Visiedocument

Rol van vergunde alarmcentrales in de integrale veiligheid

Oktober 2017

De **Alarm Centrale Associatie (ACA)** is de beroepsvereniging van de vergunde alarmcentrales, en vertegenwoordigt meer dan 95% van de aangesloten alarmsystemen in België.

Voor een overzicht van de leden van ACA verwijzen we naar de website van ACA (www.aca-monitoring.be)

De ACA stelt zich onafhankelijk op van alle andere beroepsverenigingen voor beveiliging en bewaking en verleent haar medewerking aan initiatieven die de veiligheid van de klant verbeteren. Om dat te bereiken wil de ACA een gesprekspartner zijn van de overheid, lokale besturen en publieke en private veiligheidsactoren.

Inhoudsopgave


brand
interventies
diefstal
filtering
lone workers
informatie
sluikstorten
camera's
drones
België
verificatie
overlast
mogelijkheden
politie
alarmcentrales
IoT
mens en technologie
meldkamer
ondersteunen
rol
geconnecteerd
keten
beschikbaarheid
toegevoegde waarde
samenwerking
besturen
live
visie
systemen
bijstand
artificial intelligence
integrale veiligheid
gebouwen
reactie
cameraondersteuning
kwaliteitsborging
stakeholders
slim
veiligheid
data
geweldscriminaliteit
brandweer
inbraak
remote
alarmen
pilootproject
preventie
ACA

Managementsamenvatting

Veiligheid is een actueel thema dat volop in verandering is en steeds complexer wordt. Om veiligheid op een efficiënte en effectieve manier te kunnen garanderen, werken verschillende publieke en private veiligheidsactoren in toenemende mate samen. De Alarm Centrale Associatie (ACA), de beroepsvereniging van de vergunde alarmcentrales, wil haar unieke competenties inzetten en inspelen op technologische vooruitgang om actief mee te bouwen aan de integrale veiligheid. Het belang van de maatschappij moet hierin voorop staan.

De sector van alarmcentrales vandaag

De leden van ACA, vergunde alarmcentrales, vertegenwoordigen meer dan **95% van de aangesloten alarmsystemen** in België. Als hoofdactiviteit monitoren ze signalen van **inbraaksystemen**, waar ook branddetectoren en technische alarmen op aangesloten kunnen zijn. Ze filteren ontvangen signalen op valse alarmen en zorgen voor een snelle en wettelijke afhandeling. Alleen wanneer nodig verwittigen ze de politie, brandweer en/of hulpdiensten - ze spelen dus een belangrijke rol als **filter** naar deze stakeholders. Ze garanderen een **snelle en gerichte reactie** dankzij hun permanente beschikbaarheid en zeer strenge service level overeenkomsten.

Daarnaast maken ze gebruik van **geavanceerde technologie om bewaking op afstand** aan te bieden. Meldkameroperatoren kunnen vanop afstand toegang tot een site verschaffen, of dankzij videomonitoring virtuele rondes lopen op afgesproken frequenties.

Veiligheid is in verandering, dus de sector evolueert mee

Verschillende maatschappelijk fenomenen zoals migratie, inkomensongelijkheid en de terreurdreiging leiden tot een **verhoogd gevoel van risico bij de burger en bedrijven**. Burgers en ondernemingen besteden dan ook meer aandacht aan veiligheid & beveiliging. En ze verwachten in toenemende mate **permanente toegankelijkheid en onmiddellijke reactie van veiligheidsactoren** – verwachtingen gecreëerd door spelers uit de interneteconomie zoals Uber. Deze verwachtingen moeten gebalanceerd worden met de niet-aflatende **druk om meer te doen met minder middelen** bij alle publieke veiligheidsactoren.

Het wordt dus steeds complexer voor deze publieke veiligheidsactoren om aan de vraag van burgers en ondernemingen te voldoen en veiligheid te blijven garanderen. In een zoektocht naar efficiëntie en effectiviteit zijn er dan ook steeds **meer samenwerkingen tussen private & publieke partijen**, waarbij elke partij zich op zijn **kerncompetenties** positioneert.

Hierbij is **technologie** aan het veranderen wat mogelijk is. Technologie kan een enorme **meerwaarde** betekenen voor het garanderen van de veiligheid. Zo bewijzen onder meer het **Internet der Dingen** (Internet of Things), **artificiële intelligentie** en **drones** vandaag al hun nut op het gebied van "safety & security" - in de toekomst zullen deze alleen nog maar meer mogelijkheden creëren om veiligheid beter te kunnen garanderen. Voor de leden van ACA maken deze technologieën bijvoorbeeld betere **verificatie** van alarmen en controle op alarmsystemen mogelijk, ze laten een meer **proactieve en zelfs voorspellende werking** toe en voorzien de sector van interessante **data** – data die gebruikt kan worden voor betere preventie en ter ondersteuning van hulp- en interventiediensten.

Anderzijds brengt technologische evolutie ook **uitdagingen** met zich mee. **Cybercriminaliteit** en **privacy** bijvoorbeeld. Des te meer objecten met een netwerk geconnecteerd zijn, des te gevoeliger ze zijn voor cyberaanvallen. Een gedegen **kwaliteitsborging** voor de hele keten wordt dus steeds belangrijker. Om verschillende systemen goed te laten communiceren, worden **standaardisatie en interoperabiliteit** ook steeds

belangrijker. Ten slotte verhoogt de nood om alarmen te **filteren** – het aantal (valse) signalen zal alleen maar blijven toenemen naarmate er meer objecten met een netwerk geconnecteerd worden en data kunnen uitwisselen.

Bovenstaande trends en de toenemende complexiteit om veiligheid te garanderen, bevestigen de nood aan een **integrale veiligheidsaanpak**. De sector wil hier een actieve rol in spelen.

Onze visie

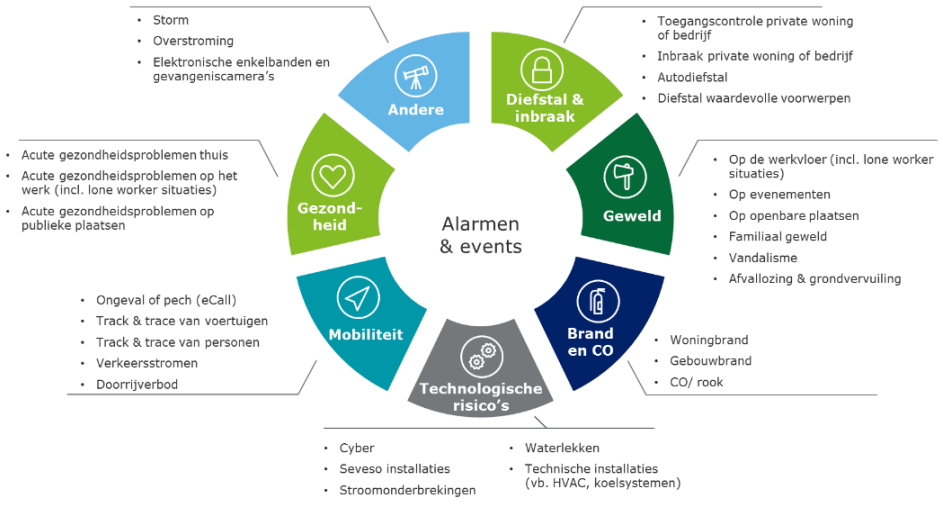
De sector creëert vandaag toegevoegde waarde voor verschillende stakeholders, met een focus op haar kerndomein van inbraak & diefstal en haar functie als filter van valse alarmen. De sector wil haar **gespecialiseerde kennis, permanente beschikbaarheid en geavanceerde technologische oplossingen breder inzetten** om op een efficiënte en effectieve manier bij te dragen aan een veiligere omgeving voor burgers, organisaties, ondernemingen en overheden. Want **veiligheid is een fundamenteel recht**.

Ze heeft volgende accenten gelegd in haar visie:

Preventie, betrouwbare bescherming & bijstand in nauwe samenwerking met relevant spelers
De sector wil een steunpilaar zijn voor elke stap in de keten van preventie, bescherming en bijstand. Ze wil meer nadruk leggen op preventie, en evolueren van het monitoren van alarmen naar het proactief managen van situaties. Tegelijkertijd wil ze streven naar een hogere verbindingsgraad van bestaande en nieuwe alarmsystemen met een meldkamer, om een betrouwbare bescherming te kunnen garanderen voor de eindklant. En ten slotte wil ze interventiediensten bijstaan dankzij (real-time) informatie-uitwisseling, en wil ze ook zelf vanop afstand bijstand blijven verlenen aan eindklanten.

Bredere rol in de strijd tegen onveiligheid: van alarmcentrale naar eventcentrale
Technologische evolutie creëert nieuwe mogelijkheden voor monitoring. De sector wil dan ook evolueren van een alarmcentrale naar een 'eventcentrale', die een breed spectrum alarmen behandelt en events en situaties beheert.

Voor een overzicht van de domeinen waar de sector zich in eerste instantie op wil toeleggen, verwijzen we naar "Operationele invulling van onze visie". Hierbij is het belangrijk om op te merken dat de sector een dynamisch geheel van individuele bedrijven is, die op basis van hun eigen sterktes zullen focussen op bepaalde domeinen.



Orkestreren van relevante stakeholders
De meldkamer is dé plaats waar alle relevante data over uiteenlopende events en alarmen op één plaats geaggregeerd worden. Deze data kan bestaan uit alarmen, maar ook beelden, geluid, locaties enzovoort. De meldkamer is uniek gepositioneerd om al deze datapunten te analyseren en de juiste stakeholders te mobiliseren en te ondersteunen om betere beslissingen te maken. Als 'regisseur' wil de sector streven naar een geïntegreerde en geoptimaliseerde samenwerking met de betrokken stakeholders.

Up-to-date kwaliteitsborging voor de hele keten
Om moderne risico's adequaat het hoofd te kunnen bieden en betrouwbare dienstverlening te garanderen, wil de sector streven naar een up-to-date kwaliteitsborging voor de hele keten, gesteund op: 1) moderne certificering voor de hele keten die de Europese normering volgt; 2) technische kwaliteit van en interoperabiliteit tussen systemen; en 3) respect voor privacy.

Lokale verankering in globale context
De sector wil lokaal verankerd blijven, om operatoren te kunnen inzetten met een adequate talenkennis & ervaring met de lokale context, en als een volwaardige partner mee te werken aan het beleid in België.

Operationele invulling van onze visie

Om haar rol als 'eventcentrale' in te vullen, wil de sector zich in eerste instantie toeleggen op een aantal aangrenzende domeinen die nauw aansluiten bij haar **fundamentele bestaansreden** (samen met andere stakeholders een veilige omgeving creëren) en waarvoor ze haar competenties kan inzetten om **toegevoegde waarde** te creëren voor de betrokken stakeholders:

Inbraak & diefstal: Inspelen op technologische voortuitgang voor een meer performante dienstverlening (vb. betere verificatie en voorspellend werken dankzij slimme camera's) en meer inzetten op remote diensten zoals remote access control en virtuele rondes.

Brand & gebouwzekerheid: Een geïntegreerd antwoord bieden op onveiligheid in gebouwen (brand, CO, waterlekken…), en verifiëren van brandalarmen in situaties waar de technologie het toelaat. Ook ondersteunen van interventies door data-uitwisseling en toegang verschaffen vanop afstand.

Geweldscriminaliteit, overlast & sluikstorten: Cameraondersteuning bieden voor de preventie van en reactie op geweldscriminaliteit, overlast en sluikstorten – ook op publiek domein. Meer in de private sfeer ook waken over mensen in risicosituaties dankzij 'virtual close protection[1]'.

'Lone workers': Waken over veiligheid ('safety & security') van mensen die alleen werken zonder rechtstreeks toezicht, zoals techniekers voor telecom- en energiebedrijven, truckchauffeurs en verkopers.

Verkeer en mobiliteit: 'Remote access control' of gecontroleerd toegang verschaffen tot gevoelige zones op publiek domein (vb. voetgangerszones). Ook filteren en verifiëren van signalen van slimme camera's in het straatbeeld, en (internationale) oplossingen bieden voor eCall[2].

[1] Vanop afstand meekijken tijdens risicomomenten zoals opening & sluiting en hulp sturen op het moment dat er zich verdachte omstandigheden of personen voordoen
[2] eCall-systeem in wagens stuurt bij een ongeluk automatisch (of manueel via een drukknop) een noodoproep uit naar een alarmcentrale. Het geeft onmiddellijk ook cruciale informatie door zoals de exacte locatie en het uur van het ongeluk

Naar een win-win voor alle stakeholders

De sector wil toegevoegde waarde creëren voor de maatschappij, burgers en publieke & private stakeholders in het kader van haar prioritaire domeinen.

Toegevoegde waarde voor publieke stakeholders

Maatschappij & burgers	• Betere **publieke veiligheid** en verhoogd **veiligheidsgevoel** • **Beperking** van potentiële **schade** als gevolg van brand, CO-gas, waterlekken, inbraak enzovoort
FOD Binnenlandse Zaken	• Samen een **toekomstgericht beleid** uitwerken dat de **samenwerking** tussen en **inzet** van **veiligheidsactoren optimaliseert**, en dat ondersteund wordt door objectieve **statistieken** en **inzichten "uit het veld"** • Reduceren van **onnodige interventies** van politie en brandweer • Stimuleren van **innovatie**
Lokale besturen	• **Kostenefficiëntie** door optimale inzet middelen en **maximale benutting bestaande camera's** op publiek domein • **Voorkomen en inperken** van **kosten** als gevolg van **geweldscriminaliteit, overlast en sluikstorten** • Verhogen **veiligheidsgevoel** van ondernemers, bezoekers en bewoners zonder ingrijpende maatregelen
Politie	• Meer focus op **kerntaken** en minder **onnodige interventies** • **Effectievere interventies** dankzij data-uitwisseling en vroegere detectie • Toegang tot **state-of-the-art technologie** zonder hoge investeringskost (in samenwerking met bewakingsondernemingen)
Brandweer	• Ondersteuning bij verwezenlijking van **strategische doelstellingen** • **Betere interventiedossiers** en **effectievere interventies** dankzij data-uitwisseling en vroegere detectie

Toegevoegde waarde voor private stakeholders

Verzekeraars	• **Aantal claims** terugdringen en de **grootte van claims** beperken • Beschikken over **statistieken en informatie** om werking en toekomstige normering te ondersteunen
Installateurs	• Samen afstemmen rond de **toepassing van nieuwe technologieën en nieuwe businessmodellen** om technologische evolutie te volgen
Bedrijven	• **Geïntegreerde aanpak** van onveiligheid in **gebouwen** • Verhoogde veiligheid voor **'lone workers'** en **personeel in risicosituaties** • **Kostenefficiëntie** door meer remote diensten
Sector zelf	• Ruimte voor de sector om te groeien, en om verder te kunnen **blijven investeren in mensen, innovatie en technologie** • **Erkenning** als betrouwbare en kwaliteitsvolle partner

Ons engagement

Om haar visie te kunnen verwezenlijken en een win-win te vinden met relevante stakeholders wil de sector zichzelf engageren op volgende fronten.

Een volwaardige partner zijn in de integrale veiligheid

- Permanente vertegenwoordiging opzetten met **capaciteit tot dialoog en actie**
- Bruggen bouwen tussen **private sectorfederaties**, en toenadering zoeken tot **FOD Binnenlandse zaken**
- Nauwer samenwerken met **publieke en private veiligheidsactoren**, en op lokaal niveau **pilootprojecten** opzetten
- Actiever worden in **CoESS*** en België meer op kaart zetten als voortrekker van de "meldkamer van de toekomst"

Voorhoede van innovatie zijn

- **Technologische vooruitgang** van dichtbij **opvolgen**
- Relevante **toepassingen** in het **buitenland** identificeren
- Inzichten publiceren/ **communiceren** naar een breed publiek
- Private meldkamers als '**labo-omgeving**' voor pilootprojecten ter beschikking stellen

Streven naar standaardisatie, interoperabiliteit en cybersecurity

- Samen met CoESS*, de **afstemming van standaarden** orkestreren en drijven in België
- Mee **cyberbedreigingen** een adequaat antwoord bieden en **respect voor privacy** garanderen

* Confederation of European Security Services

The way forward

Om de basis te leggen voor volgende stappen heeft de sector suggesties uitgewerkt voor de samenwerking met haar verschillende stakeholders en heeft ze concrete actiepunten geïdentificeerd. Voor een volledig overzicht van **actiepunten** verwijzen we naar "**Deel 7 | The way forward**" in het rapport.

Samenwerking met FOD Binnenlandse zaken

De sector wil in dialoog treden met IBZ Veiligheid & Preventie en Civiele Veiligheid, en evolueren naar **structureel overleg** dat ondersteund wordt door objectieve **statistieken**. Ze wil hierbij actief meewerken aan de **concrete invulling en evaluatie** van het **beleid**. Op het gebied van brand & gebouwveiligheid kan ze zich engageren voor **verificatie** van alarmen, wanneer de technologie het toelaat.

Ze verwacht van FOD Binnenlandse Zaken steun om **pilootprojecten** van de sector met andere stakeholders te bespoedigen. ACA zal op haar beurt FOD Binnenlandse Zaken betrekken en op de hoogte houden van de pilootprojecten die ze opzet.

Samenwerking met lokale besturen

De sector wil **publiek-private samenwerkingen** opzetten met lokale besturen, voorafgegaan door een beperkt aantal goedgekozen **pilootprojecten** in samenwerking met andere stakeholders zoals lokale politiezones.

Samenwerking met politie

De sector streeft naar een **ketengerichte samenwerking** met de politie, met wederzijds respect voor de verantwoordelijkheden van de participerende partners. Naar het model van de Regionale Toezicht Ruimten in Nederland wil ze proactief toezicht houden op publiek domein, onder regie van de politie. Om voldoende visie te ontwikkelen "vanuit het veld", stelt de sector voor om samen met lokale politiezones en lokale besturen **pilootprojecten** op te zetten.

Samenwerking met brandweer

De sector stelt voor om samen met (een) lokale brandweerzone(s) **pilootprojecten** op te zetten rond **verificatie** van brandalarmen en **informatie-uitwisseling**. Meldkamers van ACA leden kunnen hiervoor als **labo-omgeving** dienen.

Samenwerking met verzekeraars

Leden van ACA willen **statistieken** en **informatie** verzamelen en delen met verzekeraars om hun werking te ondersteunen. Daarnaast willen ze een gesprekspartner zijn voor **certificering** zoals INCERT & BOSEC, en mee streven naar een adequate aanpak voor **cyber security** van digitale (IP-gebaseerde) inbraaksystemen. Op haar

beurt verwacht ACA van verzekeraars dat ze, afhankelijk van de situatie, **de aansluiting van alarmsystemen op een meldkamer** aanmoedigen.

Samenwerking met installateurs

ACA wil intensiever samenwerken met de Belgische beroepsvereniging van de elektronische beveiliging (ALIA Security), zowel voor het domein van inbraak & diefstal als voor brand en gebouwzekerheid. ACA ziet mogelijkheden om beter af te stemmen rond de **toepassing van nieuwe technologieën en businessmodellen**.

Samenwerking met bedrijven

Specifiek rond de problematiek **van lone workers** en '**virtual close protection**' wil de sector overleg plegen met vertegenwoordigers van hoog-risicosectoren om de noden beter om te zetten in doelmatige oplossingen. De sector zal zoeken naar een pilootsector om samen een **proefproject** te lanceren, en wil streven naar voldoende **regelgeving** en **kwaliteitsgaranties**.

De sector wil ook nauw blijven samenwerken met **bewakingsondernemingen**, om samen **totaaloplossingen** in de markt te kunnen zetten.

3. Conclusie

De sector wil zich **engageren** om een **volwaardige partner** te zijn in de integrale veiligheid. ACA heeft een duidelijke **visie** met betrekking tot haar rol, en wil een **win-win** creëren samen met relevante publieke en private veiligheidsactoren. Ze nodigt haar stakeholders uit om in **dialoog** te treden.

Deel 1 | De sector vandaag

De leden van ACA, vergunde alarmcentrales, vertegenwoordigen meer dan 95% van de aangesloten alarmsystemen in België. Ze combineren gespecialiseerde kennis en technologische oplossingen om binnenkomende alarmen te filteren op valse alarmen en zorgen voor een correcte en wettelijke afhandeling.

1. De sector van alarmcentrales vandaag

De **leden van ACA** monitoren signalen van verschillende alarmsystemen zoals inbraakdetectiesystemen en volgsystemen ('track & trace'). Zij zijn **vergunde** alarmcentrales, omdat ze bewakingsactiviteiten mogen uitvoeren en hun werking te maken heeft met de maatschappelijke veiligheid. Ze staan onder het toezicht van de minister van Binnenlandse Zaken en moeten aan wettelijke voorwaarden voldoen om een vergunning te krijgen (telkens voor een periode van vijf jaar).

In België zijn er naast de vergunde alarmcentrales ook verschillende centrales en callcenters waarvan de activiteiten niet door de wet gereglementeerd zijn, zoals:

- Centrales waar dringende oproepen voor de hulpdiensten worden aangenomen (noodoproepcentrales 100/112 voor brandweer of medische hulp en de communicatie- en informatiecentra 101 voor de politie)

- Centrales voor reis- & pechbijstand en zorgcentrales (zoals Europ-Assistance, Touring, MUTAS en het Wit-Gele Kruis)
- Interne alarmcentrales van grote bedrijven

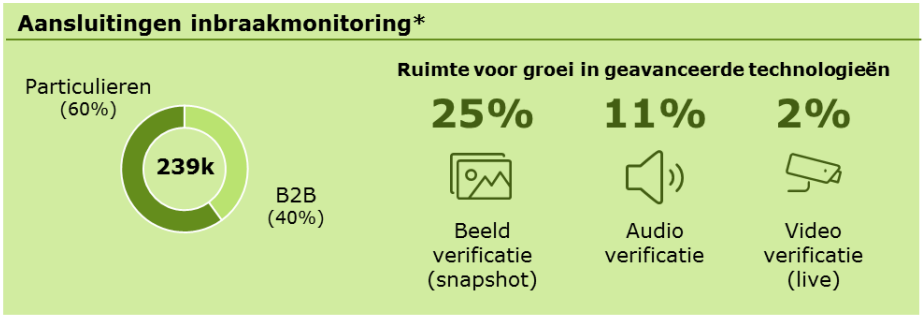
De leden van ACA **controleren ontvangen signalen**, **interpreteren**, **verifiëren** of het wel om een echt alarm gaat en **verwittigen** de **gebruiker** van het bewaakte pand/ goed of zijn contactpersoon, conform de op voorhand afgesproken instructies. Indien nodig verwittigen ze ook de **politie- en hulpdiensten**, steeds na verificatie van het alarm. Ze kunnen ook **bewakingsagenten** aansturen die een interventie na alarm uitvoeren. De **installatie** van deze alarmsystemen gebeurt door een erkende installateur. Een aantal leden van ACA zijn geïntegreerd en hebben installatieactiviteiten, anderen werken nauw samen met onafhankelijke installateurs.

In 2016 waren ongeveer **264 000 alarmsystemen aangesloten** op de meldkamers van de ACA leden – meer dan **95%** van alle aansluitingen in België. De **hoofdactiviteit** van de sector is het monitoren van **inbraaksystemen**, waar ook **branddetectoren** en **technische alarmen** op aangesloten kunnen zijn (91% van alle aansluitingen).

* Inbraakmonitoringaansluitingen inclusief inbraaksystemen waar branddetectoren en technische alarmen op aangesloten zijn

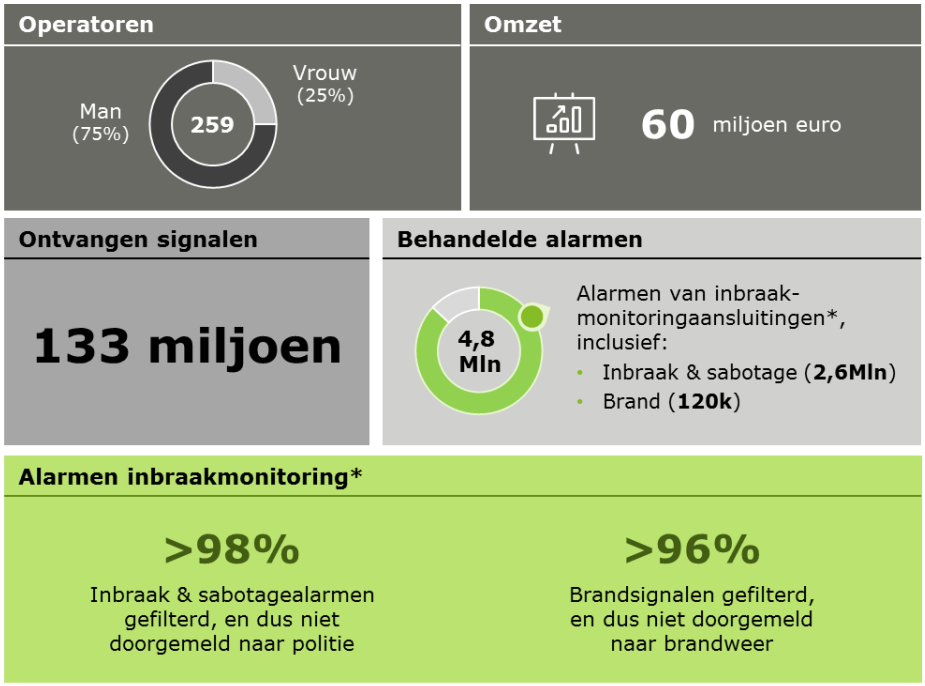
** Andere: pure technische & brandsystemen, sociale en persoonsalarmen

Het monitoren van de inbraakmonitoringaansluitingen gebeurt bij zowel particulieren (60% van de aansluitingen) als ondernemingen (40%). Naast 'traditionele' detectoren en sensoren wordt hier meer en meer gebruik gemaakt van **geavanceerde technologie** zoals beeldverificatie en live videoverificatie. En er is nog ruimte voor verdere groei van deze geavanceerde technologieën.



* Inbraakmonitoringaansluitingen inclusief inbraaksystemen waar branddetectoren en technische alarmen op aangesloten zijn

De sector is relatief **klein** in termen van omzet en aantal werknemers, maar creëert wel **belangrijke toegevoegde waarde** voor hulp- en interventiediensten dankzij haar functie als filter van (valse) alarmen. In 2016 werd van de inbraak & sabotagealarmen **meer dan 98% gefilterd**, en dus niet doorgemeld naar de **politie**. Van de brandalarmen werd **meer dan 96%** gefilterd voor de **brandweer**.



* Inbraakmonitoringaansluitingen inclusief inbraaksystemen waar branddetectoren en technische alarmen op aangesloten zijn

2. Effectieve monitoring van en reactie op alarmen, dankzij gespecialiseerde kennis en technologie

De vergunde alarmcentrales worden **24/24 en 7/7** bemand door specifiek opgeleide **alarmoperatoren**. In geval van alarm, zullen deze de nodige maatregelen treffen, steeds conform de op voorhand afgesproken **instructies en (wettelijke) procedures**.

De alarmoperatoren zijn de steunpilaren van de sector en haar klanten. Om hen optimaal te ondersteunen en op een effectieve manier de veiligheid van burgers, organisaties en ondernemingen te kunnen garanderen, maakt de sector intensief gebruik van geavanceerde **technologie**. Door het gebruik van **videomonitoring** bijvoorbeeld, kunnen meldkamers bewaking op afstand aanbieden. Zo kunnen operatoren in de meldkamer op afgesproken frequenties beelden afkomstig van verschillende camera's op een site bekijken om een '**virtuele ronde**' te lopen. Deze virtuele ronde wordt dus geïnitieerd vanuit de alarmcentrale, en wordt niet door een alarm getriggerd. Videomonitoring zorgt wel voor nuttige bijkomende informatie in geval van een alarm of incident - men kan live volgen wat er zich afspeelt, en dus sneller aangepaste maatregelen nemen.

Daarnaast kunnen operatoren vanop afstand toegang tot een site verschaffen (‘**videoportiersdiensten’**), of ongewenste personen toespreken vanop afstand (‘**audio-ontrading’**).

Ten slotte verwerkt de sector ook in toenemende mate **signalen die door slimme camera’s gegenereerd** werden. Deze camera’s functioneren als detector en worden onder meer ingezet voor het identificeren van perimeteroverschrijding en brand.

3. Toegevoegde waarde voor een ruime groep belanghebbenden

Ook al is het wettelijk niet verplicht om een alarmsysteem aan te sluiten op een alarmcentrale in België, toch heeft dit verschillende **voordelen**:

- **Menselijke verificatie & interpretatie**, met als gevolg een effectieve **filtering** van een zeer groot aantal valse alarmen: de sector houdt meer dan 98% van de alarmen voor de politie tegen, en 96% voor de brandweer
- Mogelijkheid om te **interageren** met een professioneel opgeleide operator in stresssituaties
- 24/7 beschikbaarheid, strikte ‘service level’ overeenkomsten en mogelijkheid tot rechtstreekse doormelding naar orde- en/of hulpdiensten na verificatie, voor een **garantie op een snelle en gepaste reactie**
- **Gemoedsrust** voor de eindklant – zekere en snelle reactie, ook wanneer de eindklant zich niet in het gebouw bevindt
- **Betrouwbaarheid** en **kwaliteit**: operatoren worden gescreend door Binnenlandse Zaken en veiligheidsdiensten en geselecteerd op basis van zeer strenge toelatingsvoorwaarden[3]. Elke operator krijgt een wettelijke opleiding van 70 uren en vervolgens een doorgedreven

[3] Toelatingsvoorwaarden: blanco uittreksel strafregister van maximaal 6 maanden oud, geslaagd zijn in psychotechnisch onderzoek

interne training. Er gebeuren ook frequente controles op vergunde meldkamers door externe inspectiediensten. Daarnaast zijn de leden van ACA ISO[4] en/of INCERT[5] gecertifieerd – ze leven zeer strenge kwaliteitsregels na en ondergaan regelmatige controles die borg staan voor een optimale beveiliging. De individuele leden hebben ten slotte ook interne operationele controlediensten en structuren

[4] ISO 9001:2015

[5] De toelating tot het gebruik van het INCERT-merk vloeit uit een conformiteitcertificatie van de alarmcentrales met "Het reglement voor de certificatie van alarmcentrales" en met de "Specificaties voor bewakingscentrales T020" die uitgegeven worden door het Belgisch Elektrotechnisch Comité (BEC)

Deel 2 | Trends

Verschillende maatschappelijke, economische en technologische veranderingen hebben een grote impact op het gebied van veiligheid, en dus ook op de sector van alarmcentrales.

1. Maatschappelijke trends

1.1 Verhoogd gevoel van risico

Verschillende maatschappelijk fenomenen zoals **migratie**, **inkomens-ongelijkheid** en de **terreurdreiging** leiden tot een verhoogd gevoel van risico bij de burger en bedrijven. Bij een recente peiling van De Standaard geeft bijvoorbeeld meer dan de helft van de Vlamingen (51%) aan dat ze piekeren of ze morgen nog in een veilig land zullen leven. Ook de **vergrijzing** speelt hier een rol – volgens deze peiling is dit resultaat in vrij grote mate op het conto te schrijven van de oudere generatie (56+), die beduidend meer dan jongeren vreest voor onveiligheid.

Daarnaast blijven we kampen met **agressie** in verschillende omgevingen, waaronder op de **werkvloer**. Winkelpersoneel, werknemers van ziekenhuizen en openbare instanties krijgen nog regelmatig te maken met geweld. Ook de grote groep '**lone workers**' zijn kwetsbaar voor agressie en worden er nog steeds mee geconfronteerd. Deze mensen werken immers alleen en zonder rechtstreeks toezicht. Voorbeelden zijn techniekers voor telecom- en energiebedrijven en mobiele werkers zoals truckchauffeurs en verkopers.

1.2 Vraag naar permanente toegankelijkheid en onmiddellijke reactie van veiligheidsactoren

Het verwachtingspatroon van mensen werd grondig hertekend door spelers uit de digitale economie zoals Uber - we verwachten nu toegang tot dienstverlening **waar en wanneer we dat willen**. Mensen trekken deze verwachtingen door naar alle dienstverleners – we verwachten dus ook permanente toegankelijkheid en onmiddellijke reactie van veiligheidsactoren.

2. Economische trends

2.1 Publiek-private samenwerkingen voor optimale effectiviteit & efficiëntie

Het garanderen van de publieke veiligheid is niet langer een taak voor de overheid alleen, maar is een verantwoordelijkheid van iedereen. Bovendien streven alle betrokken partijen naar maximale effectiviteit en efficiëntie, door de **druk om steeds meer te doen met minder middelen**. Er vormen zich dan ook steeds meer publiek-private samenwerkingen, waarbij elke actor zich zo veel mogelijk concentreert op zijn **kerncompetenties**.

2.2 Internationalisering van de sector, en veranderingen in de waardeketen

Criminaliteit is geen lokaal gegeven. De sector krijgt dan ook steeds meer vragen voor de ondersteuning van internationale klanten, en ziet een toenemende internationalisering en ontplooiing van **grensoverschrijdende activiteiten.**

Daarnaast kent de sector een golf van **consolidatie**, waarbij overnames meestal gebeuren door **internationale groepen**. Zeker voor kleinere spelers worden de strenge investeringsvereisten immers te zwaar.

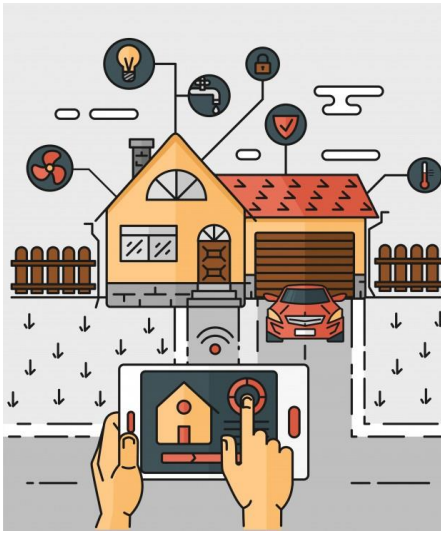
Er zijn ook **nieuwe spelers** die zich op het terrein begeven – verschillende technologiebedrijven en telecomoperatoren bieden nu beveiligings-oplossingen aan, voornamelijk voor de residentiële markt. De sector verwacht dat deze nieuwe spelers mee een **impuls** zullen geven aan de penetratie van gemonitorde alarmsystemen. De penetratiegraad van gemonitorde alarmsystemen in België (3%) ligt nog steeds lager dan verschillende landen zoals Noorwegen (17%), Zweden (11%), Ierland (11%) en Spanje (7%).

3. Technologische trends

De inzet van technologie kan een enorme meerwaarde betekenen voor het garanderen van de veiligheid, maar brengt ook uitdagingen met zich mee. De sector van vergunde alarmcentrales verwacht dat volgende trends de grootste impact zullen hebben.

3.1 Internet of Things (IoT) en slimme gebouwen

Het Internet of Things (IoT of Internet der Dingen) staat voor het verbinden van alledaagse voorwerpen met een netwerk om gegevens uit te kunnen wisselen. **Slimme objecten** spelen hierbij een sleutelrol – dankzij het gebruik van sensoren kunnen deze objecten de omgeving in zich opnemen, en ook een deel van de signaalverwerking gebeurt al door deze objecten zelf. Via ingebedde netwerktechnologie kunnen ze dan met elkaar communiceren, gebruik maken van internetdiensten en interactief communiceren met mensen.



Illustratie van een slim huis

Eén van de belangrijkste toepassingen van het IoT die de laatste jaren snel opkomt, zijn **slimme gebouwen**. De technologie achter deze slimme gebouwen bestaat uit geconnecteerde objecten die gebruik maken van netwerktechnologieën zoals Wi-Fi en LPWAN (Low-Power Wide-Area Network zoals LoRa en SigFox) om te connecteren en communiceren met andere objecten binnen en buiten het gebouw.

Voorbeelden van dergelijke IoT objecten zijn slimme camera's, geconnecteerde bewegingsdetectoren en slimme huishoudtoestellen. Daarnaast kunnen ook systemen uit de operationele technologie (OT), zoals ventilatie, verwarming, airconditioning en verlichting geconnecteerd worden.

Deze 'slimme' objecten en systemen **delen data** met de gebruiker en kunnen **vanop afstand bediend** worden, bijvoorbeeld via een app op smartphone of tablet, of via een wandterminal. Daarnaast zijn slimme gebouwen ook tot **gebouwautomatisering** in staat. Zo kan je bijvoorbeeld een slim huis programmeren om automatisch de verwarming in te schakelen als je op de terugweg bent van je werk naar huis (gebaseerd op de locatie van je smartphone).

Systemen voor **beveiliging en toegangscontrole** zijn een belangrijk **onderdeel van slimme gebouwen**. De markt voor deze systemen in West-Europa bedroeg ongeveer €1,1 miljard in 2015, en wordt verwacht te groeien naar €4,5 miljard tegen 2020.

Geconnecteerde beveiligingssystemen bestaan onder meer uit **elektronische sloten**, **geconnecteerde sensoren** (vb. deur- en raamsensoren), **camera's** en **detectoren** (vb. beweging, brand, CO, HVAC,

waterlekken). Deze worden allemaal naadloos **geïntegreerd**, en kunnen **geautomatiseerd** of **vanop afstand bediend** worden. Zo kunnen gebruikers via hun smartphone of tablet het alarm inschakelen/ uitschakelen of deursloten openen/ sluiten. Wanneer een event wordt gedetecteerd, verwittigen deze systemen de gebruiker en/of een meldkamer. Door de toenemende integratie van camera's, worden hierbij **steeds meer foto's of videobeelden** rechtstreeks doorgestuurd.

In deze markt vinden we de klassieke aanbieders van alarmsystemen, maar ook in toenemende mate **technologiespelers** (vb. Google Nest) en **telecombedrijven** (vb. Comcast Xfinity, AT&T Digital Life), zeker voor het residentiële segment. In dit segment is de vraag vooral groot naar geconnecteerde beveiligingscamera's, inbraakalarmen en rookmelders.

De opkomst van IoT en systemen voor beveiliging en toegangscontrole in de context van slimme gebouwen heeft verschillende **implicaties** voor de sector:

- Omdat slimme systemen de gebruiker verwittigen en ze gemakkelijk bediend kunnen worden, is het gemakkelijker voor gebruikers om **zelf de monitoring van hun systeem voor hun rekening te nemen**. Bepaalde gebruikers zullen denken dat dit voldoende is, maar natuurlijk weegt dit niet op tegen de voordelen van permanente beschikbaarheid en de (verplichte) snelle reactie die vergunde meldkamers kunnen bieden
- De **nood aan filtering en verificatie** zal alleen nog maar toenemen, aangezien er steeds meer objecten gemonitord worden en er dus meer alarmen gegenereerd worden. De sector verwacht dan ook dat ze voldoende toegevoegde waarde kan creëren om relevant te blijven, ondanks de opkomst van zelf-gemonitorde systemen
- IoT en slimme gebouwen creëren **mogelijkheden voor meldkamers om hun aanbod te verbreden**. Verschillende bedrijven in binnen- en buitenland die monitoring diensten aanbieden voor inbraakalarmen, hebben nu bijvoorbeeld ook energie- en watermanagement aan hun diensten toegevoegd, of waken over kritische processen zoals koelinstallaties. Het wordt ook gemakkelijker om diensten zoals toegangscontrole vanop afstand te leveren, zonder dat er ter plaatse iemand aanwezig moet zijn
- Het is van belang dat de verschillende systemen, bijvoorbeeld in een slim gebouw, voldoende met elkaar kunnen communiceren – **standaardisatie en interoperabiliteit** worden steeds belangrijker
- Het feit dat deze slimme systemen gebruik maken van netwerktechnologieën heeft ook implicaties. Enerzijds wordt het mogelijk voor meldkamers om **te allen tijde de status van sensoren, detectoren en dergelijke te controleren**, om er zeker van te zijn dat alles nog naar behoren werkt en er niet mee geknoeid is. Anderzijds zijn deze systemen **kwetsbaar voor cyberaanvallen**. Recent nog verscheen in het nieuws dat Philippe De Backer, de Belgische staatssecretaris voor Privacy, een verbod wil op onveilige IP-camera's. Er zijn namelijk verschillende websites waarop de beelden zijn te zien van niet of slecht beveiligde IP-camera's. Een **up-to-date kwaliteitsborging** voor de hele keten wordt dus steeds belangrijker.

3.2 Cognitive computing & artificial intelligence

Te diep ingaan op de definitie van en verschillen tussen 'cognitive computing' en 'artificial intelligence' (AI) zou ons te ver leiden. In grote lijnen gaan beide over zelflerende systemen die – op basis van de analyse van data en eerdere beslissingen – **voorspellingen doen en besluiten ondersteunen**. Het gebruik van deze technologieën wordt meer en meer toegepast voor beveiligingsdoeleinden, zowel door private als publieke actoren.

De **Britse politie** voorspelt bijvoorbeeld misdaad met artificial intelligence - een computersysteem met artificial intelligence voorspelt het risico dat verdachten een misdaad plegen, wat de politie moet helpen bij het besluit om verdachten langer vast te houden.

In de **private sector** ontwikkelen **AI-gebaseerde** '**smart home**'-**beveiligingssystemen** zich aan een exponentieel tempo.

Alarm.com lanceerde recent een "**Insights Engine**". Deze kan gedrag, activiteitspatronen en inzichten van geconnecteerde toestellen en sensoren (cfr. IoT) in een gebouw identificeren, om de routines van gebruikers te leren. Op basis hiervan kan de technologie dan actie ondernemen. De eerste toepassing van de technologie zou een nieuwe categorie van intelligente meldingen zijn die gebruikers op de hoogte kan stellen van veiligheidsrisico's in het gebouw, zonder dat ze zelf aangepaste regels of meldingen moeten creëren. Zo kan de technologie bijvoorbeeld het gebruik van de voordeur van een gebouw leren. Tijdens de week ziet deze typisch vaak activiteit 's morgens vroeg, wanneer mensen vertrekken naar hun werk of school. Tijdens weekends wordt deze typisch pas later op de dag geopend. Wanneer een voordeur vroeger dan normaal op een zaterdagochtend wordt geopend, genereert de Insights Engine een "onverwachte activiteit"-melding. Zo weet de familie dat de kinderen bijvoorbeeld buiten zijn gaan spelen.

Nog dit jaar lanceerde **Vivint** de "**Sky**" oplossing, een slimme assistent die artificial intelligence gebruikt om geconnecteerde toestellen in een gebouw automatisch te beheren. Sky kan bijvoorbeeld data van sensoren en toestellen gebruiken om te detecteren wanneer een gebruiker aan – of afwezig is, wat mogelijk maakt om deuren automatisch te vergrendelen en het alarm te activeren. De technologie kan ook de dagelijkse routines van gebruikers leren, op basis waarvan de beveiligingsinstellingen automatisch worden aangepast.

Een andere toepassing van AI in bewakingssystemen is **video-analyse** technologie, waarmee videobeelden in real-time worden geanalyseerd en abnormale activiteiten gedetecteerd die een gevaar voor de veiligheid kunnen betekenen. De video-analysetechnologie leert beveiligingssoftware wat normaal is, zodat het ongebruikelijk en mogelijk schadelijk gedrag kan identificeren – typisch zaken die aan de aandacht van een persoon kunnen ontsnappen. Zo kan AI in combinatie met camera's ook het verschil leren tussen bezoekers en indringers. In toenemende mate gebeurt deze **analyse door de camera's zelf**.

Daarnaast kunnen nieuwe AI-gebaseerde **audiodetectiesystemen** verdachte geluiden identificeren en catalogiseren om potentiële inbraken te identificeren en te voorkomen. Dit biedt een effectieve back-up voor visuele bedreigingsdetectiesystemen.

Veel van deze innovaties **vinden ook hun weg in zakelijke beveiligingssystemen**. Technologieën zoals gezichtsherkenning, audio- en

Case: BuddyGuard FLARE

FLARE maakt gebruik van artificial intelligence – de technologie herkent gezichten en gevaarlijke geluiden, en kan hulpdiensten verwittigen via een toegewijde app in geval van een alarm. In zo'n situatie kan FLARE alle audio en video live streamen naar BuddyGuard's monitoring center.

visuele detectie van bedreigingen kunnen ook voor bedrijven veiligheid helpen verbeteren.

Voor de sector creëert artificiële intelligentie verschillende mogelijkheden om **voorspellend** te gaan werken, en **nog beter alarmen te filteren en te verifiëren.**

3.3 Drones

Drones zijn onbemande luchtvaartuigen zonder pilot aan boord, ook wel UAV of "unmanned aerial vehicles" genoemd.

Drones worden steeds meer ingezet, door zowel publieke als private actoren. **Brandweer** en **politie** in verschillende landen gebruiken drones al om gevaarlijke situaties te verkennen, vermiste personen op te sporen, ongevallen snel te documenteren enzovoort.

Ook in de **private sector** worden drones vaker ingezet, voor inspecties van technische installaties, of ter ondersteuning van bewakingsopdrachten. Recent kondigde **Alarm.com** aan dat het een '**smart home' beveiligingsdrone** aan het ontwikkelen is. Deze drone zou zowel binnenin als buiten een gebouw kunnen vliegen – waar er ook ongewone activiteiten zijn waargenomen. In plaats van voortdurend te patrouilleren, zullen de Alarm.com-drones alleen reageren en vliegen wanneer een ander systeem wordt geactiveerd, bijvoorbeeld een bewegingssensor die aan de lichten is bevestigd. Met behulp van gegevens van andere 'smart home' toestellen, zullen de drones weten waar ze naartoe moeten – ze zullen video opnemen of live streamen naar de mobiele telefoon van een gebruiker. Als ze vliegen, zullen ze camera's en andere boordsensoren gebruiken om rond een kamer te kijken en botsingen te vermijden.

Case: Politie Dubai

Tegen eind 2017 wil de politie in Dubai een zelfrijdende robo-auto inzetten, die als een mobiele bewakingseenheid zal fungeren. De 'O-R3' heeft een ingebouwde drone met camera die ook 'off-road' personen kan volgen.

Drones zijn meestal uitgerust met **camera's** – voor de sector van vergunde alarmcentrales kunnen ze dus enerzijds een rol spelen om **alarmen te verifiëren**. Anderzijds kunnen meldkamers drones uitsturen bij **interventies**, ter ondersteuning van andere stakeholders. Ze zouden bijvoorbeeld **live beelden kunnen streamen** naar hulpdiensten of bewakingsondernemingen.

Het **wettelijk kader** rond drones in België **beperkt** vandaag de mogelijkheden nog in zekere mate – zo moet er bijvoorbeeld altijd 'line of sight' of visueel contact met de drone behouden blijven. **Zwitserland** heeft recent als eerste toestemming gegeven aan logistiekbedrijf Matternet om drones over **dichtbevolkte gebieden** te laten vliegen. Matternet zal nog dit jaar **een permanent autonoom dronenetwerk** opzetten – drones zullen laboratoriummonsters zoals bloedtesten tussen hospitalen en laboratoria vervoeren.

4. Duidelijke bevestiging van de nood aan een integrale veiligheidsaanpak

De verschillende maatschappelijke, economische en technologische trends zorgen ervoor dat het steeds **complexer** wordt om zowel objectieve onveiligheid als subjectieve onveiligheidsgevoelens aan te pakken. Er is duidelijk nood aan een **integrale veiligheidsaanpak**, en een geïntegreerde en gecoördineerde **samenwerking** tussen de verschillende veiligheidsactoren, zowel op het niveau van het beleid, als van private en publieke stakeholders. De sector wil zelf met een **duidelijke visie** komen om **actief mee te bouwen** aan deze integrale veiligheid.

Deel 3 | Onze visie

Veiligheid is een fundamenteel recht. De sector wil dan ook inspelen op technologische vooruitgang en haar kerncompetenties inzetten om op een efficiënte en effectieve manier bij te dragen aan een veiligere omgeving voor burgers, organisaties, ondernemingen en overheden.

De sector creëert vandaag toegevoegde waarde voor verschillende stakeholders, met een focus op haar kerndomein van inbraak & diefstal en haar functie als filter van valse alarmen. De sector wil haar gespecialiseerde kennis, permanente beschikbaarheid en geavanceerde technologische oplossingen **breder inzetten** om nog meer **toegevoegde waarde** te creëren voor de **maatschappij** en een **actieve rol te spelen in de integrale veiligheid**. Ze heeft volgende accenten gelegd in haar visie.

1. Preventie, betrouwbare bescherming en bijstand in nauwe samenwerking met relevante spelers

De sector wil een steunpilaar zijn voor elke stap in de keten van preventie, bescherming en bijstand.

Preventie

De sector wil meer nadruk leggen op preventie, en evolueren van het monitoren van en reageren op alarmen naar het **proactief managen van situaties**. Dit element van de visie wordt ondersteund door snelle technologische evolutie, die zelfs voorspellend werken mogelijk maakt. Ze wil hierbij **nauw samenwerken** met relevante spelers, zoals verzekeraars en (preventiediensten van) de politie en brandweer.

Verschillende **politiezones** gebruiken bijvoorbeeld **camerabeelden** om problemen te voorkomen – de politie geeft ook aan dat cameratoezicht in een wijk preventief werkt. In Nederland gebeurt dit cameratoezicht, gericht op veiligheid & leefbaarheid, al in publiek-privaat samenwerkingsverband in de Regionale Toezicht Ruimten.

Ook **verzekeraars** spelen een belangrijke rol in deze stap van de keten. Zij hechten belang aan **normering** en **kwaliteitslabels** zoals INCERT en BOSEC, die voornamelijk impact hebben op het preventieluik. Het is

belangrijk dat deze normering zich verder **aanpast aan nieuwe technologische mogelijkheden**. Daarnaast wil de sector ook een **geïntegreerde aanpak** aanmoedigen, waarbij maatregelen voor preventie en bescherming optimaal gecombineerd worden. Voor commerciële en industriële panden bijvoorbeeld kunnen verzekeraars specifieke eisen stellen – vaak hebben deze betrekking op sprinklersystemen. Door sprinklersystemen te monitoren, zou de sector een extra laag zekerheid kunnen toevoegen aan brandbestrijding.

Betrouwbare bescherming
De sector wil streven naar een **hogere verbindingsgraad** van bestaande en nieuwe installaties met een meldkamer, om een betrouwbare bescherming te garanderen voor de eindklant. Meldkamers staan namelijk voor permanente beschikbaarheid, en werken met procedures en back-up systemen die instaan voor **een permanente verwerking van alle binnenkomende alarmen**. Ze werken ook nauw samen met de politie- en andere interventiediensten om **snelle en gepaste actie** te verzekeren.

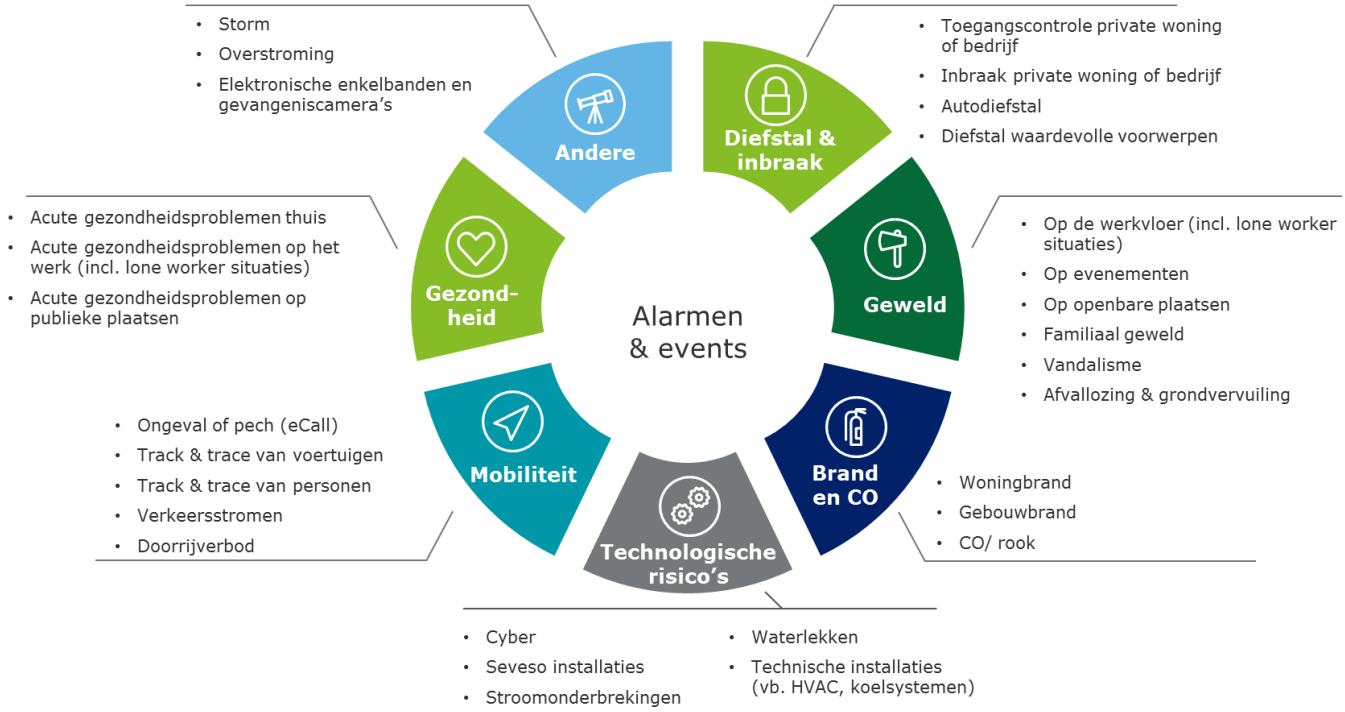
Verschillende **verzekeraars**, ook in het buitenland, **onderschrijven** deze betrouwbare bescherming. Ze geven kortingen op gebouwverzekeringen wanneer deze gebouwen een gemonitord alarmsysteem hebben, of verplichten aansluiting op een meldkamer in bepaalde situaties. Deze kortingen kunnen oplopen wanneer ook brand- en waterdetectoren zijn aangesloten.

Bijstand
Ten slotte wil de sector een belangrijke rol te spelen op het gebied van bijstand. Enerzijds kan ze **interventiediensten** bijstaan dankzij (real-time) informatie-uitwisseling en het vanop afstand toegang verschaffen, anderzijds wil ze **zelf** bijstand blijven verlenen aan eindklanten.

2. Bredere rol in de strijd tegen onveiligheid – van alarmcentrale naar 'eventcentrale'

Technologische evoluties zoals de integratie tussen alarmsystemen en slimme camera's of het gebruik van geconnecteerde sensoren, creëren **verschillende nieuwe mogelijkheden voor monitoring**. En de **expertise** die de sector heeft opgebouwd rond het uitfilteren van valse alarmen, camerabewaking en dienstverlening vanop afstand kan ook **voor een bredere groep stakeholders** toegevoegde waarde betekenen.

In de toekomstvisie van de sector zijn meldkamers **eventcentrales**, die een **breed spectrum van alarmen** behandelen en **events** beheren**.** Onderstaande **figuur** geeft een overzicht van mogelijke alarmen en events waarvoor de sector een betekenisvolle rol kan spelen.



Voor een overzicht van de **domeinen waar de sector zich in eerste instantie op wil toeleggen**, verwijzen we naar **Deel 4 | Operationele invulling visie**. Hierbij is het belangrijk om op te merken dat de sector een dynamisch **geheel van individuele bedrijven** is, die op basis van hun **eigen sterktes** zullen focussen op bepaalde **domeinen**.

3. Orkestreren van relevante stakeholders

De meldkamer is dé plaats waar **alle relevante data over uiteenlopende events en alarmen op één plaats geaggregeerd** kan worden. Deze data kan bestaan uit alarmen, maar ook beelden, geluid, locaties enzovoort. De meldkamer is **uniek gepositioneerd** om data te **analyseren**, en de juiste stakeholders te **mobiliseren** wanneer nodig. De meldkamer wil zo **efficiëntie** bevorderen (stakeholders alleen inzetten wanneer echt nodig) en bijdragen tot een **snelle en adequate respons.**

Daarnaast kan de meldkamer deze data ook gebruiken om stakeholders te **ondersteunen** om betere beslissingen te maken, en zo **effectiviteit** van preventie en interventies verbeteren.

In haar rol als '**regisseur'** wil de sector streven naar een geïntegreerde en geoptimaliseerde **samenwerking** met betrokken stakeholders:

- **Geïntegreerd**: met duidelijk afgebakende rollen en verantwoordelijkheden, procedures en structurele & tweezijdige informatie-uitwisseling (zoals goede communicatie tijdens interventies, strategisch overleg en frequente uitwisseling van geleerde lessen)
- **Geoptimaliseerd**: een strategische alliantie waarbij elke partner zich kan focussen op zijn kerncompetenties, en de sterke punten van elke partner zo veel mogelijk benut worden

4. Een up-to-date kwaliteitsborging voor de hele keten

De leden van ACA willen streven naar een up-to-date kwaliteitsborging voor de hele keten, om moderne risico's zoals **cyberbedreigingen** adequaat het hoofd te kunnen bieden en **betrouwbare dienstverlening** te garanderen. Deze kwaliteitsborging zou drieledig moeten zijn:

- **Moderne certificering** voor de hele keten die de Europese normering volgt
- **Technische kwaliteit** van en **interoperabiliteit** tussen systemen
- Respect voor **privacy**

Volgens CoESS (de "Confederation of European Security Services"), is **België koploper** op het gebied van **correct beschrijven en reglementeren van monitoringactiviteiten**. De sector in België wordt vaak als referentie gebruikt voor andere landen. Dit is mede te danken aan de **strikte wetgeving** in België voor private bewaking. In een vergelijkende studie van CoESS in 2015 werd België ingedeeld in de selecte club van zeven Europese landen met een "zeer strenge" wetgeving. Operatoren worden bijvoorbeeld verplicht gescreend door Binnenlandse Zaken en veiligheidsdiensten, geselecteerd op basis van zeer strenge toelatingsvoorwaarden, en moeten een wettelijke opleiding volgen van 70 uren. Naast wettelijk opgelegde vereisten **neemt de sector ook zelf maatregelen** om kwaliteit te garanderen, zoals doorgedreven aanvullende interne opleiding, strikte servicelevel overeenkomsten en het behalen van ISO-certificaten.

5. Lokale verankering in globale context

Ook in een internationaliserende sector blijven de menselijke factor en lokale affiniteit heel belangrijk. De sector wil lokaal verankerd blijven, om operatoren te kunnen inzetten met een **adequate talenkennis** en **ervaring met de lokale context** zoals de constructie van gebouwen en publieke omgevingen, die sterk kan verschillen per land.

Daarnaast vindt ze lokale verankering ook belangrijk om frequent met de **regulator en de overheid** af te kunnen stemmen en actief mee beleid uit te stippelen.

Deel 4 | Operationele invulling visie

Om haar rol als 'eventcentrale' in te vullen, wil de sector zich in eerste instantie toeleggen op een aantal aangrenzende domeinen.

1. Prioritering van domeinen

Om haar prioriteiten op korte termijn af te bakenen heeft de sector twee belangrijke **criteria** in rekening genomen:

- 'Fit' met het doel/ de **fundamentele bestaansreden** van de sector, namelijk bijdragen tot het creëren van een veilige omgeving voor burgers, organisaties, ondernemingen en overheden
- Mogelijkheid voor de sector om **toegevoegde waarde** te creëren voor betrokken stakeholders

De sector wil die domeinen prioriteren die nauw aansluiten bij haar fundamentele bestaansreden, en waarvoor ze haar huidige competenties kan inzetten om toegevoegde waarde te creëren voor de betrokken stakeholders.

De sector gelooft dat ze zich betekenisvol (verder) kan engageren op volgende prioritaire domeinen:

2. Zoom op prioritaire domeinen

De sector heeft een duidelijke visie voor de invulling van haar vijf prioritaire domeinen.

2.1 Inbraak en diefstal

Snelle **technologische vooruitgang** creëert mogelijkheden voor de sector om nog meer toegevoegde waarde te creëren in haar kerndomein van inbraak en diefstal.

Dankzij de toenemende **integratie tussen alarmsystemen en (slimme) camera's** beschikt de sector namelijk over betere **verificatiemogelijkheden** en een additionele schat aan **informatie**. Daarnaast wordt het ook mogelijk om steeds meer **voorspellend** en **preventief** te gaan werken. Slimme camera's (gebaseerd op artificial intelligence) zijn nu al in staat om inbraken en diefstal te voorspellen, waardoor deze beter te voorkomen zijn.

Naast het behandelen van alarmen wil de sector ook meer inzetten op het aanbieden van **remote diensten**, zoals remote access control en virtuele rondes.

Ten slotte wil ACA samen met andere stakeholders **meer awareness creëren** over de voordelen van een aansluiting op een meldkamer. Hiervoor zou ACA samen met andere spelers van de veiligheidssector communicatiecampagnes kunnen initiëren.

Case : Deep Sentinel

Startup Deep Sentinel is het gebruik van camera's in beveiligingssystemen aan het herdefiniëren. Een Artificial Intelligence programma analyseert de beelden en zoekt naar patronen/ visuele 'rode vlaggen' die zouden kunnen voorspellen dat er een misdaad zal plaatsvinden op een eigendom – zoals een inbraak of voertuigdiefstal. De startup werd opgericht door Amazon-veteraan David Selinger en trok al $7,4 miljoen financiering aan.

2.2 Brand & gebouwzekerheid

Vorig jaar stierven er 78 mensen bij woningbranden, de eerste helft van dit jaar kwamen al 32 mensen om het leven. Ter vergelijking: in Nederland – dat 6 miljoen inwoners meer telt – stierven in dezelfde periode slechts 14 mensen in een brand. Volgens brandweercommandant Marc Ceyssens, tevens voorzitter van de overkoepelende Brandweervereniging Vlaanderen (BVV), **doet België het op het vlak van woningbranden niet goed** in vergelijking met Nederland of Duitsland. Om deze redenen hebben sommige regio's in België de regelgeving aangaande brandmelders recent aangepast. Nog volgens Marc Ceyssens zijn er in veel woningen in België dan ook nog steeds **geen of te weinig rookmelders**. Vaak **werken de aanwezige brandmelders** ook allang **niet meer.** Toch is er in de nieuwe regelgeving geen verplichting om brandmelders bij een alarmcentrale aan te sluiten zodat ze de goede werking van de brandmelders en de alarmen zouden kunnen opvolgen.

In 2014 werden 18.237 **verplaatsingen zonder interventie** uitgevoerd door de brandweer. Dit wil zeggen dat de brandweer elke dag 50 keer uitrukt terwijl er niets aan de hand is. Mee aan de basis van deze valse oproepen liggen verouderde of slecht onderhouden brandalarmen, mensen die foutieve informatie geven of grappenmakers. En rekening houdend met de steeds strengere wettelijke verplichtingen voor de aanwezigheid van brandmelders, zal het aantal brandalarmen alleen nog maar toenemen.

Het is duidelijk dat er op het gebied van brand **ruimte voor verbetering** is, **voor verschillende stakeholders**. De leden van ACA kunnen de **veiligheid, integriteit en betrouwbaarheid van gebouwen** nagaan – op het gebied van brand, maar eveneens op het gebied van CO en waterlekken. Ze kunnen de nauwkeurigheid en effectieve werking van veelzijdige detectoren op afstand monitoren en een adviserende rol spelen.

In 2016 ontving de sector ongeveer 120.000 brandalarmen. Minder dan 4% van deze alarmen werd doorgemeld naar de brandweer. In situaties waar de technologie het toelaat, kan de sector alarmen van detectoren op een betrouwbare manier **verifiëren**, en zo drastisch het **aantal valse alarmen terugdringen**.

Bovendien kan ze **vanop afstand toegang verschaffen** voor de brandweer tijdens interventies. En de informatie die de leden van ACA verzamelen, kan gebruikt worden ter **ondersteuning van interventies** van de **brandweer**, en voor de **bijstandsactiviteiten** van **verzekeraars**.

Case : Stad Ronse
Een kleine stad zoals Ronse, met ongeveer 26.000 inwoners, geeft jaarlijks ongeveer **90.000 euro** uit voor het verwijderen van graffiti en sluikstorten en de aanpak van vandalisme. Bij glasbollen in bepaalde buurten is er camerabewaking.

Case: Flitsmarathon tegen zwerfvuil
Verspreid over de vijf Vlaamse provincies namen ruim duizend politieagenten, GAS-ambtenaren, stads- en gemeenschapswachters, bos- en veldwachters deel aan de handhavingsweek in september. Ze trokken een week lang de straat op om extra controles uit te voeren op sluikstorten. Er werden technologische hulpmiddelen ingezet zoals camera's.

2.3 Geweldscriminaliteit, overlast & sluikstorten

Volgens een recent onderzoek in opdracht van afvalmaatschappij OVAM, spendeerde Vlaanderen in 2015 in totaal iets meer dan 187 miljoen euro, of **29 euro per inwoner**, aan de strijd tegen zwerfvuil en sluikstort. Daarvan ging 103 miljoen euro naar zwerfvuil, een stijging van maar liefst 42 miljoen in vergelijking met 2013. Het zijn de **gemeenten die het grootste deel van de kosten dragen**, in totaal ongeveer 176 miljoen euro, of 94 procent van het totale bedrag. Ook in de rest van het land is sluikstorten een kostelijk probleem.

Omwille van de grote maatschappelijke impact zijn **geweldscriminaliteit** en **overlast** eveneens twee belangrijke veiligheidsfenomenen waaraan politiediensten en andere betrokken instanties bijzondere aandacht besteden, in het kader van het **huidige nationaal veiligheidsplan** (2016-2019).

De sector kan **cameraondersteuning** bieden voor de preventie van en reactie op deze belangrijke fenomenen, **zowel op privaat als op publiek domein**. Dankzij het **proactief** monitoren van o.a. slimme camera's kan bijvoorbeeld sneller geanticipeerd worden op samenscholingen, en verhoogt de heterdaadkracht van het reactieve overheidsoptreden tegen sluikstorten en geweldscriminaliteit.

Ten slotte kan de sector ook waken over mensen in risicolocaties dankzij '**virtual close protection'** – zo kan ze bijvoorbeeld zorgen voor openings- en sluitingsbegeleiding vanop afstand. In dit geval weet de meldkamer wanneer de werknemer van een bedrijf binnen een bepaalde perimeter komt, en kan ze meekijken tijdens het openings- of sluitingsmoment. Op het moment dat er zich verdachte omstandigheden of personen voordoen, kan de meldkamer hulp sturen of de politie waarschuwen.

2.4 'Lone workers'

De sector kan waken over de veiligheid van 'lone workers'. Deze **werken alleen, zonder rechtstreeks toezicht** en kunnen dus kwetsbaar zijn voor agressie of 'safety' risico's. Mogelijke voorbeelden van lone workers zijn techniekers voor telecom- en energiebedrijven, mensen die alleen werken in productie-omgevingen en mobiele werkers zoals truckchauffeurs, verkopers thuisverplegers en huisartsen. Verschillende landen zoals het Verenigd Koninkrijk, Duitsland, Frankrijk en Spanje hebben de bescherming van lone workers opgenomen in de wet.

De nood aan 'lone worker' oplossingen zal verder blijven toenemen, gestimuleerd door '**new ways of working'**. Ook in België wordt werkbaar en wendbaar werk aangemoedigd, inclusief occasioneel **telewerk**. De verantwoordelijkheid in geval van een ongeval van iemand die thuis werkt is vandaag nog onduidelijk.

2.5 Verkeer en mobiliteit

Ten slotte ziet de sector verschillende mogelijkheden om haar competenties in te zetten op het gebied van verkeer en mobiliteit.

Dankzij 'remote access control' of videoportierdiensten kunnen meldkamers **vanop afstand gecontroleerd toegang verlenen** tot een site en/of een site laten verlaten. Dit gebeurt onder begeleiding van remote video assistentie door een operator.

Vandaag levert de sector deze dienst al voor verschillende private sites. Voor **nachtleveringen** bijvoorbeeld, zonder dat er permanent iemand ter plaatse moet zijn. Naar de toekomst toe ziet de sector ook verschillende voordelen om deze dienst **op publiek domein** toe te passen. Om gecontroleerd toegang te verschaffen tot **voetgangerszones** bijvoorbeeld, voor uitzonderlijke leveringen of een verhuis enzovoort.

Er verschijnen ook meer en steeds slimmere **camera's** in het straatbeeld. De **nood aan filtering en menselijke verificatie** zal dus toenemen. Ook al worden camera's slimmer, toch blijven ze gevoelig aan omgevingsfactoren en genereren ze **valse alarmen**.

Ten slotte wil de sector ook een rol spelen op het gebied van **eCall**. Het eCall-systeem in wagens stuurt bij een ongeluk automatisch (of manueel via een drukknop) een noodoproep uit naar een alarmcentrale. Het geeft onmiddellijk ook cruciale informatie door zoals de exacte locatie en het uur van het ongeluk. Vanaf april 2018 moeten alle nieuwe wagens in Europa worden uitgerust met het eCall-systeem. De sector zou hier **internationale oplossingen** kunnen aanbieden.

Deel 5 | Op zoek naar een win-win

In het kader van een integrale veiligheidsaanpak wil de sector actief samenwerken met en toegevoegde waarde creëren voor publieke en private stakeholders.

1. Toegevoegde waarde voor de maatschappij & burgers

Betere publieke veiligheid

Als actieve actor in de integrale veiligheid zal de sector zijn steentje kunnen bijdragen aan de publieke veiligheid en het veiligheidsgevoel van burgers. De sector kan immers extra **gespecialiseerde expertise, permanente beschikbaarheid, technologie,** zeer **snelle reactietijden** en **informatie** in de balans gooien, voor thema's zoals brand, geweldscriminaliteit, sluikstorten en mobiliteit (zie hoofdstuk operationele invulling visie). Door een geïntegreerde en geoptimaliseerde samenwerking tussen private & publieke actoren kan de publieke veiligheid beter gegarandeerd worden, en kan een beter antwoord geboden worden op evoluerende bedreigingen.

Geïntegreerde aanpak van onveiligheid gerelateerd aan het gebruik van gebouwen

De sector kan een belangrijke rol spelen in een geïntegreerde aanpak van onveiligheid in gebouwen – **brand**, **CO**, **waterlekken**, **inbraak**, **geweld** enzovoort. De sector is uniek gepositioneerd om al deze fenomenen te monitoren, en de juiste stakeholders te activeren en te ondersteunen met informatie bij interventie wanneer nodig. Bovendien kan de sector hulp- en interventiediensten vanop afstand toegang verlenen. Hierdoor wordt **betere preventie** en **snellere & gerichtere reactie** mogelijk, en kan potentiële schade beperkt worden.

Zeker wanneer mensen niet aanwezig zijn, in een noodsituatie verkeren of geen gevolg (kunnen) geven aan lokale alarmen of notificaties op hun smartphone, kan de sector brand, waterlekken, CO-gas, inbraak of diefstal detecteren en gepast reageren. De sector staat voor 24/7 beschikbaarheid, en beschikt over back-up systemen om dit te allen tijde te kunnen garanderen.

2. Toegevoegde waarde voor publieke stakeholders

2.1 Toegevoegde waarde voor de Federale Overheidsdienst Binnenlandse Zaken

De toegevoegde waarde die de sector kan creëren voor IBZ steunt op volgende pijlers:

- Samen een **toekomstgericht beleid** uitwerken dat een geïntegreerde en gecoördineerde samenwerking tussen veiligheidsactoren mogelijk maakt, en **statistieken** krijgen ter ondersteuning van **beleidsuitwerking en evaluatie**
- Inzicht krijgen in **haalbaarheid** van beleidsaanpassingen, gebaseerd op **ervaring "vanuit het veld"**

- Positioneren van alle veiligheidsactoren op hun **kerncompetenties** en betere coördinatie tussen verschillende stakeholders, voor een **(kosten)efficiëntere inzet van middelen** en meer focus op strategische taken
- Filtering van valse en niet-dringende alarmen, betrouwbare verificatie en dus verder **reduceren van het aantal onnodige interventies** van brandweer en politie
- Verhogen van de **doeltreffendheid** door sneller situaties te detecteren die interventie van politie of brandweer vereisen
- **Inperken van schade voor maatschappij** door snellere en effectievere interventies van brandweer en politie, dankzij het delen van (real-time) data en het verlenen van toegang vanop afstand
- **Innovatievoordeel** door marktwerking: innovatie stimuleren door de markt te laten werken en publieke actoren toegang geven tot "state-of-the-art" technologie (eventueel geïmporteerd uit het buitenland)

2.2 Toegevoegde waarde voor lokale besturen

De sector kan ook voor lokale besturen toegevoegde waarde creëren op de verschillende domeinen die zij in haar visie heeft geïdentificeerd:

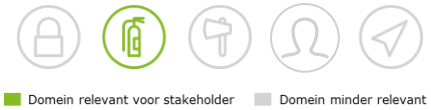
- **Kostenefficiëntie** door optimale inzet van beschikbare middelen
- Optimale **benutting van bestaande camera's** op publiek domein (zowel preventief als reactief)
- Voorkomen en effectiever tegengaan van overtredingen en **geweldscriminaliteit in risicoplaatsen** zoals binnensteden, (probleem)wijken, winkelstraten & centra, stations, pleinen, parken & recreatiedomeinen en de eigen loketwerking
- Vergroten van de **heterdaadkracht** van het reactieve overheidsoptreden
- Vergroten van het **veiligheidsgevoel** van ondernemers, bezoekers en bewoners in voetgangerszones en drukke (winkel)gebieden, **zonder ingrijpende maatregelen** (zoals betonblokken) en op een **kostenefficiënte** manier (onder meer dankzij de mogelijkheid om fysiek toezicht op deze locaties terug te brengen)
- Inperken van kosten van **sluikstorten en vandalisme**

2.3 Toegevoegde waarde voor politie

Een **ketengerichte samenwerking** met de politie, met wederzijds respect voor de verantwoordelijkheden van de participerende partners kan verschillende voordelen met zich meebrengen:

- **Verder reduceren van het aantal onnodige interventies** dankzij filtering van valse en niet-dringende alarmen en betrouwbare verificatie
- Toelaten om te **focussen op kerntaken** (vb. alternatief bieden voor vakantie- en afwezigheidstoezicht)
- **Effectievere interventies** dankzij het delen van informatie (zoals camerabeelden) of het vroeger detecteren van misdrijven
- **Toegang tot 'state-of-the-art' technologie** zoals drones en mobiele centra, zonder hoge investeringskost (in samenwerking met de bewakingssector)

2.4 Toegevoegde waarde voor brandweer



Het aansluiten van brand- en waterlekdetectoren op een meldkamer creëert verschillende voordelen voor de brandweer:

- Verbetering van **interventiedossiers** dankzij het delen van up-to-date technische informatie rond branddetectie en gebouwinformatie
- **Effectievere interventies** dankzij het delen van real-time data, zoals camerabeelden, de locatie van brandhaard(en), de aanwezigheid van bewoners/ gebruikers enzovoort of het vroeger detecteren van noodsituaties
- Bijdragen tot **strategische doelstellingen** (reduceren van aantal slachtoffers) en samen inzetten op gepaste systemen voor branddetectie

3. Toegevoegde waarde voor private stakeholders

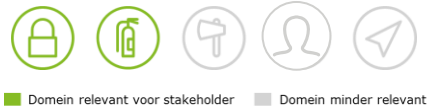
3.1 Toegevoegde waarde voor verzekeraars

Dankzij betere preventie en snellere detectie van brand, CO, waterlekken, inbraak en diefstal, en snellere en gerichte reactie, kan de sector het **aantal claims terugdringen** en de **grootte van claims beperken**.

Bovendien kunnen leden van ACA ook **statistieken** en **informatie** verzamelen en delen, om:

- De **expertise** door verzekeraars te ondersteunen
- **Ongegronde claims** te reduceren
- **Preventie** te verbeteren en **toekomstige normering** te voeden

3.2 Toegevoegde waarde voor installateurs



Installateurs worden geconfronteerd met snelle technologische evolutie, net zoals de leden van ACA. Hun **rol is aan het veranderen**, onder meer gedreven door de verschuiving van analoge naar digitale netwerken (gebaseerd op IP), de opkomst van IoT toestellen, de integratie van alarmsystemen met (slimme) camera's en verruimende klantenvragen.

De sector kan toegevoegde waarde creëren voor installateurs, door samen af te stemmen rond de **toepassing van nieuwe technologieën** en **nieuwe businessmodellen**. De sector kan installateurs ondersteunen om de technologische evolutie te blijven volgen, en aan klantenvragen te blijven voldoen. De rol van de meldkamer wordt namelijk nog belangrijker in een beveiligingsomgeving waar de camera centraal staat.

Beide sectoren kunnen middelen delen om burgers te sensibiliseren over de toegevoegde waarde van geconnecteerde alarmsystemen.

3.3 Toegevoegde waarde voor bedrijven

Ook voor bedrijven kan de sector toegevoegde waarde creëren op verschillende domeinen:

- **Geïntegreerde aanpak** van **onveiligheid** gerelateerd aan het gebruik van **gebouwen**, inclusief betere preventie, zekerdere detectie en snellere & gerichte reactie
- Specifiek voor **syndici** en **gebouwenbeheerders** wil dit zeggen dat de leden van ACA hen kunnen toelaten om te focussen op hun **kerntaken**
- **Schaalvoordelen** van een overkoepelende meldkamer voor **bedrijventerreinen**

- **Back-up voor interne meldkamers**: grote bedrijven in bepaalde sectoren zoals de chemie en de farmacie hebben een eigen brandweer, die ook de interne meldkamer bemant. Op momenten dat de brandweer op interventie is, is de meldkamer dus onbemand. In deze situaties kan de sector als back-up fungeren
- **Verhoogde veiligheid voor "lone workers" en personeel in risicosituaties**: de sector kan waken over de veiligheid van personeel om incidenten en potentiële aansprakelijkheid te beperken, verloop van personeel in te perken en imagoschade te voorkomen. Ook voor vakbonden is de veiligheid van personeel een belangrijk thema - de sector is uniek gepositioneerd om hier toegevoegde waarde te creëren
- **Kostenefficiëntie door meer remote diensten**, onder meer dankzij de mogelijkheid om fysiek toezicht terug te brengen (bijvoorbeeld voor nachtleveringen)

4. Toegevoegde waarde voor de sector

Het herdenken van de integrale veiligheid en het positioneren van alle veiligheidsactoren op hun kerncompetenties, creëert ruimte voor de sector om te **groeien**, en om verder te kunnen **blijven investeren in mensen, innovatie en technologie**.

Ten slotte is het gepast betrekken van de leden van ACA in het integraal veiligheidsbeleid ook een **erkenning** van de sector als betrouwbare en kwaliteitsvolle partner.

Deel 6 | Ons engagement

Om haar visie te kunnen verwezenlijken en effectief toegevoegde waarde te kunnen creëren voor de verschillende relevante stakeholders, wil de sector zichzelf engageren.

De sector heeft volgende belangrijke werven geïdentificeerd.

1. Een volwaardige partner zijn in de integrale veiligheid

ACA vertegenwoordigt vandaag meer dan 95% van de aansluitingen in België. Om als een volwaardige partner in de integrale veiligheid actief te kunnen zijn, wil de sector een **permanente vertegenwoordiging** opzetten met voldoende capaciteit tot dialoog en actie.

De sector wil een permanente **dialoog** opzetten met en **bruggen bouwen** tussen andere **private sectorfederaties** in de keten van preventie-interventie-bijstand en met de Belgische beroepsvereniging van de elektronische beveiliging (ALIA Security). Ze wil een win-win vinden met deze partijen. Dit kan zich vertalen in breder gedragen standpunten richting beleidsmakers en meer succesvolle pilootprojecten.

In parallel wil de sector meer toenadering zoeken tot **FOD Binnenlandse Zaken**, om als een **volwaardige partner** mee te werken aan het **beleid**. Als eerste prioriteit wil de sector samen een **invulling** geven aan de **nieuwe kaderwet** die in de zomer van 2017 is goedgekeurd.

ACA kan ook actiever worden in de **Europese sectorfederatie** Confederation of European Security Services (**CoESS)** en proberen België meer op de kaart te zetten als voortrekker van de "meldkamer van de toekomst".

Daarnaast wil de sector **nauwer samenwerken** met **lokale besturen** en **publieke en private veiligheidsactoren**. Ze wil middelen inzetten om als sectorfederatie **pilootprojecten** op te zetten, op het niveau van lokale politiezones, brandweerzones en lokale besturen, waar relevant in samenwerking met private bewakingsondernemingen.

Ten slotte wil de sector meer investeren in **communicatie** naar het brede publiek rond de voordelen van een aansluiting op een meldkamer.

2. Voorhoede van innovatie zijn

ACA wil tijd en middelen blijven inzetten op het niveau van de sectorfederatie rond **technologische ontwikkelingen** en haar toepassingsdomeinen. De sector wil technologische vooruitgang van dichtbij **opvolgen**, relevante **toepassingen in het buitenland identificeren** en inzichten publiceren/ **communiceren** naar een breed publiek.

Private meldkamers kunnen ook als **'labo-omgeving'** dienen voor pilootprojecten.

3. Streven naar standaardisatie, interoperabiliteit tussen systemen en cybersecurity

Een specifieke uitdaging rond technologie en het opereren in een keten is de interoperabiliteit van verschillende systemen, en standaardisatie. ACA wil, samen met de Confederation of European Security Services (CoESS), de **afstemming van standaarden orkestreren en drijven** in België (bijvoorbeeld richting leveranciers & installateurs, Communicatie- & Informatiecentra (CIC's) van de politie enzovoort.

Daarnaast wil ze zich mee inzetten om **cyberbedreigingen** een adequaat antwoord te bieden, en respect voor **privacy** te garanderen.

Deel 7 | The way forward

Om de basis te leggen voor volgende stappen, heeft de sector suggesties uitgewerkt voor de samenwerking met haar verschillende stakeholders en heeft ze concrete actiepunten geïdentificeerd.

1. Samenwerking met publieke stakeholders

1.1 Samenwerking met de Federale Overheidsdienst Binnenlandse Zaken

De sector wil in dialoog treden met IBZ Veiligheid & Preventie en Civiele Veiligheid, en evolueren naar **structureel overleg** dat ondersteund wordt door objectieve **statistieken** en eventueel **KPIs**.

Ze ziet volgende concrete actiepunten.

Domein(en)	Civiele Veiligheid	ACA
• **Brand & gebouw-zekerheid**	• Initiëren **overleg** met BVV, FRCSPB en brandweerkorpsen • **Terugkoppelen** wanneer doorgegeven alarm reële brand betrof • Betere **awareness** creëren rond brandveiligheid en evolueren naar een meer stringente **wetgeving**	• Engageren voor **verificatie** (wanneer technologie het toelaat) • IBZ betrekken bij **pilootprojecten** • Samen met overheid en brandweer meer **communiceren** over de voordelen van een geïntegreerde aanpak, inclusief aansluiting op een meldkamer • **Statistieken** verzamelen ter ondersteuning van beleidsuitwerking en evaluatie

Domein(en)	Veiligheid & Preventie	ACA
• **Inbraak & diefstal** • **Gewelds-criminaliteit, overlast & sluikstorten** • **'Lone workers'** • **Verkeer & mobiliteit**	• In samenwerking met ACA concrete invulling geven aan nieuwe **kaderwet**, inclusief luik **camerabewaking** op **publiek domein** – evolueren van ad hoc werkgroepen naar bredere en meer structurele samenwerking • Steun verlenen om **pilootprojecten** van de sector met andere stakeholders te bespoedigen	• Ontwikkelen tot betrouwbare **strategische partner** in het **uitvoeren** en **evalueren** van het toekomstige beleid rond veiligheid & preventie • IBZ betrekken bij **pilootprojecten** • **Statistieken** verzamelen ter ondersteuning van beleidsuitwerking en evaluatie • Toegevoegde waarde van aansluiting op meldkamer voor stakeholders **communiceren**

1.2 Samenwerking met lokale besturen

De sector wil **publiek-private samenwerkingen** met lokale besturen opzetten, voorafgegaan door een beperkt aantal goedgekozen **pilootprojecten** in samenwerking met andere stakeholders.

Specifiek voor diefstal en inbraak ziet ze mogelijkheden om het concept van het '**Keurmerk Veilig Wonen'** in Nederland en het certificaat '**Inbraak Veilig'** in bepaalde politiezones in België samen met de politie en lokale besturen uit te rollen op grotere schaal.

Ze ziet volgende concrete actiepunten.

Domein(en)	Lokale besturen	ACA

• **Gewelds-criminaliteit, overlast & sluikstorten**
• **Verkeer & mobiliteit**
	• Samen met sector en politiezone **pilootprojecten** opzetten rond:
	  • Cameraondersteuning voor preventie en reactie op geweldscriminaliteit, overlast & sluikstorten
	  • 'Remote access control' voor voetgangerszones en drukke (winkel)gebieden
	  • Cameraondersteuning op gebied van mobiliteit en access controle
		• **Samenwerken** met politie, gemeenten, burgers en ondernemers om **op een gestructureerde manier** gemeenschappelijke problemen effectief aan te pakken
		• **Gesprekspartner** zijn om de verzuchtingen van de burger goed te begrijpen (inclusief rond privacy)

• **Inbraak & diefstal**	• Sector betrekken in projecten zoals **certificaat 'Inbraak Veilig'**	• Ondersteunen van **preventie- en communicatiecampagnes** van politie

1.3 Samenwerking met politie

Voor de concrete invulling van de samenwerking met de politie, ziet de sector mogelijkheden om het concept van de **Regionale Toezicht Ruimten te Eindhoven en Nijmegen (RTR-NL)** in België toe te passen.

RTR-NL is een publiek-privaat samenwerkingsverband, gericht op veiligheid en leefbaarheid, ondersteund door cameratoezicht. Concreet zou dit concept in België zich vertalen in:

- **Proactief toezicht**, ook op **publiek domein**, door leden van ACA **onder regie van de politie**
- Een **ketengerichte samenwerking** met wederzijds respect voor de verantwoordelijkheden van de participerende partners
- Vandaag zou dit nog binnen de infrastructuur van de politie moeten gebeuren, op termijn kan het echter interessant zijn om de **infrastructuur van de private sector** te gebruiken omwille van schaalvoordelen

Daarnaast wil de sector samen met de politie werken aan **informatie-uitwisseling** – de sector kan namelijk beschikken over data die de politie kan ondersteunen bij interventies, zoals GIS-locatiemeldingen, contactgegevens, situatie, vluchtwegen enzovoort.

De sector identificeerde de volgende actiepunten.

Domein(en)	Politie	ACA

• **Gewelds-criminaliteit, overlast & sluikstorten**
• **'Lone workers'**
• **Verkeer & mobiliteit**
	• Samen met lokale besturen en politiezone **pilootprojecten** opzetten rond:
	  • Cameraondersteuning voor preventie en reactie op geweldscriminaliteit, overlast & sluikstorten
	  • 'Remote access control' voor voetgangerszones en drukke (winkel)gebieden
	  • Cameraondersteuning op gebied van mobiliteit
		• In samenwerking met politie meer **visie ontwikkelen 'vanuit het veld'** rond vereist wettelijk kader (data uitwisseling, privaat-publieke samenwerking, privacy enzovoort)
		• **Overleg** organiseren met wijkvertegenwoordigers (inclusief BINs) om de verwachtingen en uitdagingen beter te begrijpen en betrokkenheid te verhogen/ rol van BINs potentieel te verbreden

• **Inbraak & diefstal**	• Sector betrekken in projecten zoals **certificaat 'Inbraak Veilig'** • **Terugkoppelen** wanneer doorgegeven alarm reële inbraak of diefstal betrof • **Prioriteit** geven aan geverifieerde alarmen (eventueel mits voorwaarden zoals beeldverificatie)	• Ondersteunen van **preventie- en communicatiecampagnes** van politie • Streven naar **elektronische uitwisseling van gegevens**

1.4 Samenwerking met brandweer

De sector wil evolueren naar een model van **overleg** met de brandweer, en **concrete afspraken** maken over de samenwerking.

Op operationeel vlak wil de sector samen met de brandweer werken aan **informatie-uitwisseling** - de sector kan namelijk data delen zoals technische informatie rond branddetectie en gebouwinformatie.

Domein(en)	Brandweer	ACA
• **Brand & gebouw-zekerheid**	• Opzetten van een concreet **proefproject** met een (beperkt aantal) brandweerzone(s) rond verificatie van brandalarmen en informatie-uitwisseling	• Zich ontwikkelen tot **betrouwbare strategische partner** in het uitvoeren van het toekomstige beleid rond veiligheid en preventie • Meldkamer als **labo-omgeving** ter beschikking stellen

2. Samenwerking met private stakeholders

2.1 Samenwerking met verzekeraars

De sector wil een **gestructureerde dialoog** aangaan met verzekeraars, en **informatie uitwisselen** over de impact van monitoring op preventie en interventie, en ter ondersteuning van claimafhandeling. ACA ziet ook mogelijkheden om **proefprojecten** op te zetten met verzekeraars rond nieuwe technologieën.

Concreet ziet de sector volgende actiepunten.

Domein(en)	Verzekeraars	ACA
• **Inbraak & diefstal** • **Brand & gebouw-zekerheid** • **'Lone workers'**	• **Aanmoedigen aansluiting op meldkamer** (advies, verplichting en/of premieverlaging, afhankelijk van de situatie)	• Betere **statistieken** verzamelen die als input kunnen dienen voor risicoberekeningen door de verzekeraars • **Gesprekspartner** zijn voor INCERT & BOSEC **certificering**, en mee streven naar een adequate aanpak rond **cyber security** van IP gebaseerde inbraaksystemen

2.2 Samenwerking met installateurs

De samenwerking met installateurs kan grotendeels gebeuren via het bestaand samenwerkingsmodel met de Belgische beroepsvereniging van de elektronische beveiliging (ALIA Security), zowel voor het domein van inbraak & diefstal als voor brand en gebouwzekerheid. Er is wel ruimte om beter af te stemmen en **intensiever samen te werken** rond de toepassing van **nieuwe technologieën en businessmodellen**.

2.3 Samenwerking met bedrijven

Specifiek rond de problematiek **van lone workers** en '**virtual close protection**' wil de sector overleg plegen met vertegenwoordigers van hoog-risicosectoren om de noden beter om te zetten in doelmatige oplossingen.

De sector zal zoeken naar een pilootsector om samen een **proefproject** te lanceren, en wil streven naar voldoende **regelgeving** en **kwaliteitsgaranties** rond lone workers en 'virtual close protection'.

De sector ook nauw blijven samenwerken met **bewakingsondernemingen**, om samen **totaaloplossingen** in de markt te kunnen zetten.

3. Conclusie

Verschillende maatschappelijke, economische en technologische trends zorgen ervoor dat het steeds **complexer** wordt om zowel objectieve onveiligheid als subjectieve onveiligheidsgevoelens aan te pakken. Er is duidelijk nood aan een **integrale veiligheidsaanpak**, en een geïntegreerde en gecoördineerde **samenwerking** tussen de verschillende veiligheidsactoren. Zowel op het niveau van het beleid, als van private en publieke stakeholders.

De Alarm Centrale Associatie (ACA), de beroepsvereniging van de vergunde alarmcentrale, wil haar **unieke competenties** inzetten en inspelen op **technologische vooruitgang** om **actief mee te bouwen** aan de **integrale veiligheid**.

De meldkamer van de toekomst is immers een '**eventcentrale'** die een **breed spectrum van alarmen** behandelt en eveneens **proactief events en situaties kan managen**. De meldkamer is dé plaats waar alle relevante data – alarmen, maar ook beelden, geluid en locaties – op één plaats **geaggregeerd** kan worden. Leden van ACA zijn dan ook uniek gepositioneerd om deze datapunten te analyseren, de **juiste stakeholders te mobiliseren** en hen te **ondersteunen om betere beslissingen te maken**.

ACA wil zich in eerste instantie toeleggen op die domeinen waar ze een **win-win** kan creëren met andere actoren in de integrale veiligheid, namelijk:

- Inbraak en diefstal
- Brand en gebouwzekerheid
- Geweldscriminaliteit, overlast & sluikstorten
- 'Remote access control' op publiek domein
- Mobiliteit

De sector wil zich **engageren** om een volwaardige partner te zijn, en **toenadering** zoeken tot andere actoren in de integrale veiligheid. ACA wil hierbij in de voorhoede van **innovatie** spelen, en actief bijdragen aan de **ontwikkeling en evaluatie** van het **beleid**. Om voldoende visie te creëren "vanuit het veld", wil de sector **pilootprojecten** opzetten op het niveau van lokale besturen, politiezones en brandweerzones. Ze nodigt haar stakeholders uit om in **dialoog** te treden.

Appendix

Bronnen

Interviews

- ALIA Security (Olivier Demoulin)
- Assuralia (Bernard Desmedt)
- Brandweer Zone Centrum (Sam Gydé)
- BVBO (Jan Cappelle)
- CoESS (Danny Vandormael)
- Connex Center (Johan Chenot en Ludovic De Crem)
- Federale politie (Eddy De Raedt)
- FOD Binnenlandse Zaken (Philip Willekens)
- FOD Binnenlandse Zaken (Bert Hoffer)
- G4S Secure Monitoring (Filip Driesens en Mark Bormans)
- Lokale Politie Sint-Niklaas (Alain Collier)
- Oktopus (Gaëtan Lejeune en Pieter Debersaques)
- Securitas (Peter Henderickx)
- Seris Monitoring (Didier Herremans en Peter Verpoort)
- SMC (Gino Ghilardi)
- Vereniging van Vlaamse Steden & Gemeenten (Tom De Schepper)
- Verisure (Ralph Gijbels)
- Verisure (Steffen Berghman)
- Vlaams Agentschap Zorg & Gezondheid (Ilse Goossens)

Literatuurstudie

- Websites FOD Binnenlandse Zaken, Vigilis en Belgium.be
- Website Incert
- Federaal Kenniscentrum Civiele Veiligheid (2015) - Statistieken Belgische brandweer 2014
- Technavio (2016) - Smart Home M2M Market in Western Europe 2016-2020
- CoESS (2015) - The new security Company: integration of services and technology responding to changes in customer demand, demography and technology
- UGent Masterproef (2016) - Het vertrouwen in ANPR onderzocht: een analyse van de bijdrage van ANPR tot de criminaliteitsbestrijding in het kader van technology-led policing
- De Standaard (09/2017) - De grote levensvragen | Twaalf stellingen waar u het (niet) mee eens bent
- Nieuwsblad (08/2017) - Brandweer kan het niet langer aanzien: in België dubbel zoveel doden in branden als in Nederland
- Beveiliging Nieuws (08/2017) - Belgische staatssecretaris wil verbod onveilige IP-camera's
- Businesswire (05/2017) - Investors Bet That Deep Sentinel's Advanced Artificial Intelligence Can Protect American Homes by Predicting Crime
- Wingmag Pro (05/2017) - Britse politie voorspelt misdaad met Artificial Intelligence
- POM Technologies (04/2017) - A Look at Future Tech: How Artificial Intelligence and System Automation Could Impact Security
- The Verge (06/2017) - Police in Dubai have recruited a self-driving robo-car that can 'scan for undesirables'

- Tech Crunch (01/2017) - Alarm.com is building drones to monitor your home inside and out
- The Verge (09/2017) - The first autonomous drone delivery network will fly above Switzerland starting next month
- HLN (12/2016) - Stad hoest jaarlijks 90.000 euro op door vandalisme en graffiti
- Knack (04/2017) - Zwerfvuil en sluikstorten kost Vlaming jaarlijks 29 euro
- VRT (09/2017) - Eerste flitsmarathon tegen zwerfvuil