



**TKI URBAN ENERGY**  
Topsector Energie

# Handreiking cyber security voor smart energy



# INHOUD

<b>1</b>	<b>inleiding</b>	<b>04</b>
1.1	context	04
1.2	doel van het rapport	05
1.3	opbouw van het rapport	06
<b>2</b>	<b>methodische aanpak cyber security urban energy</b>	<b>07</b>
2.1	stappenplan	07
2.2	vastlegging van de risicoanalyse	09
2.3	periodieke controle	09
<b>3</b>	<b>cyber security aspecten</b>	<b>10</b>
<b>4</b>	<b>cyber security risico's</b>	<b>11</b>
<b>5</b>	<b>risicoreducerende maatregelen</b>	<b>14</b>
<b>6</b>	<b>risicoreductieoverzicht</b>	<b>15</b>
6.1	RRO: grafische weergave	15
6.2	RRO: begeleidend document	17
6.3	het maken en gebruiken van een rro	17
<b>7</b>	<b>toekomst van cyber security</b>	<b>18</b>
7.1	detectieve maatregelen	18
7.2	correctieve maatregelen	18
7.3	cyber security specialisten	19
<b>8</b>	<b>referenties</b>	<b>20</b>
<b>9</b>	<b>woordenlijst</b>	<b>20</b>

# VOORWOORD

Cyber security is een belangrijk aandachtspunt bij de ontwikkeling van moderne systemen, producten en diensten, omdat deze meer en meer met het internet verbonden zijn. De digitalisering brengt grote voordelen en leidt tot vele nieuwe mogelijkheden, ook in smart (urban) energy toepassingen. Het brengt echter ook nieuwe kwetsbaarheden met zich mee zoals we recent weer hebben ervaren. Cyber security krijgt al veel aandacht binnen meer 'traditionele' IT-oplossingen. Maar ook bij operationele technologie (OT) in energiesystemen dient cyber security onderdeel te zijn van het ontwerpproces. Security by design.

Cyber security zou niet langer alleen de verantwoordelijkheid moeten zijn van de cyber security expert, maar dient de verantwoordelijkheid te zijn van het hele ontwerp team. En van de bredere organisatie. TKI Urban Energy onderkent dit belang en wil partijen die innovaties ontwikkelen op het gebied van smart energy praktische handvatten bieden. RVO heeft daartoe, op verzoek van en in goed overleg met TKI Urban Energy, opdracht gegeven aan Technolution om een handreiking Cyber Security voor Smart Energy op te stellen voor experts in smart energy die geen achtergrond in het onderwerp hebben.

De handreiking geeft een aanpak in zeven stappen, omschreven op een toegankelijke manier, en geïllustreerd aan de hand van een voorbeeld dat de kwetsbaarheid van een Home Energy Management Systeem (HEMS) toont, indien cyber security onvoldoende aandacht krijgt. Dit voorbeeld is mede tot stand gekomen door inbreng van organisaties uit ons netwerk, die we hiervoor hartelijk willen bedanken. Voor uw gemak is er een risicolijst bijgevoegd, die u zelf kunt uitbreiden. En er is een memo-format gemaakt voor interne verslaglegging.

Cyber security houdt echter niet op bij het ontwerpproces. Door een snel veranderende wereld, maar ook door verandering in gebruik, kunnen nieuwe risico's ontstaan of kunnen gekozen cyber security maatregelen niet meer afdoende zijn. Het regelmatig opnieuw doorlopen van de risico-analyse op basis van de zeven stappen zou daarom onderdeel uit moeten maken van iedere bedrijfsvoering.

De handreiking Cyber Security voor Smart Energy en bijgevoegde documenten maken duidelijk dat cyber security een kwestie is van 'gezond verstand' in combinatie met een methodische aanpak. De grootste waarde zit in het bewust omgaan met het onderwerp en in de discussie die door de ontwikkelaars onderling en met het management wordt gevoerd. Het toepassen van deze handreiking leidt tot een product met een hoger veiligheidsniveau voor minder geld, en maakt cyber security tot een team effort. Deze handreiking draagt bij aan een efficiëntere manier van het implementeren van cyber security en zal zorgen voor een breed gedragen cyber securitybeleid binnen de gehele organisatie.

TKI Urban Energy bedankt Technolution voor hun prima werk, en RVO voor de goede samenwerking tijdens deze opdracht.

Wij wensen alle smart energy experts veel leesplezier en veel succes bij het toepassen van deze handreiking.

*Namens het Bestuur van TKI Urban Energy,*

**Frits Verheij**

# 1 INLEIDING

## 1.1 Context

Cyber security is in de digitale wereld van steeds groter wordend belang. Doordat steeds meer systemen met elkaar verbonden zijn en koppelingen met het publieke internet onvermijdelijk zijn, moet cyber security goed op orde zijn. Ook in de energiesector neemt de digitalisering een vlucht. Door zaken als teruglevering en vraagsturing (demand-response) krijgt de eindgebruiker een actievere rol in het energiesysteem en worden de systemen van de energieleveranciers en de netbeheerders uiteindelijk verbonden met de systemen, diensten en apparaten van en voor consumenten.

Cyber security is tot nu toe vaak gericht op het beveiligen van grote systemen (backoffices, PC etcetera). Dat is niet meer voldoende, ook bij de ontwikkeling van kleinere energieregelsystemen en -diensten en 'slimme' apparaten voor consumenten dient er voldoende aandacht te zijn voor cyber security. Omdat de software op de kleinere systemen niet wordt 'beheerd' door de gebruikers, hebben deze systemen een ander dynamiek. Achteraf security toevoegen is daarmee niet mogelijk, en moet er voor deze systemen en apparaten vanaf het ontwerp al rekening worden gehouden met cyber securityaspecten. Cyber security moet een onderdeel worden van het ontwerp- en ontwikkelproces van het bedrijf dat de energieregelsystemen en -diensten en apparaten ontwikkelt en aanbiedt op de marktplaats. Cyber security is daarmee niet slechts de verantwoordelijkheid van de cyber securityexpert, maar ook van de directie, architecten en ontwikkelaars.

De handreiking die voor u ligt, is bedoeld om het concept 'Security by Design' meer handen en voeten te geven voor leveranciers van producten en diensten in de energiesector.

'Security by Design' is een verantwoordelijkheid van het gehele ontwerpteam. Deze taak begint bij het uitvoeren van een goede risicoanalyse. Meestal wordt het uitvoeren van zo'n risicoanalyse niet als kerntaak van het ontwerpteam gezien en wordt daarom vaak uitbesteed aan een cyber securityexpert die geen verdere bijdrage levert aan het ontwerpteam. Hierdoor ontstaat het gevaar dat er gebrek aan draagvlak is binnen het ontwerpteam voor de voorgestelde maatregelen in de risicoanalyse. En dat cyber security maatregelen niet voldoende aansluiten bij eisen in de gebruiksfase van de energieregelsystemen en -diensten en apparaten.

Deze handreiking bevat een methode van risicoanalyse die het mogelijk maakt het gehele ontwerpteam te betrekken.

De voorbeelden die ter illustratie worden gebruikt in deze handreiking komen voort uit de toepassing van een Home Energy Management System (HEMS).

Een HEMS is een sturingssysteem dat in huis wordt geplaatst, primair om het binnenklimaat en comfort te regelen door aansturing van installaties (bijvoorbeeld warmtepomp, ventilatie). In de toekomst wordt verwacht dat de functionaliteit van HEMS verder uitgebreid zal worden, en dat er naast optimalisatie van energiegebruik en comfort op gebouwniveau, ook interactie zal zijn met energiemarkten (bijvoorbeeld door het aanbieden van flexibiliteit voor balanshandhaving, vermijden van netcongestie of portfolio optimalisatie van de programma verantwoordelijke partij). Een HEMS is in dat geval niet alleen aangesloten op installaties in huis, maar ook op een backoffice van de HEMS-leverancier en/of een aggregator.

Deze handreiking richt zich op connected systemen ('slimme' apparaten) binnen de energiesector (zogenoemde OT-kant). Het richt zich op de technische zaken en minder of niet op de organisatorische zaken. Ditzelfde geldt voor de privacy. Privacyaspecten met een technische achtergrond worden behandeld, maar juridische zaken zijn geen onderdeel van deze handreiking.

## 1.2 Doel van het rapport

Het doel van deze handreiking is het aanreiken van een methode om na te denken over en oplossingen te definiëren op het gebied van cyber security voor connected systemen die gebruikt worden in de energiesector.

De doelgroep van dit rapport zijn cyber securityexperts, directie, architecten en ontwikkelaars van bedrijven die dit soort systemen ontwikkelen en/of leveren.

Naast de handreiking 'Cyber security voor smart energy (dit document)' zijn ook de volgende documenten ontwikkeld:

- **Template cyber security (leeg)**
- **Template cyber security voorbeeld HEMS**
- **Template cyber security voorbeeld transformatorhuis**
- **Risico-maatregel lijst**

Met dit rapport bent u in staat om op een praktische manier een gedegen risicoanalyse te maken. Het eerste document beschrijft de methodiek en hoe in de verschillende stappen te komen tot een set van maatregelen waarmee de geïdentificeerde risico's voldoende zijn afgedekt.

Het template is een document waarin kan worden vastgelegd wat de geïdentificeerde risico's en maatregelen zijn, en welke geaccepteerde restrisico's er nog zijn. Dit document kan gebruikt worden om de rest van de organisatie mee te nemen in de conclusies. Tevens is het een startpunt voor de periodieke check-up. Als voorbeeld worden twee ingevulde templates meegeleverd.

Het laatste document is een lijst van risico's en maatregelen. Deze kan gebruikt worden ter inspiratie en ter aanvulling van de zelf gevonden risico's en maatregelen. Niet alle risico's zullen voor ieder project relevant zijn. Daarnaast zijn er wellicht risico's die wel relevant zijn, maar nog niet in deze lijst staan. Daarom wordt de lijst aangeleverd in Excel format, zodat u deze zelf kunt aanvullen met eigen risico's of met ervaringen uit de praktijk.

### 1.3 Opbouw van het rapport

Hoofdstuk 2 beschrijft op hoofdlijnen de voorgestelde methodische aanpak in de vorm van een stappenplan en daarbij het belang van vastlegging van de risicoanalyse en een periodiek controle hierop. Hoofdstuk 3 gaat dieper in op een aantal specifieke aspecten van cyber security die van belang zijn voor stappen 2 en 5 van het stappenplan.

In hoofdstuk 4 wordt uitgelegd wat een risico is en uit welke componenten een risico is opgebouwd. Het doel is om tot een waardering van het risico te komen (stappen 3 en 6 uit het stappenplan).

Hoofdstuk 5 geeft een classificatie van maatregelen die genomen kunnen worden om risico's te reduceren. De classificatie is nuttig in stap 4 van het stappenplan.

Hoofdstuk 6 beschrijft een techniek om de relatie tussen risico's, maatregelen en restrisico's gestructureerd vast te leggen (stap 7 van het stappenplan).

Hoofdstuk 7 geeft een beknopte visie op wat ons in de toekomst staat te wachten op het gebied van cyber securitymaatregelen en risicoanalyse.

## 2 METHODISCHE AANPAK CYBER SECURITY URBAN ENERGY

De methodische aanpak bevat een voorstel om risico's in beeld te brengen en risico-reducerende maatregelen te nemen bij het ontwerpen van nieuwe energieregelsystemen en diensten en 'slimme' apparaten. Deze handreiking geeft een aanpak, die ontstaan is door combinatie van verschillende methodes.

De aanpak in deze handreiking kan aangepast worden en daarmee de basis vormen voor een bedrijfsspecifieke aanpak van 'security by design'. Hierbij is het belangrijk dat het gehele ontwikkelteam zich bewust is van het belang van cyber security, van de belangrijkste risico's die er bestaan, en kan meedenken aan oplossingen/maatregelen die deze risico's adresseren.

### 2.1 Stappenplan

Voor het uitvoeren van de methodiek zijn de volgende stappen opgesteld:

#### 1 Hoe ziet de omgeving eruit?

In deze stap wordt bekeken vanuit welke (externe) bronnen bedreigingen kunnen komen. Het gaat er dus om welke verbindingen het slimme apparaat /systeem heeft met de buitenwereld en welke mogelijkheden deze buitenwereld heeft om het apparaat/systeem binnen te dringen.

#### 2 Wat zijn de risico's?

In deze stap wordt (gekeken vanuit een apparaat/systeem zoals dit nu is, zonder extra maatregelen) geïnventariseerd welke kwetsbaarheden en risico's er zijn. Dit zijn risico's die vanuit externe bronnen komen (zie vorige stap) en risico's die vanuit het systeem zelf komen. Een risico kan een bedrijfsrisico zijn, maar ook een risico voor consumenten of andere partijen die afhankelijk zijn van het bedrijfsmiddel. Ook deze risico's dienen te worden meegenomen in de risico-analyse. Ter inspiratie kan de risicomaatregelenlijst "Handreiking cyber security voor smart energy v0.2 - Risico-maatregel lijsten" worden gebruikt. Nieuwe risico's die niet op de lijst staan, kunnen (voor toekomstig gebruik) zelf worden toegevoegd.

#### 3 Zijn de risico's acceptabel?

Na het vaststellen van de risico's moet gekeken worden wat de waarschijnlijkheid van optreden en de impact na optreden is. Dit kan bijvoorbeeld in geld worden uitgedrukt: iets dat waarschijnlijk iedere 10 jaar optreedt en dan € 100.000 aan schade veroorzaakt, wordt ingeschat op een bedrag van € 10.000 per jaar. Op deze manier kan worden geanalyseerd of het om een acceptabel risico gaat. Niet alle risico's kunnen direct in geld worden uitgedrukt (zoals imagoschade, letselschade), maar door er een schatting van te maken kan wel geanalyseerd worden hoe groot dit risico is voor de organisatie. Op basis van stap 3 kan worden bepaald voor welk risico's maatregelen moet worden genomen om ze te verminderen.

#### 4 Welke maatregelen beperken deze risico's?

Voor de risico's die vanuit de vorige stap zijn aangemerkt als té groot, worden maatregelen gedefinieerd. Deze maatregelen moeten een (groot) deel van het risico wegnemen. Het is voor de analyse nuttig om ook de maatregelen uit te drukken in geld, met andere woorden, wat

gaat de implementatie van de gekozen maatregel kosten. Hiermee kan worden bepaald of de maatregel wel kosteneffectief is en bijvoorbeeld niet duurder is dan de kosten die in stap 3 zijn bepaald voor schade door het betreffende risico. In een situatie waar 'je onderbuikgevoel' zegt dat een maatregel wel genomen moet worden, maar waar de kosten voor de maatregel hoger zijn dan de geschatte schade als gevolg van het risico, kan heroverwogen worden of het ingeschatte jaarbedrag voor de schade wel reëel is.

## 5 Wat zijn restrisico's en zijn er nieuwe risico's?

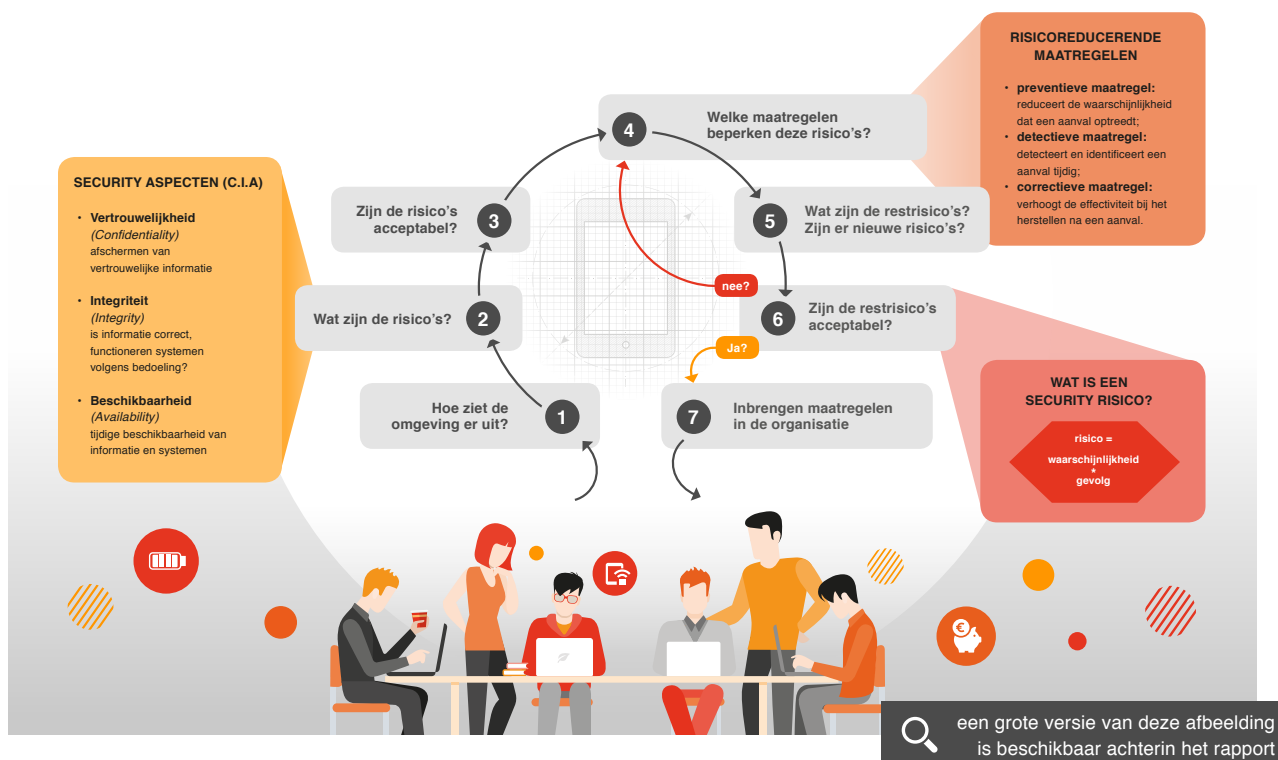
Nadat in de vorige twee stappen de risico's en de maatregelen zijn bepaald, wordt in stap 5 bepaald welk restrisico nog bestaat na toepassing van de gekozen maatregel(en) én welke mogelijke nieuwe risico's de gekozen maatregelen met zich mee brengt. Zie voor toelichting hoofdstuk 3.

## 6 Zijn de restrisico's acceptabel?

Op identieke wijze als in stap 3, waar bepaald is welke risico's acceptabel zijn, wordt ook van de restrisico's en eventuele nieuwe risico's bepaald of zij wel of niet acceptabel zijn. Indien deze risico's (nog) niet acceptabel zijn, ga je terug naar stap 4 waar nieuwe maatregelen opgesteld worden. Daarna worden stap 5 en stap 6 weer herhaald, net zo lang tot de restrisico's acceptabel zijn. Als de restrisico's acceptabel zijn, dan ga je door naar stap 7.

## 7 Inbrengen maatregelen in de organisatie.

Vanuit alle voorgaande stappen kan nu worden bepaald welke risico's het systeem zou lopen, welke maatregelen dienen te worden genomen en wat dan de te verwachten restrisico's zijn. Deze informatie wordt vastgelegd en kan worden gebruikt om de gehele organisatie bewust te maken van de cyber securityrisico's. Voor de directie is het van belang om te weten wat de starisico's waren, wat de maatregelen kosten, en wat de restrisico's zijn. Voor de ontwikkelaars is het van belang om te weten waarom bepaalde maatregelen zijn genomen en waarom bepaalde maatregelen (bewust) niet zijn genomen.





## 2.2 Vastlegging van de risicoanalyse

Het hele proces dat doorlopen is in de bovenomschreven zeven stappen methode, en informatie over de risico's en maatregelen kan worden vastgelegd in het memo template dat bij de handreiking is bijgevoegd. Daarnaast kunnen het proces en de belangrijkste resultaten ervan kunnen gevisualiseerd worden door middel van de **Risico Reductie Overzicht (RRO)-methode**, een methode die het gemakkelijk maakt de keuzes en consequenties te delen (zowel binnen als buiten het ontwerpteam). Zie voor meer informatie over het RRO hoofdstuk 6.

## 2.3 Periodieke controle

Een cyber security oplossing is nooit af. De digitale wereld om ons heen verandert snel en daarmee veranderen de risico's en kwetsbaarheden ook. Dat kan zijn omdat het apparaat een tot nu toe onbekende kwetsbaarheid bevat, omdat het apparaat in een andere context (bijvoorbeeld bereikbaar via internet) wordt gebruikt of omdat bepaalde geaccepteerde restrisico's nu anders (hoger) worden ingeschat.

Het is daarom nodig dat er met enige regelmaat, bijvoorbeeld **tweemaal per jaar, een risicoanalyse** plaats vindt. Hierbij wordt gekeken of de risicoanalyse zoals deze eerder is gedaan, nog actueel is en of het risico dat gelopen wordt nog acceptabel is. Eventuele wijzingen en/of extra maatregelen naar aanleiding van deze nieuwe risicoanalyse kunnen vervolgens worden geïmplementeerd.

## 3 CYBER SECURITY ASPECTEN

Als we het hebben over cyber security, dan moeten we rekening houden met een aantal verschillende aspecten. Securityaspecten worden vaak ingedeeld onder **Confidentiality, Integrity, Availability**, ook wel weergegeven als het acroniem 'CIA'.

Hieronder zijn vragen weergegeven per categorie. Deze vragen helpen bij aan het inventariseren van de risico's (stap 2 en stap 5).

### Vertrouwelijkheid

Dit gaat over het afschermen van vertrouwelijke informatie. Om te toetsen of vertrouwelijkheid geborgd is, kun je de volgende vragen stellen:

- *Is er voldoende borging dat vertrouwelijke of privacygevoelige informatie alleen toegankelijk is voor geautoriseerden?*
- *Is informatie 'in transit' voldoende beschermd tegen ongeautoriseerde toegang?*
- *Is informatie 'in rust' voldoende beschermd tegen ongeautoriseerde toegang?*
- *Wie zijn de geautoriseerden?*

### Integriteit:

Dit gaat over of informatie en systemen correct zijn en volgens de bedoelingen functioneren. Om de integriteit te toetsen kun je de volgende vragen stellen:

- *Wat is bron van de informatie?*
- *Is de informatie niet gemanipuleerd of gecorrumpeerd?*
- *Werkt het systeem correct?*
- *Ben ik verbonden met juiste systeem?*

### Beschikbaarheid (Availability):

Dit gaat over de tijdige beschikbaarheid van informatie en systemen. Om dit te toetsen kun je de volgende vragen stellen:

- *Wat gebeurt er als een systeem uitvalt?*
- *Wat gebeurt er als de communicatie tussen systemen uitvalt?*
- *Wat gebeurt er als de dataopslag kapot gaat?*
- *Hoe snel ben je weer operationeel na een 'calamiteit'?*

## 4 CYBER SECURITY RISICO'S

Om te beoordelen of een risico acceptabel is (stap 3 en stap 6) is het belangrijk te weten uit welke bestanddelen een risico is opgebouwd en hoe een risico kan worden gekwantificeerd.

Een risico is een functie van: **bedreigingen, kwetsbaarheden, bedrijfsmiddelen** en **waarde**. Een risico kan een bedrijfsrisico zijn, maar ook een risico voor consumenten of andere partijen die afhankelijk zijn van het bedrijfsmiddel. Ook deze risico's dienen te worden meegenomen.

Het risico is gebaseerd op een inschatting van de waarschijnlijkheid dat er een aanval wordt uitgevoerd en het gevolg van deze aanval. Een risico kan gekwantificeerd worden door de waarschijnlijkheid van optreden te vermenigvuldigen met de impact bij optreden (uitgedrukt in bijvoorbeeld euro's).

Een risicoanalyse begint met inzicht in wat je wilt beschermen. In zijn algemeenheid gaat het om **bedrijfsmiddelen**. Bedrijfsmiddelen kunnen verschillende dingen zijn: informatie, een proces, een systeem, een reputatie. Een bedrijfsmiddel heeft een **waarde**, meestal uitgedrukt in geld.

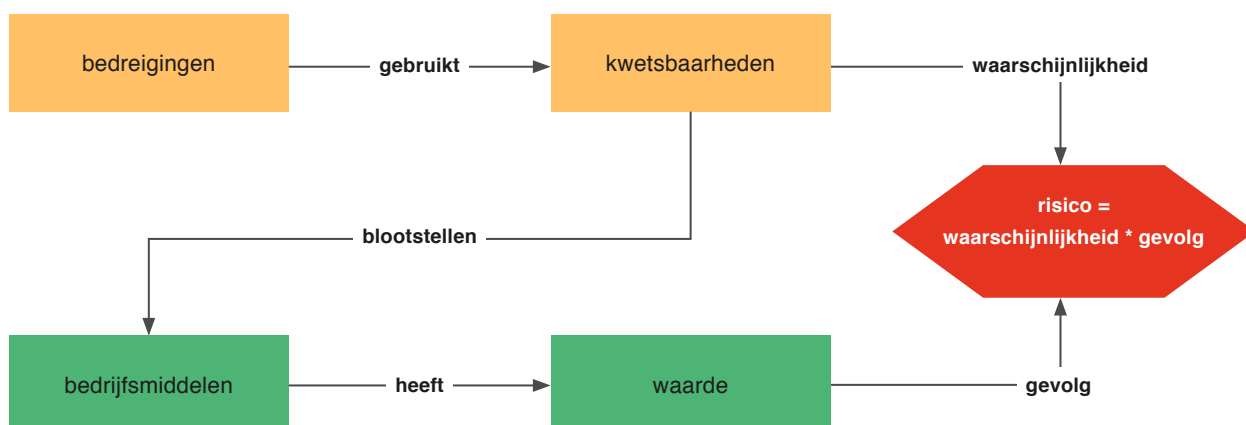
**Kwetsbaarheden** zijn systeemeigenschappen die ertoe kunnen leiden dat een bedrijfsmiddel blootgesteld wordt aan iets ongewenst. Denk hierbij bijvoorbeeld aan een 'buffer overflow' in software of een slecht beveiligde remote beheerinterface.

Cyber security gaat er vanuit dat iemand bewust een aanval uitvoert. Deze aanvaller is de **bedreiging**. Deze maakt gebruik van kwetsbaarheden in het systeem om bedrijfsmiddelen aan te vallen.

Er zijn grofweg twee werkwijzen te identificeren van aanvallers:

- **Gerichte aanval:** de aanvaller heeft het gemunt op bedrijfsmiddelen van een specifieke organisatie. De aanvaller gaat op zoek naar systemen van deze specifieke organisatie, die de gewenste bedrijfsmiddelen bevatten. Als zo'n systeem gevonden is, dan wordt geprobeerd deze aan te vallen door een breed spectrum aan potentiële kwetsbaarheden uit te proberen.
- **Gelegenheidsaanval:** de aanvaller heeft het niet gemunt op een specifieke organisatie, maar weet specifieke kwetsbaarheden in systemen te benutten. De aanvaller gaat op zoek naar systemen met deze specifieke kwetsbaarheden. Dit gebeurt meestal automatisch. Als zo'n systeem gevonden is, dan kan het aangevallen worden met een zeer grote kans van slagen.

Een *risico* is een functie van: *bedreigingen, kwetsbaarheden, bedrijfsmiddelen* en *waarde* (zie Figuur 1)



Figuur 1 • Risico vanuit bedrijfsperspectief

Bovenstaande wordt hieronder geïllustreerd aan de hand van een Home Energy Management System (HEMS) dat in staat is flexibiliteit te leveren (door energiegebruik in de tijd te verschuiven).

Een HEMS is een sturingssysteem dat in huis wordt geplaatst, primair om het binnenklimaat en comfort te regelen door aansturing van installaties (bijvoorbeeld warmtepomp, ventilatie). In de toekomst wordt verwacht dat de functionaliteit van HEMS verder uitgebreid zal worden, en dat er naast optimalisatie van energiegebruik en comfort op gebouwniveau, ook interactie zal zijn met energiemarkten (bijvoorbeeld door het aanbieden van flexibiliteit voor balanshandhaving, vermijden van netcongestie of portfolio optimalisatie van de programma verantwoordelijke partij). Een HEMS is in dat geval niet alleen aangesloten op installaties in huis, maar ook op een backoffice. Deze backoffice kan van een aggregator zijn, maar ook van de leverancier van de HEMS die de gegevens vervolgens doorzet naar een aggregator.

In de woning zelf is het HEMS verbonden met sensoren, bijvoorbeeld om energiegebruik te meten en/of met installaties om deze te schakelen of te voorzien van een instelling voor hun functioneren. Bijvoorbeeld om een elektrisch voertuig sneller of minder snel te laden afhankelijk van de belasting van het elektriciteitsnet. De **betrokken informatie wordt gezien als een bedrijfsmiddel**.

De waarde van deze informatie is lastig uit te drukken in geld, maar de informatie maakt het mogelijk om flexibiliteit aan te bieden. Flexibiliteit kan bijdragen aan balanshandhaving, maakt het vermijden van netcongestie, of portfolio-optimalisatie, drie zaken die in een financiële waarde kunnen worden uitgedrukt. Daarnaast kunnen de **gegevens van en naar een HEMS persoonlijk zijn** en moet er zorgvuldig met deze gegevens worden omgegaan, het beschermen van deze gegevens moet dus onderdeel uitmaken van deze risicoanalyse.

Een aanval kan pogingen doen om dit soort gegevens te verzamelen om hieraan geld te verdienen (verkoop van privacy gevoelige informatie aan derden). Daarnaast kan de aanval het HEMS zodanig beïnvloeden dat het HEMS de **netbelasting op piekmomenten juist vergroot** in plaats van dempt. Of in plaats van dat het meewerkt aan de programmaverantwoordelijkheid van een energieleverancier deze tegenwerkt. Een aanval met dergelijke intenties vormt een bedreiging. Hieronder wordt verder gegaan op het onderscheppen en verkopen van data.

De aanvaller kan data onderscheppen door de communicatie tussen de HEMS en de backoffice af te tappen. Bijvoorbeeld door op slinkse wijze een gratis app aan te bieden voor een tablet of smartphone, die dit soort verbindingen kan aftappen op het lokale wifinetwerk van de gebruiker. Dit is een kwetsbaarheid.

De waarschijnlijkheid dat persoonlijke gegevens worden afgetapt, kan als laag tot middelgroot worden ingeschat. Het gevolg is dat er persoonlijke gegevens worden verstrekt aan buitenstaanders via het HEMS. Dit kan tot imagoschade leiden voor de leverancier en mogelijk ook tot boetes van de Privacy Autoriteit. Het risico moet daarom als onacceptabel gezien worden.

De waarschijnlijkheid dat een HEMS wordt gebruikt om de netbelasting op piekmomenten te vergroten, is onduidelijk, maar komt steeds meer in de actualiteit met berichten over de mogelijkheden om energiesystemen in huis, zoals omvormers voor zon-PV panelen, op afstand en op een ongewenste manier massaal te beïnvloeden. Het gevolg van een gecoördineerde aanval kan zijn, dat de netbeheerder, op een moment dat deze de piekbelasting graag ziet afnemen, geconfronteerd wordt met een toenemende piekbelasting, wat kan leiden tot uitval van de elektriciteitsvoorziening in een gebied. Of dat een ongewenste dip ontstaat in de elektriciteitsopwekking als zon-PV omvormers massaal worden uitgeschakeld. Dit brengt kosten met zich mee voor de regionale netbeheerder, de TSO, de partijen aangesloten op het net, en/of voor een aggregator of energieleverancier die hierdoor mogelijk zijn programmaverantwoordelijkheid niet kan nakomen. Op basis van de gevolgen kan er toch besloten worden met maatregelen het risico te beperken, ondanks de onduidelijkheid over de waarschijnlijkheid van een uitval van de elektriciteitsvoorziening.

Uit bovenstaand voorbeeld wordt al duidelijk dat het belangrijk is om in de risicoanalyse de vraag te stellen: "Van wie is het risico?" Is het een risico voor de **eigen bedrijfsvoering** (de producent/leverancier van de HEMS), of is het een risico voor de **bedrijfsvoering van anderen**, zoals de netbeheerder, aggregator of een energieleverancier. In het voorbeeld van het aftappen van persoonlijke gegevens, ligt het risico bij de **eindgebruiker** van het HEMS. Echter, door privacy wetgeving en het risico op imagoschade, is er uiteindelijk impact op de bedrijfsvoering van de producent/leverancier van het HEMS, waardoor deze mogelijk toch maatregelen gaat treffen om dit soort risico's te verkleinen.

De inschatting van een risico is een momentopname. Een risico dat eerder als acceptabel werd beschouwd (bijvoorbeeld het risico op het vergroten van de netbelasting op piekmomenten) kan door veranderende inzichten en omstandigheden zomaar onacceptabel worden. Daarom is een periodieke controle/evaluatie van groot belang. (zie ook de methodische aanpak in paragraaf 2.3).

## 5 RISICOREDUCERENDE MAATREGELEN

Als een risico als onacceptabel wordt gezien (stap 3 en stap 6), dan moeten één of meerdere maatregelen getroffen worden om dit risico te reduceren (stap 4). Om een risico te reduceren, kan je de volgende soorten maatregelen nemen:

- **preventieve maatregel:** reduceert de waarschijnlijkheid dat een aanval optreedt;
- **detectieve maatregel:** detecteert en identificeert een aanval tijdig;
- **correctieve maatregel:** verhoogt de effectiviteit bij het herstellen na een aanval.

In het HEMS-voorbeeld is een voorbeeld van een preventieve maatregel het gebruiken van een secure tunnel op basis van Transport Layer Security (TLS) om af luisteren van persoonlijke gegevens tegen te gaan.

Een voorbeeld van een detectieve maatregel is het detecteren dat de verbinding tussen het HEMS en de backoffice wordt afgetapt. Een aanvaller kan proberen de verbinding via het lokale wifinetwerk af te tappen met behulp van ARP-spoofing. ARP-spoofing kun je detecteren in de wifigateway. De wifigateway kan de gebruiker van het HEMS op de hoogte stellen van de ARP-spoofing aanval die van een specifiek apparaat afkomstig is.

Indien de aanval is gedetecteerd en het apparaat is geïdentificeerd, kan de gebruiker ingrijpen door het apparaat dat wordt afgetapt/afgeluisterd uit het wifinetwerk te halen. Dit is een correctieve maatregel.

In dit specifieke voorbeeld zal alleen de preventieve maatregel volstaan. In het geval de preventieve maatregelen te duur of te gebruikersonvriendelijk worden, kan worden gekozen voor detectieve en/of correctieve maatregelen.

Een maatregel kan ook nieuwe bedrijfsmiddelen introduceren en dus ook nieuwe risico's.

### Bijvoorbeeld:

*Een maatregel om een secure tunnel te gebruiken heeft als gevolg dat er cryptografische sleutels nodig zijn. Deze sleutels zijn een nieuw bedrijfsmiddel en moet veilig gegenereerd, gedistribueerd, opgeslagen en uiteindelijk vernietigd worden. Als dit sleutelbeheer niet goed is ingevuld, dan is de secure tunnel minder effectief.*

## 6 RISICOREDUCTIEOVERZICHT

Maatregelen om cyber security te borgen, kosten vaak geld en leveren geen extra functionaliteit op. Om de organisatie ervan te overtuigen toch te investeren in maatregelen om de cyber security te verbeteren, is het noodzakelijk om het nut van een bepaalde set aan maatregelen inzichtelijk te maken, evenals bijbehorende kosten en baten. Het Risico Reductie Overzicht (RRO) biedt dit inzicht.

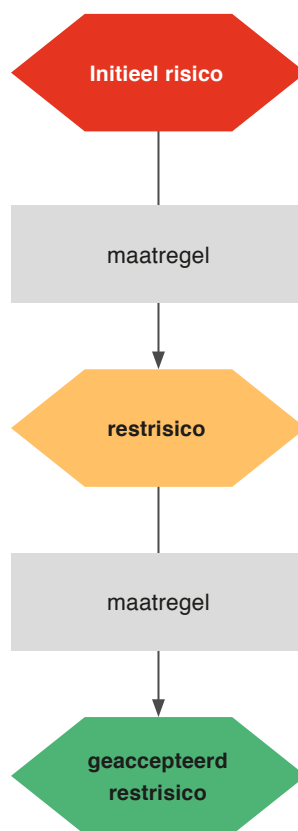
De genomen maatregelen kunnen in de praktijk nooit 100% alle risico's wegnemen. Het is daarom ook noodzakelijk om een goed beeld te hebben van alle **restrisico's en mogelijk nieuw geïntroduceerde risico's** die overblijven na het nemen van alle maatregelen. Ook deze worden in het RRO inzichtelijk gemaakt.

Daarnaast is **cyber security zoals gezegd een continu proces en niet een éénmalige exercitie**. Geïdentificeerde risico's worden groter of juist kleiner, genomen maatregelen kunnen hun effectiviteit verliezen en de IT/OT-omgeving verandert. Om cyber security goed te kunnen blijven borgen, is het noodzakelijk om de genomen maatregelen regelmatig tegen het licht te houden en indien nodig aan te passen. De laatste RRO vormt een goed startpunt voor de nieuwe risicoanalyse.

Kortom, een RRO is een methode die op een simpele manier inzicht geeft in de samenhang van geïdentificeerde risico's, de genomen maatregelen en de geaccepteerde restrisico's. **Een RRO bestaat uit twee onderdelen. Een grafische weergave van alle relevante risico's en maatregelen, en een begeleidend document waarin de details zijn beschreven.** Het RRO blijkt erg nuttig te zijn voor discussies, optimalisaties, evaluaties en besluitvorming in het proces van risicoanalyse.

### 6.1 RRO: grafische weergave

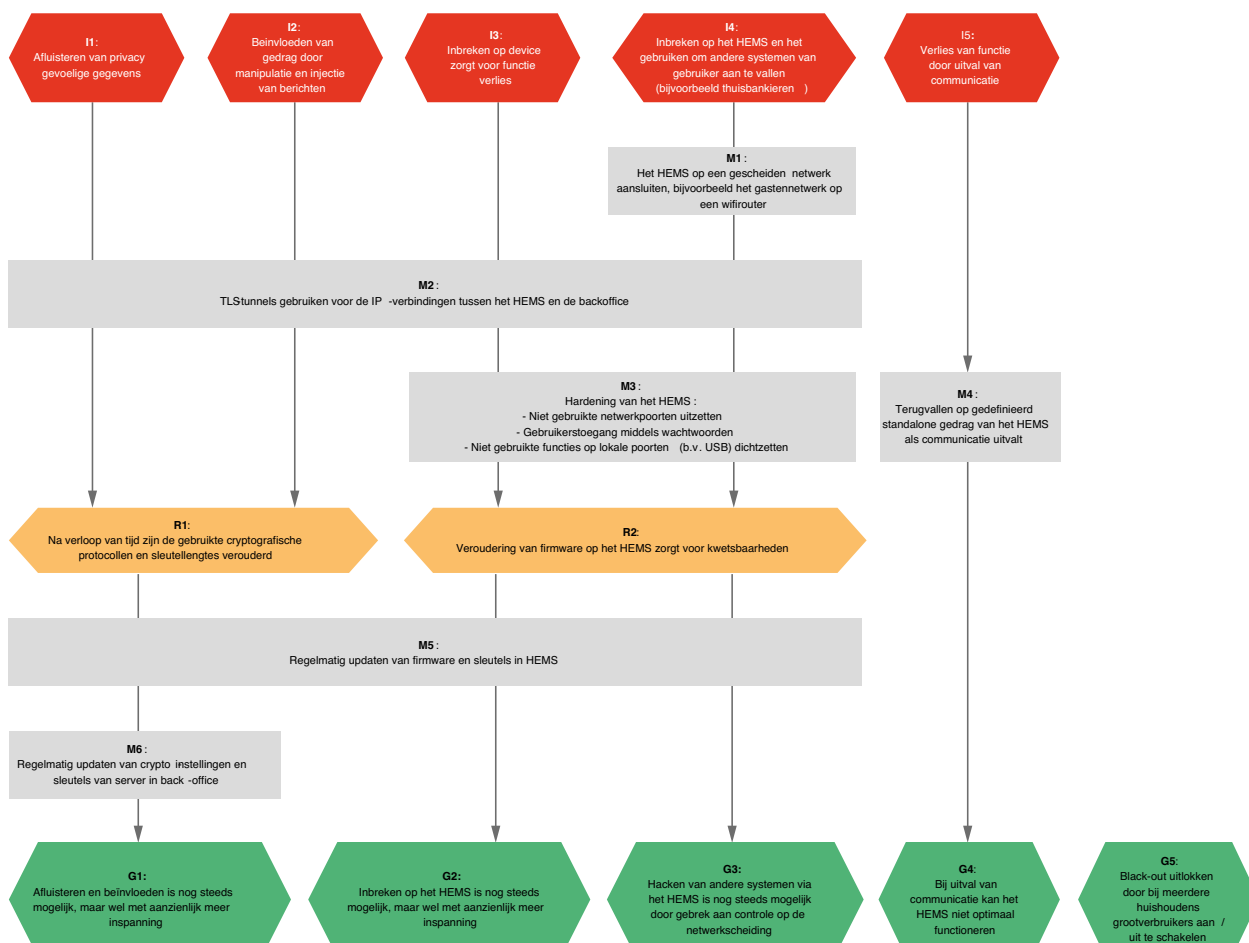
Een RRO (zie figuur 2) begint met een aantal initiële risico's (rode zeshoeken). Door het nemen van maatregelen (blauwe rechthoeken) worden de initiële risico's gereduceerd (pijl) in restrisico's (gele zeshoeken en groene restrisico's). Als restrisico's niet geaccepteerd kunnen worden (gele zeshoeken), dan kan gekozen worden om deze verder te reduceren met extra maatregelen. Deze risicoreductie gaat door totdat er uiteindelijk alleen maar geaccepteerde risico's (groen zeshoeken) over zijn.



Figuur 2 • methode en toelichting gebruikte vormen en kleurcodering

Om de RRO-methode te illustreren, is een praktisch voorbeeld van een Home Energy Management System (HEMS) uitgewerkt (zie hoofdstuk 4). Het voorbeeld vindt u in figuur 3.

In dit voorbeeld worden vijf initiële risico's (I1 t/m I5) met behulp van zes maatregelen (M1 t/m M6) gereduceerd tot vier geaccepteerde restrisico's (G1 t/m G4). Daarnaast is er een initieel risico dat zonder maatregelen geaccepteerd wordt (G5).





## 6.2 RRO: begeleidend document

### 6.3 Het maken en gebruiken van een RRO

Het maken van een RRO is een activiteit die tijdens de ontwerp- en realisatiefase van een product uitgevoerd wordt. Het is een activiteit van het gehele ontwerpteam en niet alleen van een cyber securityexpert.

De eerste aanzet voor een RRO vindt typisch plaats in een workshop met het hele ontwerpteam eventueel aangevuld met een cyber security expert. Het team gaat brainstormen en kan met behulp van 'geeltjes' risico's en maatregelen op een whiteboard plaatsen. Op deze manier kan geprobeerd worden een eerste ruw RRO-overzicht te maken.

De resultaten van zo'n workshop worden uitgewerkt door een klein team en ter review aangeboden. Na een aantal reviewslagen is er een RRO waarin het hele ontwerpteam zich kan vinden.

Het resulterende RRO legt vast aan welke initiële risico's gedacht is, welke maatregelen er genomen worden en welke restrisico's geaccepteerd worden. Het RRO kan gebruikt worden als discussiestuk binnen het ontwerpteam om te evalueren of aan alle significante risico's gedacht is en om de set aangenomen maatregelen te optimaliseren.

Het betrekken van het ontwerp team in de risicoanalyse, draagt bij aan bewustwording en draagvlak bij het ontwerpteam. Op deze manier wordt geborgd dat het ontwerpteam zich ook verantwoordelijk voelt voor de juiste implementatie van maatregelen.

Ook het creëren van draagvlak bij management is belangrijk. Zij moet immers budgetten en tijd reserveren om de geselecteerde maatregelen te implementeren. Ook hier kan het RRO een cruciale rol spelen.

Gedurende de gebruiks- en onderhoudsfase van een product kan het RRO als naslagwerk gebruikt worden. Als in het RRO geïdentificeerde risico's groter of juist kleiner worden, genomen maatregelen hun effectiviteit verliezen en de IT/OT-omgeving verandert, is het tijd voor een nieuwe risicoanalyse. Het is daarom belangrijk om de RRO regelmatig te toetsen aan deze nieuwe inzichten en eventueel bij te werken als dit nodig is. Bijvoorbeeld:

Mocht om praktische redenen het niet haalbaar zijn om het HEMS op een eigen wifi netwerk aan te sluiten, dan kan met één blik op de RRO gezien worden dat Risico I4 minder goed gereduceerd wordt en dat opnieuw geëvalueerd moet worden of restrisico G3 wel acceptabel is.

## 7 TOEKOMST VAN CYBER SECURITY

Cyber security is een 'rat race' (een race die nooit gewonnen zal worden) tussen de kwaadwillenden en de bouwers van apparatuur/software. Deze race resulteert in steeds ingewikkeldere systemen vooral gebaseerd op preventieve maatregelen. Dit is voor de toekomst niet houdbaar. In dit hoofdstuk staan enkele visies op de toekomst ter inspiratie.

### 7.1 Detectieve maatregelen

Veel cyber securitymaatregelen die nu in processen en systemen zijn ingebouwd, bestaan uit preventieve maatregelen (firewalls, hardening, patchmanagement, wachtwoorden, two-factor authentication et cetera). Dit zijn maatregelen die bedoeld zijn om misbruik te voorkomen.

De huidige manier van werken binnen cyber security kan gezien worden als 'steeds een hoger muurtje bouwen'. Als de hacker een manier heeft gevonden om net over de muur te komen, maken we de muur een klein stukje hoger. Doordat hackers steeds handiger worden in het omzeilen van deze preventieve maatregelen, worden er steeds meer en steeds stringenter preventieve maatregelen getroffen. Al deze extra maatregelen zijn vaak zeer duur, dreigen de bruikbaarheid van de processen en systemen te ondermijnen en zijn achteraf gezien vaak niet effectief.

Een van de trends binnen cyber security is de beweging naar detectieve maatregelen. Deze detectieve maatregelen richten zich op het detecteren van (cyber)aanvallen en het afslaan van deze aanvallen door actief ingrijpen in processen en systemen als er een aanval wordt gedetecteerd.

Het is van belang dat er een goede detectie is van een aanval. Dit kan juist bij systemen die een hele specifieke functie hebben, redelijk goed. Bijvoorbeeld: afwijkingen van de standaardwerking van een HEMS kan worden gedetecteerd.

Ook het controleren van de integriteit en authenticiteit van de code die wordt uitgevoerd, is een goede detectiemethode om aanvallen met codemanipulatie te detecteren.

### 7.2 Correctieve maatregelen

Naast detectieve maatregelen is er ook een trend richting meer correctieve maatregelen. Dit heet ook wel resilience. Een correctieve maatregel is gericht om, na het plaatsvinden van een aanval en het afslaan hiervan, weer op een efficiënte manier in bedrijf komen (al is het maar gedeeltelijk).

#### Bijvoorbeeld:

*na detectie van een afwijking van de software van een HEMS, kan het apparaat al dan niet automatisch terug worden gezet naar zijn default software. Deze default software hoeft niet alle functionaliteit van het HEMS te omvatten, maar moet voldoende zijn voor de basale functies van het HEMS en moet de mogelijkheid hebben om nieuwe, authentieke software op te kunnen halen uit een betrouwbare bron.*

### 7.3 Cyber security specialisten

Een derde toekomstvisie is dat de securityspecialisten steeds minder aan het ontwikkelen zijn, maar zich bezighouden met een visie op cyber security en het aanleveren van methodieken om het toe te passen. Cyber security wordt pas echt goed geïmplementeerd als het behapbaar en te begrijpen is voor de 'gewone' ontwikkelaars en architecten en er ook draagvlak is bij hun directie.

In de toekomst zal cyber security onderdeel worden van de bedrijfscultuur. Het zal even normaal worden het hebben van een bedrijfspas om het pand binnen te komen, of om je als bezoeker te moeten melden bij de receptie. Waar de IT-kant nu al standaard een aantal maatregelen neemt, moet cyber security ook een standaard onderdeel worden van OT. Een methodiek zoals omschreven in deze handreiking dient een integraal onderdeel te zijn van het ontwikkelproces en iedere software- en hardwarearchitect neemt het mee als onderdeel van het ontwerp.

## 8 REFERENTIES

- [ISO] "27005: Information security risk management", NEN-ISO/IEC, 2011
- [NIST] "NIST SP 800-30: Guide for Conducting Risk Assessments", NIST, 2012, Revision 1, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- [RRO] "Risk Reduction Overview: A visualization method for Risk Management", H.N.J Havinga, O.D.T. Sessink, 2014, <http://rro.sourceforge.net/>, [https://olivier.sessink.nl/publications/Risk\\_Reduction\\_Overview-A\\_visualization\\_method\\_for\\_risk\\_management.pdf](https://olivier.sessink.nl/publications/Risk_Reduction_Overview-A_visualization_method_for_risk_management.pdf),

## 9 WOORDENLIJST

**ARP-spoofing** • Het Address Resolution Protocol (ARP) wordt gebruikt om een fysiek netwerkadres (MAC-adres) te associëren met een IP-adres op een lokaal netwerk. ARP-spoofing is een techniek om het ARP zodanig te misbruiken dat het MAC-adres van de aanvaller wordt geassocieerd met het IP-adres van een ander. Met deze techniek kan een aanvaller zichzelf tussen de communicatie van twee systemen op een lokaal netwerk in plaatsen.

**Bufferoverflow** • In een computersysteem staat executeerbare code en data door elkaar heen in hetzelfde geheugen. Een buffer is een stukje geheugen dat bedoeld is voor data. Door onbedoeld buiten dit buffer te schrijven (een bufferoverflow) kan executeerbare code worden overschreven. Dit levert vaak onbedoeld en onverwacht gedrag op van het systeem en daarom wordt een bufferoverflow gezien als een programmeerfout. Bufferoverflows worden veelvuldig door een aanvallers misbruikt om het computersysteem binnen te dringen.

**HEMS** • Home Energy Management System. Een HEMS is een apparaat dat in een huis wordt geplaatst en dat het energieverbruik afstemt met externe belanghebbenden (netbeheerder en/of energieleverancier).

**Informatie 'in transit'** • Informatie die wordt uitgewisseld tussen systemen.

**Informatie 'in rust'** • Informatie die wordt opgeslagen op een systeem.

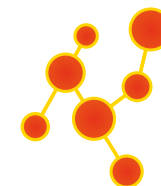
**IT** • Information Technology is techniek waarbij het beheer van informatie centraal staat.

**OT** • Operational Technology is techniek waarbij het operationeel houden van een proces centraal staat.

**RRO** • Risico Reductie Overzicht. Een techniek om de relatie tussen risico's, maatregelen en rest risico's gestructureerd vast te leggen.

**Wifi** • Een techniek voor draadloze netwerken op basis van de IEEE 802.11-standaard.

# Cyber security voor Smart Energy



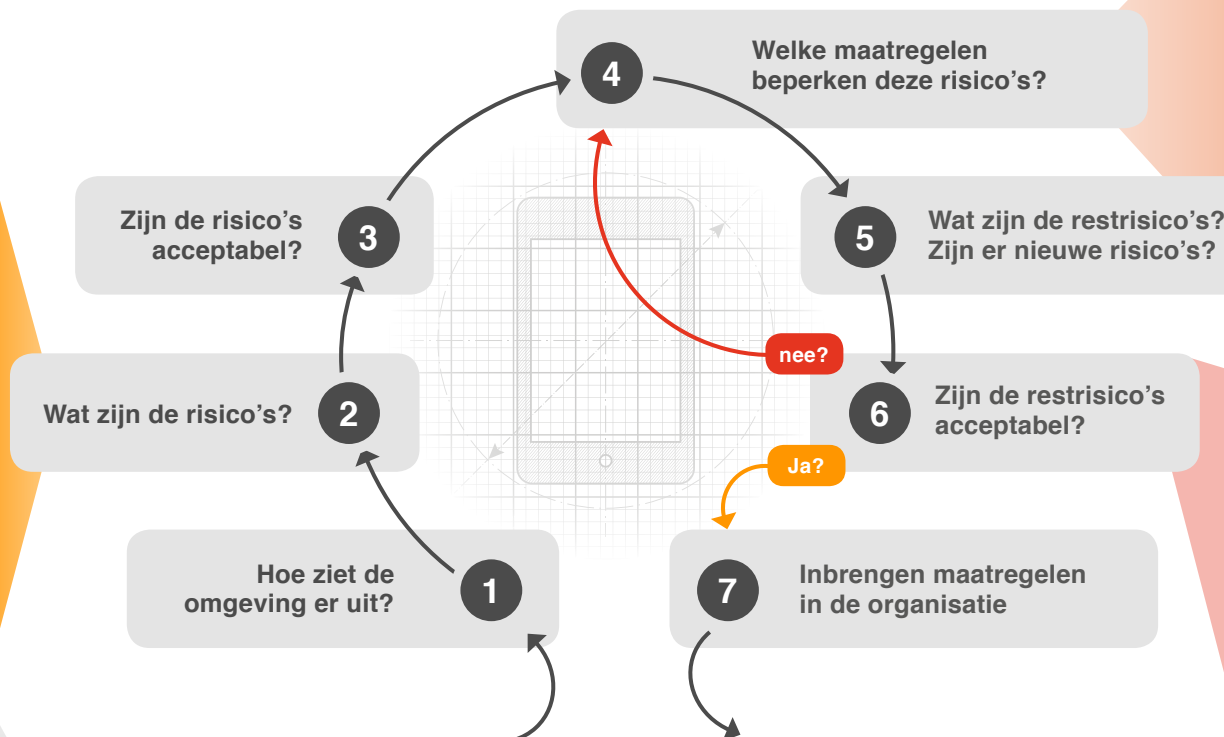
TKI URBAN ENERGY  
Topsector Energie

## Security by design:

een breed gedragen risicoanalyse  
in 7 stappen

### SECURITY ASPECTEN (C.I.A)

- **Vertrouwelijkheid**  
(Confidentiality)  
afschermen van vertrouwelijke informatie
- **Integriteit**  
(Integrity)  
is informatie correct, functioneren systemen volgens bedoeling?
- **Beschikbaarheid**  
(Availability)  
tijdige beschikbaarheid van informatie en systemen



### RISICOREDUCERENDE MAATREGELEN

- **preventieve maatregel:**  
reduceert de waarschijnlijkheid dat een aanval optreedt;
- **detectieve maatregel:**  
detecteert en identificeert een aanval tijdig;
- **correctieve maatregel:**  
verhoogt de effectiviteit bij het herstellen na een aanval.

### WAT IS EEN SECURITY RISICO?

risico =  
waarschijnlijkheid  
\*  
gevolg



