Geïntegreerde veiligheidssystemen.

Veiligheidssystemen kunnen niet bestaan uit één zelfde standaard oplossing!

Geïntegreerde veiligheidssystemen.

Een veiligheidsinstallatie is niet hetzelfde als een algemene elektrische installatie die gebouwd is volgens noodwendigheden en normen. Dit werk is er onder meer gekomen na tientallen jaren het gebrek aan gezond boerenverstand te zien ontbreken in realisaties!

Robert Verhulst

Robert Verhulst

ISBN: 9789464657678

Met dank voor de foto overname:
HTC parking & security bv Nederland
Dormakaba België
Idemia Frankrijk
Proton Data USA
Axis communications Zweden
Boon Edam Nederland
CDVI Frankrijk

Heeft U vragen over dit boek:
info@rcms.expert

www.rcms.expert

Doel van dit werk:
Met dit werk wil ik iedereen die betrokken is bij het ontwerpen van een geïntegreerd veiligheidssysteem met vernieuwende technologische beveiliging een leidraad geven en naar een nieuw tijdperk brengen qua technologie. Toegangscontrole is ook de meest praktische en efficiënte bestrijding tegen inbraak, werkverstoring en fysieke bescherming als onderdeel van NIS2..

Het werk bevat dertien hoofdstukken:
I. Algemene begrippen.
II. Geïntegreerde veiligheid.
III. Toegangscontrole.
IV. Audio en video.
V. Andere middelen.
VI. Afstandsoverwaking
VII. Onderhoud en aanpassingen
VIII. Cybersecurity
IX. Algemene informatie materialen
X. Vragenlijst
XI. Ontwerp
XII. Economische duurzaamheid
XIII. Algemene informatie en normeringen

Robert Verhulst

Revisie 20.0. April 2024

Opmerking: in dit werk wordt regelmatig gewaarschuwd voor het beschermen van de wettelijke private veiligheidsregels (GDPR) maar dit werk is geen leidraad in deze wettelijke verordeningen.

Veiligheid het begin!

In werkelijkheid haast nooit aanwezig is een veiligheidsstudie van plaats, omgeving, structuur, terrein,… van een nieuw te bouwen gebouw of site! Nochtans hoort een veiligheidsoverweging voor het ogenblik dat de architect een potlood op papier zet. Samen met de eerste lijnen van een ontwerp moet de belangrijke fysieke inplanting gevolgd worden met veiligheidsadvies. Risico's achteraf oplossen met elektronische middelen is vaak moeilijk en een dure ingreep.

I. Algemene begrippen

Safety of security?

In de Nederlandse taal spreekt men, vrij algemeen, van veiligheid. Toch is er een zeer groot onderscheid qua veiligheid tussen de volgende sectoren:
Sector van humane veiligheid en gezondheid of safety
- Brandveiligheid en evacuatie
- Rampspoed
- Noodsituatie
- Werkomstandigheden
- Machineveiligheid
- Rellen

Sector ter bescherming van mens en waarden of security
- Inbraak veiligheid
- Toegangscontrole
- Spionage
- Sabotage
- Elke vorm van agressie
- Cyber veiligheid
- Algemene overwaking en observatie
- Branddetectie

Met bovenstaande sectoren als voorbeeld tracht ik verder in dit werk het onderscheid te maken door het gebruik van de termen “security” en “safety”. Uit de aangehaalde factoren is het duidelijk dat in de security sector het onverwachte of onberekenbare gevaar een belangrijke rol spelen.

Drie essentiële punten voor een veiligheidssysteem:

Sensoren, camera's, onderstations, … alle elementen die deel uitmaken van een veiligheidssysteem moeten beschermd zijn tegen sabotage, vernieling, schijnwerking, defect, beïnvloeding van elke soort… Dit kan in veel gevallen niet vermeden worden, maar het is uiterst belangrijk dat hiervan een alarm signalering het gevolg is. (vb. een schutter of laser schiet van buiten een omheining op een beveiligingscamera)

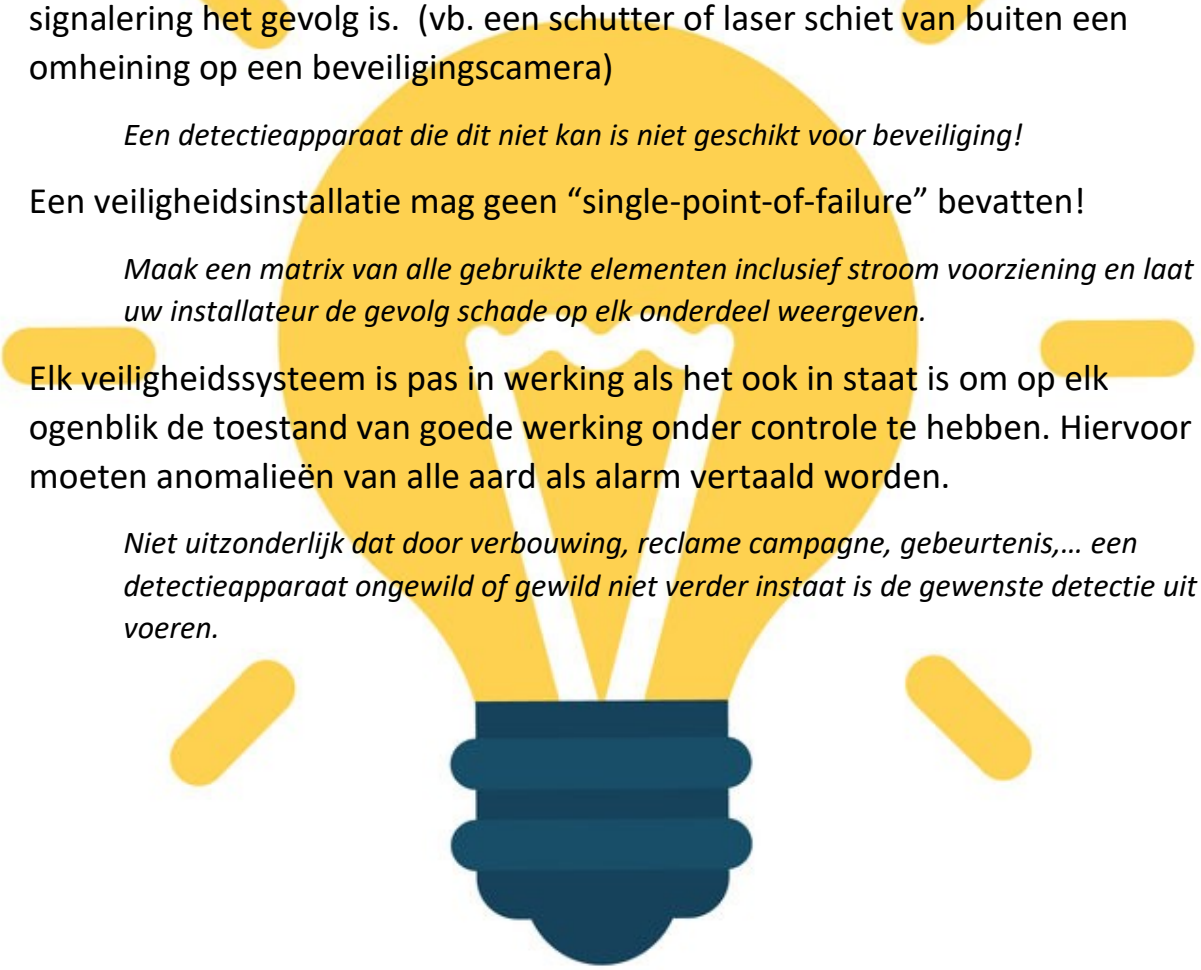
Een detectieapparaat die dit niet kan is niet geschikt voor beveiliging!

Een veiligheidsinstallatie mag geen "single-point-of-failure" bevatten!

Maak een matrix van alle gebruikte elementen inclusief stroom voorziening en laat uw installateur de gevolg schade op elk onderdeel weergeven.

Elk veiligheidssysteem is pas in werking als het ook in staat is om op elk ogenblik de toestand van goede werking onder controle te hebben. Hiervoor moeten anomalieën van alle aard als alarm vertaald worden.

Niet uitzonderlijk dat door verbouwing, reclame campagne, gebeurtenis,… een detectieapparaat ongewild of gewild niet verder instaat is de gewenste detectie uit te voeren.



Credentials?

In dit werk spreekt men meestal van credential wanneer men een middel bedoelt dat gebruikt wordt om een persoon te identificeren. Dit kan, afhankelijk van de installatie, een badge zijn, een tag, een elektronische sleutel, een smartphone, maar ook een vorm van barcode of QR-code zijn.

Overwaking of bewaking ?

Is blijkbaar geen Nederlands woord. Toch kies ik ervoor om dit woord te gebruiken omdat dit woord een beter beeld geeft. Overwaking in de betekenis van een vorm van volledige observatie en controle. Dit is niet alleen een alarm bekijken en actie ondernemen, maar ook proactief een evolutie volgen, een dreigend gevaar vermijden en hiervoor de nodige actie ondernemen. Overwaking kan alleen door mensen met kennis ter zake, mensen die dag op dag de activiteit op het te overwaken domein kennen. Bewaken is het opvolgen van vooraf bepaalde instructies en opvolgen van alarmen na de feiten, meestal door mensen met weinig affiniteit met het dynamische gebeuren.

Onsite overwaking of remote bewaking!
Bij onsite of plaatselijke aanwezige overwaking heeft de overwaker kennis van het gebeuren en de omgeving waardoor hij detectie veel beter kan evalueren en **proactief** beslissingen nemen.
Remote bewaking is steeds post event met weinig kennis van het gebeuren op de site en zal steeds grotere schade tot gevolg hebben. Spijtig genoeg wordt deze keuze gemaakt uit kost overweging.

Onafhankelijkheid:

Een overwaking van een onderwerp of een domein moet onafhankelijk zijn van de werking van dit onderwerp.

Voorbeelden uit ervaring ter verduidelijking:
- Een computercenter wordt overwaakt met een aantal camera's en sensoren, een zware fout bestaat erin de ononderbroken voeding of de software van de overwaking in deze ruimte te voorzien.
Een aanval tot sabotage op het computercenter zal eveneens het veiligheidssysteem buiten werking stellen en de klant zonder enig bewijs laten zonder enige verdere controle!

- Een camera observeert een noodstroomaggregaat, maar is voor zijn voeding afhankelijk van het aggregaat.
-Een netwerk moet onafhankelijk zijn en door de veiligheidsdiensten beheerd worden. Gebruik van VLAN op een bestaand netwerk is niet toegestaan vermits steeds de fysieke kabel en apparatuur door anderen toegankelijk zijn en niet aan dezelfde veiligheidsvoorschriften voldoen.
- Een observatie camera wordt gevoed op een plaatselijk stopcontact, andere toestellen als een koelkast dewelke een fout vertoont of een aardlek veroorzaakt zal de camera buiten werking stellen.

Bunker?

De plaats waar in reële tijd beslissingen worden genomen inzake veiligheid moet gehuisvest zijn op een veilige en goed beschermde plaats. Een aanval zal meestal gericht zijn op een directe wijze naar het target en in deze omstandigheden moet de veiligheid in werking blijven. Mocht een aanval gelijktijdig of vooraf toch gericht zijn naar de veiligheid overwaking dan moet deze voldoende versterkt zijn om uitwendige interventietijd mogelijk te maken.

Praktisch gezien moet het centrale systeem en controle zich op een veilige plaats bevinden dewelke afgeschermd is met fysieke middelen, toegangscontrole en onzichtbaar van buitenaf. Te dikwijls wordt een overwaking aanzien als een nachtportier job.

Internet !

Internet communicatie is heden niet meer weg te denken, op de meeste plaatsen kan men een zeer hoge betrouwbaarheid verkrijgen. Echter bij gevaar zoals oorlog en terrorisme is het de meest gezochte middel tot sabotage!

Binnen veiligheidsgrenzen:

Een geïntegreerd systeem maakt meestal tal van verbindingen met andere technieken. Echter mag men de aandacht van een operator niet onttrekken door niet veiligheid gebonden meldingen. Achter elke niet veiligheid gebonden opdracht kan een kritische veiligheidstoestand schuilgaan. Kritische technische toestanden die niet direct verbonden zijn met veiligheid kunnen eventueel gemeld worden en doorgegeven worden aan andere bevoegde personen, deze uitzondering met korte afhandeling moet echter beperkt blijven. Het is evenmin de taak van de veiligheid beambte om de temperatuur van een lokaal te gaan aanpassen, daar tegenover kan een waterlek wel een veiligheidsrisico vormen.
Maak een onderscheid tussen security en non-security, vermijd ingewikkelde constructies als PSIM (Physical security information management) waarin eveneens technische overwaking en besturing gebeurt. BCS (Building Control Systems) zijn een must voor complexe systemen, maar vereisen andere vaardigheden en kunnen gemakkelijk op afstand worden bediend.

Sleutels:

Ondanks alle nieuwe technologieën zijn fysieke sleutels nog steeds niet verdwenen. Afhankelijk van de grote van een site zie je soms duizenden ongebruikte fysieke sleutels, maar die ondanks de elektronische toegangscontrole toegang verschaffen. Fysieke sleutels en lopers kunnen vrij gemakkelijk nagemaakt worden en vormen een bijkomende bedreiging. (het is niet omdat de eerlijke slotenmaker een sleutel laat aanmaken bij de fabrikant dat een inbreker deze niet kan maken) Let op: veelal kan door boren en/of vijlen een sleutel met lagere toegang aangepast worden om hogere toegang te verkrijgen!

Nog grotere zorgen bestaan er voor sleutels van technische kasten dewelke meestal universeel zijn! Hou rekening dat het tamper contact van de kast een alarm zal veroorzaken maar de sabotage niet kan vermijden.

Een tamper contact is een elektrische schakelaar binnen de veiligheidskast geplaatst om een toegang tot de kast te melden als een alarm.

Bekabeling in het algemeen:

Factor 1 is de schendbaarheid, een beschadigde of doorgeknipte kabel heeft ongetwijfeld een gevolg als uitschakeling van een gedeelte van de beveiliging. Een installatie uitgevoerd volgens goed vakmanschap zal de fout signaleren maar een deel van de installatie staat en blijft hiermee buiten controle!

Edge bekabeling of bekabeling tussen sensor en plaatselijke controle eenheid wordt in vele vormen uitgevoerd en behoeft zonder uitzondering een alarm bericht wanneer een storing of onderbreking ontstaat!

Netwerk bekabeling tussen centrale eenheden en plaatselijke controllers worden nooit anders uitgevoerd dan met een goed geconcipieerd netwerk met PoE. Dit netwerk bestaat uit een TCP/IP ethernet communicatie met geëncrypteerd communicatie en controle van de trunk tussen ethernet switch en edge device. Liefst zorgt men voor voldoende bandbreedte om audio mogelijk te maken. Tussen switches en de centrale eenheden dient het een voorkeur om een redundant net te voorzien zoals een lusbekabeling.

Sleutelkasten :

Heel wat instellingen na het dagelijks zoeken naar de gepaste sleutel in het bezit van wie, besluiten om een sleutelkast aan te kopen.
Deze stap heeft één groot nut, met een goed beheer kan men de sleutel terug vinden, echter de veiligheid en de kost van beheer zijn een belangrijke negatieve factor die niet te onderschatten valt.

Twee veel voorkomende vormen:
- Gewone kast met sleutel waar met labels plaats van de sleutel kan gevonden worden, het ontbreken van de sleutel duit aan dat iemand hem heeft meegenomen. Een dergelijke kast vraagt toch een minimaal beheer door een verantwoordelijke die de deur van de kast bezit en controle met dagboek bijhoud van wie neemt wat mee en wanneer is de sleutel terug. Efficiëntie besparing is te overwegen tussen gemak van terugvinden juiste sleutel en beperkte veiligheid. Meestal is dit een vorm die goed kan toegepast worden voor een kleiner aantal sleutels. Nochtans bestaan er toestanden waar honderden sleutels bewaard worden en er zeven beheerders in dienst zijn om telkens met minimum twee personen 24h/24h in de sleutelkamer het beheer uit te voeren!
-Vrijwel gelijkaardige kast met elektronische controle. Het openen van deze kast gebeurd door een identificatie middel zoals badge, tag of smartphone. Deze identificatie geeft toegang tot de kast en een aantal sleutels die uit locksysteem kunnen verwijdert worden. Bij het verwijderen van de sleutel(s) wordt er een chronologische informatie opgeslagen van de persoon die toegang kreeg en de sleutels die hij heeft meegenomen. Ongetwijfeld een hogere veiligheid maar dure investering waarbij het kopiëren en stelen van sleutels, beheer en identificatie middel niet opgelost wordt.

Besluit: mechanische sleutels zijn nooit veilig en beperken de efficiëntie op de werkvloer.

Of gebruik je een traditionele sleutel… of gebruik je een elektronische sleutel?

De gebruiker zal onvoorwaardelijk toegang krijgen zonder dat de juiste persoon geïdentificeerd wordt!

Voordeel met elektronische sleutels: de toegang kan uitgeschakeld worden zonder het slot te vervangen.

Ouderdom:

Wanneer fysieke veiligheidsmiddelen zeker een lange levensduur bezitten is dit niet het geval voor elektronische producten in de sector. Net als de evolutie van sleutels over de laatste eeuw, heeft de veiligheidstechnologie stappen gezet om bescherming te bieden tegen nieuwe uitdagingen in overeenstemming met de evolutie van informaticatechnologie. Men kan in het algemeen zeggen dat een installatie van twintig jaar oud niet meer beantwoordt aan de huidige verwachtingen qua veiligheid en efficiëntie.

Paraatheid:

Een state of the art installatie werkt op een onzichtbare manier aan het overwaken van de goede werking van alle onderdelen in de installatie. Vroeger werd dikwijls een goede passief infrarode detector als kwaliteitsvol beschouwd omdat hij nooit een alarm heeft veroorzaakt! In huidige technologie moet elke sensor of besturing op een netwerk verbonden zijn en voldoende informatie verschaffen om de oorspronkelijke gevoeligheid en doel te waarborgen. Zorg ervoor dat camerabeelden regelmatig bekeken worden! Een camera uitval, of een slecht beeld zal tot frustratie leiden pas na het opzoeken van feiten.

Weg met de PIR-detector :

PIR-detectoren die worden gebruikt voor bewegingsdetectie zijn aan het einde van hun leven, omdat camera's veel betere detectie kunnen uitvoeren en kunnen bewijs leveren van detectie. Een PIR kan uit richting geplaatst worden of met een spray gesaboteerd. Een camera is sabotage vrij door interne beeld analyse en constante communicatie. Gebruik een dergelijke detector voor het automatisch aansteken van het licht maar zeker niet als sensor voor een veiligheidsdoel.

Daarbij vraagt een PIR een voeding terwijl de camera gevoed wordt langs PoE. In het algemeen zou een detectie niet langer een alarm mogen geven zonder het bewijs te hebben van de oorsprong van het alarm.

Wetten en reglementering:

In de laatste decennia zijn reglementering, standaarden, wetten, verordeningen,… ontstaan die niet altijd de zaak vergemakkelijken. Nog erger gesteld is het met de opvatting dat een systeem hierdoor kan aanzien worden als conform. Deze regelgevingen moeten echter aanzien worden als een fundament van een veiligheid systeem en niet als het eind objectief. Franse, Duitse en Engelse nationale instituten voor de veiligheid spreken op een moderne manier van "*guides*", "*guidelines*", "*richtlinien*" in gepubliceerde documenten.

Wetten en normen worden opgemaakt onder invloed van fabrikanten en lobby's en hebben vaak tot gevolg dat niet meer wordt nagedacht maar uitgevoerd. Nog erger is een huidige tendens van keuringen volgens norm in plaats van op werking!

In mijn persoonlijk advies studies gaat er geen maand voorbij zonder een confrontatie met onzinnige situaties waar veiligheid door wettelijkheden beperkt wordt.

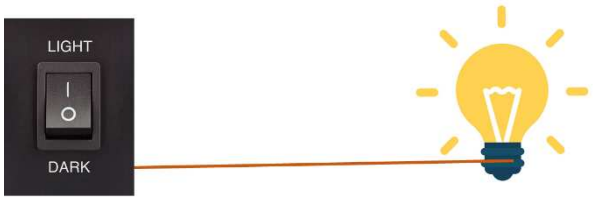
Voedingen:

Elk toestel heeft een voeding nodig, een tabel moet opgemaakt worden en een bepaling over welke autonomie elk apparaat moet beschikken. Ga na van welke factoren de algemene netvoeding afhankelijk is en welke aardlekken een onderbreking kunnen veroorzaken. As built documenten moeten een ééndraadschema van netvoeding aansluitingen bevatten voor alle aansluitingen in het systeem van elektrische aankomst tot elk toestel. Laag spanning voedingen van toestellen moeten een afgewogen autonomie bezitten.

Functiebehoud en functiecontrole :

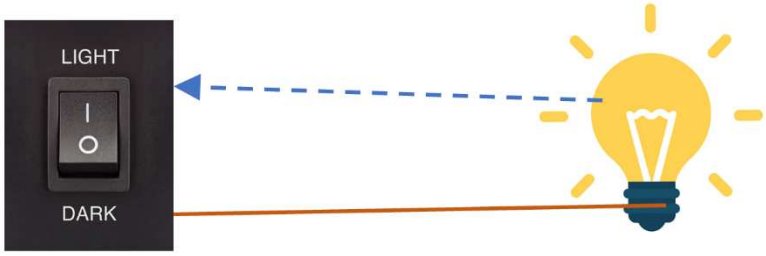
In contrast met elektrische installaties moet een veiligheidsinstallatie gebouwd worden met een functiebehoud. Enkelvoudige fouten mogen de verdere werking van een veiligheidsinstallatie niet verstoren.

Verlichtinginstallatie schakelaar bedient lamp zonder controle:



Beveiligingstechniek:

Functiecontrole schakelaar bedient de lamp maar het resulterende licht wordt gecheckt als bevestiging:



Functiebehoud wordt gegarandeerd door een lusbekabeling of redundante bekabeling:

Bovenstaande principes zijn een eerste stap, doch voor veel toepassingen en zeker voor brand moet men ook bepalen wat men kan verliezen aan functionaliteit bij een enkele fout.

Interventie, evacuatie, invacuatie:

Deze drie begrippen houden verband met elkaar en hebben zowel elk een model van uitvoering als elk een onderling verband. Een op voorhand bepaald programma van uitvoering en verband moet hiervoor opgesteld worden. Hiervoor is duidelijke observatie en bestuurbaarheid noodzakelijk vanuit een operatief centrum.

Interventie algemeen :

In dit artikel laat ik de veiligheidsexpert nadenken over de veiligheid en het safety aspect van blinde interventie. Reeds vele jaren is het mogelijk dat een alarmsysteem op directe of indirecte weg een interventie laat gebeuren zonder dat er maar één luttele aanwijzing is over het gevaar dat zich voordoet voor de interventieploeg en voor de betrokken personen!
Deze ondenkbare situatie is enkel in geval van safety met als voorbeeld brand te begrijpen.

Besluit: een interventie zou niet mogen plaats grijpen zonder dat men de noodsituatie heeft kunnen vaststellen met beelden, geluiden of andere gedetailleerde informatie die de aard van de noodtoestand weergeven.

Interventie :
-Moet steeds gebeuren volgens plan in functie van de gegevens betreffende de aan de hand zijnde feiten.
-Het operatief centrum van beveiliging, die ontoegankelijk is, mag nooit verlaten worden, behalve wanneer het zelf in het gedrang komt (vb. brand)
-De allereerste interventie bestaat erin alle mogelijke op afstand bestuurbare middelen aan te wenden om vanuit het operationeel centrum de toestand te verhelpen, mensen en middelen te beveiligen.

-De tweede fase van interventie is eigen aanwezige mensen opdrachten verschaffen om handelingen uit te voeren ter bescherming. (personeel met kennis van risico's en site kennis)
-De derde fase bestaat erin uitwendige professionele versterking op te roepen met gelimiteerde kennis over plaatselijke risico's en infrastructuur. Belangrijk is een onmiddellijke inschatting te maken van de noodwendige kracht en tijd .

Enkele factoren dewelke in rekening moet worden gebracht:
1.De afteleggen weg van de intervenant tot aan plaats van interventie rekening houdende met tijd van optreden en hindernissen onderweg. Let wel in geval van een aanval zal de bedreiger de weg wellicht niet vrij laten en hoogst waarschijnlijk bemoeilijken!
2. Is toegang tot de site mogelijk op ogenblik van interventie, wie heeft de middelen om het doel te bereiken.
3. Is begeleiding van een kenniscentrum op de hoogte van de site tijdens de interventie mogelijk?
4. De aanval kan langs een door de interventieploeg ontoegankelijke weg gebeurd zijn. (vb. dak)
5. De aanvaller met kennis van de site kan de terugweg van uit de site anders plannen dan de heenweg.
6. De bemanning van het security centrum kan nooit fysiek deelnemen aan de interventie en moet voor begeleide communicatie zorgen.

Evacuatie:

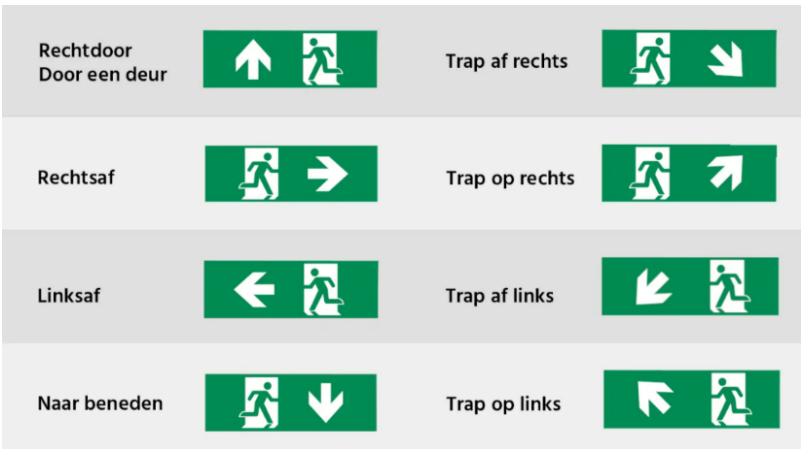
-Een bevel tot evacuatie is een gevaarlijke onderneming waarbij mensen blootgesteld worden aan een onbekende vlucht in paniek toestand om een omgeving te verlaten.

-Verschillende hulpmiddelen kunnen een evacuatie verbeteren:

- Voer geen totale evacuatie uit wanneer niet noodzakelijk.
- Gebruik audio begeleiding om de evacuatie te leiden. Geefnamen aan vertrekken, gangen, bouwdelen…Denk aan geografische plaatsen, belangrijke personages, eigen productnamen,….Dit zijn de beste te herinneren oriëntaties in het audio bericht.
- Gebruik dynamische evacuatie richting aanduiding.
- Gebruik identificatie van personen dewelke het verzamelpunt hebben bereikt. (mustering)

Twee wegen ?

Huidige standaard pictogrammen voor vluchtwegen:



Dynamische vluchtweg aanduiding:

Net zoals de standaard pictogrammen hebben dynamische vluchtweg borden dezelfde figuur van de persoon die door een deur loopt aan één zijde van het bord terwijl de tweede helft van het bord een bestuurbaar pictogram heeft. Voorbeeld:

Met deze nieuwe technologie kan men een evacuatie oriënteren in functie van informatie uit de branddetectie of de toegangscontrole.

Invacuatie:

Invacuatie gebeurt om personen veilig te stellen in een beschermende ruimte bestand tegen het gedetecteerde gevaar. Dit gevaar kan komen van agressie, actieve schutter, ontploffingsgevaar, toxische stoffen en gassen, straling… Een goed gelegen en beveiligde ruimte met afzonderlijke luchtverversing moet echter door de architect voor de constructie ingepland worden. Invacuatie vraagt net als evacuatie een identificatie van de personen die de beschermde ruimte betreden. (mustering)