselstoffer

I dette kapitlet beskrives de viktigste kjemiske, biologiske og radiologiske trusselstoffene (CBR) og noen av deres egenskaper, samt viktige forhold som deteksjon, filtrering og rens av de ulike trusselstoffene. Noen av de mest sannsynlige angrepsformene beskrives, med hovedfokus på byggets ventilasjonsanlegg.

FOR-KORTELSER

CBRN
Chemical, Biological, Radiological, Nuclear

CCA
Contamination Control Area, område for inn- og utpassering mellom rent og forurenset område

Det meste av vår kunnskap og dokumentasjon om CBR-trusselstoffer er relatert til virkning, beskyttelse og rens av personell og utstyr som er eksponert for stoffene. Det foreligger mindre dokumentasjon og kunnskap om beskyttelse av bygg og anlegg. Den dokumentasjon som finnes, er i hovedsak knyttet til fjellanlegg, flystasjoner og tilfluktsrom med fasiliteter for inn- og utpassering, filtrering av luft, påvisning av kjemiske stridsmidler og radioaktivitet.

Kjemiske trusselstoffer

De kjemiske trusselstoffene omfatter kjemiske stridsmidler, bioregulatorer og toksiner. I tillegg kommer trusselen fra giftige industrikjemikalier som dekker alt fra industrigasser til insekts- og plantevernmidler. Det er vanskelig å si hva som kan være en sannsynlig trussel mot bygg og anlegg. De rene stridsmidlene er meget effektive mot mennesker, men er vanskelige tilgjengelige og ikke lette å produsere. Industrikjemikalier er på den annen side mindre giftige, men lettere tilgjengelige fordi de til daglig anvendes i industri og næringsliv. På neste side gis en oversikt over de viktigste trusselstoffene og noen av deres virkninger på mennesker.

Bioregulatorer

Bioregulatorer er naturlig forekommende forbindelser i levende organismer og regulerer celleprosesser. Bioregulatorer er hurtigvirkende i små konsentrasjoner. Eksempler på slike stoffer er nevrotransmittere og hormoner. Effekten av disse stoffene på mennesker kan spenne over et bredt spektrum avhengig av typen bioregulator. Det skjer en kontinuerlig utvikling av bioregulatorer innenfor medisin. Av den grunn bør disses stoffene i økende grad ses på som mulige trusselstoffer i terrorsammenheng.

Kjemiske stridsmidler

De kjemiske stridsmidlene er delt opp i ulike grupper utfra deres virkning på mennesker. Typisk for de fleste kjemiske trusselstoffene er at de gir umiddelbar effekt. Virkningen varierer også fra hemmende til dødelig. Noen av stoffene kan gi virkning etter noen timer. Dette gjelder for eksempel stoffer som virker på lungene og hudstridsmiddelet sennepsgass.

Toksiner

Toksiner er naturlig forkommende giftstoffer. Eksempler på toksiner er ricin som er et plantetoksin, og botulinum toksin, som produseres av bakterien Clostridium botulinum. De kan

Kjemiske stridsmidler og deres virkning på mennesker

Stridsmiddel	Typisk tilstand/ leveringsform	Virkning på mennesker	Dødelighet
Nerve	→ Væske/aerosol	→ Ødelegger signal-overføringen i nervene. Kramper og pustestans	→ Høy
Hud	→ Væske/aerosol	→ Brannsår, lungeskader	→ Lav
Kvele	→ Gass	→ Lungeødem	→ Middels til høy
Blod	→ Gass	→ Slår ut sentral-nervesystemet	→ Høy
Irriterende	→ Fast fase/aerosol	→ Irriterer slimhinner/øyne	→ Ikke dødelig
Psykokjemiske	→ Fast fase/aerosol og mat/drikke	→ Nedsatt fysisk og psykisk aktivitet	→ Ikke dødelig

ha ulike effekter på mennesker, men felles for disse stoffene er at de er svært giftige og dødelige i små konsentrasjoner.

Industrikjemikalier

Industrikjemikalier finnes i alle varianter og med ulik grad av hvor giftige de er. De anvendes i til dels stor skala som del av industriproduksjon eller i landbruk. Utbredt anvendelse kombinert med lettere tilgjengelighet gjør at vi må være forberedt på at stoffene kan anvendes for eksempel i terrorsammenheng. Noen av industrikjemikaliene har også vært brukt som kjemiske stridsmidler både under første verdenskrig og i Midtøsten. I ***tabellen Industrikjemikalier*** på neste side gis eksempler på noen viktige industrikjemikalier og deres virkning.

Biologiske trusselstoffer

Biologiske trusselstoffer kan være bakterier, virus, sopp og parasitter. Forskjellen på kjemiske og biologiske trusselstoffer er at noen av de biologiske trusselstoffene kan overføres eller smitte mellom mennesker. I motsetning til kjemiske trusselstoffer ses virkningen av biologiske trusselstoffer etter en tid (inkubasjonstid). Hvis man vet at personer er eksponert for et biologisk trusselstoff, er det derfor mulig å gi behandling hvis dette finnes.

Eksempler på noen typiske biologiske trusselstoffer og virkning på mennesker er vist i ***tabellen Bakterier og virus med deres virkning på mennesker***.

Industrikjemikalier

Vanlig tilstand ved lagring og transport og deres virkning på mennesker

Kjemisk forbindelse	Form	Virkning
Ammoniakk	→ Gass. Transporteres og lagres som væske nedkjølt under trykk	→ Irriterende på øyne og åndedrett. Gir lungeødem
Klor	→ Gass. Transporteres og lagres som væske nedkjølt under trykk	→ Sterkt irriterende på øyne og åndedrett. Gir lungeødem
Svoveldioksid	→ Gass. Transporteres og lagres som væske nedkjølt under trykk	→ Skader øyne, hud og åndedrett. Gir lungeødem

Radiologiske trusselstoffer

Radioaktiv stråling er såkalt ioniserende stråling som kommer fra nedbrytning av radioaktivt materiale, radiologiske trusselstoffer. Denne type stråling inneholder så mye energi at materialer og organisk vev som blir truffet av strålingen, kan bli ødelagt. Eksempelvis kan radioaktiv stråling forårsake endringer eller ødeleggelse av arvestoffet i våre celler og dermed reproduksjon av cellene.

Det finnes fire former for radioaktiv stråling. Disse er gamma-, nøytron-, beta- og alfastråling. Gammastråling er elektromagnetisk stråling på samme måte som lys og inneholder svært stor energi. Den kan enkelt måles med for eksempel geigerteller. Alfa-, beta- og nøytronstråling er partikler med masse. Alfastråling består av heliumkjerner, betastråling er elektroner med høy hastighet, og nøytronstråling er nøytroner med forskjellige hastigheter. Gammastråling trenger gjennom de fleste materialer. Nøytronstråling vekselvirker meget lite med andre materialer og har derfor høy gjennomtrengningsevne. Alfa- og betastråling har mye dårligere gjennomtrengningsevne, men forårsaker stor skade hvis radioaktivt materiale som sender ut disse typene stråling, kommer inn i kroppen.

Man kan dele virkningen av radioaktiv stråling på mennesker i akutte effekter og langtidseffekter. De akutte virkningene er avhengig av dose/mengde radioaktiv stråling et individ har vært utsatt for, og kan være generell sykdomsfølelse, oppkast, rød hud, øyeskader og ødeleggelse av indre organer og eventuelt død. Langtidseffektene kan være økt sannsynlighet for kreft – spesielt i organer med stor celleutskiftning – og feil i arvestoffet som overføres til avkommet.

Sikring av bygg mot CBR-trusselstoffer

Angrepsform

CBR-trusselstoffer kan anvendes på flere ulike måter for å ramme viktige virksomheter og funksjoner. Et CBR-angrep vil være rettet mot de mest sårbare delene av et bygg som ventilasjonsanlegg, dører, vinduer, åpninger, inn- og

Bakterier og virus med deres virkning på mennesker

Bakterier	Virkning på mennesker
Yersinia pestis	→ Byllepest → Hovne lymfeknuter, byller, blodforgiftning → Lungepest → Lungebetennelse med 100 % dødelighet dersom ubehandlet
Francisella tularensis (tularemi eller harpest)	→ Halsbetennelse, sår, lungebetennelse, mageinfeksjon
Salmonella	→ Mage, tarm (diaré og uttørring)
Antrax (miltbrann)	→ Eksponering på hud kan gi sår som ikke gror → Eksponering lunge – skader i lunge med ødem, skader på hjerne og ryggmarg → Høy dødelighet
E.coli	→ Mage, tarm, mulig nyresykdom
Virus	**Virkning på mennesker**
Variola major (kopper)	→ Utslett, blødninger, mulig multiorgansvikt. Høy dødelighet
Ebola (hemoragisk feber)	→ Indre blødninger. Høy dødelighet
Marburg (hemoragisk feber)	→ Indre blødninger. Høy dødelighet

utpasseringsområder og post- og varemottak. I tillegg kommer eventuelt angrep gjennom vannforsyningen (vannledningsnettet eller i dispenservann).

Eksempel på en sannsynlig angrepsmetode er utslipp av trusselstoff i form av gass eller aerosol i avstand fra bygget/anlegget. Trusselstoffet vil da drive med vinden mot bygget, og uten beskyttelsestiltak vil trusselstoffet raskt transporteres inn gjennom ventilasjonsanlegg eller åpne vinduer og dører og fordeles i bygget. Et annet scenario kan være at en glassflaske eller knuselig konteiner med trusselstoff kastes mot et av luftinntakene. En tredje angrepsform kan være leveranse av trusselstoff i væskeform eller fast form (pulver) i beholdere eller pakker inn i bygget/anlegget gjennom post- og varemottak, eller at noen prøver å ta det med inn via vanlig inn- og utpasseringsområde.

Ventilasjonsanlegg

Ventilasjonsanlegget i et bygg må regnes som spesielt sårbart og kan være et aktuelt angrepspunkt for terror eller fiendtlig handling. Hensikten med å sikre ventilasjonsanlegg er å hindre at CBR-trusselstoffer kan spres til det indre av bygget gjennom dette. Avhengig av hvor kritisk virksomheten inne i bygget er, kan man velge ulike nivåer på CBR-sikring. Dette kan være alt fra enkle løsninger som tetting av vinduer, lokalisere luftinntak over tak og

lett overtrykk i bygget til mer omfattende tiltak med filtrering av innluft, trykktestede ventilasjonskanaler, kameraovervåkning og deteksjon/påvisning ved hjelp av sensorer.

Ved et eventuelt angrep med CBR er det uavhengig av sikringsnivå viktig at ventilasjonsanlegget slås av så fort som mulig, for eksempel ved bruk av hurtiglukkende spjeld. Det vil forsinke inntrengning av trusselstoffer til bygget og gi virksomheten tilstrekkelig beskyttelse til en evakuering kan iverksettes, eller CBR-trusselstoffene er borte.

For høyere nivåer av sikring vil deteksjon/påvisning ved hjelp av sensorer og eventuell filtrering av innluften til bygget være aktuelt. Det er viktig å være klar over at både deteksjonsutstyr og filtre kan kreve betydelig innsats når det gjelder drift av disse.

I det følgende gis en beskrivelse av deteksjon og filtrering av ulike trusselstoffer.

Det bør vurderes egne eller adskilte ventilasjonsanlegg for kritiske funksjoner som både kan være spesielt viktige eller spesielt utsatte.

Deteksjon

Angrep med CBR-trusselstoffer kan skje overraskende og uten forvarsel. Mange av trusselstoffene kan ikke luktes eller ses. For å kunne iverksette tiltak må man derfor vite om trusselstoffet enten gjennom etterretning eller ved påvisning/deteksjon. Tidlig deteksjon/påvisning gir mulighet for varsling av utsatt personell og andre tiltak som for eksempel automatisk stenging av ventilasjonsanlegg. Påvisning vil også gi nødetater kunnskap om hvilke tiltak som må iverksettes ved redning, og eventuell behandling av pasienter. Et deteksjonssystem kan enten settes i drift ved forhøyet beredskap eller være kontinuerlig operativt.

På grunn av de alvorlige konsekvensene av et angrep stilles det store krav til pålitelighet i deteksjon/påvisning. Systemet skal reagere umiddelbart ved eksponering for trusselstoff. I tillegg bør systemet være enkelt å operere og ha lave driftskostnader og driftsressurser.

Deteksjon og påvisning av kjemiske, biologiske og radiologiske trusselstoffer bygger i hovedsak på grunnleggende forskjellige prinsipper. I det følgende gis en kort beskrivelse av hovedprinsippene for de ulike formene for påvisning og deteksjon og muligheter for anvendelse av disse i beskyttelse av bygg og anlegg.

Kjemisk deteksjon

Deteksjon/påvisning av kjemiske trusselstoffer ble før i tiden gjort med rene våtkjemiske metoder, for eksempel ved bruk av påvisningspapir og påvisningspulver som skifter farge i kontakt med kjemisk trusselstoff. I de senere årene er disse metodene i stor utstrekning erstattet med moderne teknologiske instrumenter basert på fotometriske og spektrometriske metoder. Felles for instrumentelle deteksjonsmetoder er de er avanserte og potensielt krever høy kompetanse for å kunne kjøres tilfredsstillende. Imidlertid har produsentene lagt ned store ressurser på å forenkle driftsrutinene og grensesnittet mot operatør.

Fordeler med dagens kjemiske deteksjonssystemer er at de stort sett har kort responstid (typisk inntil 30 sekunder). Det er imidlertid viktig å være klar over at dagens deteksjonsutstyr har begrensninger. Systemene kan fortsatt gi en del falske alarmer samt at de ikke uten videre dekker alle typer kjemikalier. Et system som eksempelvis kan detektere alle kjente kjemiske stridsmidler, gir ikke nødvendigvis alarm når det blir utsatt for giftige industrikjemikalier. Det er likevel vanlig at instrumentene kan programmeres til å dekke noen av industrikjemikaliene. Deteksjonsutstyret trenger også tid på å reagere og vil derfor kreve at det er en viss distanse mellom luftinntaket og forgreningen

fra aggregatet og inn i bygget. Dette sikrer at man får tid til å gjennomføre tiltak, og at man reduserer behov for rens i etterkant.

Biologisk deteksjon

Det finnes to hovedveier å gå for biologisk deteksjon og identifikasjon av biologiske trusselstoffer. Den «tradisjonelle» veien er mikrobiologiske metoder som består i å dyrke frem mikroorganismene og/eller benytte mikroskopiske metoder. Fra slutten av 1950-tallet har biologene benyttet molekylærbiologiske metoder til å karakterisere, isolere og manipulere de molekylære komponentene av celler og organismer. Av disse metodene er for eksempel PCR (Polymerase Chain Reaction) en mye anvendt metode for identifikasjon av biologiske trusselstoffer.

I tillegg benyttes i dag lasermetoder for å påvise biologiske organismer i væske og i luft. Disse metodene gir et varsel om antall partikler i luften plutselig stiger. Det finnes likevel i dag ikke metoder som raskt kan både detektere og identifisere B-trusselstoffer.

De metodene vi har i dag, er mer for prøvetaking og analyse for å identifisere trusselstoffet etter et eventuelt angrep som man for eksempel har oppdaget ved et unormalt antall like sykdomstilfeller. Dermed gir deteksjon mulighet for å sette inn behandling for de typer trusselstoffer som er mulige å behandle.

Deteksjon av radioaktivitet

Gammastråling er relativt enkelt å måle for eksempel med geigerteller. Denne benytter de ioniserende egenskapene til gammastrålingen. Partikkelstråling er derimot vanskeligere å måle på grunn av at denne strålingen avtar kraftig når den går gjennom luft. For rutinemessig bruk ved påvisning av et terrorangrep mot et bygg eller anlegg er det derfor gammastråling man enkelt kan påvise.

Filtrering

Når ventilasjonsanlegget stanses som følge av et angrep med CBR, vil luftkvaliteten gradvis bli dårligere. For å sikre at kritisk virksomhet i bygget kan opprettholdes, vil det være nødvendig med filtrering av innluften. Dette gjøres vanligvis ved at et eget inntakssystem med filter sjaltes inn.

CBR-filtrering skjer i to stadier: Radioaktivt støv og biologiske partikler filtreres bort i et HEPA-filter, mens damp, gass eller væskeformig aerosol absorberes i et kullfilter.

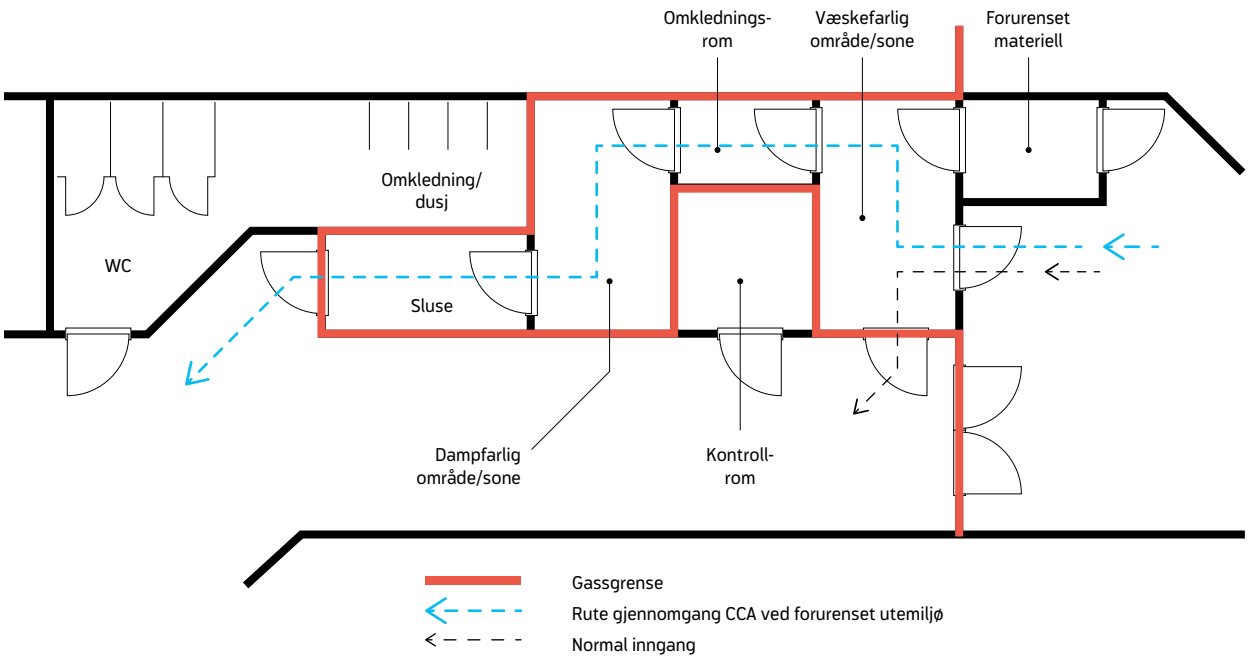
HEPA-filter

HEPA-filter er et absoluttfilter som filtrerer ut partikler ned til 0,3um med 99,995 prosent virkningsgrad. Filteret fjerner derfor en del bakterier og virus samt noen radioaktive partikler. HEPA-filtrene har stor luftmotstand og kort driftstid før de må skiftes. Montering av HEPA-filtre er plasskrevende og kostbart. Ved omkobling til HEPA-filter bør luftmengden reduseres for eksempel til det halve.

CBR-filtrering

CBR-filteret er en kompakt enhet som gir god beskyttelse mot kjemiske trusselstoffer i gass- , damp- eller som væske- eller fastfase aerosol. CBR-filtrene skal normalt stå plombert og tilkobles ventilasjonsanlegget ved behov. Systemet skal kobles inn på byggets vanlige anlegg, men må ha egen vifte. Også her anbefales det å gå ned til halv luftmengde når filterdelen er i drift. All uteluft må tas inn gjennom gasstette inntakskanaler og passere CBR-filtrene før den går inn i det vanlige ventilasjonsanlegget. Ved bruk av CBR-filter må det alltid etableres et overtrykk i bygget. Alle avtrekksvifter må stanses, og tilluften går ut av bygget som kontrollert overtrykk.

Rensestasjon/ Contamination Control Area



Vannforsyning

Tiltak for sikring av vannforsyning kan bestå av fysisk og/eller elektronisk sikring av vannmagasin, vanntårn og andre sårbare punkter i vannettet. Videre kan flere og mer omfattende tester av vannkvalitet gjøres ved renseverkene. Rensing av vann kan omfatte filtrering, kjemisk rensing, UV-bestråling og ozonbehandling.

Mange trusselstoffer overlever ikke eller vil fortynnes betydelig hvis de tilføres tidlig i vannettet. Den største problemet er hvis et angrep settes inn nær et bygg. De viktigste sikringstiltakene vil derfor være å hindre tilgang til denne delen av vannettet, enten gjennom overvåkning eller fysisk sikring av kummer og rørnett.

Dører, vinduer og åpninger

For bygg der CBR-trusselen er reell må dører, vinduer og åpninger være utført på en slik måte at de tetter mot trusselstoffene. Lister rundt åpningene må være heldekkende og helst sjekket for tetthet. Vinduer bør helst ikke være slik at de kan åpnes. Det kan, hvis man har forhøyet beredskap, være aktuelt å øke sikkerheten ved å tape rundt vinduer og luker.

Rensestasjon

I anlegg der virksomheten er avhengig av å kunne være operativ selv under lengre eksponering for CBR-trusselstoffer, vil det være nødvendig å kunne sluse personell og forsyninger inn og ut av anlegget. I slike anlegg opprettes et spesialkonstruert inn- og utpasserings-

område, såkalt Contamination Control Area (CCA) med utstyr og prosedyrer blant annet for å håndtere forurenset personell som går fra forurenset område til rent område inne i bygget. Slike fasiliteter er basert på at luften gjennom anlegget passerer fra rent område til forurenset område. Forurenset personell som skal inn gjennom en CCA, kler av seg forurenset tøy og utstyr etter strenge rutiner. Personellet dekontamineres, dusjes og tar på rent tøy før de til slutt sluses inn i ren sone. Et eksempel på en CCA er vist i ***Rensestasjon/Contamination Control Area***.

Rens

Etter at et bygg eller anlegg har vært utsatt for CBR-angrep, kan rens være nødvendig. Rensemetoder som anvendes, varierer for de ulike trusselstoffene. Generelt for CBR-rens er at den hvis mulig må gjennomføres av kyndig personell.

Noen av de kjemiske trusselstoffene er så flyktige at de kan luftes ut over noen dager, mens andre er meget lite flyktige og må renses og destrueres med ulike kjemikalier. Til dette trenger man spesielt utstyr og personell med gode kunnskaper i håndtering av kjemiske stridsmidler. Stridsmidlene kan trenge inn i mer eller mindre porøse materialer slik at det beste er å fjerne materialene og destruere dem.

Biologiske trusselstoffer brytes normalt ned i løpet av relativt kort tid. Noen bakterier danner imidlertid såkalte sporer som kan være svært motstandsdyktige. Et eksempel på dette er sporer av Bacillus antracis (som forårsaker miltbrann). Disse sporene kan overleve i mange tiår, for så å «vekkes» opp igjen når de kommer inn i menneskekroppen. Sporer av Bacillus antracis representerer derfor et betydelig renseproblem hvis de har trengt inn i både ventilasjonsanlegg og rom i et bygg. Rensingen må gjøres mekanisk og eventuelt med sterke kjemikalier og kan bli svært kostbar. Også når det gjelder rens av biologiske trusselstoffer er det nødvendig med kyndig personell.

Rens etter et radiologisk angrep vil på mange måter være som for tilfeller med Bacillus antracis. Vi snakker her om fast materiale som kan sende ut stråling i alt fra noen dager til mange tusen år. Rensingen består i mekanisk fjerning og transport til deponi for radioaktivt materiale.


VBW 1 MHz

Kapittel 19

Elektromagnetiske trusler

I dette kapitlet vil vi først gå gjennom prinsippene for hvordan radiobølger brukt som våpen kan genereres, og hvordan forskjellige trusler kan fremstå. Deretter blir det beskrevet hovedtrekk i hvordan skjerming kan utføres for å beskytte elektroniske installasjoner.

Tiltak for å beskytte mot elektromagnetisk puls (EMP) og high power microwaves (HPM) kan også fungere som Tempest-beskyttelse. Noen forskjeller finnes, og det kan være behov for spesielle tiltak. EMP/HPM er mer grundig forklart i mer spesialiserte håndbøker. I litteratur om elektromagnetiske våpen finnes det mange forkortelser, noen med delvis overlappende betydninger. Noen av disse finnes i listen til høyre.

Effekter

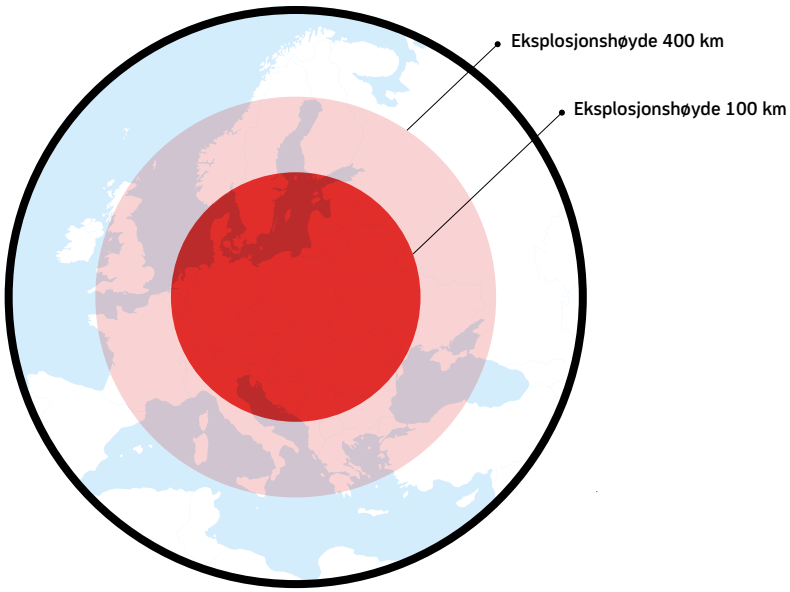
EMP/HPM er våpen som kan ødelegge elektronikk. Det trengs vesentlig høyere strålingsstyrke for å skade personell enn for å skade elektronikk. Imidlertid finnes det et system basert på elektromagnetisk stråling (Active denial) som kan brukes mot mennesker og som genererer smerte, men som ifølge produsenten ikke er skadelig. Dette systemet kan f.eks. brukes til å løse opp store folkemengder slik at de ikke kommer ut av kontroll. Disse våpnene stråler på høyere frekvens (94 GHz) enn de som er laget for å ødelegge elektronikk. Dette vil ikke bli videre utdypet her.

Bortsett fra elektriske installasjoner vil bygninger ikke kunne ta skade av EMP eller mikro-

FORKORTELSER

EMP Elektromagnetisk puls: radiobølgepuls fra kjernefysiske våpen, spesialvåpen, lyn eller andre elektriske utladninger. Flere bokstaver kan angi kilde til strålingen eller andre egenskaper (lyn – LEMP, non-nuclear – NNEMP, high altitude – HEMP etc.).
HPM High power microwave: Ofte brukt generelt om radiofrekvente våpen. I litteraturen beskrives det som «smalbandet stråling».
HPEM High power electromagnetics.
EMI Elektromagnetisk interferens: forstyrrelser fra brytere og annet elektrisk utstyr.
IEMI Intentional EMI: stråling som har til hensikt å forstyrre/ødelegge.
EMC Electromagnetisk kompatibilitet (elektronisk utstyr ved siden av hverandre skal ikke forstyrre hverandre).
UWB Ultra wide band, korte pulser med bredt frekvensinnhold.
RFV Radiofrekvente våpen, våpen basert på radiostråler.
Tempest Elektromagnetisk stråling som kan gjøre gradert informasjon tilgjengelig, se *kapittel 17 om sikring mot avlytting.*

Rekkevidde for NEMP med eksplosjonshøyder



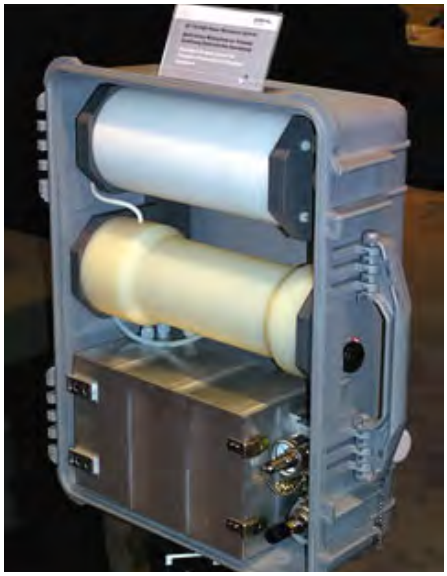
bølgevåpen. Virkninger fra slike våpen kan for mange synes eksotiske, og utviklingen av slike våpensystemer har i stor grad vært holdt hemmelig, og ytelsen til slike våpen er lite kjent. Skaden som oppstår, er som følge av overspenninger som kan forstyrre funksjoner i elektronikk, eller kortslutte isolasjonslag i utstyr. Avhengig av hvor sterk radiostrålingen er, kan virkningen være forstyrrelser, degradering eller ødeleggelse av utstyr. Forstyrrelsen kan bety at utstyr fortsetter å fungere umiddelbart eller etter noe tid, eller at inngrep fra operatør er nødvendig.

I objektsikkerhetsforskriften er det satt krav om at beskyttelse mot denne type våpen skal vurderes. For tele- og kraftinstallasjoner er det stilt krav i klassifiseringsforskriften og beredskapsforskriften om at anlegg av en viss viktighet skal beskyttes.

EMP/RFV

Det har lenge vært kjent at kjernefysiske eksplosjoner kan generere kraftige radiopulser som kan ødelegge elektriske/elektroniske installasjoner over store områder. En sprengning i stor høyde (40–400 km) vil ikke gjennom trykk og varmevirkning ødelegge noe på bakken, men på grunn av stråling i luften og ionisering vil det oppstå en sekundærvirkning med kraftig elektromagnetisk puls (EMP) som vil kunne ødelegge elektriske installasjoner over hele kontinent.

Det er også blitt utviklet strålingskilder som kan brukes lokalt med forskjellige størrelser og rekkevidder. Forskjellige teknologier finnes, alt fra små kilder i koffertstørrelse drevet på batteri med liten rekkevidde, til de som er basert på eksplosjonsdrevne dynamoer (Compression flux generators). Strålingen kan være svingninger på en bestemt frekvens (HPM, high power microwaves), korte pulser (UWB, ultra wide



Koffertstørrelse DS-kilde, rundstrålende, Diehl

FOTO Diehl Gmbh

band) eller svingekretser som har blitt eksitert (DS, damped sinus). Rekkevidden vil være avhengig av mange parametere som amplitude, pulslengde, frekvens, antennestørrelse og repetisjonsfrekvens.

Noen idealiserte pulsformer er presentert i ***figuren Felt-tidsforløp for noen typer pulser***.

Våpen kan til en viss grad tilpasses målet siden energioverføring inn i målet vil være svært avhengig av frekvens. Høye frekvenser kan kobles inn på små gjenstander, mens lave frekvenser blir fanget opp av lange kabler som kan ledes til apparater som kan bli påvirket.

Det er ofte hensiktsmessig å presentere strålingen i frekvensdomene, se ***figur Elektromagnetisk stråling presentert i frekvensspekteret.***

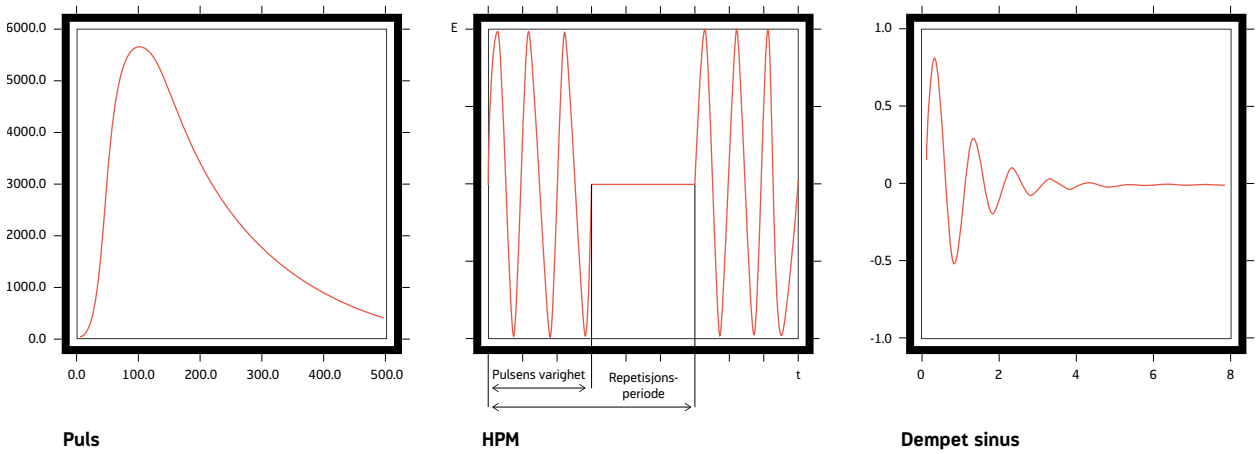
Enkelte ganger kan utstyr bli satt ut indirekte fordi støttefunksjoner svikter, som f.eks. strømforsyning, kjøling eller ventilasjon. Under stormen «Dagmar» julen 2011 sviktet telekom-

JOLT. Langtrekkende strålingskilde utviklet ved Air Force Research Laboratory

FOTO Air Force Research Laboratory

Felt-tidsforløp for noen typer pulser

Idealiserte pulsformer



Puls **HPM** **Dempet sinus**

munikasjon og kringkasting få timer etter at strømmen forsvant, da batteriene var tømt.

En motivasjon for å benytte et slikt våpen kan være at man ikke vil tiltrekke seg oppmerksomhet. Det kan være vanskelig å oppfatte hva som skjedde når slike våpen blir brukt fordi det ikke er noen store smell, og bygninger blir ikke skadet. Hvis offeret ikke har skjønt hva som skjedde, kan man gjøre et nytt forsøk etterpå. For angriper kan det være problematisk å se om angrepet har hatt effekt. Har man lyktes med å skape kaos med et HPM-angrep, vil et angrep etterpå med andre midler kunne ha større effekt enn det ellers ville hatt. En annen motivasjon kan være å forstyrre alarm- og kommunikasjonssystemer med andre midler rett før anslag.

HPM-våpen i droner eller fly brukt mot militære mål kan være en «myk» måte å uskadeliggjøre motstanderen på. Flere firmaer jobber med bilstoppere basert på HPM.

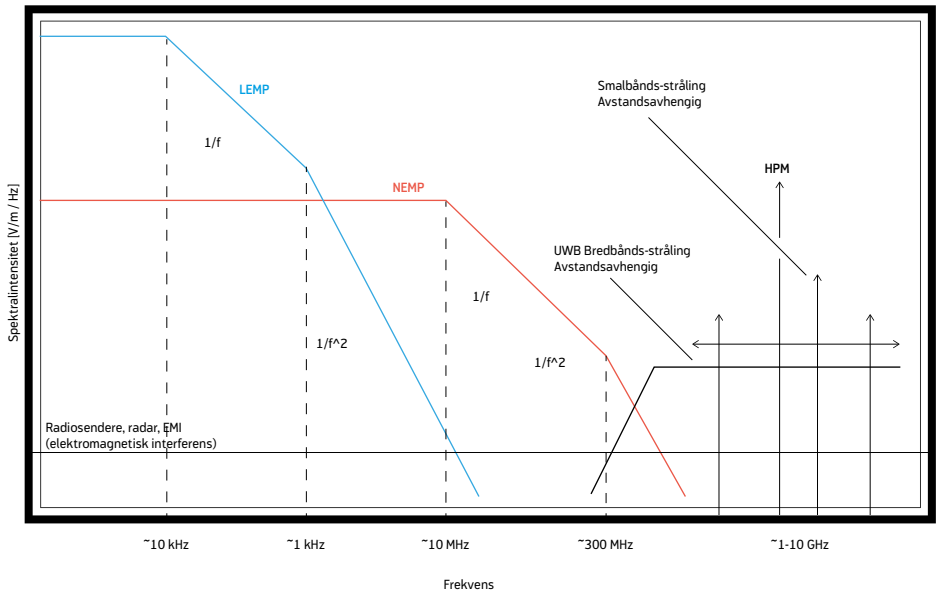
RFV vil være et middel for en ganske avansert trusselaktør.

Planlegging

De fleste vanlige bygningsmaterialer beskytter lite mot EMP/HPM. Vanlig betong bidrar i liten grad med skjerming mot denne typen stråling. Armeringen kan utføres på en måte som vil skjerme mot noe av LEMP (lyn-EMP) og de lavfrekvente delene av NEMP (nuclear-EMP), og termovinduer kan skjerme mot andre typer stråling. Åpninger i skjerm, f.eks. overganger mellom to skjermmaterialer, kan slippe inn store energimengder. Flekkvis skjerming vil ha beskjeden nytte.

Rom som skal skjermes ordentlig mot EMP/HPM eller Tempest, trenger mange forskjellige spesialkomponenter. Vegger må kles med metall. Det kreves spesialdører, og metalliske kabler må ha spesielle avledere. Rørgjennomføringer og ventilasjonsåpninger krever også spesialtiltak. Den ødeleggende energien fra et RFV kan komme som stråling som treffer elektronisk utstyr, eller strålingen kan bli fanget opp av ledninger som leder overspenninger frem til det elektroniske utstyret.

Elektromagnetisk stråling presentert i frekvensspekteret



Den ideelle løsningen er en totalskjerming fra verden utenfor i et stålskall. Praktiske løsninger krever åpninger for adgang, krafttilførsel, vann og avløp, kommunikasjon, ventilasjon etc.

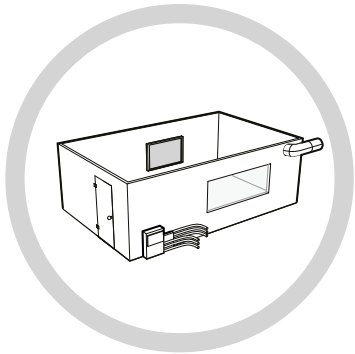
Det er viktig å planlegge skjermingstiltak tidlig i prosessen under utforming av nye bygg for å begrense skjermingskostnader. På den måten kan man unngå dyre og kompliserte installasjoner innen VVS, elektro og IKT samt kompliserte skjermløsninger. I mange tilfeller vil bare begrensede deler av en bygning ha behov for skjerming. Det gjelder gjerne funksjoner som må være operative til enhver tid, eller der tap av data over et kort tidsrom ikke er akseptabelt. Dersom skjermsonen består av mange små celler rundt omkring, vil det f.eks. være behov for mange dører.

De fleste skjermdørene på markedet er dyre, men har ingen klassifisering mot innbrudd eller brann. I en skjermsone skal alle kabler, som skal inn og ut av området, føres gjennom skjerm på en enkel plass, et såkalt «single entry». Kabelføringer kan bli lange når de må via et «single entry». Det kan bli behov for ekstra mange gjennomføringer for luft eller vann.

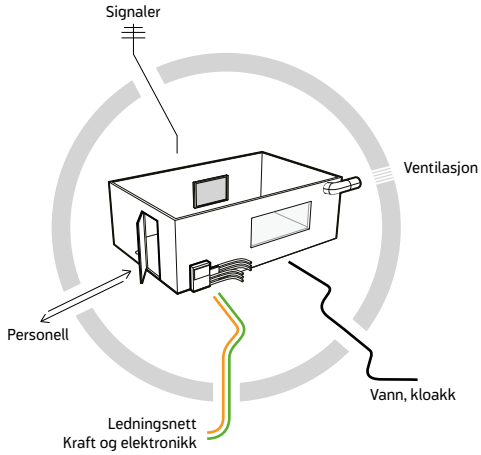
I mange tilfeller kan det også være fordelaktig å dele skjermingstiltak inn i flere soner. Noen deler av anlegget er viktigere enn andre, og det er også forskjell på hvor robust installasjoner er. Den ytterste beskyttelsen kan være bare beskyttelse mot lyn. Flere skall kan redusere strålingen innover i bygget. Man plasserer da det mest viktige eller det mest sårbare utstyret innerst i den mest beskyttede sonen. Ved en slik tilnærming kan man summere skjermingseffekten for hvert lag gitt i desibel for å finne total beskyttelse i innerste sone. En god EMC-jording vil også bidra med en del beskyttelse.

Utstyr i de ytre sonene kan være utstyr som anses å være robust med hensyn til elektro-

Skjerming

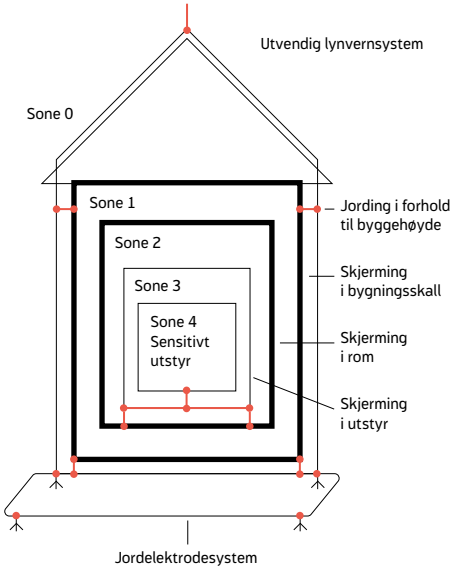


Ideell skjerming
Den ideelle løsningen er en totalskjerming fra verden utenfor i et stålskall.



Reell skjerming
Praktiske løsninger krever åpninger for adgang, krafttilførsel, vann og avløp, kommunikasjon, ventilasjon etc.

Soneskjerming



magnetiske påvirkninger, som f.eks. motorer som ikke inneholder avansert styreelektronikk eller kan styres med manuelle brytere, eller funksjoner man kan klare seg uten i korte perioder. Kan f.eks. kjølingen være borte i én time? Kan manuell styring overta for automatikk? Kan man basere seg på å ha reservedeler som man bytter i en kritisk situasjon?

Krav til skjerming

Skjerming er uttrykt ved størrelsen desibel (dB), som er en logaritmisk størrelse, og som beskriver et forholdstall. Når vi tenker felt, er det doble av 40 bare 46, det doble av 100 er 106, halvparten av 50 er 44 etc. Når vi tenker energi, er det doble av 40 bare 43, det doble av 100 er 103 etc. Dersom man har to vegger med 10 dB skjerming i hver vegg, vil man kunne oppnå 20 dB demping når strålingen må gå gjennom først den ene og så den andre veggen for å nå målet. Skjermingen vil være frekvensavhengig.

Illustrasjon av størrelsen dB (desibel)

($E_{uskjermet}/E_{skjermet}$)

S = 20 x log ($E_{uskjermet}/E_{skjermet}$)

Demping dB	demping felt	demping energi
10	1/3	1/10
20	1/10	1/100
30	1/31	1/1 000
40	1/100	1/10 000
50	1/316	1/100 000
60	1/1000	1/1 000 000
70	1/3162	1/10 000 000
80	1/10 000	1/100 000 000
90	1/31622	1/1 000 000 000
100	1/100 000	1/10 000 000 000

Elektromagnetisk stråling består av elektriske felt og magnetiske felt. Energitetthet i strålingen er foretatt ved multiplikasjon av feltene. I avstand over ½ bølgelengde fra kilde vil feltene ha et fast forhold mellom hverandre (377 ohm). Styrke på puls kan beskrives med feltstyrke eller med energiinnhold. Energiinnhold vil da være proporsjonal med kvadratet av feltstyrken, slik at om feltstyrken blir redusert til 1/10, vil energien bli redusert til 1/100. Ref. ***Illustrasjon av størrelsen dB (desibel)***.

Alt elektronisk utstyr som skal selges, må kontrolleres for immunitet og utstråling av radiobølger, og får da CE-merke. CE-merket utstyr skal fungere garantert uten forstyrrelser i feltstyrker opp til 5 V/m, men praktisk erfaring viser at mange typer utstyr tåler stråling høyere enn 500 V/m. For å unngå skade fra NEMP vil det ut fra erfaring fra tester på mange typer utstyr, være tilstrekkelig med 30–40 dB demping. For å være sikker på å unngå forstyrrelser trengs opp mot 80 dB. For radiofrekvente våpen vil beskyttelse delvis kunne bestå i å holde angriper på avstand. Rekkevidde på våpen vil være avhengig av størrelse blant annet. Behov for skjerming vil da være avhengig av en rekke faktorer.

Plassering av rom/anlegg som skal beskyttes mot HPM

Plassering av anlegg under bakken vil kunne bidra med en del skjerming. Stråling i mikrobølgeområdet vil bli kraftig dempet av jord- og fjelloverdekning. For lavfrekvent stråling vil dempingen være mer beskjeden. Skjermingsbidrag fra overdekning kan bidra til å senke skjermingskrav i bygningskroppen.

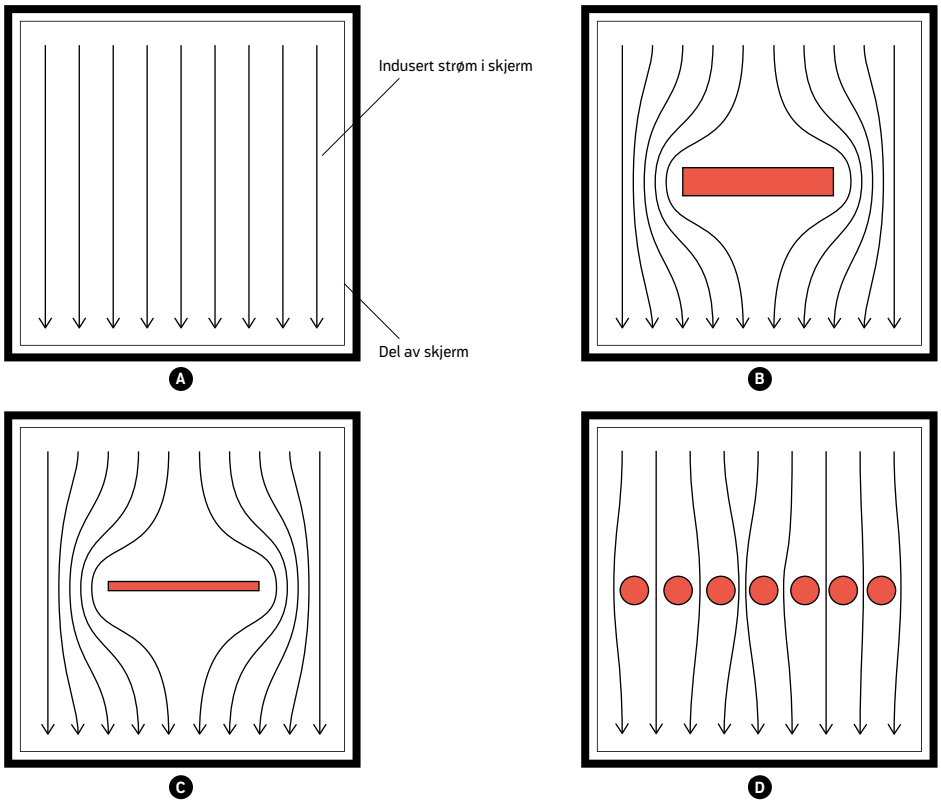
Venstre: Prefabrikkert skjermrom

FOTO Norshield

Høyre: Plassbygd skjermrom med naglede stålplater

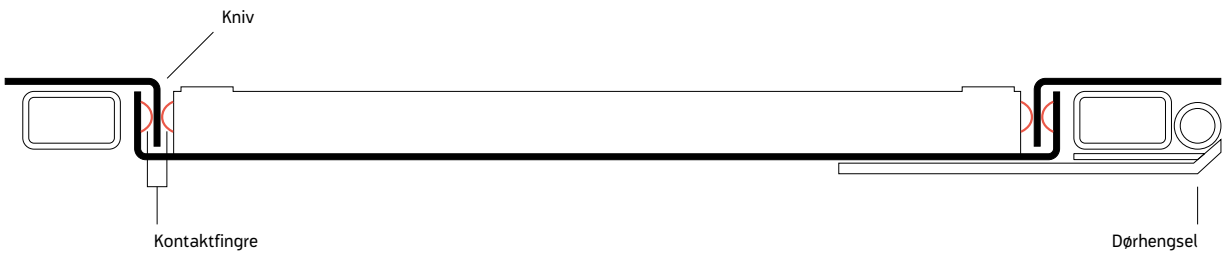
FOTO Forsvarsbygg

Effekter av åpninger i skjerm



A: Elektromagnetiske felt vil indusere strømmen i skjerm.
B: Spalter vil hindre denne strømmen og slik medføre at felt går gjennom skjerm.
C: Om spalter er smale eller brede, har liten betydning.
D: Mange små hull i skjerm har mindre effekt.

Vanlig skjermdørkonstruksjon



Mikrobølger spres i rette linjer og kan i liten grad gå rundt hjørner. Slike våpen kan ha lang rekkevidde, men for en kraftig effekt og lang rekkevidde trengs et stort våpen. Som beskyttelse mot mindre, mobile våpen – spesielt små bærbare våpen samt mot avlytting – vil sikkerhetssoner ha effekt siden avstanden til målet er viktig. Hindring av fri bane mot mål vil også gjøre angrep fra store våpen vanskelig, som for andre flatbanevåpen.

Skjerming av rom

Når bygninger eller rom skal skjermes, bygges faradaybur. Et faradaybur er et elektrisk ledende skall som omslutter det skjermede volumet. Hvis det er åpninger i skallet, vil stråling kunne komme inn, men hvis bølgelengden på strålingen er vesentlig større enn åpningen, vil det likevel være en viss skjerming. Tidligere har det derfor vært vanlig med kyllingnetting eller armering for å skjerme mot NEMP. I dag blir helst metallplater brukt i en eller annen form.

Rehabilitering

Rehabilitering av gamle bygninger for å bygge inn EMP-skjerming vil som regel bli vesentlig dyrere enn å implementere skjerm i nye konstruksjoner siden gamle kabler og rørføringer gjerne må fjernes. En god løsning kan i mange tilfeller være å sette inn prefabrikkert skjermrom som vil kreve litt ekstra plass. Mer omfattende arbeid, men billigere materialer, vil være å kle vegger, gulv og tak med metall. Da må alle gamle installasjoner ryddes vekk og installeres på nytt, med de kostnader det vil medføre.

Nybygg

Ved nybygg er det ingen gamle installasjoner å ta hensyn til. Ofte er det beste å bygge plater inn i veggen.

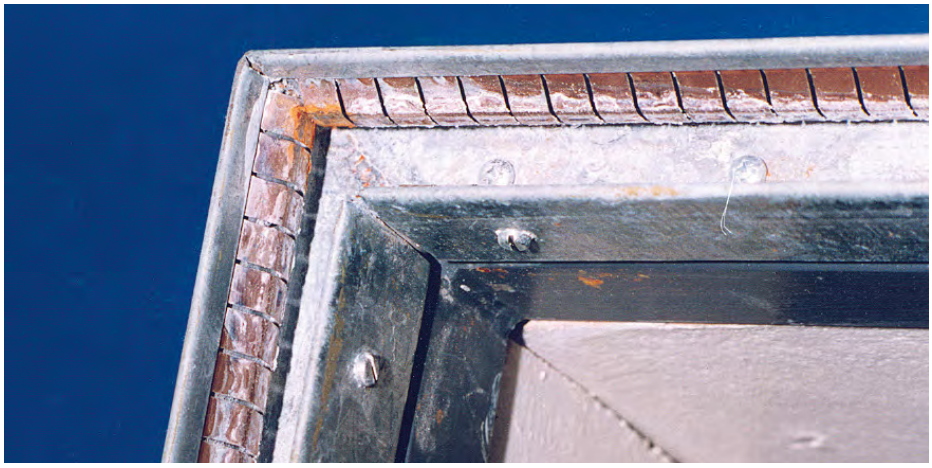
Ved høye skjermingskrav (over 60 dB) vil plassbygd løsning være stålplater som er sveiset. Prefabrikkert rom fungerer også. Her er det krav om at det ikke skal finnes sprekker. Sveisede plater bør være 3–5 mm tykke for at de skal tåle sveisetemperaturen uten å bli for deformerte. Jo tykkere platene er, desto enklere er de å sveise. Skjermingen blir god nok selv med 1 mm plater.

Ved skjermingskrav på 40 dB anbefales det å bruke naglete plater. Nagling bør være i sikksakkmønster med 10 cm mellom naglene. Det er viktig å ha rene kontaktflater når platene blir montert sammen for å få god kontakt mellom platene.

Smale spalter i skjerm vil ha nesten like stor lekkasje som sirkulære åpninger med diameter lik lengden på spalten. Derfor er det viktig at man sveiser kontinuerlig, og at nagling blir ordentlig utført.

Dører

Dører må være metalliske og ha kontinuerlig



Korrosjon på kontaktfingre i dørskjerm
Kontaktfingre av kobberlegering som over tid ikke har blitt renset og smurt. Dette hindrer god kontakt, og skjermdør vil ikke fungere som forventet. Støv og skitt på terskel er også et vanlig problem.

FOTO Forsvarsbygg

elektrisk kontakt hele veien rundt karmen mellom karm og dørblad. Den mest vanlige typen er den når en stålkniv kommer i kontakt med kontaktfingre av beryllium-kobberlegering.

En annen variant er at magneter i karmen trekker dørbladet inn mot karmen. Dette er en variant som trenger lite daglig vedlikehold. Sterke statiske magnetiske felt kan da forekomme nær døren, noe som for eksempel kan forvrenge bilder på dataskjermer.

En enklere og billigere variant er å ha RF-pakninger (metallpakninger) mellom karm og blad, men det gir begrenset skjermeffekt. God skjerming (40 dB) her krever stor kraft på lukking av dør samt at trykket rundt døren er jevnt.

Hvis det er krav til f.eks. høy innbruddsikring der skjermdøren er, er det vanlig å sette to dører som vender hver sin vei inn i åpningen.

Montering av dører

Dørkarm må ha god kontakt mot skjerm hele veien rundt. Består skjermen av sveisete stålplater, må karmen sveises hele veien rundt til skjerm. Innmontering må være på samme måte som montering av skjerm ellers, enten det er sveiset eller naglete plater, netting eller armering.

Vedlikehold av dører

Den viktigste grunnen til dårlig skjerming i dører er støv og skitt. Dører som er lite i bruk, kan bli utsatt for korrosjon. Regelmessig rensing og smøring av dører er viktig. Syrefri vaselin er mye brukt siden den ikke etser kontaktfingrer eller lignende.

Andre grunner til svikt i ytelse er fysisk skade på kontaktfingrer eller pakninger. Bytte av fingrer/pakning er da løsningen.

Vinduer

Vinduer er ikke vanlig i skjermede rom. Gode termoglass kan skjerme opp til 30 dB på mikrobølgefrekvenser, men det kan finnes ulineære effekter ved store energimengder. Vinduskarmer er normalt heller ikke konstruert for skjerming. Enkelte leverandører produserer spesielle skjermvinduer. Ved høye skjermkrav blir optiske egenskaper gjerne dårlige. Det vil resultere i et betydelig lystap og begrenset gjennomsyn i de fleste tilfeller. Slike vinduer vil normalt ikke være mulige å åpne.

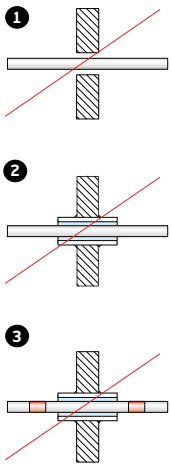
VVS, vann/avløp, kjøling, ventilasjon og eksos

Åpninger i skjerm kan tettes for stråling ved å lage bølgefeller. Dette er rør som er sveiset til skjerm, og som har 5 x diameter lengde på rør.

Rørgjennomføring

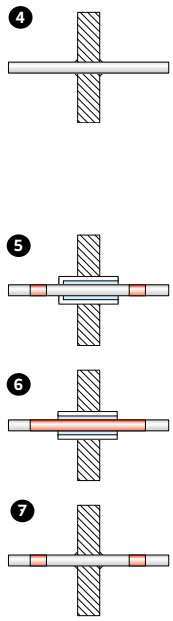
Eksempler på feil rørgjennomføringer, samt anbefalte løsninger

Feil gjennomføring



1. Puls vil følge rør inn i anlegget.
2. Puls vil følge rør inn i anlegget.
3. Skaffer avbrudd på røret, men stopper ikke stråling inn gjennom åpning. For å rette på dette kan løsning 5 brukes.

Anbefalt gjennomføring



4. Ikke ønskelig, men blir gjerne brukt på eksosgjennomføringer fordi det ofte er vanskelig å lage gode avbrudd på rørene som tåler risting fra aggregatene. Det finnes keramiske koblinger man kan bruke på eksos, men de er ofte sprø og kan lett bli mekanisk ødelagte.
5. Utbedring av løsning 3
6. Nr. 6 og 7 er løsningene som er ønskelig. Dersom rørene står med elektrisk ledende væske, er nr. 7 beste løsning, spesielt dersom det er fare for at innhold i rør har litt ledningsevne.
7.

Dette vil kunne gi ca. 100 dB demping. Denne konstruksjonen vil stoppe stråling på frekvenser opp til en grensefrekvens der bølgelengden er dobbelt så stor som diameter. Elektrisk ledende konstruksjoner inne i bølgefellen vil forstyrre denne effekten.

Ved gjennomføring av rør i skjerm må man ta hensyn til at puls kan følge rørledninger. Ved å sette inn isolerende muffer vil man kunne unngå at puls når frem til anlegget.

Illustrasjon Rørgjennomføring viser ulike måter rør kan gå gjennom skjerm på god og dårlig måte.

Når det gjelder ventilasjon, er det som oftest lurt å dele rør opp i små celler, såkalte honeycombs. Fysiske dimensjoner på gjennomføring kan da bli beskjeden. Flere leverandører tilbyr ferdige honeycombs, se ***Honeycomb-ventilasjon***.

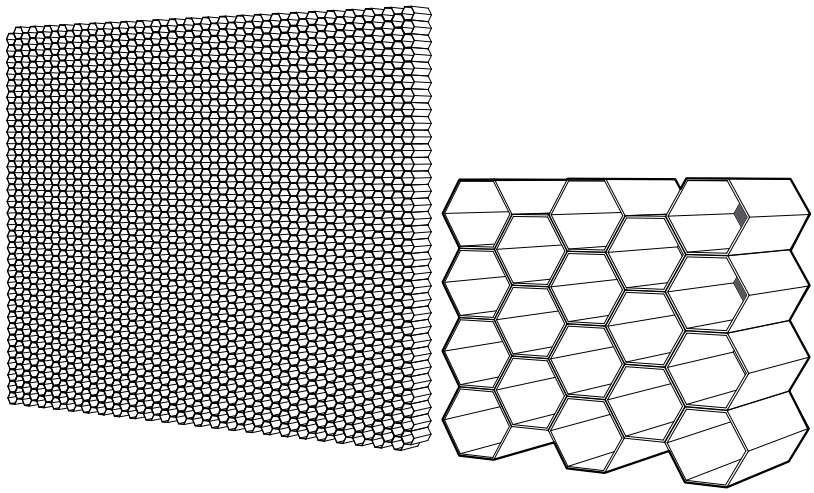
Jording

All jording inne i anlegg skal føres til en bolt sveiset til innsiden av single entry-plate. Jording skal ikke føres gjennom skjerm. Jordreferanse for jordtilførsel utenfra skal føres til en tilsvarende bolt på utsiden av single entry-platen. Boltene skal være ca. 1 meter fra hverandre.

Inne i rom vil god EMC-jording, stjerne- eller maskenett, bidra til beskyttelse. Bruk av kabelbruer eller kabelkanaler vil bidra ytterligere.

Honeycomb-ventilasjon

Åpning for luftgjennomgang er delt opp i mange små rør



Overspenningsvern

Overspenningsvern kan være gassavledere, varistorer, zenerdioder eller andre komponenter som virker isolerende opp til en viss spenning, eller kombinasjoner av disse. Noen gassavledere er utstyrt med motstander for å begrense følgestrømmer, og noen varistorer er utstyrt med sikringer for å unngå varmgang ved slitasje, siden de ellers kunne være brannfarlige.

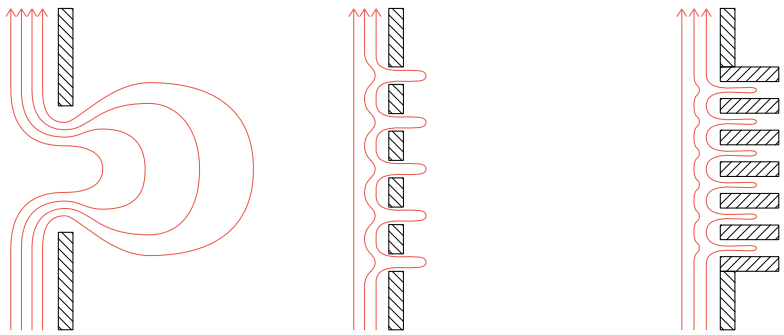
Ofte er vernet oppdelt i grovvern (ofte gassavleder) som kan håndtere store energimengder, og så et finvern som er raskt nok til å gi tilstrekkelig beskyttelse. Finvernet er da i single entry, mens grovvernet kan være et stykke utenfor. I mange tilfeller er finvernet filter som stopper signal over en bestemt frekvens. Filter vil da også fungere mot Tempest. Andre typer overspenningsvern vil ikke ha effekt på Tempest.

UPS/nødstrøm

Etter EMP/HPM-angrep vil elektriske installasjoner utenfor beskyttet område kunne bli ødelagt, og man vil da miste ekstern kraftforsyning. Dersom skjermet område må kunne fungere under og rett etter angrep, som oftest er tilfellet, trengs kraftforsyning internt. UPS fungerer så lenge batteriene har kapasitet. Etter den tid trengs aggregat. Ved dimensjonering bør man gå gjennom hva man egentlig trenger strøm til, for å slippe overdimensjonering av kraftforsyning, som i tillegg til å være ekstra kostbar også kan fordyre skjermingstiltak.

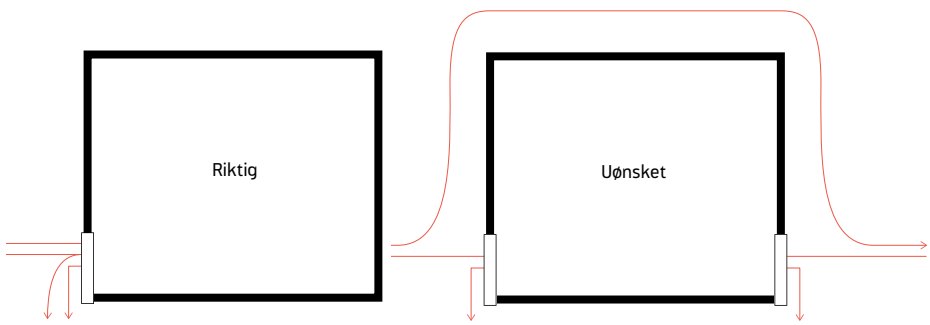
Punktbeskyttelse av aggregat og UPS er mulig, men ofte er det best å ha det innenfor skjermet område. Fra sovjetiske kjernefysiske tester i 1962 er det rapportert at dieselgeneratorer har blitt ødelagt av EMP.

Åpninger i skjerm



Illustrasjonen viser hvordan felt brer seg inn gjennom åpninger. Tetthet på linjer viser feltstyrke. Vi ser at felt brer seg inn gjennom store åpninger. Mindre åpninger gir mindre utbredelse av felt innenfor skjerm, og ved hjelp av bølgefeller unngår man at feltet kommer innenfor skjerm.

Single entry



Kabler og rør vil fungere som antenner som fanger opp energien i EMP. Hvis disse «antennene» blir ført inn i skjermede rom på mange plasser, kan de sette opp strømmer mellom de forskjellige tilkoblingspunktene, og disse strømmene kan bli ført gjennom utstyr og påføre skade. Strømmer i skjerm kan sette opp felt inne i skjermrommet, som deretter kan indusere skade. Alle metalliske kabler og rør som skal føres gjennom skjerm, skal derfor føres inn på et «single entry». Dette single entry-området er gjerne definert til en bestemt stålplate, der alt som skal jordes, blir jordet, og metallkabler blir utstyrt med overspenningsvern.

Sterkstrøm og svakstrøm må nødvendigvis separeres i forskjellige skap, men de kan stå ved siden av hverandre.

DEL 4

SPESIELLE FUNKSJONER OG SPESIALROM

Del 4 Spesielle funksjoner og spesialrom
gir innsikt i hvordan oppnå nødvendig beskyttelse og sikring av spesielle funksjoner som post- og varemottak og VIP-bolig og kontor.


8331-8336
8345-8355
GRADERTE
8376-8392
8394-8400
8009
8010-8013

Kapittel 20

Spesialrom

Dette kapitlet omhandler overordnede forhold tilknyttet spesialrom, og hva det er hensiktsmessig å ta hensyn til ved etablering og bruk.

Spesialrom er bygningsmessige avgrensede volum for dedikerte funksjoner med særlige behov for sikkerhet. «Særlige behov» er i denne sammenhengen konkrete målsettinger for sikkerhet knyttet til f.eks. personell, vesentlige funksjoner, sensitiv informasjon/informasjonssystemer, kritisk materiell eller en kombinasjon av dette.

Sammensatte krav

Spesialrom stiller normalt sammensatte krav til sikringen, der ulike og ofte samtidige trusler gjør seg gjeldende.

Etablering av spesialrom

Etablering av spesialrom i eksisterende bygninger, men også i nybygg, er kostbart, så det er derfor lurt å vurdere om funksjonene kan:

- *Kombineres, slik at ett rom kan tjene flere spesialfunksjoner*
- *Samlokaliseres, for bedre utnyttelse av sikringstiltak*
- *Benyttes av flere brukere (f.eks. felles resepsjon)*

Samtidig må det nevnes at ikke alle rom egner seg til samlokalisering med andre funksjoner eller brukere, og noen rom kan heller ikke sammenstilles i soner.

Prosjektering

Ved prosjektering av spesialrom er det viktig å tilstrebe mest mulig generelle løsninger for å kunne imøtekomme eventuelle endringsbehov. Plassering av spesialrom kan følge direkte av funksjonen (f.eks. resepsjon), men i de fleste tilfeller er det anledning til å velge en sikkerhetsmessig mer hensiktsmessig plassering. Dette innebærer en plassering vekk fra fasade og andre bygningsdeler som grenser til uvedkommen aktivitet, og/eller områder det er vanskelig å kontrollere. En plassering mot kjernen av bygningen vil normalt være å foretrekke, da vi i tillegg til sikkerhet i dybden frigjør verdifullt fasadeareal til funksjoner med normalt høyere krav til dagslys. Spesialrom må planlegges nøye og bør derfor prosjekteres av et kompetent fagmiljø.

Utførelse

Det er avgjørende at rommene faktisk yter den sikkerheten som forventes, så det må stilles strenge krav til kvalitet i utførelsen. Dette gjelder særlig rom med høye krav til tetthet i gjennomføringer og overganger mellom ulike bygningsdeler. Videre kan sikringsprodukter som er godkjent etter en bestemt standard, yte lavere enn forventet dersom monteringen er feil, forenklet eller på annen måte mangelfull.

Godkjenning

Mange rom, avhengig av sikringsnivå, må godkjennes før bruk. Dette må gjøres for å være sikker på at rommet er i den stand som det skal være i, for å yte den sikkerheten som forventes. Godkjenningsorgan for rom med krav stilt i sikkerhetsloven er normalt Nasjonal sikkerhetsmyndighet (NSM), men for enkelte rom med lavere sikkerhetsbehov kan det være tilstrekkelig at lokal sikkerhetsansvarlig godkjenner etter egne vurderinger. Godkjenningen gis etter en helhetsvurdering basert på bl.a. risikovurderinger, tekniske sikkerhetsundersøkelser (TSU), lydmålinger m.m. avhengig av type rom.

Bruk

Etter at et spesialrom er godkjent, følger det særskilte krav til den videre bruken.

Begrenset adgang der kun dedikert personell har direkte tilgang, er et minimum av tiltak for forsvarlig bruk av spesialrom. Samtidig kan det også gjelde andre og mer omfattede krav. Alle kravene som stilles til bruk av rommet, skal nedtegnes i en brukerinstruks som må være kjent for det personellet som er autorisert for bruk. Eksempler på forhold som vil være med i en slik instruks, kan være:

- *Hvem har adgang, og hvem har ikke adgang?*
- *Skal det føres besøksprotokoll/logg?*
- *Hva skal rommet brukes til, og hva kan rommet eventuelt ikke brukes til?*
- *Hva er konsekvensene ved feilaktig bruk? (Ny TSU?)*
- *Liste over godkjent inventar, f.eks. møbler osv.*

Eksempler på spesialrom

Eksempler på spesialrom er beskrevet i andre kapitler:

- *Rom for presentasjon av sensitiv informasjon er tatt med i **kapittel 14, Avlytting og avlesing***
- *Rom for oppbevaring av informasjon eller materiell er tatt med i **kapittel 11, Fysisk sikring mot inntrengning***
- *Rom for oppbevaring av materiell med behov for skjerming mot EMP/HPM er tatt med i **kapittel 19, Elektromagnetiske effekter***


NORGE
50
POSTFRIM 50 KR

Kapittel 21

Post- og varemottak

Dette kapitlet handler om hvordan en virksomhet kan avdekke og håndtere farlige objekter som er skjult i post- og vareleveranser.

Post- og vareleveranser kan inneholde en rekke trusler som kan utgjøre en risiko for en virksomhets ansatte og operasjoner. Truslene kan være kjemiske, biologiske, radiologiske, nukleære, eksplosiver (CBRNE) eller farlige gjenstander som våpen, kniver og lignende. Etablering av et system for kontroll av post og varer vil være en del av en helhetlig sikring for å redusere mulighetene for at denne type trusselstoffer og farlige gjenstander kommer inn i virksomhetens eiendom, bygg og anlegg (EBA).

Et post- og varemottak (PVM) kan være et tiltak for å hjelpe å identifisere og minimalisere virkningen av post og varer som kan representere en trussel, eller medfører forstyrrelser eller avbrudd i virksomhetens aktiviteter og operasjoner.

Ved utvikling og implementering av tiltak for kontroll av post- og vareleveranser, er det en rekke vurderinger som bør gjøres:

- *Vurdere risikoen for at virksomheten kan bli utsatt for postleverte trusler*
- *Velge kontrollnivå som er i samsvar med risikoen*
- *Identifisere egnet lokasjon for kontrollfasilitet og hensiktsmessige fysiske sikringstiltak*
- *Formalisere virksomhetens krav til kontroll og sikring mot post- og vareleverte trusler*
- *Implementere post- og varekontroll og sikring*
- *Regelmessig revidering og oppdatering på bakgrunn av hendelser, interne og eksterne endringer*

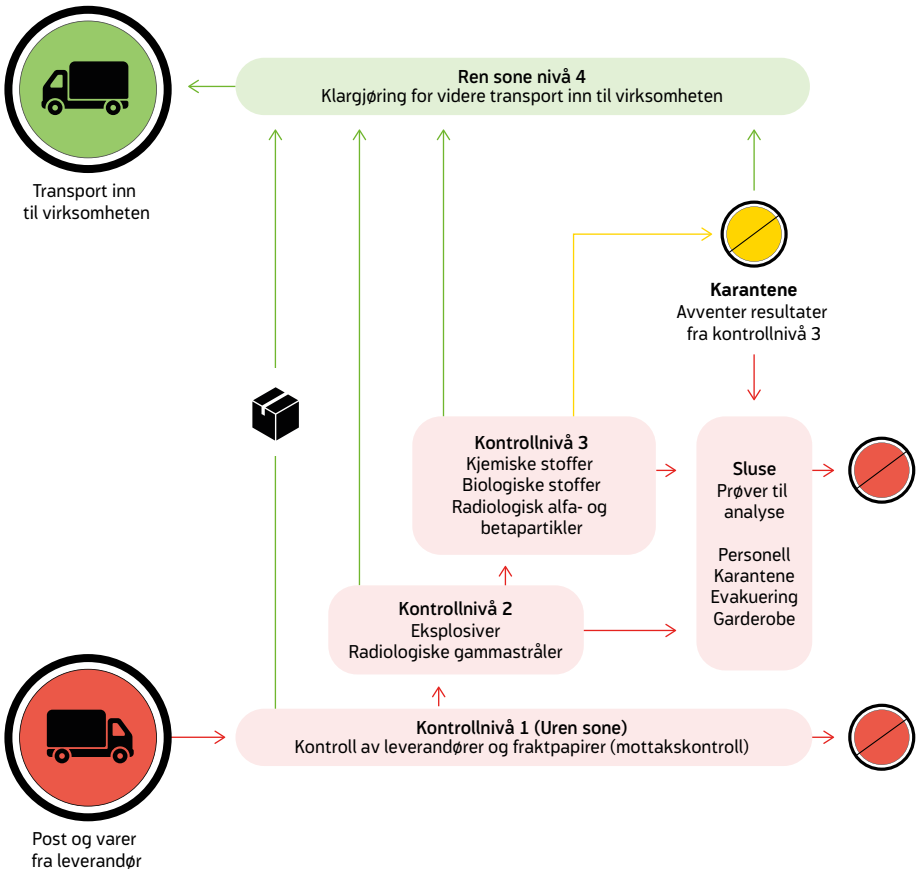
Utforming

Når virksomheten har gjennomført en risikovurdering og har bestemt seg for hvilket kontrollnivå som skal legges til grunn, er neste steg å vurdere egnet lokasjon for kontrollfasiliteten. Da er det flere muligheter:

- *Den laveste risikoen oppnås ved etablering av PVM utenfor virksomheten med egen interndistribusjon. Ved å plassere PVM i en sikker avstand fra andre funksjoner og verdier, vil det som oftest kun være selve mottaket som vil bli berørt av en eventuell hendelse med CBRE (kjemiske, biologiske, radiologiske, eksplosive) trusselstoffer. Virksomheten for øvrig vil kunne fungere tilnærmet upåvirket. Det vil være naturlig å etablere PVM i forbindelse med eiendomsgrensen eller en definert ytre grense for et sikringsobjekt, en leir eller en base.*
- *For større virksomheter kan det være aktuelt å etablere et sentralt mottak med eget logistikk- og distribusjonssystem. Dersom avstanden er for stor, kan det likevel være*

Flytskjema for post- og varemottak

Eksempel på vareflyt fra en leverandør gjennom et post- og varemottak



1. Alle leveranser betraktes i utgangspunktet som «urene», og første trinn i kontrollen (merket 1) vil være at man kontrollerer leverandør, selve kjøretøyet, sjåfør og hjelpemannskap og utfører kontroll av alle fraktdokumenter opp mot selve leveransen.

2. Her kontrolleres selve vareleveransen for eksplosiver, ulike typer av stråling, generelle trusselstoffer.

2A. Er varene kontrollert og funnet å være «rene», kan de sendes videre til klargjøring (trinn 4) for videre distribusjon.

2B. Er man usikker på om varene er rene, kan de sendes til et nytt kontrolltrinn 3 hvor man fysisk sjekker varene eller har bedre forutsetninger for å kunne gjøre analyser.

2C. Dersom det gjøres funn av ulike trusselstoffer, skal enten varemottaket evakueres for at stoffene kan uskadeliggjøres, eller de sendes via en sluse til en karantene.

3. Dette kan være et ekstra kontrollpunkt dersom man av ulike årsaker har delt kontroll, skannere og annen type deteksjonsutstyr i ulike seksjoner eller rom.

4. Klargjøring for videre distribusjon. I dette trinnet betraktes post og varer som «Rene» og håndteres for videre distribusjon til sine respektive mottakere.

nødvendig å etablere et lokalt PVM for å håndtere lokale forsendelser (mat, drikke og annet lokalt levert materiell).

- *En virksomhet som er villig til å ta en høyere risiko, kan etablere PVM innenfor eget perimeter i et separat bygg. Her kan en hendelse påvirke verdier som ligger i nærheten av mottaket, og det vil være utfordringer knyttet til å ha kontroll på leverandører som slippes gjennom ytre perimeter.*
- *En virksomhet som er villig til å ta ytterligere risiko, kan etablere PVM i tilknytning til virksomhetens primærfunksjon (i samme bygg). Her vil det være utfordringer knyttet til å begrense skade og nedetid av hele fasiliteten ved en eventuell hendelse. Det vil i så fall kreve separat ventilasjon, undertrykksrom og beskyttelse av øvrig virksomhet mot virkning av eksplosiver og CBR-trusselstoffer.*
- *Siste alternativ er å akseptere risikoen og ikke iverksette noen spesielle tiltak for å håndtere CBRE-trusler levert gjennom post- og varesystemet.*

Andre forhold

Prinsipielt regnes varer fra en leverandør som urene og krever en fullstendig kontroll av om leveransen inneholder trusselstoffer. Basert på risikovurderinger kan kravene som stilles til kontroll av varer fra ulike leverandører, variere.

Det er en stadig utvikling av sensorteknologien for å detektere og identifisere CBRE trusselstoffer. Hvilke sensorer som skal implementeres i det enkelte post- og varemottak, må derfor vurderes spesielt i hvert prosjekt.

For å få kontroll av post- og vareleveranser til å fungere i praksis er det avgjørende at logistikk- og sikkerhetspersonell arbeider tett sammen i utvikling av løsningen. Det er også behov for et grundig arbeid med å utvikle prosedyrer for hvordan vareflyten skal være, og hvilke handlinger som skal utføres ved ulike typer hendelser.

I tillegg vil det være behov for fysisk og elektronisk sikring av fasiliteten, overvåknings- og kommunikasjonsanlegg, system for risikohåndtering, rutiner for varsling og rapportering, samt medisinske mot- og støttetiltak.

Kapittel 22

VIP-funksjoner

Dette kapitlet gir en generell innføring i hvordan sikre bolig og kontor for VIP-personell. Her fokuseres det på sikringstiltak knyttet til bygninger og tilhørende administrative tiltak. Fysiske og elektroniske tiltak på reise og aktive mottiltak beskrives derfor ikke.

En VIP (Very Important Person) er i denne sammenheng en person som kan være spesielt utsatt for uønskede hendelser som overfall, attentat og lignende, og som på grunn av sin posisjon, stilling, oppdrag, symbolverdi eller annet krever spesiell sikring. Dette kan være politikere, ledere ambassadører, nøkkelpersoner i Forsvaret og statsforvaltning eller andre enkeltpersoner.

Det er i Europa en rekke eksempler på angrep på VIP-personell. Disse spenner fra terrorangrep til overfall fra ustabile personer med fiksering på enkeltindivider.

Sikring av VIP

Overordnet kan sikringstiltak for VIP-personell deles i:

- *Administrative sikringstiltak*
- *Bygningsmessige sikringstiltak på arbeidsplass og i bolig*
- *Fysiske og elektroniske sikringstiltak på reise*
- *Aktive mottiltak (livvakt, utrykningsstyrke, reaksjonsapparat)*

Sikringen av VIP-bolig/kontor gjennomføres etter følgende prinsipper:

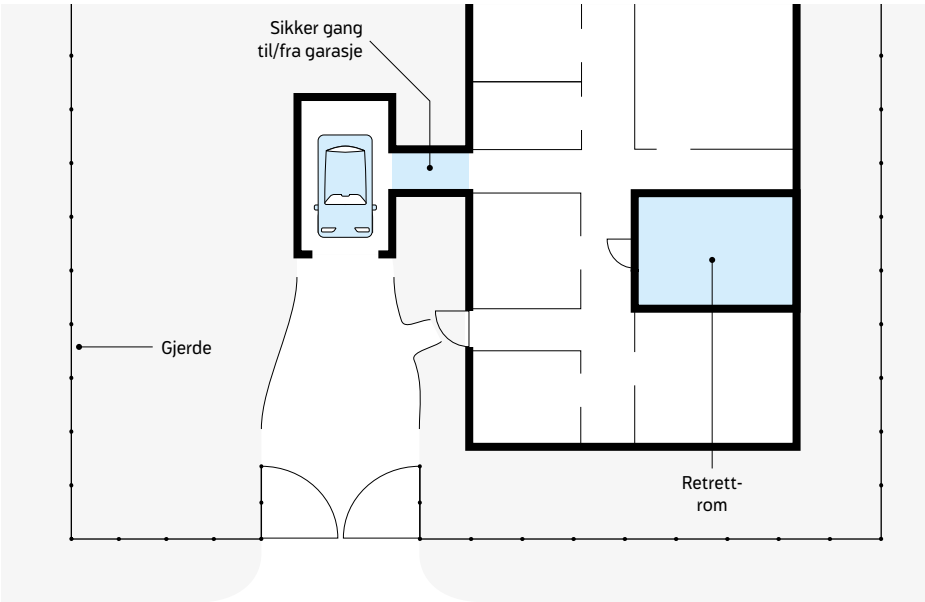
- *Tiltakene bør gjennomføres med basis i en risikoanalyse*
- *Tiltakene skal i størst mulig grad avdekke en potensiell overfallssituasjon*
- *Tiltakene skal gi VIP-personell mulighet til en effektiv varsling om en trusselsituasjon*
- *Tiltakene skal i størst mulig grad beskytte VIP mot relevante trusler og vanskeliggjøre et overfall/attentat*
- *Tiltakene skal i rimelig grad forsinke en inntrengning i VIP-boligen/kontoret*
- *Tiltakene skal gi VIP-personell en mulighet for å søke tilflukt i et retrettrom*

Administrative sikringstiltak

Administrative sikringstiltak er det viktigste for det store flertallet av VIP-personell. Opplæring i hvilke forsiktighetsregler man skal følge, hvilke trusler man kan stå overfor, og rutiner for hvordan man skal forholde seg hvis trusler materialiserer seg, er vesentlig. Dette gjelder alle fra landets symbolpersoner til enkeltpersoner på tjenestereise.

Det er PST som vurderer sikring av Norges «symbolpersoner». Basert på sine vurderinger vil de plassere VIP i ulike risikogrupper og iverksette tilhørende sett av sikkerhets- og

VIP-bolig



beskyttelsestiltak. Enhver bedrift eller organisasjon er selv ansvarlig for å vurdere om det er enkeltpersoner som er så trusselutsatte eller viktige for virksomheten at personen trenger spesiell beskyttelse.

Bygningsmessige sikringstiltak

Sikringshåndboka har fokus på bygningsmessige sikringstiltak. Det vil i denne sammenheng være sikringstiltak på VIP-personells arbeidssted og bolig, og etablering av retrettrom.

Sikringsmessig er det vesentlig at VIP får varsel om et angrep slik at det er tid til evakuering eller å trekke seg tilbake til et retrettrom.

a. Sikring av VIP-kontor

Det primære tiltaket er et system for varsling av VIP ved mulige trusselhendelser i bygget. Det vil si varsling til VIP fra AIA eller vakt-/resepsjonsbetjening. VIP må også ha en enkel måte å varsle om uønskede hendelser på fra sitt kontor. Kontoret må plasseres fornuftig i forhold til truslene mot VIP og gis tilstrekkelig fysisk og elektronisk sikring. Minimumsløsningen er normalt AAK, FG-godkjent avlåsning og AIA. Sikringsløsningene må imidlertid basere seg på en risikovurdering.

b. Sikring av VIP-bolig

De fleste norske bolighus kan normalt benyttes som VIP-boliger dersom de forsterkes. Med dette menes primært alarmlegging (AIA) slik at et angrep oppdages og varsles. En slik deteksjon gir personer som oppholder seg i boligen, muligheten til å komme seg i sikkerhet, enten ved at de evakueres, eller rømmer til et retrettrom hvor det påkalles assistanse. Ideelt sett bør boligen ha en fysisk barriere i perimeteret som en eventuell inntrenger må forsere, og dermed utsettes for eksponering.

Denne barrieren er sannsynligvis et gjerde som kan fungere som alarmbærer. I tillegg må det vurderes i hvilken grad boligens skall med dører, vinduer og vegger må fysisk sikres slik at det tar lengre tid å forsere. Se ***kapittel 10, Perimeter- og områdesikring,*** og ***kapittel 12, Elektronisk sikring*** for mer detaljerte beskrivelser av systemer og tiltak.

Boligen bør ha et automatisk innbruddsalarmanlegg dimensjonert mot trussel angitt i risikoanalysen. Anleggets detektorer bør minimum dekke alle utvendige dører og andre sannsynlige adkomstveier inn i boligen, og det bør i tillegg plasseres overfallsalarmutløsere på sentrale oppholdssteder. Sentralutstyr for AIA-anlegget skal plasseres i retrettrommet.

Et tv-overvåkningsanlegg skal gi beboerne sanntidsopplysninger om sikkerhetstruende forhold i boligens umiddelbare nærhet, samt gi tilsvarende opplysninger om forhold som har skjedd i løpet av natten eller til andre tider, dersom beboerne ikke umiddelbart har blitt varslet om hendelsene. Betjeningsrommet for TVO-anlegg bør plasseres i retrettrommet. Merk at det er personopplysningsloven som regulerer omfang av overvåkning.

Når det gjelder de enkelttiltak som iverksettes for sikring av vinduer, dører, porter, romdeteksjon, overvåkning og annet, så vil dette følge samme prinsipper for et VIP-anlegg som for øvrige sikringstiltak som beskrives tidligere i denne boken. Forskjellen på en VIP-bolig og en ordinær bolig ligger gjerne i vurderingen av trusselaktøren, som normalt vil kreve at man går opp i valg av sikringsklasser.

Sikringsbelysningen skal dels virke preventivt med tanke på å avskrekke en potensiell angriper, samt gi muligheter for å observere boligens nærområder via TVO-anlegget eller visuelt fra inn-/utsiden av boligen.

Områdets beskaffenhet

Et veletablert boligområde med liten utskifting av beboere er å foretrekke. Det bør ikke være næringsbygg, forsamlingsbygg eller lignende i nærheten (siktavstand) av VIP-boligen. Heller ikke ubebodde hus, ubebygde og gjengrodde tomter eller andre steder hvor attentatpersoner kan gjemme seg i forbindelse med en eventuell aksjon. Uteområder for opphold bør skjermes for innsyn. Tomten generelt bør ellers være så oversiktlig som mulig, og skal verken ha beplantning eller elementer som kan gi skjul og dekke for en potensiell angriper.

Tomtens beskaffenhet og beliggenhet

VIP-boligen bør ha størst mulig oversiktlig tomteareal på alle sider, som er fri for skjermende elementer. Beliggenheten bør være på et sted hvor det ikke er generell gjennomgangstrafikk, verken med kjøretøy eller til fots. Garasje bør ligge i tilknytning til boligen, med inngang fra denne. I høysikringsløsninger bør gjerdet ha minimum en gangport og en kjøreport. Alternativ inn/utkjøring til eiendommen er ønskelig, og krever da at man har to kjøreporter. Gangport bør utstyres med porttelefon, fjernbetjening og tv-overvåkning. Kjøreport bør kunne fjernbetjenes og tv-overvåkes.

Det bør være færrest mulige attraktive rømningsveier for en attentatperson. Med dette menes for eksempel at VIP-boligen/kontoret ikke bør ligge i nærheten av hovedveier/trappeganger med alminnelig ferdsel, og at rømningsvei for en attentatperson må foregå lengst mulig på oversiktlige områder hvor sannsynligheten for å bli observert er størst mulig.

VIP-personell bør ha mulighet til å benytte alternative transportruter mellom kontor og bolig. En alternativ transportrute bør kunne velges helt fra boligen.

Det bør utarbeides en instruks for beboerne i VIP-boligen. Denne må inneholde beskrivelse av og instruks for bruk av de tekniske anleggene.

Vel så viktig er å beskrive forhold knyttet til beboernes gjøren og laden både i forhold til normal dagligdags virksomhet i tilknytning til boligen og i forhold til situasjoner med forhøyet beredskap eller i reelle trusselsituasjoner.

VIP-bolig/kontor bør ligge i nærheten av et reaksjonsapparat, slik at dette kan komme til unnsetning i løpet av kortest mulig tid. Reaksjonstiden må ses opp mot de fysiske sikringstiltakene i boligen.

c. Retrettrom (saferoom)
Et retrettrom etableres for at VIP, ved et angrep, skal kunne trekke seg tilbake dit, tilkalle assistanse og avvente at et reaksjonsapparat (politiet) når frem og kan avverge angrepet.

Retrettrommet er et spesielt sikret og utrustet rom med en plassering som gjør at VIP-personene raskest mulig kan nå dit, uavhengig av hvor de befinner seg når angrepet detekteres. Rommet må sikres på en måte som gir tilstrekkelig beskyttelse mot den (i risikoanalysen) definerte trussels kapasitet og intensjon, og utstyres deretter. Retrettrommet bør være et innvendig rom som kan låses, og det må være kommunikasjonsmulighet fra rommet.

Retrettrommet plasseres sentralt helst vegg i vegg med et VIP-kontor og slik at det er enkelt å nå det fra vanlige oppholdsrom i en VIP-bolig. Rommet skal konstrueres slik at det kan motstå inntrengningsforsøk fra trusselaktør og således gi VIP og tilhørende personer et sikkert sted de kan rømme til ved et angrep på boligen/kontoret.

Behovet for fysisk sikring avhenger av hvilken trusselaktør man skal sikre seg mot. Selv avlåste rom med lav fysisk sikring har reddet liv ved tidligere terrorangrep, og en vanlig solid dør med hensiktsmessig avlåsning kan være tilstrekkelig. Skal man ha et retrettrom som skal motstå en mer avansert trusselaktør i en viss tid, er det imidlertid nødvending med betydelig fysisk sikring i dører og vegger. Se ***Del 3*** for løsninger.

Hvis boligen har tv-overvåkning, bør retrettrommet ha monitor for å kunne følge trusselbildet i boligen og nærmeste omegn. Minimumsutrustningen i rommet er kommunikasjons- og førstehjelpsutstyr. Annet utstyr avhenger av hvor lenge man antar å tilbringe der og kan omfatte blant annet brannslukningsapparat, nødstrøm, separat ventilasjon, drivstoff, lager for mat og drikke.

I spesielt utsatte områder kan man med fordel konstruere retrettrommet slik at det også vil fungere som en alternativ operasjonssentral. Personellet kan evakuere ned i retrettrommet, og derfra holde kontakt med verden på utsiden. Et ideelt retrettrom har også en egen fluktrute via en sikret sekundær adkomst som kan bringe VIP-personellet så raskt og sikkert som mulig bort fra trusselen.

Livvakt

PST definerer rollen «offentlig-VIP», grupperer de ulike personene og har føringer for hvilke minimumstiltak som skal iverksettes. VIP knyttes gjerne til livvakt, men dette gjelder et fåtall personer i Norge.

Ønsker man å sikre en VIP, er det hensiktsmessig å varsle lokale myndigheter om sin tilstedeværelse, slik at lokalt politi har nødvendig informasjon for å reagere riktig ved en mulig aksjon. Ideelt sett bør de utarbeide en objektplan for objektet som det skal rykkes ut til, med opplysninger om VIP og boligen, dens etasjer og rom, adkomstveier og relevante kontaktpersoner.

FAKTA

Det er PST som avgjør hvem som faller inn under betegnelsen VIP, og avgjør hvilken beskyttelse de skal tilbys.

Norske virksomheter og interesser i utlandet

For bedrifter og organisasjoner som har sine virksomheter i andre land, kan det være helt nødvendig å etablere en ramme av sikkerhet for alt personell som har sitt tilhold i kontorer og boliger som er under bedriftens ansvarsområde. Det vil i de fleste tilfeller være lokale politimyndigheter som har ansvaret for å iverksette bistand under en trusselsituasjon, men i mange tilfeller kan en erfare at lokale myndigheter har svært begrensede ressurser, og tiden det tar for bistanden å nå frem, kan være lang. Det er derfor å anbefale at både organisasjoner, offentlige etater og private selskap selv bidrar til å etablere best mulig sikkerhet for sine egne utsendte.

Etablering av VIP-bolig/kontor i utsatte land krever en grundig sikkerhetsvurdering, hvor lokale forhold som byggeteknikk og rammer for regelverk tas med i betraktning. Det kan antagelig være vanskelig å finne en optimal beliggenhet, men dersom vilkårene er ugunstige i så stor grad at sikkerheten vanskelig kan ivaretas, må flytting vurderes.

DEL 5

VEDLEGG

- Ordliste og definisjoner
- Sikringsklasser
- Trusselaktører
- Skjema Verdivurdering

Vedlegg

Ordliste og definisjoner

Ord og begreper er definert slik Nasjonalt kompetansesenter for sikring av bygg benytter dem. I merknadsfeltet er det tatt med henvisninger når definisjonen er tatt fra lovverket, standarder eller offentlige veiledninger, og i en del tilfeller gitt forklaringer og eksempler.

→ = *Referanse/merknad/forklaring*

DEFINISJONER

A

Adgangskontroll
Evnen til å tillate eller nekte adgang forbi en grense.

Administrative sikringstiltak
Samlebegrep for menneskelige og organisatoriske sikringstiltak.

Aktiv kjøretøysperre
Kjøretøysperre som kan åpnes for å la kjøretøy passere.
→ *En aktiv kjøretøysperre kan være manuell eller automatisk*
→ *Aktive kjøretøysperrer kan være veisperrer, bommer, porter, aktive pullerter og flyttbare kjøretøysperrer*
→ *Tilsvarer dynamiske kjøretøysperrer*

Alarmmottak
Sted hvor alarmer fra elektroniske sikringssystemer tas imot, presenteres og bearbeides.
→ *Oppgaver, bemanning og sikring vil avhenge av den verdien som skal beskyttes*
→ *Krever at noen er gitt et ansvar for behandling av alarmene, men omfatter hele spennet av mottak fra en enkel løsning i en resepsjon til et spesielt alarmmottak med omfattende sikringstiltak og dedikert personell*
→ *For FG-godkjente alarmmottak er det egne krav til bygningsmessig utforming og sikring*

Angrep
Ulovlig eller uønsket, tilsiktet handling som kan medføre skade på eller tap av verdier.

B

Balansert sikring
Sikringskonsept hvor kombinasjonen av barriere, deteksjons-/verifikasjonstiltak og reaksjonsapparat forhindrer tap av verdier.
→ *Sikringstiltakene detekterer et angrep og forsinker angriperen så lenge at reaksjonsstyrken når frem og kan avverge angrepet før verdier skades eller ødelegges. Se også tidsregnskap*
→ *Snakker man om balanse i sikringstiltakene, er dette en helhetlig sikring i forhold til en trussel. For eksempel at dører, vegger og vinduer har samme motstandskraft mot inntrengning*

Barriere
Sikringstiltak som skal forhindre eller redusere muligheten for at sikkerhetstruende hendelser kan inntreffe.

Beredskap
Forberedt evne til på kort varsel å kunne øke et sikkerhetsnivå, håndtere en uønsket hendelse eller tilstand, eller evne til å gjenopprette tilfredsstillende tilstand etter en uønsket hendelse eller tilstand.
→ *Fra NS 5830:2012*

Beskyttelse
Sikring mot våpenvirkninger.
→ *Beskyttelse er et fagområde innen sikring*

Beskyttelsesinstruksen
Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter.
→ *Hentet fra Lovdata*
→ *Benytter graderingene FORTROLIG og STRENGT FORTROLIG*

Beskyttet område
Område hvor det behandles eller oppbevares sikkerhetsgradert informasjon eller sikkerhetsgodkjente informasjonssystemer.
→ *Fra sikkerhetsloven, Forskrift om informasjonssikkerhet § 6–5*
→ *Beskyttet område kan f.eks. være rom, bygning eller del av bygning*

D

Dekningsrom
Rom som gir beskyttelse mot våpenvirkninger.
→ *Et dekningsrom kan gi forskjellig grad av beskyttelse. For eksempel mot beskytning, splinter, gass eller fulltreffsikre mot visse typer bomber/granater*
→ *Normalt et mindre rom med plass til 3–20 personer*

Deteksjonstiltak
Tiltak som etableres for å avdekke hvorvidt etablerte barrierer brytes eller blir forsøkt brutt.
→ *For eksempel alarmsystemer med forskjellige sensorer*

E

Elektromagnetisk effekt
Virkning fra elektromagnetiske felt.
→ *I Sikringshåndboka knyttet til Tempest og EMP-/HPM-våpen*

Elektronisk krigføring
Militær aktivitet som gjør bruk av elektromagnetisk (EM) energi for å utnytte og beherske spektret i offensive og defensive operasjoner.
→ *Omfatter innhenting og identifikasjon av EM-utstråling, bruk av EM-energi for å redusere eller forhindre fiendtlig bruk av spektret og tiltak for å sikre egne styrkers bruk av dette*

Elektroniske sikringstiltak
Elektroniske tiltak og systemer som skal forebygge, forsinke, detektere, varsle og verifisere uønskede handlinger.
→ *Ofte en fellesbetegnelse for automatisk innbrudds-alarm-anlegg (AIA), tv-overvåknings-anlegg (TVO) og automatisk adgangskontroll (AAK)*

Entitet
Et samlebegrep for et menneske, en stat, en gjenstand, en tanke eller et annet subjekt som eksisterer.
→ *Fra NS 5830:2012*

Etterretning
Innhenting, bearbeidelse og analysering av informasjon.

F

Fare
Handling eller forhold som kan føre til en uønsket hendelse.
→ *Fra NS 5830:2012*
→ *Handlingen eller forholdet kan være både tilsiktet og utilsiktet*

Fortifikasjon
Læren om hvordan man bygningsteknisk skal oppnå dekning mot skadevirkninger av fiendtlige våpen.
→ *I motsetning til befestningskunst har fortifikasjon et moderne taktisk/teknisk tilsnitt og brukes som fellesbetegnelse for hele fagområdet*

Fysiske sikringstiltak
Fysiske tiltak som skal hindre eller forsinke uønsket adgang til verdier.
→ *Fra NS 5830*
→ *Omfatter tidsforsinkende barrierer som gjerder, porter, dører, låser, vegger samt barrierer som sikkerhetsbelysning, skilting, m.m.*

G

Grunnsikring
Kombinasjonen av barrierer, deteksjon, verifikasjon og reaksjon som er tilpasset verdiene som skal sikres.
→ *Grunnsikringen kan gjelde et fysisk objekt, et individ, en virksomhet eller en annen enhet som hensiktsmessig passer inn i den aktuelle sammenhengen*
→ *Reaksjonstiltak forberedes som en del av grunnsikringen*

I

Informasjonssikkerhet
Sikringstiltak som skal sørge for nødvendig grad av konfidensialitet, integritet, tilgjengelighet og autentisitet ved behandling av informasjon i alle situasjoner, uavhengig av verktøy og metoder.
→ *Omfatter både etablering av barrierer, deteksjon av sikkerhetstruende hendelser og reaksjon på slike med tanke på gjenoppretting av sikker tilstand for informasjon og systemer*

Inn-/utpasseringsområde
Åpninger i perimetersikringen med adgangskontroll.

Innbruddstid
Tiden det tar for en angriper å trenge gjennom én eller flere barrierer.
→ *Vurdering av innbruddstiden baserer seg på fysiske tester, hvor angrepsverktøy og angriperens kompetanse er definert*
→ *Innbruddstiden kan spesifiseres som verktøytid, det vil si kun den tiden som benyttes med innbruddsverktøyet, eller angrepstid som inkluderer rigging og plunder og heft*

Intensjon
Vilje og hensikt til å gjennomføre en handling.
→ *Fra NS 5830:2012*

K

Kapasitet
Evne, herunder ressurser, kunnskap og ferdighet, til å gjennomføre en handling.
→ *Fra NS 5830:2012*

Katastrofe
Uønsket hendelse som medfører eksistensielle og uakseptable konsekvenser for den entiteten som rammes.
→ *Fra NS 5830:2012*

Kjøretøyhinder
Konstruksjon som er utformet og installert for å stoppe eller avvise et angripende eller truende kjøretøy.
→ *Konstruksjonen er ikke testet eller godkjent i henhold til en internasjonal standard*

Kjøretøysperre
Testet og godkjent konstruksjon som er utformet og installert for å stoppe eller avvise et angripende eller truende kjøretøy.
→ *Kjøretøyets hastighet ved kjøretøysperren og størrelse/vekt må være definert*
→ *Kjøretøysperrer kan være aktive eller passive*
→ *Kun løsninger og produkter som er testet og godkjent, defineres som kjøretøysperrer. Aktive kjøretøysperrer i henhold til en internasjonal standard (fortrinnsvis den britiske PAS 68 eller IWA 14-1.) (PAS 69 og IWA 14-2 forklarer bruk av kjøretøysperrer). Passive kjøretøysperrer kan i unntakstilfeller godkjennes ved beregninger*

Klassifisering
Skalering som angir verdien objektet har i forhold til skadefølger, ved en uønsket hendelse.
→ *En generalisering av sikkerhetslovens definisjon*
→ *Sikkerhetsloven, veileder for objektsikkerhetsforskriften, definerer det som «skalering som angir den sikkerhetsmessige verdien objektet har i forhold til skadefølger ved sikkerhetstruende virksomhet» (sikkerhetsloven § 17a)*

Konsekvensvurdering
Vurdering av de potensielle negative konsekvensene for én eller flere verdier dersom en uønsket hendelse skulle inntreffe.
→ *Fra NS 5830*

Kontrollert område
Ute- eller inneområde som virksomheten eier, bruker eller på annen måte kontrollerer, herunder deler av bygning eller et område rundt virksomheten.
→ *Fra sikkerhetsloven, Forskrift om informasjonssikkerhet § 6-4*
→ *Kontrollert område omgir normalt beskyttet eller sperret område*

Krise
Situasjon med høy grad av usikkerhet og potensielt uakseptable konsekvenser for den entiteten som rammes.
→ *Fra NS 5830:2012*
→ *En krise er en situasjon som truer en entitets kjernevirksomhet og verdier*

Kritisk infrastruktur
Anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner, som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse.
→ *Fra NOU 2006:6 Når sikkerheten er viktigst*

L

Logiske sikringstiltak
Tiltak for sikring av informasjon som lagres eller overføres elektronisk.
→ *Fra NS 5830:2012*

M

Mannhull
Åpning som er stort nok til at en person kan ta seg gjennom.
→ *Skal det sikres mot inntrengning, bør åpninger/hull over 600 cm² sikres*
→ *Ved inntrengningstester anbefales bruk av en ellipseformet kloss på 400 mm x 225 mm med en dybde på 300 mm som måleverktøy*

Menneskelige sikringstiltak
Tiltak som påvirker atferd og reell evne til å bruke teknologiske sikringstiltak, og følge organisatoriske sikringstiltak, samt menneskelige handlinger som utføres for å hindre en uønsket hendelse.
→ *Fra NS 5830:2012*

Monitorering
Avlytting av tale eller avlesing av elektroniske signaler som kommuniseres i eller mellom informasjonssystemer.
→ *Fra sikkerhetsloven § 3, 1. ledd nr. 11*

O

Objekteier
Virksomhet eller person som eier eller på annen måte råder over skjermingsverdig objekt.
→ *Fra sikkerhetsloven § 3, 1. ledd nr. 14*

Objektkartlegging
Kartlegging og beskrivelse av et objekt i en sikkerhetsmessig setting.
→ *Kartleggingen kan omfatte alt som har betydning for sikring av objektet. Herunder organisasjon, formål, beliggenhet, bygningsmasse, verdier, sikringsmål, infrastruktur, fysisk og elektronisk sikring, vakthold og reaksjonsapparat og administrative rutiner som er relevante for analysen*

Områdesikring
Sikring av verdier i området mellom et perimeter og bygninger.

Operativ evne
Evnen til å utføre en bestemt oppgave.
→ *Sier noe om planforberedelser, beredskap, evne, kapasitet, tilgjengelighet, deployerbarhet og utholdenhet*

Organisatoriske sikringstiltak
Skriftlige eller muntlige beskrivelser som regulerer prosesser, rutiner, atferd og/eller anvendelse av andre sikringstiltak.
→ *Fra NS 5830:2012*

Overvåkning
Systematisk og kontinuerlig observasjon av aktiviteter i tilknytning til en verdi for å oppnå en hensiktsmessig situasjonsforståelse.

P

Panserstål
Høyfast stål som har en karakteristisk flytegrense som er høyere enn 420 N/mm².

Passiv kjøretøysperre
Kjøretøysperre bestående av ikke bevegelige elementer.
→ *Passive kjøretøysperrer kan være utplasserte hindringer eller permanente kjøretøysperrer. Det kan være murer, voller, faste pullerter eller betongelementer. Se aktiv kjøretøysperre*
→ *Tilsvarer statisk kjøretøysperre*

Perimetersikring
Barriere som etableres i forbindelse med en eiendomsgrense eller en definert ytre grense rundt et bygg eller en verdi med det formål å markere en avgrensning og hindre uautorisert adgang til området.
→ *Kan bestå av gjerder, porter, bommer, sikringsbelysning, skilting, kjøretøysperrer m.m.*

Pullert
Kjøretøysperre/kjøretøyhinder bestående av en vertikal stolpe forankret i et fundament og utformet for å hindre kjøretøy i å passere.
→ *En pullert kan være aktiv eller passiv*

R

Rans-/overfallssikring
Alarm som kan utløses manuelt ved overfall og ran (angrep).

Reaksjonsstyrke
Personer og enheter som tilkalles for å hindre, avverge eller begrense skadene av en uønsket hendelse.
→ *Mandat, type og bemanning vil avhenge av verdien som skal beskyttes*
→ *Spenner fra vektere til bevæpnet politi eller militære styrker*

Reaksjonstiltak
Tiltak som skal sikre opprettholdelse av objektets funksjonalitet ved en tilsiktet uønsket hendelse, eller sikre forutsetninger for gjenopprettelse av funksjonalitet etter en slik hendelse.
→ *Generalisering av sikkerhetslovens definisjon*
→ *Utrykning fra vakt/vekter/politi*

Reell trussel
Trussel forbundet med en entitet som innehar en kjent intensjon og kapasitet til å true en annen entitets sikkerhet.
→ *Fra NS 5830:2012*

Regulerende effekt
Fysiske barrierer uten tidsforsinkende effekt.
→ *Eksempel: skilting og sperrebånd*

Risiko
1) Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarheter overfor den spesifiserte trusselen.
→ *Fra NS 5830:2012*

2) Uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse.
→ *Fra NS 5814:2008*

Risikoaksept
Risiko som aksepteres av verdieier.

Risikoanalyse
Risikoanalyse består av risikovurdering, samt vurdering av strategier og tiltak.
→ *Fra NS 5831:2014*

Risikobilde
Tidsavgrenset situasjonsbeskrivelse av en entitets risiko.
→ *Fra NS 5830*

Risikohåndtering
Å fatte overveide beslutninger basert på identifisert risiko, med det mål å oppnå en akseptabel grad av risiko.
→ *Fra NS 5830:2012*

Risikovurdering
1) Helhetsvurdering basert på verdivurdering, trusselvurdering og sårbarhetsvurdering, med mål om å angi en entitets risiko i en definert sikringsmessig kontekst.
→ *Fra NS 5830:2012*

2) Samlet prosess som består av planlegging, risikoanalyse og risikoevaluering.
→ *Fra NS 5814:2008*

S

Sabotasje
Tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet, eller tilsiktet uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering.
→ *Fra sikkerhetsloven § 3, 1. ledd nr. 4*

Sannsynlighet
En kunnskapsbasert kvalitativ og subjektiv vurdering av hyppigheten for at en hendelse inntreffer.
→ *Finnes det relevant frekvensbasert datagrunnlag for en tilsiktet uønsket handling, bør dette tas med i vurderingen*
→ *Sannsynlighet angis i en kvalitativ skala. Eksempel: lav – moderat – høy – meget høy*
→ *Generelt kan sannsynlighet vurderes ved hjelp av statistiske metoder om relevant statistikk er tilgjengelig, eller som en ikke-statistisk kunnskapsbasert vurdering dersom det ikke finnes egnet statistisk grunnlag. Kombinasjon av statistisk og ikke-statistisk tilnærming kan også benyttes*

Sentralisering
Konsentrasjon av verdier i få og avgrensede områder for enklere å kunne sikre dem.

Sikkerhet
Reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare.
→ *Fra NS 5830:2012*

Sikkerhetsavstand
Avstand som etableres mellom en trussel og en verdi for å hindre uakseptable konsekvenser for verdien dersom trusselen realiseres.
→ *Benyttes normalt i forbindelse med avstand fra en eksplosivtrussel, for eksempel bilbombe*

Sikkerhetspreg
Synlige sikringstiltak som kan virke avskrekkende for en potensiell trusselaktør.
→ *Kan være reelt eller oppfattet*

Sikkerhetstruende virksomhet
Forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje, terrorisme eller annen kriminalitet, samt medvirkning til slik virksomhet.
→ *Utvidet ift. sikkerhetsloven § 3*
→ *Sikkerhetstruende hendelse – uønsket hendelse tilknyttet sikkerhetstruende virksomhet*

Sikring
Risikohåndtering forbundet med tilsiktede uønskede handlinger.
→ *Fra NS 5830:2012*
→ *Sikringshåndboka benytter begrepet sikkerhet som et overordnet mål eller tilstand, og all aktivitet for å oppnå sikkerhet er sikring*
→ *Sikring omfatter også begrepene beskyttelse og skjerming, som er benyttet i fagkapitler*

Sikring i dybden
Etablering av flere lag med fysiske, elektroniske og administrative barrierer mellom usikret område og de verdiene vi ønsker å sikre.
→ *Sikring i dybden kan bestå av perimetersikring, områdesikring, skallsikring og sikring av soner og objekter*

Sikkerhetsbelysning
Belysning benyttet i en sikringsmessig kontekst.

Sikringsklasse
Beskriver motstandsnivå for en enkelt barriere mot en trussel.
→ *Kategorisering av barrierer i styrkeklasser*

Sikringsmål
Ønsket eller akseptabel tilstand for verdier under eller etter en uønsket hendelse.
→ *Utledet fra NS 5832:2014*

Sikringsnivå
Beskrivelse av en skadegrad som er akseptabel for verdien eller funksjonen.

Sikringsstyrke
Personer og enheter fra politiet eller Forsvaret som har til oppgave å beskytte et objekt mot en mulig eller konkret trussel.
→ *Fra Lovdata: «Instruks om sikring og beskyttelse av objekter», 2012*

Sikringstiltak
Tiltak for å redusere risiko forbundet med tilsiktede uønskede handlinger.
→ *Fra NS 5830:2012*
→ *NKSB fokuserer på fysiske, elektroniske og administrative sikringstiltak*

Sjikane
Fysiske tiltak i en angrepsvei for å redusere hastigheten til et trusselkjøretøy.
→ *Typisk er fysiske sperrer som gjør at et kjøretøy må svinge rundt dem og således ikke kan holde stor hastighet*

Skadevurdering
Vurdering av konsekvenser ved bortfall eller ødeleggelse av en verdi, og skadepotensialet dersom en verdi blir utsatt for en sikkerhetstruende hendelse.

Vurdering av de negative konsekvensene for én eller flere verdier som følge av at en uønsket hendelse har inntruffet.
→ *Fra NS 5830:2012*

Skallsikring
Sikring av virksomhetens ytterste bygningsmessige elementer.
→ *Normalt vil dette være et byggs yttervegger, etasjeskiller, tak, dører, vinduer og lignende, men hvis virksomheten kun har råderett over en del av bygget eller et rom, vil sikringen av en sone, et rom eller område være skallsikringen*

Skjerming
Sikring mot etterretningstrusler og elektromagnetiske effekter.
→ *Skjerming er et fagområde innen sikring*
→ *Omfatter blant annet sikring mot avlytting, stråling, EMP-/HPM-våpen og Tempest*

Skjermingsverdig informasjon
Opplysninger unntatt offentlighet og sikkerhetsgradert informasjon.
→ *Fra «Veileder for objektsikkerhetsforskriften», NSM (2014)*
→ *Omfatter også informasjon som graderes etter beskyttelsesinstruksen*

Skjermingsverdig objekt
Eiendom, områder, bygninger, anlegg, transportmidler, annet materiell eller deler av slik eiendom som kan skade rikets selvstendighet og sikkerhet ved sikkerhetstruende virksomhet.
→ *Fra «Veileder for objektsikkerhetsforskriften», NSM (2014)*

Sonesikring
Sikring i dybden innenfor en skallsikring.
→ *Romsikring er variant av sonesikring*

Sperret område
Område hvor adgang gir direkte tilgang til sikkerhetsgradert informasjon.
→ *Fra sikkerhetsloven, Forskrift om informasjonssikkerhet § 6-6*
→ *Sperret område kan være arkiv, operasjonsrom, kommunikasjonsrom eller serverrom*
→ *Beskrivelse av et sperret område må angi hvilket graderingsnivå det skal gjelde for*

Spionasje
Innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt.
→ *Fra sikkerhetsloven § 3, 1. ledd nr. 3*

Styrkebeskyttelse
Tiltak og midler som benyttes for å redusere sårbarheten til eget personell, infrastruktur, materiell, operasjoner og aktiviteter for å sikre egen handlefrihet og operativ effektivitet.
→ *Opprinnelig et engelsk militært uttrykk: Force protection*

Sårbarhet
Forhold som reduserer eller begrenser en entitets evne til å motstå en uønsket hendelse, eller til å opprette ny stabil tilstand dersom en verdi er blitt ødelagt, kompromittert, forstyrret eller på annen måte utsatt for uønsket påvirkning.
→ *Fra NS 5830:2012*

Sårbarhetsvurdering
Vurdering av en entitets sårbarheter overfor identifiserte trusler.
→ *Fra NS 5830:2012*
→ *Aktuelle trusler identifiseres i en trusselvurdering*
→ *I hvilken grad det er mulig for ulike trusselaktører å utføre uønskede handlinger uten å bli stanset eller påvirket*

T

Teknologiske sikringstiltak
Samlebegrep for fysiske, elektroniske og logiske sikringstiltak.
→ *Fra NS 5830:2012*
→ *Logiske sikringstiltak behandles ikke i Sikringshåndboka*

Tempest
Elektromagnetisk stråling fra elektronisk utstyr som utilsiktet kan forårsake at uvedkommende kan få tilgang til sikkerhetsgradert informasjon, samt undersøkelser og analyser knyttet til dette fenomenet.
→ *Ordet Tempest er ingen forkortelse eller akronym, men et kodeord som er brukt på fenomenet siden 1950-tallet*
→ *Tempest dekker både metoder for å spionere på andre og hvordan du kan beskytte utstyr mot slik spionasje*
→ *Mange spesifikasjoner i forhold til Tempest er sikkerhetsgraderte*
→ *Ugraderte informasjonssystemer kan også sikres mot kompromitterende elektromagnetisk stråling etter samme overordnede prinsipper*

Terrorisme/terrorhandlinger
Ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål.
→ *Fra sikkerhetsloven § 3, 1. ledd nr. 5*

Tidsregnskap
En utregning for å se på motstandstiden i de fysiske sikringstiltakene i forhold til når angrepet detekteres, og hvor lang utrykningstid reaksjonsapparatet har.
→ *For å oppnå balansert sikring, må man ha positivt tidsregnskap.*

Forts. neste side →

→ Forts.

Positivt tidsregnskap
Sikringskonsept hvor kombinasjonen av barriere, deteksjons-/verifikasjonstiltak og reaksjonsapparat forhindrer tap av verdier.
→ *T1 > T2+T3*
→ *T1 – tiden det tar å forsere alle sikringstiltakene*
→ *T2 – tiden fra angrepet starter, til det detekteres*
→ *T3 – tiden det tar for utrykningsapparatet fra varsling til de når frem til verdiene*

Tilsiktet uønsket hendelse
Uønsket hendelse som forårsakes av en aktør som handler med hensikt.
→ *Fra NS 5830:2012*

Trussel
Mulig uønsket handling som gir en negativ konsekvens for en entitets sikkerhet.
→ *Fra NS 5830:2012*
→ *Trusselaktøren kan være ukjent*

Trusselaktør
Entitet som forbindes med en trussel.
→ *Fra NS 5830:2012*

Trusselbilde
Tidsavgrenset beskrivelse av identifiserte trusler mot en bestemt entitet.
→ *Fra NS 5830:2012*

Trusselnivå
Beskrivelse av trusselaktør med motiv og erfaring, samt disponible verktøy og modus operandi.
→ *Innenfor de enkelte trusselområder (spionasje, sabotasje, terrorhandlinger og annen kriminalitet) defineres det fire trusselnivåer (Alfa, Bravo, Charlie og Delta)*

Trusselvurdering
Beskrivelse av en entitets trusselbilde og en vurdering av trusselaktørenes intensjon og kapasitet.
→ *Fra NS 5830:2012*

U

Utilsiktet handling
En handling utført uten hensikt.
→ *For eksempel en ulykke*

Utrykningsstyrke
Se Reaksjonsstyrke.

Uønsket hendelse
Hendelse som kan medføre ødeleggelse, kompromittering, forstyrrelse av eller på annen måte utsette en verdi for uønsket påvirkning.
→ *Fra NS 5830:2012*

V

Veisperre
Aktiv kjøretøysperre bestående av en platekonstruksjon forankret i et spesifisert fundament og utformet for å hindre kjøretøy i å passere.
→ *Fra engelsk «road blocker»*

Verdi
Ressurs som hvis ødelagt, kompromittert, forstyrret eller på annen måte utsatt for uønsket påvirkning, vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen.
→ *Fra NS 5830:2012*
→ *Verdier kan for eksempel være liv og helse, infrastruktur, informasjon, operativ evne eller penger/gjenstander*

Verdivurdering
1) Kartlegging og rangering av en entitets verdier.
→ *Fra NS 5830:2012*

2) Identifisering av verdier og vurdering av konsekvenser dersom verdiene fjernes, skades eller ødelegges, for å rangere dem og identifisere hvilke som er så viktige at de må sikres spesielt
→ *Fra «Veiledning i verdivurdering», NSM (2009)*
→ *Formålet med vurderingen er å identifisere hvilke verdier som er de viktigste for virksomhetens oppdrag og leveranser*
→ *Virksomheten skal utføre verdivurderingen på en systematisk måte ved å vurdere hvilke konsekvenser det kan få dersom verdiene skulle rammes*

Verifikasjonstiltak
Tiltak som tar sikte på å etablere en situasjonsforståelse hvis en sikkerhetstruende hendelse inntreffer.
→ *Tiltakene skal ha som formål å kunne identifisere og avdekke aktører, identifisere skadeomfang og identifisere de midler som eventuelt er anvendt av en aktør*

Villedning
Tiltak for å forlede en motstander gjennom manipulasjon, forvrengning og forfalskning av informasjon til å handle kontraproduktivt i forhold til egen interesse.

FORKORTELSER

AAK
Automatisk adgangskontroll.
→ *Anlegg som kontrollerer og regulerer adgangen til et område*

AIA
Automatisk innbruddsalarmanlegg.
→ *Anlegg som detekterer og varsler dersom barrierer brytes eller angripes*

BFF
Beredskapssystem for Forsvaret.

C-IED
Counter Improvised Explosive Devices.
→ *Beskriver hele bredden av offensive og defensive innsatsområder for å hindre en aktør eller organisasjon i å oppnå ønskede effekter ved bruk av IED*

CBRN
Fellesbetegnelse på kjemiske toksiske stoffer (C), biologiske agens (B), som omfatter mikroorganismer eller giftstoffer av biologisk opprinnelse – toksiner), radioaktive stoffer (R) og kjernefysiske ladninger (N), som kan forårsake tap av liv eller skade på helse, miljø og materielle verdier.
→ *Fra Forsvarets fellesoperative doktrine*
→ *Et samlebegrep som brukes internasjonalt og er basert på de engelskspråklige begrepene Chemical, Biological, Radiological og Nuclear*
→ *CBRNe: i noen tilfeller tas det med en liten «e» for mindre eksplosiver*

CCA
Contamination Control Area.
→ *Område for inn- og utpassering mellom rent og forurenset område*

DSB
Direktoratet for samfunnssikkerhet og beredskap.

EBA
Eiendom, bygg og anlegg.
→ *Fra Sikringshåndboka 2005*

EK
Elektronisk krigføring.

EMC
Electromagnetic compatibility, norsk elektromagnetisk kompatibilitet.
→ *Elektronisk utstyr ved siden av hverandre skal ikke forstyrre hverandre*

EMI
Elektromagnetisk interferens.
→ *Forstyrrelser fra brytere og annet elektrisk utstyr*

EMP
Elektromagnetisk puls.
→ *Radiobølgepuls fra kjernefysiske våpen, spesialvåpen, lyn eller andre elektriske utladninger*
→ *Bokstaver foran angir kilde til strålingen eller andre egenskaper (lyn – LEMP, non-nuclear – NNEMP, high altitude – HEMP etc.)*
→ *Effekten av en EMP kan være alt fra forstyrrelser til ødeleggelser av kretser i elektronisk utstyr*

FFI
Forsvarets forskningsinstitutt.

FG
Forsikringsselskapenes Godkjennelsesnemnd.

HPEM
High power electromagnetics.

HPM
High Power Microwave.
→ *Ofte brukt generelt om radiofrekvente våpen. I litteraturen beskrives det som «smalbandet stråling»*
→ *NSM: En variasjon av EMP med retningsdirigert kapasitet*

IED
Improvised explosive device.
→ *En innretning som er plassert eller fabrikkert på en improvisert måte, som inneholder ødeleggende, dødelige, skadelige, pyrotekniske eller ildspåsettende kjemikalier, og som er designet for å ødelegge, uskadeliggjøre, forstyrre eller distrahere*

IEMI
Intentional EMI.
→ *Stråling som har til hensikt å forstyrre/ødelegge*

IR
Infrarød.
→ *Infrarød (IR) stråling er elektromagnetisk stråling av bølgelengder lengre enn synlig lys, men kortere enn mikrobølger. I sikringssammenheng benyttes IR-stråling i nattsyn-utstyr for bruk ved utilstrekkelig synlig lys og alarmdetektorer (se PIR). Strålingen detekteres og omgjøres til et bilde på en skjerm. Varme objekter fremtrer lysere og gjør det mulig å operere mer effektivt i mørke*

MTO
Menneskelige, teknologiske og organisatoriske (sikringstiltak).
→ *Brukes ved gruppering av sikringstiltak*
→ *Begrepene er forklart under definisjoner*

NBS
Nasjonalt beredskapssystem.

NKSB
Nasjonalt kompetansesenter for sikring av bygg.

NSM
Nasjonal sikkerhetsmyndighet.

PIR-detektor
Passiv infrarød detektor.
→ *En elektronisk detektor som registrerer infrarød stråling/varmestråling fra alle typer objekter og reagerer på varme i bevegelse*

POD
Politidirektoratet. Forvaltningsorgan under Justis- og beredskapsdepartementet og øverste ledelsesnivået i politiet.

PST
Politiets sikkerhetstjeneste.

RFV
Radiofrekvente våpen.
→ *Våpen basert på radiostråler*

SK
Sikringsklasse definert i Sikringshåndboka.

TVO
TV-overvåkningsanlegg.
→ *Anlegg som bildeovervåker et definert område. Bilder kan også lagres og/eller overføres. Kan også kombineres med AIA – bevegelse i bilde medfører alarm*

UWB
Ultra wide band.
→ *Korte pulser med bredt frekvensinnhold*

VBIED
Vehicle-borne improvised explosive device.
→ *Eksplosiver fraktet med kjøretøy*
→ *Ofte kalt bilbombe*

Vedlegg

Sikringsklasser

Summen av sikringstiltak er avgjørende for hvilket sikringsnivå som oppnås mot dimensjonerende trussel.

For å kunne anslå den samlede effekten av sikringstiltakene er det nyttig å kunne bestemme effekten av hver enkelt barriere. Sikringshåndboka benytter sikringsklasser for fysiske og elektroniske barrierer, som kort forklart kategoriserer barrierer i «styrkeklasser».

Sikringsklasser ble primært innført i første utgave av Sikringshåndboka for å dokumentere balansert sikring ved positivt tidsregnskap. Dette innebærer at summen av innbruddstid til deteksjon og tiden det tar før reaksjonstiltak virker, er mindre enn summen av tiden vunnet ved fysiske hindringer som angriper må forsere for å nå verdien. Sikringsklasser kan også benyttes for å definere motstandsklasser til barrierer mot andre trusler enn inntrengning, se relevante kapitler i ***del 3, Metoder for sikring.***

Det er viktig på være oppmerksom på at dette er NKSB sine anbefalinger. I enkelte tilfeller vil våre krav innenfor en sikringsklasse være strengere i forhold til motstandsklasse i standarder.

Sikringklasse brukes for å dokumentere at et sikringnivå er oppnådd. Sikringklasser kan kobles til motestandsklassene i relevante standarder. Dette er nyttig ved anskaffelse av sikringsprodukter.

Sikringsklasser AAK

Sikringsklasse	Beskrivelse/krav
1	**En adgangskontroll basert på en låst dør:** → Med kodetastatur → Med enkel kortleser (offline)
2	**Et adgangskontrollbasert system som:** → Basert på bruk av adgangskort eller ID-kort med PIN-kode
3	**Et automatisk adgangskontrollanlegg (AAK) som:** → Skal benytte adgangskort med foto og bruk av PIN-kode → Alle sentraler, dørkontroller, koplingsbokser og kortlesere skal ha sabotasjealarm → Har adgangskontroll med hendelses- og systemlogg → Overvåket overføring av alarmer til en sentral enhet → Sentralstyrt database med tilgang- og nivåstyring → Autonomt uten servertilkopling og lagrer hendelser i eget internt minne. Alle loggføringer og databaser har automatisk backup til annen ekstern enhet. Systemet skal automatisk overføre alle logger til server når kommunikasjon reetableres Utføres minimum iht. NEK EN 50133
4	**Et automatisk adgangskontrollanlegg (AAK) som:** → Skal benytte adgangskort med foto og bruk av PIN-kode → Alle sentraler, dørkontroller, koplingsbokser og kortlesere skal ha sabotasjealarm → Feil kode på kortleser skal varsles → Har adgangskontroll med hendelses- og systemlogg → Overvåket overføring av alarmer til en sentral enhet som reagerer på alarm → Sentralstyrt database med tilgang- og nivåstyring → Autonomt uten servertilkopling og lagrer alle hendelser i eget internt minne. Systemet skal automatisk overføre alle logger til server når kommunikasjon reetableres → Alle loggføringer og databaser har automatisk backup til annen ekstern enhet → Servere i clusterløsning e.l. og har redundant intern kommunikasjon → Personellsperre for singel inn- og utpassering Utføres minimum iht. NEK EN 50133

Sikringsklasser AIA

Sikringsklassene (SK) for AIA velges ut ifra kravet man har til sikring. Dersom det ikke foreligger spesielle verdier, konsekvenser eller en trussel, kan følgende tommelfingerregel benyttes:

- *SK1 Bolig*
- *SK2 Virksomheter med lavt risikobilde*
- *SK3 Virksomheter med moderat-høyt risikobilde*
- *SK4 Virksomheter med høyt risikobilde*

Sikringsklasse	Beskrivelse/krav
1	→ Minimum NEK EN 50131 Grad 1 → Et system brukt under de premisser hvor potensielle inntrengere har liten kunnskap om alarmsystemer og et begrenset utvalg av lett tilgjengelig verktøy.
2	→ Minimum NEK EN 50131 Grad 2 – ATS 4[2] → Et system som normalt benyttes der et sofistikert angrep ikke er overhengende sannsynlig. Inntrengere er ventet å ha begrenset kunnskap om alarmsystemer, og har kun basisverktøy og bærbare instrumenter. → Det tillates å benytte kortleser tilknyttet AAK (min. SK2) for å styre alarmområder.
3	→ Minimum NEK EN 50131 Grad 3 – ATS 4[2] → Et system som tilbyr sikkerhet mot inntrengere som er fortrolig med AIA-systemer og har betydelig mengde verktøy og transportabelt elektronisk utstyr tilgjengelig for å sabotere dem. → Det tillates å benytte kortleser tilknyttet AAK (min. SK3) for å styre alarmområder.[1] → Systemet etableres med grafisk fremstilling av alarmer på kart/plantegning for å raskere kunne lokalisere alarm, og mulighet for tilknytning i felles presentasjonssystem med AAK og/eller TVO.
4	→ Minimum NEK EN 50131 Grad 3 – ATS 6[2] → Anvendelse for et system hvor sikkerheten er den viktigste faktoren. → Skal sikre mot en inntrenger som har planlagt angrepet i detalj, har meget stor kompetanse og avansert utstyr til sabotasje av AIA. Systemet suppleres med andre omfattende fysiske tiltak og sikkerhetsprosedyrer. Alle utvendige kabler skal legges i stålrør. → Minimum 2 ulike teknologier for overføring av alarm. → Systemet etableres med grafisk fremstilling av alarmer på kart/plantegning for å raskere kunne lokalisere alarm, og mulighet for tilknytning i felles presentasjonssystem med AAK og/eller TVO.

[1]Dersom dette ikke kommer i konflikt med sikkerhetslovens bestemmelser.
[2] ATS = Alarmoverføringssystem (deles i 6 klasser). ATS blir beskrevet som en kombinasjon av 5 parametere:
D: Overføringstid (klasse)
T: Rapporteringsintervall
M: Overføringstid (maksimum)
S: Sikkerhet mot utskiftning
I: Informasjonssikkerhet

Sikringsklasser for dører og glass i dører

Sikringsklasse	NS-EN 1627: 2011 Gjeldende standard	NS-EN 3170: 1992 Utgått standard	NS-EN 1143-1:2012 Gjeldende standard	NS-EN 1627: 2011 Gjeldende standard
1	1	–	–	P6B
2	2	1	–	P7B
3	3	2	–	P8B
4	4	3	–	
5	5	4	I–II	–
6	6	–	II–IV	–
7	–	–	V–VI	–
8	–	–	VII	–

Sikringsklasser elektronisk perimetersikring

Sikringsklasse	Beskrivelse/krav
1	→ System som varsler brudd på perimeteret → Skal kunne indikere hvor/hvilken sone det er foretatt uautorisert adgang → Lokal monitorering
2	→ System som varsler brudd på perimeteret → Skal kunne indikere hvor/hvilken sone det er foretatt uautorisert adgang → Lokal monitorering → Har mulighet for overføring til vakt/alarmstasjon
3	→ System som varsler brudd på perimeteret → Skal kunne indikere hvor/hvilken sone det er foretatt uautorisert adgang → Lokal monitorering → Har mulighet for overføring til vakt/alarmstasjon → Skal kunne samhandle med AIA- og AAK-anlegg → TVO-verifikasjon → Alle sentralkomponenter skal være tilkoplet UPS
4	→ System som varsler brudd på perimeteret → Skal kunne indikere hvor/hvilken sone det er foretatt uautorisert adgang → Minimum to forskjellige teknologier på perimeteret → Lokal monitorering → Har mulighet for overføring til vakt/alarmstasjon. → Skal kunne samhandle med AIA- og AAK-anlegg → TVO-verifikasjon → Har billedoverføring til godkjent alarmstasjon ved alarmsituasjon eller på kommando, som kan lagre video → Skal ha mekanismer som kan hindre en avansert trusselaktør i å sabotere anlegget (krav til plassering av komponenter, skjerming av kabler, etc.) → Alle komponenter skal være tilkoplet nødstrøm og UPS

Sikringsklasser for gitter

Sikringsklasse	Gitter
3	→ Alternativ 1: I henhold til EN 1627, klasse 3 → Alternativ 2: Maskevidde maks 6 x 6 cm, minimum 10 mm rundjern eller tilsvarende Skjøter skal være sveisede
4	→ Alternativ 1: I henhold til EN 1627, klasse 4
5	→ I henhold til EN 1627, klasse 5
6	→ I henhold til EN 1627, klasse 6

Sikringsklasser gjerder

Sikringsklasse	Beskrivelse/krav
1	→ Et hvilket som helst gjerde. → Ingen krav til materialer eller utforming. → Angir visuelt og juridisk en eiendomsgrense. → Har kun en regulerende effekt – ingen tidshindrende effekt.
2	→ Et tradisjonelt flettverksgjerde montert på T-jern som er slått ned i bakken. → Gjerdehøyden skal være minimum 2 meter. → Stolpeavstand maks 2,5 meter. Trådtykkelse min. 2,5 mm. Maskestørrelse maks 50x50mm. Min. hver 3. stolpe settes i betong. → Bør forsterkes med tre eller flere piggtrådrader på toppen, kan forsterkes med kveilehindre m.m. → Gjerdet har i hovedsak en regulerende effekt.
3	→ Sikkerhetsgjerde, minimum 2,5 meter høyt. → Gjerdet bør være testet etter en innbruddsstandard, f.eks. den britiske LPS 1175. → Løsningen bør vurderes av spesialist i forhold til trusselen. Vanligvis sveiset gittergjerde, panelgjerder eller sveiset palisandergjerde med hensiktsmessig maskestørrelse, spiletykkelse og -avstand. → Kan forsterkes med piggtrådrader på toppen, kveilehindre m.m.
4	→ Et dobbelt gjerde med minimum et klasse 2-gjerde som ytterste gjerde, og et klasse 3-gjerde som innerste gjerde. → Mellom gjerdene bør det være et deteksjons- og overvåkningssystem. → Begge gjerdene bør utstyres med minst tre rader piggtråd på toppen.

Sikringsklasser for innbruddshemmende vinduer

Sikringsklasse	NS-EN 1627: 2011 Gjeldende standard (minimumskrav)	NS-EN 356: 1999 Sikkerhetsglass (minimumskrav)
1	1	→ P6B
2	2	→ P7B
3	3	→ P8B
4	4	
5	5	→ Glass skal ikke benyttes i sikringsklasse 5–8
6	6	

For at vindu skal oppnå respektiv sikringsklasse, skal både minimumskrav i tabellen til RC-klasse iht. NS-EN 1627 og minimum klasse iht. NS-EN 356 for glass som oppgitt i tabellen, oppfylles. Merk at det her er stilt strengere krav til klasse på glasset enn det som følger av standarden NS-EN 1627. Dette er begrunnet i tester gjennomført av Forsvarsbygg.

Sikringsklasser med innbruddstider – fysisk sikring

2016	Trusselaktør				Sikringsklasser i Sikringshåndboka 2005
	A	B	C	D	
1	5 minutter*	1 minutt*	1 minutt*	Oppgis ikke	–
2	10 minutter	5 minutter	3 minutter	Oppgis ikke	–
3	15 minutter	10 minutter	5 minutter	Oppgis ikke	1
4	30 minutter	20 minutter	15 minutter	Oppgis ikke	2
5	90 minutter	30 minutter	20 minutter	Oppgis ikke	3
6	**	50 minutter	Oppgis ikke	Oppgis ikke	4 og 5
7	**	Oppgis ikke	Oppgis ikke	Oppgis ikke	6 og 7
8	**	**	Oppgis ikke	Oppgis ikke	8

* Det er svært kort innbruddstid for sikringsklasse 1, og det er vanskelig å definere noen eksakt tid.
** Det er lite trolig at en inntrenger i denne kategorien med verktøy som beskrevet for aktuell kategori, vil klare å forsere sikringstiltakene innen rimelig tid.

Sikringsklasser for kjøretøysperrer

Sikringsklasse	Beskrivelse/krav
1	→ En kjøretøyhindring som er etablert ved bruk av sperrematerieller som kråkeføtter, betongklosser eller lignende. → Avskrekkende effekt. → Vil ofte kunne stoppe mindre kjøretøy i lave hastigheter, men dette kan ikke garanteres.
2	→ En enkel linje med passive og aktive kjøretøysperrer dimensjonert for å stoppe trusselkjøretøyet i en definert hastighet. Det må besluttes hvilket kjøretøy som skal stoppes (personbil, liten lastebil, m.m.), og hvilken hastighet kjøretøyet kan oppnå (50, 60, 80 km/t). → (Single line of Vehicle Security Barriers (VSBs))
3	→ En enkel linje med passive kjøretøysperrer og de aktive kjøretøysperrer suppleres med en sluseløsning. → En adgangskontroll i form av bom eller lignende før man kommer frem til den aktive kjøretøysperren. → (Final denial VSBs)
4	→ En enkel linje med passive kjøretøysperrer og sluseløsninger med aktive og passive kjøretøysperrer. → (Interlocked VSBs)

Sikringsklasser for låsenheter

Sikringsklasse	Låser
0	→ Ingen krav til godkjente låsenheter.
1	→ FG-godkjent låsenhet.* (Alle komponenter minimum FG-klasse 3)
2	→ Godkjente låsenheter i FG-klasse 3 eller høyere.
3-8	→ Normalt krav knyttet til dør låsen skal stå i. Minimum låsenheter i FG-klasse 3.

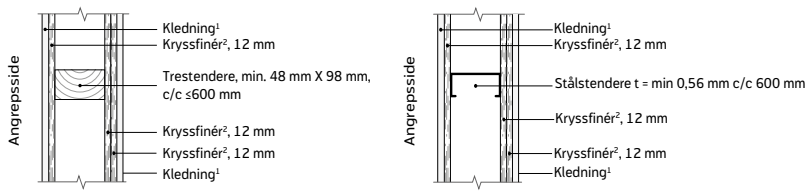
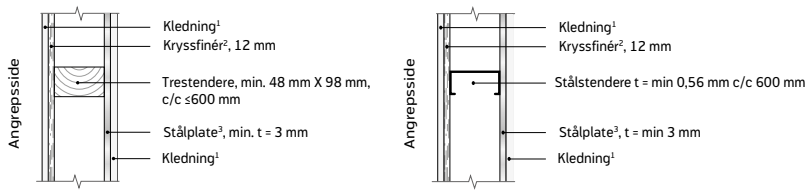
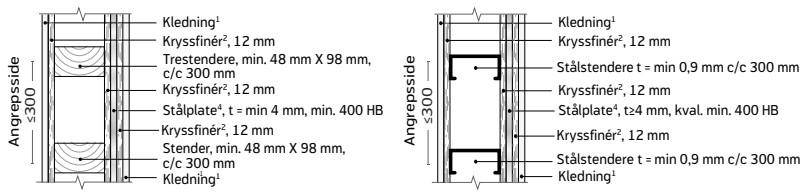
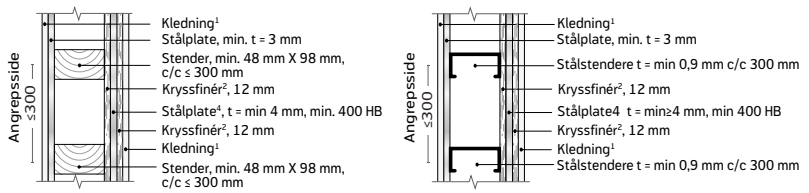
* FG-310:1 (1.9.2012)

Sikringsklasser for massive vegger, tak/gulv

Sikringsklasse	Massive vegger	Tak/gulv/etasjeskiller
1	→ Udefinert yttervegg	→ Tak, gulv, dekker, etasjeskiller skal ha minst samme innbruddsmotstand som vegger. Det er vanligvis minst like god motstandskraft i ordinære etasjeskiller som i veggene opp til klasse 3 (med mindre det er snakk om et trehus). Fra klasse 4 og oppover bør man vurdere forsterking også av etasjeskiller.
2	→ 150 mm massiv lettklinker utført og armert etter produsentens anvisning.	
3	→ 250 mm lettklinker utført og armert etter produsentens anvisning.	
4	→ 150 mm enkeltarmert*	
5	→ 180 mm dobbeltarmert*	
6	→ 200 mm dobbeltarmert betong*	
7	→ 300 mm dobbeltarmert betong*	
8	→ 500 mm dobbeltarmert betong*	

* Min. betongkvalitet B30, maks 150 mm senteravstand for armering.

Sikringsklasser for sammensatte vegger

Sikringsklasse	Sammensatte vegger	Tak/gulv/etasje-skiller
1	→ Ikke spesifisert. SK 3 kan benyttes.	Tak, gulv, dekker, etasjeskiller skal ha minst samme innbruddsmotstand som vegger.
2	→ Ikke spesifisert. SK 3 kan benyttes.	
3		
4		
5		
6		
7	→ Ikke spesifisert. Prosjekteres særskilt.	
8	→ Ikke spesifisert. Prosjekteres særskilt.	

1. F.eks. 12 mm gips eller sponplate. Innfestet iht. Byggforsk/produsentens anvisning
2. Innfestet iht. Byggforsk/produsentens anvisning
3. Innfestet med min. 4 mm skruer c/c t ≤ 200 mm
4. Innfestet med min. 4 mm skruer c/c t ≤ 200 mm i både tre- og stålstendere
5. Samlet tykkelse, f.eks. 22 mm + 12 mm

Sikringsklasser TVO

Sikringsklasse	Beskrivelse/krav
1	**Krav til TV-overvåkningsanlegg (TVO) som:** → Kun har lokal monitorering og lagring
2	**Krav til TV-overvåkningsanlegg (TVO) som:** → Har lokal monitorering og lagring → Har mulighet for overføring til vakt/alarmstasjon Skal minimum tilfredsstille NEK EN 62676
3	**Krav til TV-overvåkningsanlegg (TVO) som:** → Har lokal monitorering og lagring → Lokal lagring på redundant løsning → Skal kunne samhandle med AIA- eller AAK-anlegg → Har videooverføring til alarmstasjon ved alarmsituasjon eller på kommando → Har mulighet for videoanalyse eller integrasjon mot analysesystem → Alle sentralkomponenter er tilkoplet UPS → Kameraer og andre nettverksenheter skal varsle ved feil Skal minimum tilfredsstille NEK EN 62676 og NEK EN 50132. Kravspesifikasjon*
4	**Krav til TV-overvåkningsanlegg (TVO) som:** → Har lokal monitorering og lagring → Har lokal lagring på redundant løsning → Skal kunne samhandle med AIA- eller AAK-anlegg → Har kontinuerlig lagring av opptak på sikringsobjektet → Har videooverføring til godkjent alarmstasjon, kontinuerlig, ved alarmsituasjon eller på kommando, som kan lagre video → Skal ha alle mekanismer som kan hindre en avansert trusselaktør i å sabotere anlegget (krav til plassering av komponenter, skjerming av kabler, etc.) → Har mulighet for videoanalyse eller integrasjon mot analysesystem → Alle komponenter er tilkoplet nødstrøm og UPS → Kameraer og andre nettverksenheter skal varsle ved feil Skal minimum tilfredsstille NEK EN 62676 og NEK EN 50132. Kravspesifikasjon*

* Nasjonalt kompetansesenter for sikring av bygg har utarbeidet egen kravspesifikasjon. Denne er gradert.

Sikringsklasser reaksjonsstyrker

Sikringsklasse	Beskrivelse
1	→ Eget eller eksternt personell uten spesiell kompetanse og utstyr
2	→ Vektere med kunnskap og utstyr
3	→ Politi eller militær vakt
4	→ Trenede spesialmannskaper fra politiet eller Forsvaret

Vedlegg

Trusselaktører

Aktørene fra ALFA til DELTA innenfor de fire kategoriene oppsummeres på følgende måte:

Nivå		Terrorisme	Etterretning	
ALFA	**Hvem**	→ Enkeltstående personer som styres av irrasjonelle tanker.	→ Enkeltpersoner.	
	Motiv	→ Kan ha et motiv om å skape nasjonal oppmerksomhet om en sak, eller ta hevn for et eller annet forhold.	→ Skaffe kunnskap om potensielle mål for kriminelle handlinger og/eller økonomisk gevinst.	
	Erfaring	→ Ingen spesiell.	→ Liten eller ingen erfaring.	
	Verktøy	→ Stikk-, slag- og skytevåpen.	→ Ingen avanserte verktøy.	
	MO	→ Har ikke nødvendigvis kunnskap om objektet hvor aksjonen gjennomføres. Kan være handlinger uten særlig planlegging i forkant, herunder trusler, ofte i affekt.	→ Benytter åpne kilder på Internett, karttjenester, eiendomsinformasjon og lignende for å kartlegge informasjon om virksomheten.	
BRAVO	**Hvem**	→ Enkeltstående personer, ofte med tidligere eller eksisterende tilknytning til målet.	→ Enkeltpersoner eller grupper.	
	Motiv	→ Kan ha et motiv om å skape nasjonal oppmerksomhet om en sak, eller ta hevn for et eller annet forhold.	→ Skaffe opplysninger om verdier og sikkerhetsopplegg rundt verdiene, kartlegge personer/virksomheter.	
	Erfaring	→ Ingen spesiell, men kan ha kunnskaper om våpenbruk og lignende pga. tidligere virksomhet, eller skaffer seg kunnskaper fra Internett, litteratur eller lignende.	→ Kan ha kriminell erfaring. Kunnskap om enkle spionasjemetoder.	
	Verktøy	→ Sprengstoff, hjemmelagde bomber, brevbomber, skyte-, stikk- og slagvåpen, kjemikalier eller trusler om bruk av forannevnte.	→ Enkelt avlyttingsverktøy, fotoapparat.	
	MO	→ Forsøker å skade spesiell person(er) eller tilfeldige personer, enten direkte ved egen tilstedeværelse (skyte-, stikk- og slagvåpen, kjemikalier), eller indirekte ved bruk av brevbombe eller utplassering av sprengstoff.	→ Observasjon/fotografering fra nærområdet. Benytter andre åpne kilder som for eksempel byplankontor (tegninger over bygg) og lignende.	

	Sabotasje	Kriminalitet
	→ Enkeltpersoner eller grupper.	→ En tilfeldig leilighetstyv. Ungdommer på jakt etter spenning, narkomane på jakt etter et lett bytte, personer som blir inspirert av en oppdukkende mulighet.
	→ Ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet som en politisk markering ifm. demonstrasjoner eller lignende.	→ Skaffe penger eller lett omsettelige varer. Er fornøyd med «småpenger».
	→ Ingen spesiell.	→ Liten eller begrenset.
	→ Stein (kasting), molotovcocktails, slagvåpen, håndverktøy, improviserte våpen.	→ Lett mekanisk verktøy: skrutrekker, lite brekkjern, avbitertang og lignende.
	→ Kan delta i organiserte demonstrasjoner som kommer ut av kontroll, for eksempel ifm. aksjoner mot utbygging, alliert/nasjonal øvingsaktivitet eller lignende.	→ Inspireres av muligheter som oppstår der og da. (For eksempel åpen/dårlig sikret dør eller vindu.) Velger angrepsmål som synes attraktive og dårlig sikret. Opererer ofte alene, eller to og to/tilfeldige grupper. Vil flykte dersom de oppdages. Er sannsynligvis ikke bevæpnet.
	→ Representanter for nasjonale/internasjonale, ikke-statlige grupper.	→ En kriminell person/personer.
	→ Ødelegge eller skade en virksomhet, eller som en forberedelse til annen kriminell handling.	→ Skaffe penger, våpen/utstyr eller lett omsettelige varer. Tar ikke risiko for «småpenger».
	→ Kan ha innsikt i sabotasjeteknikker. Ofte kriminell erfaring. Kan ha militær erfaring.	→ Har en viss kriminell erfaring. Har antakelig sittet i fengsel, og der lært visse elementære kriminelle teknikker av mer erfarne kriminelle. Har erfart nødvendigheten av å kjenne målet på forhånd.
	→ Tyngre mekanisk utstyr som slegge, spett og lignende, lett elektrisk verktøy som vinkelsliper, tigersag, sirkelsag og lignende.	→ Tyngre mekanisk utstyr som slegge, spett og lignende, lett elektrisk verktøy som vinkelsliper, tigersag, sirkelsag og lignende.
	→ Benytter ulike typer verktøy som slegge o.l. for å sabotere virksomheten, eller for å forberede en kriminell handling. Kan bryte seg inn i virksomheten for så å ødelegge verdier.	→ Vil som minimum befare objektet og objektets nærmiljø før et angrep. Velger angrepsmål som synes attraktive og dårlig sikret. Opererer alene, eller to og to/tilfeldige grupper. Har en løs plan for gjennomføring av angrepet og for flukt etter angrepet. Vil flykte dersom de blir oppdaget. Kan være bevæpnet.

Forts. neste side →

forts. **Trusselaktører i kategoriene ALFA til DELTA**

Nivå		Terrorisme	Etterretning	
CHARLIE	**Hvem**	→ Enkeltpersoner eller grupper inspirert av internasjonale grupper.	→ Personer tilknyttet kriminelle nasjonale/internasjonale organisasjoner.	
	Motiv	→ Skape nasjonal oppmerksomhet om en sak. Ødeleggelse av nasjonale symboler, skade personer og ta menneskeliv.	→ Skaffe kunnskap om konkrete virksomheter for kriminelle handlinger eller til bruk for fremmede stater.	
	Erfaring	→ Liten, men kan ha kunnskaper om våpenbruk og sprengstoff fra Internett, litteratur eller lignende.	→ Har betydelig erfaring fra tilsvarende aksjoner. Behersker avanserte teknikker.	
	Verktøy	→ Sprengstoff, hjemmelagde bomber, brevbomber, skytevåpen, kjemikalier, trusler om bruk av forannevnte.	→ Har tilgang på avansert verktøy for avlytting/avtitting. Kan også benytte avansert innbruddsverktøy.	
	MO	→ Aktør(er) eller samarbeidende team har kartlagt objektet på forhånd. Benytter ulike type våpen. Kan skade personer og ta menneskeliv.	→ Skaffer seg på forhånd kunnskap om objektet som skal angripes. Benytter gjerne en tredjeperson som med eller uten egen viten hjelper med å avdekke lokale forhold, utplassere utstyr e. a., gjerne ifm. trusler. Planlegger operasjonen i detalj.	

	Sabotasje	Kriminalitet
	→ Agenter for fremmede makter.	→ Kriminelle personer, godt organisert.
	→ Ødelegge/skade militær eller sivil kapasitet.	→ Skaffe penger, våpen/utstyr eller lett omsettelige varer. Er ute etter «store penger».
	→ Utdannelse i sabotasjeteknikker. Har gjerne lokalkunnskap.	→ Betydelig kriminell erfaring. Har deltatt i kriminelle angrep mange ganger før. Kan betegnes som profesjonell. Vet at det er nødvendig med kunnskaper om sikringstiltak på målet og rutiner ifm. vakthold og lignende.
	→ Håndvåpen, sprengstoff, HPM-våpen, BC-våpen.	→ Et bredt sett av mekanisk verktøy, alle typer av elektrisk-, gass- og skjæreverktøy. Kan i noen tilfeller dirke vanlige låser.
	→ Gjennomføres i en krise-/krigssituasjon, eller i opptakt til dette. Har opplysninger/god kunnskap om målobjektet fra tidligere spionasje. Kan være «innsider». Utføres fortrinnsvis på en måte som gir mulighet for at aksjonsgruppen kan komme uoppdaget fra aksjonen. Det kan være en målsetting at ødeleggelse/skade i første omgang ikke avsløres som sabotasje. Anslag mot personell kan skje på bopel, under transport eller på tjenestested. Kan benyttes til mindre viktige mål enn S-D.	→ Kartlegger objektet i forkant av operasjonen, gjerne i lang tid. Planlegger angrepet i detalj. Angrepet er motivert av å skaffe utstyr til bruk i kriminell virksomhet eller å skaffe penger eller andre lett omsettelige verdier. Kan benytte informanter/innsidere som verves på forhånd, eller trues/presses, eller som lures til å gi fra seg informasjon om angrepsobjektet. Kan benytte seg av avledende manøvrer. Kan benytte seg av trusler/gisseltaking for å tiltvinge seg adgang/opplysninger. Har en detaljert plan for gjennomføring og flukt. Kan forventes å benytte våpen aktivt for å gjennomføre sitt forsett.

Forts. neste side →

forts. **Trusselaktører i kategoriene ALFA til DELTA**

Nivå		Terrorisme	Etterretning	
DELTA	**Hvem**	→ Internasjonale aktører/organisasjoner.	→ Agenter fra militær/statlig etterretningstjeneste.	
	Motiv	→ Skape stor internasjonal oppmerksomhet, destabilisering og frykt, påvirke norsk opinion/myndigheter.	→ Skaffe sikkerhetsgraderte dokumenter eller materiell og/eller utplassere avlyttings-/overvåkningsutstyr, kartlegge personer/virksomheter.	
	Erfaring	→ Opplæring i utenlandske treningsleire eller militær/politi utdanning og erfaring.	→ Betydelig erfaring og spesialutdannelse innen spionasje, teknikker og psykologi. Social engineering.	
	Verktøy	→ Sprengstoff, hjemmelagde bomber, kjøretøybomber, brevbomber, skytevåpen, kjemikalier, trusler om bruk av forannevnte.	→ «State of the art-verktøy», dirkeverktøy, verktøy/utstyr for å sabotere sikrings- og kommunikasjonssystemer, avlyttingsverktøy.	
	MO	→ Samarbeidende team har kartlagt objektet på forhånd. Ønsker spektakulære aksjoner som skaper stor frykt, gjerne mange døde og skadede. Går etter store personansamlinger, objekter som kan forsterke virkningene av primæraksjonen (for eksempel drivstoff-gasstanker og lignende), objekter med symbolverdi. Ofrer gjerne eget liv.	→ Skaffer seg på forhånd inngående kunnskap om objektet som skal angripes, benytter gjerne en tredjeperson som med eller uten egen viten hjelper med å avdekke lokale forhold, utplassere utstyr e.a. Planlegger operasjonen i detalj. Legger stor vekt på å ikke bli oppdaget under aksjonen.	

	Sabotasje	Kriminalitet
	→ Militære spesialstyrker.	→ Internasjonale organiserte bander, ofte med bakgrunn fra militære stridende styrker og lignende. Kan ha bakgrunn fra spesialstyrker.
	→ Ødelegge/skade vital militær eller sivil kapasitet.	→ Store økonomiske verdier. Spesielle verdier, som våpen, ammunisjon og militært materiell for salg eller for egne operasjoner.
	→ Spesialutdannelse i alle former for sabotasje, spesialtrening for oppdraget.	→ Erfaring fra voldelig, grov kriminalitet, meget god kunnskap om innbruddsteknikker, bruk av våpen og sprengstoff. Kan ha spesialutdannelse og trening i skjulte operasjoner.
	→ Alle typer verktøy og våpen, for eksempel håndvåpen, rakettvåpen, sprengstoff m.m.	→ Alle mulige verktøy: mekaniske, motoriserte, gass og hydrauliske. Kjøretøy (som rambukk). Sprengstoff.
	→ Gjennomføres i en krise-/krigssituasjon som en militær operasjon med stor profesjonalitet og god planlegging. Har opplysninger om målobjektet fra tidligere spionasje. Av kapasitetsmessige grunner benyttes spesialstyrker kun på spesielt viktige mål.	→ Samler informasjon om objektet i forkant av operasjonen, gjerne i lang tid. Planlegger angrepet i detalj. Benytter ofte informanter/innsidere som verves på forhånd, eller trues/presses, eller som lures til å gi fra seg informasjon om angrepsobjektet. Benytter seg ofte av avledende manøvrer. Har en detaljert plan for gjennomføring av angrepet og for flukt etter angrepet. Kan benytte seg av trusler/gisseltaking for å tiltvinge seg adgang/opplysninger. Legger stor vekt på kraft og hurtighet. Forventes å benytte våpen aktivt for å gjennomføre sitt forsett.

Vedlegg

Verdivurdering

Skjema skadenivå

Skjema til hjelp i vurdering av verdiers viktighet og av skadepotensial ved bortfall av verdier. Benyttes til å fastsette konsekvensnivå, som benyttes i verdivurderingsskjemaet. Konsekvensene må tilpasses den enkelte virksomhet.

Skadenivå	Liv og helse	Nedetid/ operativ evne	
0	→ Ingen personskader	**Ubetydelig nedetid**	
1	→ Få mennesker blir skadet, mindre personskader	**Nedetid under 6 timer**	
2	→ Flere alvorlige personskader	**Nedetid under 1 dag**	
3	→ Mange alvorlige personskader/inntil tre døde	**Nedetid 1 dag–1 uke**	
4	→ Flere enn tre døde	**Nedetid mer enn 1 uke**	

	Informasjon	Økonomi	Omdømme
	→ Kompromittering av **UGRADERT** informasjon eller ikke-sensitiv informasjon	→ Økonomisk tap som ikke skader virksomheten	→ Ingen fare for omdømmetap og liten innvirkning på tillit
	→ Kompromittering av informasjon som i noen grad kan skade virksomheten, eller **BEGRENSET** informasjon	→ Økonomisk tap som i noen grad kan skade virksomheten	→ Omdømme kan skades, noe nasjonal mediedekning, kan redusere tillit
	→ Kompromittering av informasjon som kan skade virksomheten, eller **KONFIDENSIELL** informasjon	→ Økonomisk tap som kan skade virksomheten	→ Omdømme kan alvorlig skades, betydelig nasjonal mediedekning, kan redusere tillit betydelig
	→ Kompromittering av informasjon som alvorlig kan skade virksomheten, eller **HEMMELIG** informasjon	→ Økonomisk tap som alvorlig kan skade virksomheten	→ Omdømme skades alvorlig, internasjonal mediedekning, alvorlig redusert tillit
	→ Kompromittering av informasjon som har helt avgjørende skadefølger for virksomheten, eller **STRENGT HEMMELIG** informasjon	→ Økonomisk tap som har helt avgjørende skadefølger for virksomheten	→ Omdømme uopprettelig skadet, fravær av tillit

Skjema for verdivurdering

SLIK FYLLES SKJEMAET UT				
Funksjon	**Beskrivelse av funksjonen**	**Antall/omfang/behov**	**Bidrag fra**	**Leveranse til**
Betegnelse på funksjon	→ Virksomheten har ansvar for å levere A og B, konsultere med C og videreformidle D og E til F	→ Sett kryss eller angi antall. Angivelse av antall/omfang og behov. Kommenter dersom dette ikke er aktuelt for virksomheten	→ Personell med spesiell kompetanse	→ Underliggende etater → Sektoren → Virksomhetens leder → Andre virksomheter

VERDIER: ULIKE VERDIKATEGORIER				
Verdier grupperes gjerne etter type som spesialrom, IKT-systemer, informasjon osv. på en hensiktsmessig måte for virksomheten. Målet er at det skal være oversiktlig og logisk for de som skal bruke skjemaet.				
Spesialrom	**Spesialrom som er nødvendig for utførelse av funksjonen**	**Antall/omfang/behov**	**Bidrag fra**	**Leveranse til**
→ Operasjonsrom	→ Spesialrom som er nødvendig for utførelse av funksjonen	→ Romnummer (eks. «Rom 210 og 211»)	→ VIP, IKT-systemer (gradert og ugradert), sikringssystemer, skudd-, inntrengnings- og eksplosjonssikrede vegger, vinduer og dører, lydisolering 52 dB, K-skap	→ Etater over og under i kommandokjeden
→ VIP-kontor	→ Kontor med tilfredsstillende sikring for VIP som mulig angrepsmål. Muligheter for at VIP kan tale gradert	→ Romnummer (eks. «Rom 301»)	→ VIP, IKT-systemer (gradert og ugradert), sikringssystemer, skudd-, inntrengnings- og eksplosjonssikrede vegger, vinduer og dører, assistent, mulig livvakt, lydisolering 52 dB, K-skap	→ Effektiv utøvelse av VIP-funksjonen via kommunikasjon til lederskap på nivået over, ledere på samme nivå i andre sektorer/etater/avd., beslutninger nedover i egen organisasjon

	Gradert	Skadenivå	Verdivurdering	Begrunnelse
	→ Sett inn aktuelle graderingsnivåer fra UO-SH	→ Skadenivå fra 1–4, basert på vurdering av skadepotensial og konsekvenser ved bortfall (se eget skjema)	→ Angi klassifisering av verdi fra 1–4, hvorav 1 er lavest og 4 er høyest	→ Kort oppsummert bakgrunnen for angivelse av verdi. Dersom verdivurderingen er høyere/lavere enn skadenivå, begrunn dette

	Gradert	Skadenivå	Verdivurdering	Begrunnelse
	→ Opp til HEMMELIG tale	2 (Nedetid operativ evne)	2	→ Tap av funksjon kan medføre at kommunikasjon mellom etater ikke blir tilfredsstillende løst i krisesituasjoner
	→ Opp til HEMMELIG tale, oppbevaring av KONFIDENSIELL informasjon	3 (Liv og Helse) 2 (Informasjon)	4	→ Tap av VIP-funksjonen kan hindre effektiv ledelse og beslutningstagning

Forts. neste side →

Forts. **Skjema for verdivurdering**

IKT-systemer/ komponenter	**Systemer som understøtter saksbehandling**	**Antall/omfang/behov**	**Bidrag fra**	**Leveranse til**	
→ Server	→ Server for IKT-systemer. Krever spesiell sikring iht. graderingsnivå og kritikalitet	→ Romnummer (eks. «Rom U010») med plass for tre server-rack	→ Egnet rom med tilfredsstillende sikring, nødstrøm, kjøling, drift- og servicepersonell, redundante løsninger	→ Etater over og under i kommando-kjeden	
Tekniske systemer/ støttefunksjoner	**Systemer som understøtter funksjonen**	**Antall/omfang/behov**	**Bidrag fra**	**Leveranse til**	
→ Strømforsyning	→ Både regulær strøm-forsyning og nød-strøm	→ Kontinuerlig strøm-forsyning til prioriterte kurser, UPS som sikrer gapless overføring til aggregat, 24 timers varighet	→ Sivil strøm-leverandør	→ Kurser som dekker operasjonsrom, kritisk IKT, VIP-møterom med VTC, sikringssystemer	
Informasjon		**Antall/omfang/behov**	**Bidrag fra**	**Leveranse til**	
→ Gradert informasjon (skriftlig)	→ Dokumenter som produseres eller mottas, må skjermes med sikringstiltak iht. til graderings-nivå. Krever hjelpe-midler som egnede skap og rom for å sikre dokumentene	→ Store mengder gradert informasjon	→ Overliggende etater, underliggende etater, etater på samme nivå, etater i andre sektorer	→ Overliggende etater, underliggende etater, etater på samme nivå, etater i andre sektorer	
Kommunikasjonsrom/ systemer		**Antall/omfang/behov**	**Bidrag fra**	**Leveranse til**	
Gradert VTC	→ Tale som er gradert, må beskyttes mot avlytting fra tredje-part. Dette krever sikring iht. til grade-ringsnivå	→ Romnummer (eks. «rom nr 210 og 211»)	→ Etater over og under i kommandokjeden, strøm-forsyning, sikringssystemer, personell som kan benytte systemet	→ Etater over og under i kommando-kjeden	

	Gradert	Skadenivå	Verdivurdering	Begrunnelse
	→ Opp til **BEGRENSET**	3 (Informasjon)	3	→ Tap av server for IKT-systemer vil hindre utførelse av saksbehandlingsfunksjonen
	Gradert	**Skadenivå**	**Verdivurdering**	**Begrunnelse**
	→ Nei	4 (Nedetid operativ evne)	4	→ Tap av strømforsyning vil føre til tap av funksjonalitet i operasjonsrom, kritiske IKT-systemer, VIP-møterom med VTC, sikringssystemer
	Gradert	**Skadenivå**	**Verdivurdering**	**Begrunnelse**
	→ Opp til **STRENGT HEMMELIG**	4 (Informasjon)	4	→ Tap av informasjon SH kan få helt avgjørende skadefølger for riket eller alliertes sikkerhet, se sikkerhetsloven
	Gradert	**Skadenivå**	**Verdivurdering**	**Begrunnelse**
	→ Opp til **HEMMELIG**	3 (Informasjon)	2	→ Tap av gradert tale kan føre til kompromittering av informasjon som kan ha betydning for rikets sikkerhet

Forts. neste side →

Forts. **Skjema for verdivurdering**

Servicefunksjoner		**Antall/omfang/behov**	**Bidrag fra**	**Leveranse til**	
→ Vakttjeneste	→ Vakter ved byggene både ved normal-situasjon, ved hevet beredskap og ifm. ulike typer VIP-besøk	→ 20 personer og egnet vaktsentral	→ Vaktpersonell, sambandsutstyr, vaktleder	→ Trygg arbeidsdag for personell, sikker avvikling av VIP-besøk	
Personalet		**Antall/omfang/behov**	**Bidrag fra**	**Leveranse til**	
→ Spesiell kompetanse (fag)	→ Spesialistkompe-tanse som kan være utfordrende å erstatte. Utdanning og erfaring til å kunne utføre enkelte kritiske oppgaver	→ 1 person fra hver avdeling med spesi-ell opplæring i krisehåndtering	→ Gjennomføring av spesiell opplæring	→ Utøvelse av spesi-elle funksjoner ved krise	

	Gradert	Skadenivå	Verdivurdering	Begrunnelse
	→ Nei	2 (Nedetid operativ evne)	3	→ Tap av vakttjenesten vil vanskeliggjøre leveransen av trygt arbeidssted for personell og VIP

	Gradert	Skadenivå	Verdivurdering	Begrunnelse
	→ Nei	3 (Nedetid operativ evne)	3	→ Tap av spesialkompetanse er utfordrende å erstatte, hindre utøvelse av spesielle funksjoner

SIKRINGSHÅNDBOKA

Tittel
SIKRINGSHÅNDBOKA
Håndbok i sikring av eiendom, bygg og anlegg mot terror, sabotasje, spionasje og annen kriminalitet

Utgiver
Utgitt av Forsvarsbygg

Opplag
2. utgave, 1. opplag 3000 eksemplarer
desember 2016
3. opplag 1000 eksemplarer mars 2008
2. opplag 500 eksemplarer oktober 2005
1. utgave 1. opplag 500 eksemplarer 2005

ISBN 978-82-7972-200-7

Kontakt
Forsvarsbygg,
Nasjonalt kompetansesenter for sikring av bygg
Telefon 815 70 400
sikringshandboka@forsvarsbygg.no

Grafisk utforming
Itera Gazette

Foto
Hans Fredrik Asbjørnsen
Side 28, 56, 72, 96, 124, 154, 156, 188, 198, 208, 214, 230, 240, 250, 266, 270, 274
Annichen Piene
Side 10, 24, 42, 64, 96, 274
Forsvarsbygg
Side 116, 117, 133, 162, 170, 223, 224
CPNI
Side 116
Avon
Side 117
iStock
Omslag, side 14, 166

Illustrasjoner
Børre Gammelsrud
Itera/Itera Gazette
Forsvarsbygg

Tekst
Forsvarsbygg,
Nasjonalt kompetansesenter for sikring av bygg

Trykk
Merkur Grafisk AS

Papir
115 g Profimatt/350 Tom&Otto Silk

→ *www.forsvarsbygg.no*

Sikringshåndboka gir kunnskap og råd om hvordan eiendom, bygg og anlegg kan sikres mot terror, sabotasje, spionasje og annen kriminalitet. Boken retter seg mot deg som planlegger, utvikler og iverksetter sikringstiltak. Sikringshåndboka er utarbeidet av Forsvarsbygg ved Nasjonalt kompetansesenter for sikring av bygg.

Nasjonalt kompetansesenter for sikring av bygg (NKSB) er et tverrfaglig miljø som leverer sikkerhetsfaglig rådgivning til byggeprosjekter i forsvarssektoren og staten for øvrig.

9 788279 722007

Forsvarsbygg