

Sikringsteknik

Undervisningsmateriale til Grundlæggende Vagt

SUS, Serviceerhvervenes
Efteruddannelsesudvalg
Konsulent Mogens Sørensen

Januar 2020



© Børne- og Undervisningsministeriet (Januar 2020). Materialet er udviklet af Serviceerhvervenes Efteruddannelses-udvalg i samarbejde med Konsulent Mogens Sørensen. Materialet kan frit kopieres med angivelse af kilde.

Illustrationer/fotos uden anden angivelse af ophavsret, er udviklerens egne eller fra gamle SUS materialer.

SUS

Serviceerhvervenes Efteruddannelsesudvalg

Vesterbrogade 6D, 4.

1620 København V.

Tlf. 32 54 50 55

www.susudd.dk

sus@sus-udd.dk



Indholdsfortegnelse

Indledning	5
Forsikringsvilkår	5
Sikringsniveauer	6
Den maksimale reaktionstid	7
Gennemsnitlige reaktionstider	8
Hovedsikringsområder	8
Perimetersikring	8
Hegn	9
Skalsikring	10
Rumsikring (celle- og objektsikring)	10
AIA anlæg (Automatisk Indbruds Alarm)	10
Centraludstyret	11
Centralenheden	11
Kontrol- og indikeringsenheden	11
Betjeningsenheden	11
Strømforsyning	11
Senderudstyret	12
Detektorer	13
Elektroniske detektorer	13
Aktiv infrarød detektor	13
Passiv infrarød detektor	14
Ultralydsdetektor	15
Mulige fejlkilder	15
Mikrobølge detector	16
Antimaskering	16
Kombinerede detektorer	16
Kamera overvågning	17
Præventiv belysning	17
Nøgleboks	18
Brudfolie	18
Magnetkontakter	19
Glasbrudsdetektor	19
Passiv glasbrudsdetektor	19
Akustisk glasbrudsdetektor	19



Seismisk detektor	20
Vinduesgitre.....	20
Sikringsglas.....	20
Låsecylindre.....	21
Systemnøgler	21
Adgangskontrolanlæg	21
Tågesikring	22
Forbikobler	22
Overfaldstryk	23
Mærkning	23
Tyverimærkning kan.....	23
Typer af tyverimærkning	24
Grader af sikkerhed	25
Indbrud i private hjem: Det kriminalpræventive råd 2017	26
Nyttige links	27



Indledning

Vagtfirmaernes kunder kan vælge forskellige løsninger, når de vil sikre deres værdier mod indbrud, tekniske svigt, miljøuheld, brand mv.

Forsikringsvilkår

Det er forsikringsselskabet, der fastsætter hvilket sikringsniveau og hvilken sikringstype, der skal gælde for en virksomheds forsikringsaftale. I sikringsniveauet, beskrives kravene til den mekaniske sikring og til den elektroniske overvågning (AIA-anlæg). Dette vil sige, at det er F&P der stiller krav omkring hvilke former for sikring, den enkelte virksomhed skal leve op til for at få sine værdier forsikret. Og dermed er det indirekte F&P der sørger for at vi som vagter har et arbejde. *Se afsnittet sikringsniveau*



Forsikring & Pensions mission er at varetage branchens interesser.



Sikringsniveauer

Forsikringsselskaberne stiller en række krav, når man skal forsikre sin virksomhed.

Forsikringskravene udmønter sig i et sikringsniveau – og sikringsniveauet er et udtryk for den risiko, virksomheden har for et indbrud.

Niveauet fastlægges ud fra de varer, virksomheden opbevarer og værdien af disse varer samt værdien af det it-udstyr, der bruges i virksomheden.

Jo mere attraktive varerne er for indbrudstyve, des bedre indbrudssikring kræves. Og jo større koncentration af attraktive varer, des bedre indbrudssikring kræves.

Der er i alt 6 sikringsniveauer, 10, 20, 30, 40, 50, 60 og hvert niveau beskriver nøje hvilke krav, der er til låse, forstærkninger af bygningsdele, gitre, elektronisk alarmovervågning m.v. Sikringsniveau 10 er det laveste niveau, og sikringsniveau 60 er det højeste. Med tillæg af S (skalsikring), C (cellesikring) eller O (objektsikring) eks. 40-S.

Virksomheden kan således selv vælge, om de ønsker at leve op til sikringsniveauet ved at sikre med skalsikring, cellesikring eller objektsikring.

Ved sikringsniveau 20 til og med 60 skal man for at tegne en forsikring, blandt andet opfylde kravene om opsætning af et AIA-anlæg, og reaktionstider ved alarm.

På dette [LINK](#) kan du finde en nærmere uddybning af kravene der er tilknyttet de enkelte sikringsniveauer.

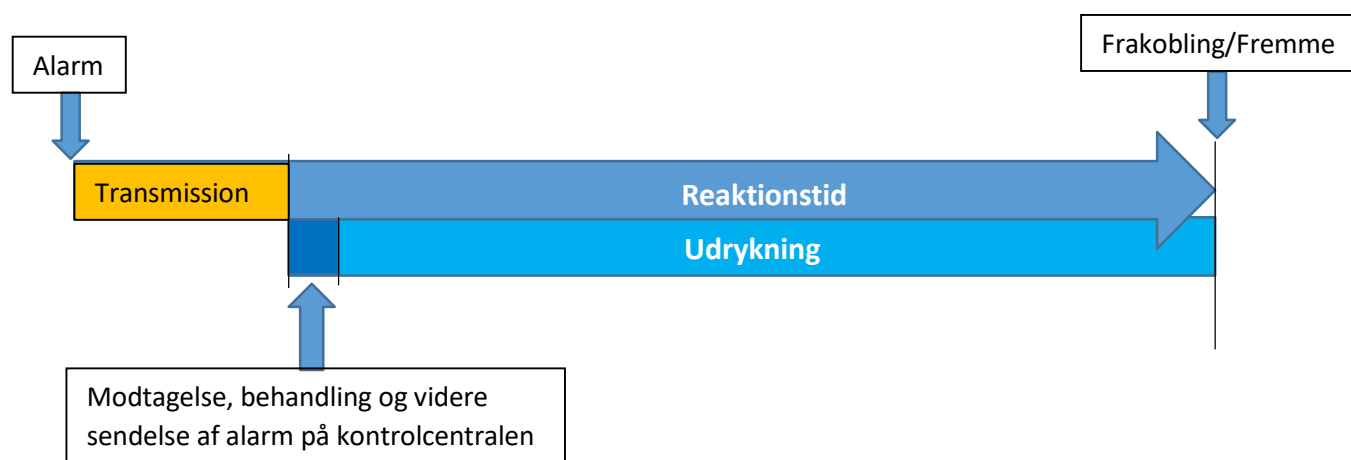


Den maksimale reaktionstid

Er der i sikringsniveauet krav om installation af et AIA-anlæg, medfører dette også et krav om en maksimal reaktionstid. Kunden eller dennes stedfortræder (almindeligvis et professionelt vagtfirma) skal i tilfælde af alarm fra AIA-anlægget kunne møde frem på virksomheden, inden for den maksimale reaktionstid, som angivet i skemaet nedenfor. Forsikringsselskabet kan stille krav om andre sikringsforanstaltninger, hvis reaktionstiden ikke kan opfyldes.

Sikringsniveau	10	20	30	40	50	60
Maks. Reaktionstid	-	35 Min	35 Min	30 Min	25 Min	20 Min

Den maksimale reaktionstid er den samlede tid, fra alarmen modtages på kontrolcentralen, til kundens eller dennes stedfortræder frakobler alarmen. Frakobling er i denne forbindelse den handling, der sikkert indikerer, at man er fremme på gerningsstedet.



I praksis vil reaktionen normalt være aftalt på forhånd via en skriftlig forholdsordre, som kontrolcentralens personale anvender, når der indløber en alarm fra en kunde. Kontrolcentralen tilkalder vagtfirmaet, der samarbejder med AIA-installatøren. Forsikringsselskabet og/eller kunden kan vælge at skærpe de maksimale reaktionstider. Det er kundens ansvar, at de sikringskrav, der er defineret i forsikringsvilkårene, er opfyldt. Som en hjælp kan kunden kræve, at de installatører, der etablerer sikringen, udfylder en installationserklæring. Denne erklæring opbevarer kunden sammen med sin forsikringspolice.

I tilfælde af en skade er den kundens dokumentation over for forsikringsselskabet, for at sikringskravene er overholdt.

Kunden kan selv vælge at opfylde kravene til reaktion, eller købe opgaven hos et vagtfirma.

Vagtfirmaet skal være godkendt hos F&P.



Gennemsnitlige reaktionstider

Ud over de maksimale reaktionstider skal vagtvirksomheden overholde følgende gennemsnitlige reaktionstider:

- 15 minutter i gennemsnit for samtlige kørsler hvor maksimum 20 minutter er kravet.
- 20 minutter i gennemsnit for samtlige kørsler hvor maksimum 25 minutter er kravet.
- 25 minutter i gennemsnit for samtlige kørsler hvor maksimum 30 minutter er kravet.
- 30 minutter i gennemsnit for samtlige kørsler hvor maksimum 35 minutter er kravet.

Målt for udrykninger, hvor der har været indbrud, og som er gennemført siden forrige audit. Hvor vagtvirksomheden har undtaget visse kortere tidsrum på dagen fra kravene om bestemte reaktionstider, under henvisning til myldretid i deres kontrakt med kunden, skal disse tidsrum udgå, når certificeringsorganet skal vurdere, om reaktionstider og gennemsnitlige reaktionstider er overholdt.

Virksomhederne skal altid anvende en certificeret installatør til at montere sikringen. De skal endvidere have en installationserklæring fra installatøren som dokumentation for at sikringen er udført i henhold til det gældende sikringsniveau.

På nedenstående link kan du se de forskellige sikringsniveauer, og forsøge dig frem med at indtaste forskellige varetyper og beløb, for at se hvordan kravet til sikrings- niveauerne ændre sig.

[Find dit sikringsniveau på F&P's hjemmeside](#)



Hovedsikringsområder

Man skelner imellem 3 typer for hovedsikringsområder, inden for sikringsteknik.

Perimetersikring

Dette sikringsområde er virksomhedens ydre grænse, fra skel til bygning. *Perimeter omkreds.* Denne sikring kan udføres enten som en mekanisk sikring eller en elektronisk overvågning. Du kan læse mere omkring perimetersikring på dette [LINK](#)



SCAN ME



Hegn

Et hegn eller en mur rundt om virksomheden kan forsinke de fleste indbrudstyve, men det pynter ikke ligefrem, og det er som regel ikke en billig løsning.



Pigtråd eller ”NATO pigtråd” må kun findes på hegn, hvis folk der går forbi ikke kan komme til skade på det. Elektrisk hegn er ifølge [Hegnslovens](#) §3, lovligt at opsætte.

[§ 3.](#) Elektriske hegn langs gade, vej, sti eller plads, hvor andre end hegnets ejer har færdselsret, skal være fjernet mindst 1/2 m fra færdselsbanen. Pigtrådshegn skal under tilsvarende forhold være fjernet mindst 1 m fra færdselsbanen, for gangstiers vedkommende mindst 1 m fra stiens midtlinje.

Hegnet kan yderligere være forsynet med en elektronisk sikring, således at hvis hegnet gennembrydes, forsøg på at klatre over det eller andet. Så sendes der et signal til Kontrolcentralen.



Indgangene i hegnet er som regel sikret med bomme, port eller lignende. Du kan læse mere om porte på dette [LINK](#) under pkt. 50.





Skalsikring

Skalsikring er en fælles betegnelse for forskellige metoder til at sikre bygningers ydre ”skal” – mure, loft, gulv, vinduer, indgangsdøre og andre flader i bygningen. Såfremt de varer eller genstande, som er omfattet af varegruppeskemaet, ønskes opbevaret i valgfrie rum på forsikringsstedet, skal alle bygningsmæssige grænsefalders sikres – såkaldt skalsikring.

Denne sikring kan udføres enten som en mekanisk sikring eller en elektronisk overvågning.

Du kan læse mere om skalsikring på dette [LINK](#)



Rumsikring (celle- og objektsikring)

Rumsikring – også benævnt celle- og objektsikring, er en fælles betegnelse for metoder, der kan bruges til at sikre værdier i virksomhedens enkelte rum – f.eks. computere – projektorer – pengeskabe mv.

Denne sikring kan ligeledes udføres enten som en mekanisk sikring eller en elektronisk overvågning.

AIA anlæg (Automatisk Indbruds Alarm)

Et AIA-anlæg (Automatisk Indbruds-Alarm-anlæg) er et elektronisk overvågningsanlæg, der kort fortalt består af en *centralenhed* og et antal *detektorer*. Hvis et begyndende indbrud bliver detekteret, sender centralenheden alarm til en døgnbemandet *vagtcentral*. På vagtcentralen behandles alarmerne, og afhængig af hvilken aftale, der er indgået, ringes der til kunden, eller også sender man en vagt. Når kunde eller vagt når frem til forsikringsstedet, registrerer alarmcentralen tidspunktet for, hvornår alarmerne tilbagestilles.

Herefter kan eventuelle følgeskader begrænses. Ved indbrud skal kunden kunne dokumentere, at den mekaniske tyverisikring og den elektroniske overvågning opfylder det krævede sikringsniveau. Denne dokumentation kan være installationserklæringer udstedt af en F&P-registreret installatør. Der kan ligeledes være krav om, at kunden skal dokumentere, at den maksimale *reaktionstid* er overholdt, hvilket kan dokumenteres ved hjælp af kontrolcentralens log.

I tilfælde af indbrud er en hurtig og målrettet indsats oftest en forudsætning for at redde de værdier, som opbevares i det sikrede og overvågede område. For at kontrolcentralen kan prioritere indsatsen i forbindelse med et indbrudstyveri, må denne råde over tilstrækkelig information fra det overvågede område. Dette kan sikres ved at anvende en metode, som bekræfter eller underbygger sandsynligheden for, at der er tale om et indbrud. En metode til bekræftelse af indbrudsalarmsignaler kan være projekteringen af AIA-anlægget på en måde, som sikrer, at kontrolcentralen i tilfælde af indbrud modtager information fra flere af hinanden uafhængige detektorer. En metode kan også være supplerende information i form af billeder fra et ITV-anlæg eller overførsel af lyd fra det overvågede område, i henhold til gældende lovgivning.



Centraludstyret

Centraludstyret består af følgende:

Centralenheden

Er den computer der styrer anlægget, et hvert forsøg på at åbne eller opbryde centralenheden, vil medføre en *sabotagealarm* til kontrolcentralen. En sabotagealarm kan ikke afstilles af brugerens brugerkode eller *AP-koden* på et *F&P* godkendt AIA-anlæg, men kun som udgangspunkt af en *teknikerkode* også kaldet *servicekoden*.

Kontrol- og indikeringsenheden

Enheden der kontrollerer funktionerne i anlægget og viser (indikerer) alarm tilstande.

Betjeningsenheden

Normalt et tastatur til at betjene anlægget. Dette kan enten være sammenbygget med centralenheden, eller en separat enhed, der gør at man kan betjene anlægget enten med en personlig kode, nøgler eller brikker.

Strømforsyning

Strømforsyningen skal mindst omfatte 2 uafhængige forsyningskilder, normalt net strøm (220 volt) og et genopladeligt batteri som:

- a. Oplades automatisk af AIA-anlægget
- b. Ikke automatisk oplades af AIA-anlægget

Minimumskapaciteten for alternativ (batteri) strømforsyningen

Batteritype	Klasse 1 Timer:	Klasse 2 Timer:	Klasse 3 Timer:	Klasse 4 Timer:
Type a, Genoplades af AIA-anlægget	12	12	60	60
Type b, Genoplades ikke af AIA-anlægget	24	24	120	120



Senderudstyret

Behandler alarmsignalerne og videresender dem. Alarmsignalerne kan videresendes på flere forskellige måder:

1. Dial-up modem

Som benytter det offentlige telefonnet. Denne type forbindelse er ikke overvåget, og sender kun et kontrolsignal til kontrolcentralen 1 gang i døgnet, for at kontrollere at telefonlinjen ikke er afbrudt og er derfor ikke en særlig sikker forbindelse. Og har heller ikke mulighed for at melde til kontrolcentralen, hvis der er andet galt i virksomheden.

2. ATU (Alarm Terminal Universal)

Som benytter ATN (Alarm- og Teknik Nettet), fordelen ved ATN er en større sikkerhed for at kontrolcentralen modtager alarmerne og der foretages en løbende kontrol af forbindelsen og udstyret, i modsætning til modemforbindelsen. ATN systemet meddeler ikke blot hvad der er galt men også hvor i virksomheden, og der er mulighed for at koble mange andre overvågnings systemer sammen via ATN-nettet.

Alarm- og Tekniknettet kontrolleres hvert andet sekund døgnet rundt, ved at der sendes et kontrolsignal ud til ATUén hos kunden. Hvis der sker brud på ATN- nettet, vil kontrolcentralen modtage en *linjealarm*.

Der er tilknyttet en døgnbemandet servicedesk, hos TDC som er til rådighed i forbindelse med etablering, fejlretning og generelle spørgsmål.

ATU tilslutningen til Alarm- og Tekniknetværket kan ske på 2 forskellige måder:

- a. Kablet forbindelse (Bredbånd, DSL/fiber)
- b. Mobil forbindelse (3/4G)

Er ”kablet forbindelse med mobil backup” valgt, vil ATU-3G teste mobilforbindelsen én gang i døgnet.

3. TCP-IP

- a. Som enten benytter en ADSL-linje (Asymmetric Digital Subscriber Line), i daglig tale en bredbåndsforbindelse, hvilket er en billigere løsning end ATN, da alle i forvejen har en ADSL forbindelse. Ulempen ved dette er dog at ADSL er leveret og styret af mange forskellige leverandører, og ved strømsvigt (230v) vil signal-transmissionen udeblive, da routeren ikke kan sende uden en strøm backup, hvilket de færreste har installeret. Derfor er mange af disse systemer kombineret med andre transmissions systemer f.eks. *GPRS (GSM)*.
- b. Eller/og benytter GPRS (GSM) trådløst netværk (mobiltelefon netværket). En TCP-IP sender kan købes i flere udgaver, og udvalget vokser med eksplosiv hastighed. Købes en Forsikring & Pensions registreret transmissionssender, er man sikker på at udstyret er testet og overholder nuværende transmissionsstandarder.

En IP-sender kan byde på mange udfordringer, og der er flere ting som skal tages stilling til når udstyret vælges, som f.eks.: pris, faciliteter, mulighed for alternativ transmissionsvej (backup), godkendelse, er udstyret montørvenligt/hurtigt at sætte op, kan udstyret krypteres/køre høj sikkerhed osv.



Detektorer

Er en fælles betegnelse for de ”følere” der detekterer om alt er som det skal være i virksomheden. Det være en dør der dirkes op, en rude der knuses, en pludselig temperaturstigning forårsaget af nogen der bevæger sig inden for detektorens område.

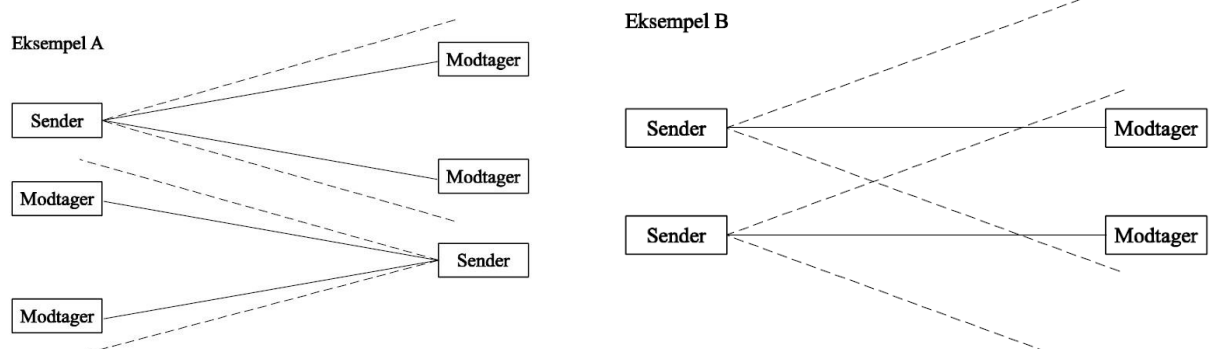
Elektroniske detektorer

Aktiv infrarød detektor

En aktiv infrarød detektor er en aktiv detektor, hvor signalsender og signalopsamler er indbygget i hver sin enhed. Signalsenderen i en aktiv infrarød detektor består af en infrarød lysdiode, og signalopsamleren består af en fotodiode. Aktive infrarøde detektorer anvendes til overvågning af gangarealer, facader og lange lagerhaller eller i områder, hvor miljøet ikke tillader brug af almindelige bevægelsesdetektorer. Ved at bryde en usynlig lysstråle mellem en sender og en modtager forårsages en alarmtilstand.

Detektoren bør installeres i en højde af 50 cm til 60 cm over gulv. Rækkevidden kan være op til 400 meter. Der kan kompenseres for det smalle overvågningsområde ved at sammenbygge flere detektorer. Hvis lyset mellem de forskellige par af sendere og modtagere har samme frekvens, eller er kodet på samme måde, skal opbygningen være som illustreret i eksempel A i nedenstående figur. Hvis man vælger en opbygning som i eksempel B, vil modtagerne først give alarm, når begge lysstråler brydes.

Hvis lyset mellem de forskellige par af sendere og modtagere har forskellige frekvenser (kan indstilles til forskellige frekvenser), kan de monteres som illustreret i eksempel B.



Det infrarøde lys, som udsendes fra senderen, spredes. Spredningsvinklen er ikke stor, men på afstande på over 20 meter kan den få betydning. De fleste detektorers rækkevidde er 50 meter til 60 meter. Selvom det infrarøde lys tilsyneladende går direkte fra senderen til modtageren, kan det være, at det bliver reflekteret på de flader (vægge, glasfacader, gulv eller loft), som detektoren overvåger. Herved opnås et andet dækningsområde end det, man havde regnet med refleksion kan også forekomme, hvis en sender og/eller modtager går ud af justering.

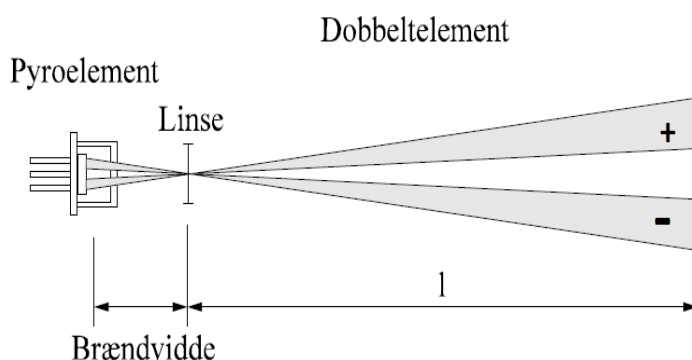
Modtageren skal placeres således, at direkte solbestråling undgås. Skarp belysning eller direkte solbestråling kan blænde modtageren.



Man skal også være opmærksom på at detektoren kan dækkes af dug eller is, derfor har nogle detektorer indbygget varmetråde ligesom el bagruden på en bil. Tåge, og især is tåge kan forstyrre det infrarøde lys, sådan at modtageren ikke kan se senderen, og derved opstår der fejl alarmer.

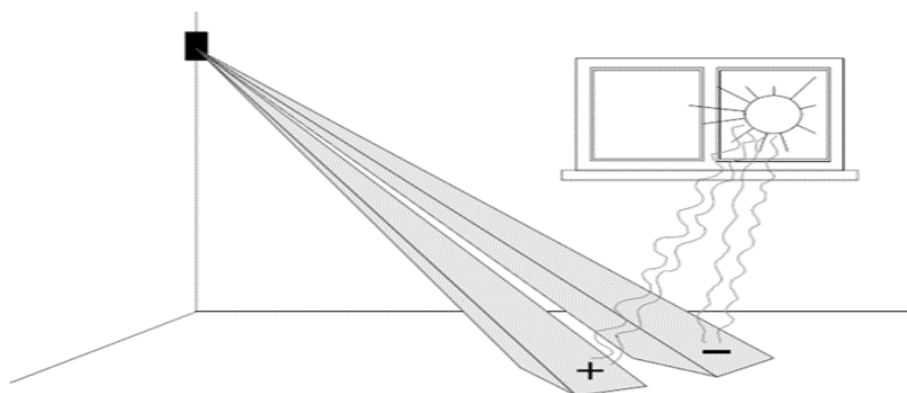
Passiv infrarød detektor

I en passiv infrarød detektor er der ikke nogen sender men derimod en modtager, eller en føler der består af en *Pyroelektrisk krystal* der har den egenskab, at der ved pludselige ændringer i den modtagne infrarøde stråling (temperaturændringer), som for eksempel når en person bevæger sig ind i et af detektorens delområder, genererer pyroelementet et målebart elektrisk signal, som anvendes til at aktivere alarmen.



I dag anvendes dobbeltelementer, det vil sige, at to pyroelektriske elementer er bygget sammen i samme hus. I dobbelt-elementet består hvert delområde af to parallelle områder, kaldet "gardiner". De to pyroelektriske elementer sidder i serie, modsat rettede, således, at det ene område genererer en positiv spænding og det andet genererer en negativ spænding.

Rammer en solstråle et delområde, og der pludselig sker en temperaturændring på det punkt, hvor den føler, genereres en negativ og en positiv spænding, som er lige store, hvilket resulterer i summen nul. Detektoren bliver ikke aktiveret. Hvis der kun havde været ét pyroelement, ville der være blevet genereret en spænding, og detektoren var blevet aktiveret.



Hvis en person bevæger sig forbi et delområde med et positivt område og et negativt område, vil vedkommende først ramme det positive område, som skaber en positiv spænding og derefter det negative område, som skaber en negativ spænding. Derfor er den bedste placering af en passiv infrarød detektor, sådan at man bevæger sig på tværs af dækningsområdet.



Ultralydsdetektor

En ultralydsdetektor er en aktiv detektor som består af en sender og en modtager der er sammenbygget i én enhed. Rækkevidden er afhængig af rummets udformning samt indretningen i rummet. Ultralyd bliver nemlig absorberet af tæpper, gardiner og andre lyddæmpende genstande og materialer, hvilket reducerer rækkevidden. Detektorens følsomhed og rækkevidde kan justeres i de fleste detektorer.

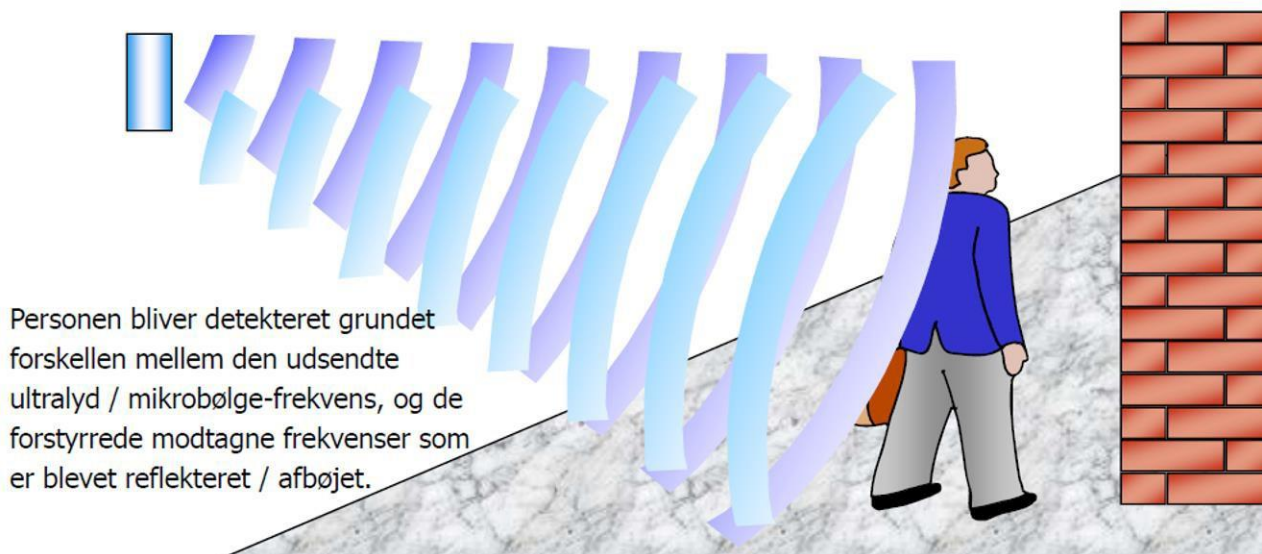
Ultralydsdetektoren anvendes på steder, hvor der er store temperatursvingninger eller direkte solbestråling. Den kan også anvendes i små rum og skabe. Dyr (specielt hunde) kan reagere allergisk overfor den ultralyd, som detektoren udsender i det rum, som skal overvåges. Nogle mennesker kan mærke ultralyden som en ubehagelig trykken i ørerne.

Dette problem kan løses ved at frakoble senderen i detektoren, når indbrudsalarmanlægget er frakoblet. Detektoren reagerer bedst på bevægelser imod eller væk fra denne, og bevægelser på tværs registreres derimod ikke så godt, eller slet ikke.

Mulige fejlkilder

Undgå at placere detektoren pegende imod eller nær ting, der er i bevægelse. (Ventilatorblade, skilte m.m.). Eller ting der kan udsende ultralyd (Utætte trykluftrør, ventilationsrør, ringeklummer m.m.). 2 ultralyds- detektorer i samme rum kan forstyrre hinanden og forårsage fejlalarmer.

Ultralydsdetektoren tåler ikke træk (ventilation, varmluftopvarmning, og lignede) i detektorens dækningsområde.





Mikrobølge detector



Rækkevidden for en mikrobølgedetektor ligger normalt, afhængig af type, mellem 15 meter og 30 meter. Men enkelte detektorer har dog en rækkevidde på helt op til 450 meter.

Detektoren er mere følsom over for bevægelser imod og bort fra detektoren, mens bevægelser på tværs af detektoren ikke detekteres så godt.

På grund af de mange forhold, der skal tages i betragtning, når der skal anvendes en mikrobølgedetektor, er der ikke blevet anvendt så mange detektorer af denne slags. Mikrobølgedetektorer er også dyrere end andre bevægelsesdetektorer. Hvor der stilles store krav til detekteringssikkerhed, er en mikrobølgedetektor i mange tilfælde den bedste detektor. I detekteringsmåden adskiller mikrobølge detektoren sig væsentlig fra de øvrige bevægelses detektorer. Luftturbolens, påvirkning fra lyskilder eller stærke lydkilder kan ikke påvirke detektoren, mens en indbrudstyv registreres med stor sikkerhed.

Antimaskering

Antimaskering er en sikring imod at detektorerne tildækkes, sådan at de ikke kan detektere korrekt, denne antimaskering kan udføres på mange måder, men foregår typisk ved at man i detektoren indbygger yderligere en detekteringsmetode, som kontrollerer om detektoren har frit udsyn til det område den overvåger. Dette kan gøres ved at indbygge en passiv infrarød sender og modtager i detektoren, eller en mikrobølge detektor der er justeret til minimum, at kunne se X antal meter ud i rummet. Hvis detektoren tildækkes i mere end typisk 20 sekunder, vil antimaskeringen aktivere alarmen også hvis alarmen ikke er tilkoblet, sådan at det ikke først er når alarmen skal tilkobles at man finder ud af nogen har tildækket detektoren.

Kombinerede detektorer

I dag eksisterer der flere typer af kombinations bevægelsesdetektorer, som i daglig tale kaldes kombidetektorer.

Kombinationen ligger i, at der er indbygget to detekteringsprincipper i samme detektor som f.eks. kombinationen af passiv infrarød detektor, og ultralydsdetektor eller kombinationen af passiv infrarød detektor og mikrobølge detektor hvor begge typer er indbygget i samme hus, og hvor begge systemer skal have set den samme fejlkilde inden for 2 sekunder, for at gå i alarm, det vil sige, at alarmkredsene er forbundet parallelt med hinanden.



Denne måde at detektere en alarm på giver meget få fejlalarmer, men når det er sagt skal det ligeledes siges, at man ikke bør bruge denne type til højsikkerhedsanlæg for, hvis man kan undgå den ene type af alarmkredsene vil den ikke gå i alarm.

Der er udviklet nye typer af kombidetektorer, som arbejder efter andre principper, hvor alarmkredsene er to uafhængige systemer med en indbygget mikroprocessor, som gør at detektoren analysere signalerne og hvor hver enkelt detekteringsprincip kan give alarm selvom den anden ikke er i alarm, ved at mikroprocessoren slukker for den ene detekterings metode, hvis den er i tvivl om der er en kilde der giver anledning til alarm, og dette giver en højsikkerhedsdetektor som kan anvendes, hvor der er ekstremt vanskelige forhold og hvor man ønsker en høj sikkerhed.

Kamera overvågning

Overvågningskameraer kan i dag optage under alle lysforhold, og kvaliteten af billederne eller videoerne, gør det lettere at finde de personer der ulovligt optræder på kameraet. Nogle kameraer har et indbygget ICR-filter, der blokerer infrarødt lys for at øge billedkvaliteten om dagen. Mens det om natten bruger en IR LED-diode, så kameraet kan overvåge områder, der ligger henlagt i totalt mørke. Lovgivningen for tv- overvågning kan du finde på dette [LINK](#)

Præventiv belysning

I forbindelse med kameraovervågning kan man med fordel opsætte projektører, sådan at området der filmes bliver oplyst, og dermed giver bedre billedkvalitet.

Præventiv belysning kan også med fordel anvendes, på områder der normalt henligger i mørke, sådan at indbrudstyvene ikke vælger netop dette område for at få adgang til bygningen.

Projektørerne kan kombineres med aktive infrarøde detektorer, der tænder lyset når nogen bevæger sig inden for et afgrænset område. Desuden kan de kobles sammen med AIA anlægget, sådan at området bliver oplyst når anlægget går i alarmtilstand.





Nøgleboks

I muren kan der sidde en *Nøgleboks*, hvor der skal anvendes en særlig nøgle (en såkaldt AP-nøgle), en nøgle, som kun vagten eller montøren hos vagtselskabet er i besiddelse af. I denne nøgleboks opbevares et sæt af virksomhedens nøgler, som alarmpatruljen eller servicemontøren har brug for, hvis de skal ind på virksomheden efter lukketid. Hvis nøglerne tages ud af nøgleboksen, eller boksen forsøges opbrudt sendes der et alarmsignal til kontrolcentralen. Denne form for alarm vil kun vagten eller montøren kunne afstille. Denne form for alarm kan IKKE afstilles ved hjælp af brugerkoden (kunden).

Når man som AP-vægter ”trækker nøgleboksen” så vil dette også være bevis for om *reaktionstiden* er overholdt.

På dette [LINK](#) kan du læse mere om nøglebokse



Brudfolie

Da disse metalfolie strimler er under udfasning, vil gennemgangen af disse blive yderst sammenfattet. Men det skal siges, at man som vagt kun må udføre en nødreparation af disse foliestrimler, hvis vagtfirmaet tillader dette. Og husk altid at få denne nødreparation godkendt af kontrolcentralen. Den endelige reparation skal foretages af en F&P godkendt reparatør.

Du kan læse mere om brudfolie på dette [LINK](#) under Pkt. 30





Magnetkontakter

Hvis man vil sikre, at der går en alarm, når porte, døre eller vinduer åbnes, så er magnetkontakter et godt bud på dette problem, disse kaldes ofte for åbningskontakter.

Magnetkontakten består af en magnet, der er monteret i vinduesrammen, eller i dørbladet, og en kontaktdel der sidder i karmen. Disse er placeret sådan, at når døren eller vinduet er lukket så sidder magneten og kontaktdelen lige ud for hinanden. Når døren eller vinduet åbnes mere end max 6 cm, så vil magneten slippe forbindelsen til kontaktdelen, og alarmen vil starte. Nogle af disse kontakter er afbalancerede til magnetens styrke, sådan at hvis man holder en kraftigere eller svagere magnet på, for at omgå åbningskontakten, så vil alarmen starte.

I de fleste AIA anlæg vil der forekomme en *tilkoblingsfejl*, hvis man forsøger at tilkoble alarmen, når der er vinduer eller døre med magnetkontakter der står åbne. Da man som kunde ikke ønsker at sikringskomponenter til alarmsystemerne er synlige, kan det ofte være svært at se disse indborede magnetkontakter, da de oftest sidder gemt i karmen og er indfarvede i samme farve som døren.

Glasbrudsdetektor

En glasbrudsdetektor aktiverer alarmen når vinduesglasset knuses. Der findes overordnet 2 typer af disse detektorer.

Passiv glasbrudsdetektor

Består af en krystal, som registrerer de svingninger i glasset, der indikerer glasset bliver knust.

Denne detektor på limes glasset indvendigt på ruden.

Akustisk glasbrudsdetektor

Består af en mikrofon der reagerer på lyden af knust glas, den monteres sådan at den dækker flere vinduer eller døre samtidigt. Eksempelvis i store glasfacader. Sådan at man ikke skal montere en detektor på hvert enkelt glas. Denne detektor har et dækningsområde på op til 9 meter.

Du kan læse mere om glasbrudsdetektorer på dette [LINK](#) under Pkt. 62





Seismisk detektor

Den seismiske detektor afløser for de gamle bokskontakter, som indeholder en rystekontakt og et termoelement. Den seismiske detektor er en passiv detektor, der kan registrere de rystelser, som opstår ved mekaniske eller termiske angreb (angreb med for eksempel iltlanse, skærebrænder, boreværktøj, hammer og sprængstof) på materialer som metal og armeret beton.

Vinduesgitre

Virksomheder kan sikre sine vinduer med gitre eller skodder. De er som regel lavet af enten aluminium eller stål. Og kan enten placeres uden på glasruden, denne placering sikrer bedst imod hærværk, da ruden derved ikke er så let at smadre, ligesom opklæbning af reklamer mm vanskeligsgøres. Eller de kan placeres indvendigt bag glasset, hvilket sikrer bedst imod indbrud, da tyven først skal smadre glasset, inden gitteret er tilgængeligt, og med en kombination med glasbrudsdetektor enten passiv eller akustisk, så vil AIA anlægget afsende en alarm allerede når glasset smadres.

Sikringsglas

Glas med indbrudshæmmende egenskaber benævnes sikringsglas. Glas klassificeret i modstandsklasse A1- A3 giver beskyttelse mod hærværk. Disse glas vil desuden have tilstrækkelig modstandsevne til delvist at hæmme indbrudsforsøg.

Der findes forskellige former for sikringsglas, men de mest almindeligt forekommende typer er:

1. Lamineret glas

Lamineret glas består af 2 eller flere lag glas, der er "klæbet" sammen med en folie i mellem. Det kaldes folielaminering.

2. Hærdet glas

Glas hærdes ved først at blive opvarmet til ca. 600 grader og derefter "chokafkølet". Den hurtige afkøling betyder, at der opstår spændinger i glasset, som gør det stærkt. Styrken af hærdet glas er 3-5 gange større end almindeligt glas i samme tykkelse.

3. Varmeforstærket glas

Varmeforstærket glas er fremstillet ved at glasset varmes op til ca. 600o og derefter afkølet langsomt. Det betyder, at glasset er delhærdet, og resultatet er et stærkere glas end normalt floatglas. Hærdningseffekten er ca. halvdelen af hærdningseffekten for normalt hærdet glas.

Du kan finde et [LINK](#) til mere om sikringsglas her.





Låsecylindre

Virksomhedernes låsecylindre betyder selvfølgelig meget for sikkerheden. De udvendige låsecylindre er de vigtigste. Men også indvendige låsecylindre kan gøre det svært for uvedkommende at færdes i bygningerne.

Der findes et utal af forskellige låsecylindre og nøgler. Mange almindelige låsecylindre, kan ret nemt dirkes op ved anvendelse af en ”bankenøgle”

Bankenøgle åbner let en almindelig låsecylinder.

Ved hjælp af en 3D printer, kan man let fremstille en sådan bankenøgle, eller kopiere en almindelig nøgle med denne.

Du kan se den 3D printede bankenøgle her på dette [LINK](#)

Systemnøgler

Nøglesystemet er ofte en del af virksomhedens *adgangskontrolsystem* for medarbejderne. Hvor hovednøglen (A-nøglen) kan åbne alle døre.

De andre nøgler (B-C-D OSV. Nøgler), kan kun åbne de døre, til de rum, den enkelte medarbejder skal have adgang til.

Adgangskontrolanlæg

Ved adgangskontrolanlæg forstås et anlæg, som har til formål at kontrollere adgangen til og/eller fra et fysisk afgrænset område. Eksempler på adgangskontrolanlæg, kan være:

- Enkeltstående enhed indeholdende energiforsyning (batteri) samt lås til montering direkte på en dør – bom med tilhørende kontrol i forbindelse med udkørsel fra parkeringsplads eller garageanlæg
- Et anlæg indeholdende mange kortlæsere, elektromekaniske låseanordninger eventuelt tilsluttet lokalt datanet og med tilslutning af pc-anlæg for programmering samt til løbende registrering af hændelser.

En af de vigtigste fordele ved adgangskontrolsystemet er netop en fleksible styring, af hvem der må komme hvor, hvornår og på hvilke betingelser. Dette åbner en lang række muligheder for fleksibilitet, i kraft af adgangsstyring i forhold til eksterne samarbejdspartnere - eksempelvis i forbindelse med outsourcing. Via rapporteringsmulighederne, kan man til enhver tid se hvem der har været hvor - og igen - hvornår. Dermed kan leverandører, kantinepersonale, rengøringspersonale, konsulenter m.v. have deres egne id-kort, og der kan gives adgang til de relevante områder inden for bestemte tider.

Kilde: Forsikring og Pension



Tågesikring

En enhed, eller en række komponenter, der tilsammen fungerer som en enhed, som – når den aktiveres – producerer en tåge, der reducerer sigtbarheden i det beskyttede område. Automatisk aktivering af tågesikringen må kun være mulig når AIA-anlægget, der overvåger det sikrede område, er tilkoblet.

Tågegeneratoren må ikke aktiveres uden forudgående aktivering af mindst to af hinanden uafhængige detektorer, hvoraf den ene skal dedikeres til tågegeneratoren. Hvor kunden ønsker det, kan andet skriftligt aftales.

Røgen som tågegeneratoren producerer er ufarlig over for mennesker og dyr, men nedsætter sigtbarheden, og vanskeliggør det for den indtrængende at orientere sig. Som oftest er der tale om en glykolvæske der opvarmes (lidt amme princip, som i en E-cigaret), og omdannes til røg.



I adgangsvejen(e) til det eller de sikrede områder skal der tydeligt markeres ved skiltning, at der er installeret tågesikring, af hensyn til brandmyndighederne

Det er vigtigt at der efterfølgende udluftes grundigt i det område, der har været udløst en tågegenerator, da røgen hvis den får lov til at fortætte vil frembringe et fedtet lag på alle overflader, og dette lag kan i visse tilfælde opløse stregkoder på papkasser mv. Du kan læse mere om tågesikring på dette [LINK](#)

Forbikobler

Forbikobleren er en enhed (typisk et tastatur, kortlæser, nøgleafbryder eller biometrisk læser) der ”undertrykker” alarmsignalerne fra *adgangsvejens* detektorer og ”køber brugeren tid” til at komme ind igennem *adgangsvejen* til at frakoble alarmanlægget inde i bygningen. Når forbikobleren aktiveres starter indgangstiden, som er den tid man har til at nå at indtaste den korrekte kode på betjeningsenheden (tastaturet).

Denne tid kan programmeres fra 10 sekunder til maksimalt 45 sekunder. Denne undertrykkelse af alarmsignalerne medfører at en leverandør, der skal aflevere varer uden for åbningstiden, kan have koden til forbikobleren, men ikke koden til alarmen. På den måde får leverandøren 45 sekunder til at stille varerne inden for døren og lukke denne igen inden indgangstiden udløber, og derved ikke aktiverer alarmen.



Overfaldstryk

Overfaldstryk er en fælles betegnelse for en kontakt, der sender iværksætter den reaktion der på forhånd er aftalt imellem kunden og vagtfirmaet. Disse overfaldstryk sidder ofte placeret på en sådan måde, at en eventuel røver ikke vil kunne se om der bliver trykket på denne. Overfaldstrykket kan kombineres med andre sikringsformer, sådan at der ruller et gitter op foran skranken, eller der aktiveres en *DNA spray*.

Denne oversprøjter røveren med en unik væske, som indeholder kunstigt DNA og mikrodots. Der er typisk tale om meget små partikler, der indeholder et antal cifre eller bogstaver, og disse partikler fastgøres til røveren med en lim, der i tørret form er nærmest usynlig. Således er kun de meget små partikler kun synlige ved brug af ultraviolet lys. Cifrene/bogstaverne i partiklerne kan kun ses gennem et kraftigt forstørrelsesglas. De benyttede cifre/bogstaver er en entydig identifikation, der via en database kan oplyse om ejerens identitet.

Butikkerne der har installeret DNA spray har haft færre røverier, siger hovedforfatteren bag evalueringen af DNA væske, Rune Holst Scherg, specialkonsulent og ph.d. i NFC, Nationalt forebyggelsescenter hos rigspolitiet. Der er et fald i udsathed for røveri på 65 procent, hvis man sammenligner røverierne i forsøgsbutikkerne med kontrol butikkerne, siger han.

Mærkning

Ved tyverimærkning påføres den enkelte værdigenstand/objekt et kendetegn, der typisk viser hvem ejeren er, og som ikke kan fjernes igen uden at efterlade sig spor. I praksis kan man mærke alle genstande, men vigtigst er de ting, som tyvene går efter, og oftest går tyvene efter 'varer' som let kan sælges.

Tyverimærkning anvendes på en lang række objekter, blandt andet bærbare PC'ere, tablets, fladskærme, mobiltelefoner/smartphones, kameraer, musik- og måleinstrumenter, fotoudstyr, smykker samt designermøbler og værktøj.

Tyverimærkning kan

- Virke præventivt - og dermed afholde tyven fra indbrud
- Afsløre tyveriet, hvis tyven bliver standset af politiet på vej væk fra gerningsstedet
- Hjælpe politiet med at bevise at de fundne effekter er tyvekoster
- Gøre det vanskeligt for tyven at afsætte de stjålne effekter til hæler
- Afsløre hæleren, der har købt de stjålne og mærkede effekter
- Give politiet mulighed for opklaring af andre tyverier, fx ved ransagning efter anden forbrydelse
- Sikre, at genfundne effekter kommer tilbage til den rette ejermand
- Gøre ting uinteressante for andre end den rette ejermand



Typer af tyverimærkning

Der findes flere forskellige typer af produkter og metoder som virksomheder, borgere og institutioner kan benytte til mærkning af genstande.

- Skabelonmærkning
 - En skabelonmærkning består af en engangsskabelon og en mærkepasta. I skabelonen udskærer leverandøren den tekst, som ønskes skrevet på objektet, og når selve mærkningen skal finde sted, klistres skabelonen på værdigenstanden, hvorefter der påføres en mærkepasta, der går ned gennem de udskårne bogstaver eller tegn i skabelonen, og bider sig fast på objektet.
- Skiltemærkning – med/uden underskilt
 - Skiltemærkning uden underskilt er et ét-lags-skilt, fx i akryl. Denne form for skiltemærkning er meget udbredt, og leverandøren lasergraverer en tekst i et skilt, der så efterfølgende fuldlimes på værdigenstanden med en lim, der gør det nærmest umuligt at fjerne tyverimærket igen
- Grovmærkning
 - Med en ridsepen skrives en kode, navn eller fx virksomhedens SE nummer efter en skabelon.
- Graving
 - Graving kan foretages i træ, laminat, plast, rustfrit stål, aluminium, metal, læder og gummi. Indgraving skal udføres hos specialfirmaer. Her kan indgraveres navn, logo, telefonnummer osv.
- Chipmærkning
 - RFID-chip mærkning er en anden form for usynlig mærkning. Små elektroniske chips RFID (Radio Frequency Identification), kan bygges ind i produktet. De kan efterfølgende aflæses elektronisk, og kan gemme oplysninger om genstanden.
- Usynlig mærkning (DNA mærkning)
 - Usynlig mærkning er en unik væske, som indeholder kunstigt DNA og mikrodots. Der er typisk tale om meget små partikler, der indeholder et antal cifre eller bogstaver, og disse partikler fastgøres til værdigenstanden med en lim, der i tørret form er nærmest usynlig. Således er kun de meget små partikler kraftigt forstørrelsesglas. De benyttede cifre/bogstaver er en entydig identifikation, der via en database kan oplyse om ejerens identitet.

Du kan læse mere om DNA mærkning på dette [LINK](#)



Grader af sikkerhed

Produkter (låsekasser, cylindre, sikringsskabe, vægkonstruktioner mv.) der skal F&P-registreres, skal prøves efter de europæiske standarder eller de nordiske standarder, som forsikringsbranchen anerkender. Der skal altid anvendes den nyeste udgave af disse standarder ved prøvning.

Du kan finde mere om kravene til sikringsprodukter efter de nye standarder på dette [LINK](#)



Farvekoderne der førhen henviste til sikringsklassen for låse enheder, er efter den pr. 31 december 2013 udfasede ”standardtyvmetode”, blevet afløst af låseenhed.

I – IV. Låseenhed er en samlet betegnelse for en låseenhed (låsekasse, cylinder og beslag), skal afprøves efter EN-standarder.

Sikringsniveau	Farveklasse – STM (Udgået)	Ny betegnelse
10	-	Låseenhed I
20	GRØN	Låseenhed I
30	BLÅ	Låseenhed II
40	BLÅ	Låseenhed III
50	BLÅ	Låseenhed IV
60	RØD	Låseenhed IV

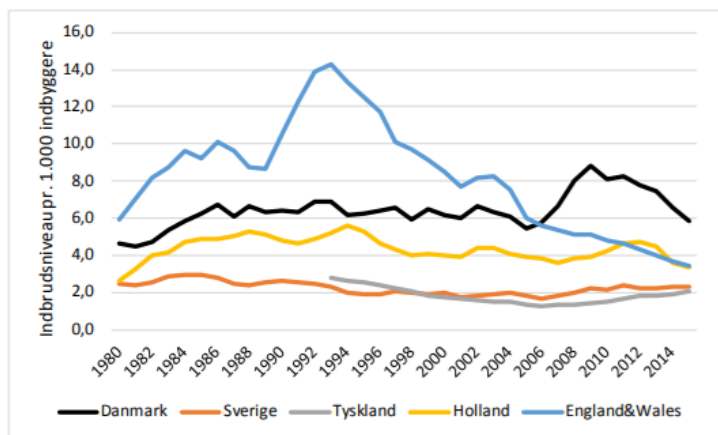
Du kan finde mere om kravene til låseenheder på dette [LINK](#)



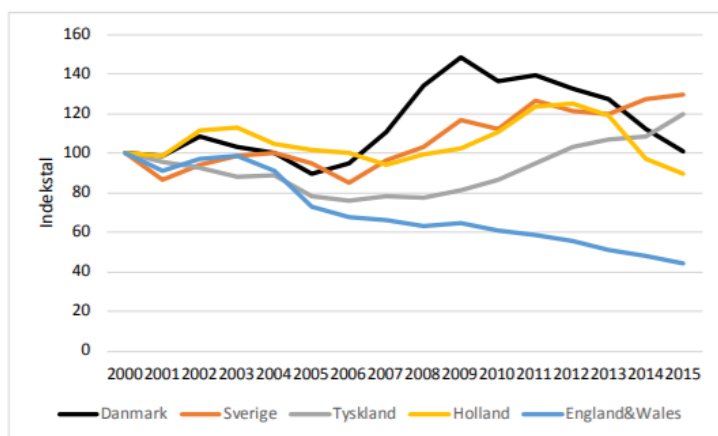


Indbrud i private hjem: Det kriminalpræventive råd 2017

Figur R.1: Indbrudsrate pr. 1.000 indbyggere i de fem undersøgte lande i perioden 1980-2015



Figur R.2: Indeksret udvikling i omfanget af indbrud i beboelse i de fem undersøgte lande i perioden 2000-2015 (2000 = 100)



Vagtbranchens medarbejdere kan medvirke til råde og vejlede private kunder, så de selv bliver opmærksomme og aktive, ved sikring af egne hjem og værdier.

Du kan læse meget mere om, hvordan du som vagt vejleder kunder, venner, familie i bedst muligt at sikre deres hjem ved at klikke på nedenstående billede.



Nyttige links

3D printet nøgle	LINK
AIA-KATALOG – FANE 040 Samledåser, forgreningsdåser, detektorer, alment, brudfolie, kontaktråde (snorekontakter), åbningskontakt, overfaldstryk, bevægelsesdetektor/registreringsdetektor, objektovervågning	LINK
Bekendtgørelse af lov om hegn	LINK
Find dit sikringsniveau	LINK
Forsikring og Pensions AIA katalog	LINK
Sikringsguiden F&P	LINK
Forsikring og Pensions SIKRINGSNIVEAUER 2019	LINK
Låseenheder F&P	LINK
F&P registrerede sikringsprodukter	LINK
Sammenligningsnøgle tekniske specifikationer	LINK
Sikkerheds Branchens Fælles Symbolsamling	LINK
SikkerhedsBranchens hjemmeside	LINK
Sikkerheds branchens samling af hyppigt forekommende ”sikringsord”	LINK
Perimetersikring & overvågning	LINK
Sikringskatalog Kapitel 8 Gitre, porte og jalousier	LINK
Sikringskatalog Kapitel 11 Perimetersikring & overvågning	LINK
Sikringskatalog Kapitel 12 Nøglebokse	LINK
Stop indbruds hjemmeside	LINK
Suppleringskataloget Kapitel 3 Tågesikring	LINK
Vejledning om reaktion ved alarm fra indbrudsalarmanlæg	LINK
Det kriminal præventive råd	LINK