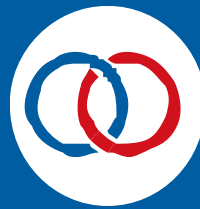


Hoe wordt de IEC 62443 toegepast over de gehele keten, van product leverancier tot asset owner?



NIS II



IEC 62443



Compliance



Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch





Bart Scholten

- Commercieel manager cyber security IoT / OT.
- 5> werkzaam bij Kiwa
- IEC 62443 Certified security professional



Mischa van der Geld

- Manager Business Acceleration Cyber Security – Kiwa Group
- MSc and BBA in Safety and Security management
- >5 year experience in TIC business for Fire Safety & (cyber) Security
- IEC 62443 Certified security professional



Content



Het wettelijk kader:

De NIS II.



IEC 62443:

IEC 62443 in de keten.



Praktijkcase
gebouwgebonden systemen:

Toepassing IEC 62443 in fire safety
branche.



Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch



NIS II richtlijn (EU) 2022/2555

*“De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten **passende en evenredige technische, operationele en organisatorische maatregelen nemen** om de risico’s voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.”*



NIS II richtlijn (EU) 2022/2555

- **Essentieel:**
 - Sectoren bijlage 1
 - ≥ 250 medewerkers
 - Of jaaromzet $> \text{€}50\text{mln.}$
- **Belangrijk:**
 - Sectoren bijlage 1 & 2
 - ≥ 50 medewerkers
 - Of jaaromzet $> \text{€}10\text{mln}$
- Kleine ondernemingen met kritieke functie op aanwijzing van minister.
- **Zorgplicht, meldplicht & toezicht.**

Sectoren bijlage 1	Sectoren bijlage 2
Energie	Digitale aanbieders
Transport	Koeriersdiensten
Bankwezen	Afvalstoffen beheer
Financiële markt (infra)	Levensmiddelen
Gezondheidszorg	Chemische stoffen
Drinkwater	Onderzoek
Digitale infrastructuur	Manufacturing
Beheerders van ICT diensten	
Afvalwater	
Overheidsdiensten	
Ruimtevaart	



NIS II richtlijn (EU) 2022/2555

Eisen (zorgplicht)

- a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;
- b) incidentenbehandeling;
- c. Bedrijfscontinuïteit
- d. Beveiliging toeleveringsketen
- e. Beveiliging verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen
- f. Beleid en procedures t.b.v. beoordelen effectiviteit van maatregelen
- g. Basispraktijken cyberhygiëne en opleiding
- h. Beleid en procedures m.b.t. cryptografie
- i. Beveiligingsaspecten personeel, toegangsbeleid en beheer van activa
- j. Authenticatieoplossingen en noodcommunicatie

• Wanneer van kracht:

- 27 december 2022 NIS II gepubliceerd in OJ.
- Consultatie najaar 2023
- 18 oktober 2024 nationale wetgeving van kracht. (voormalig WBNI)

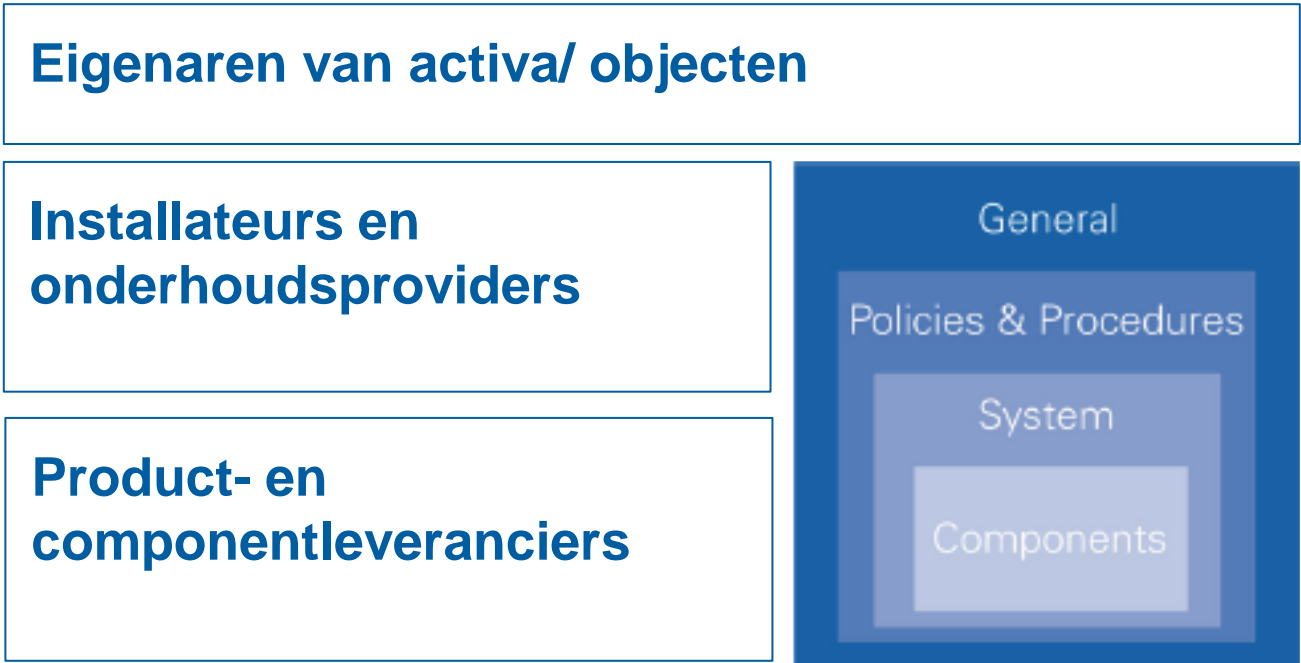
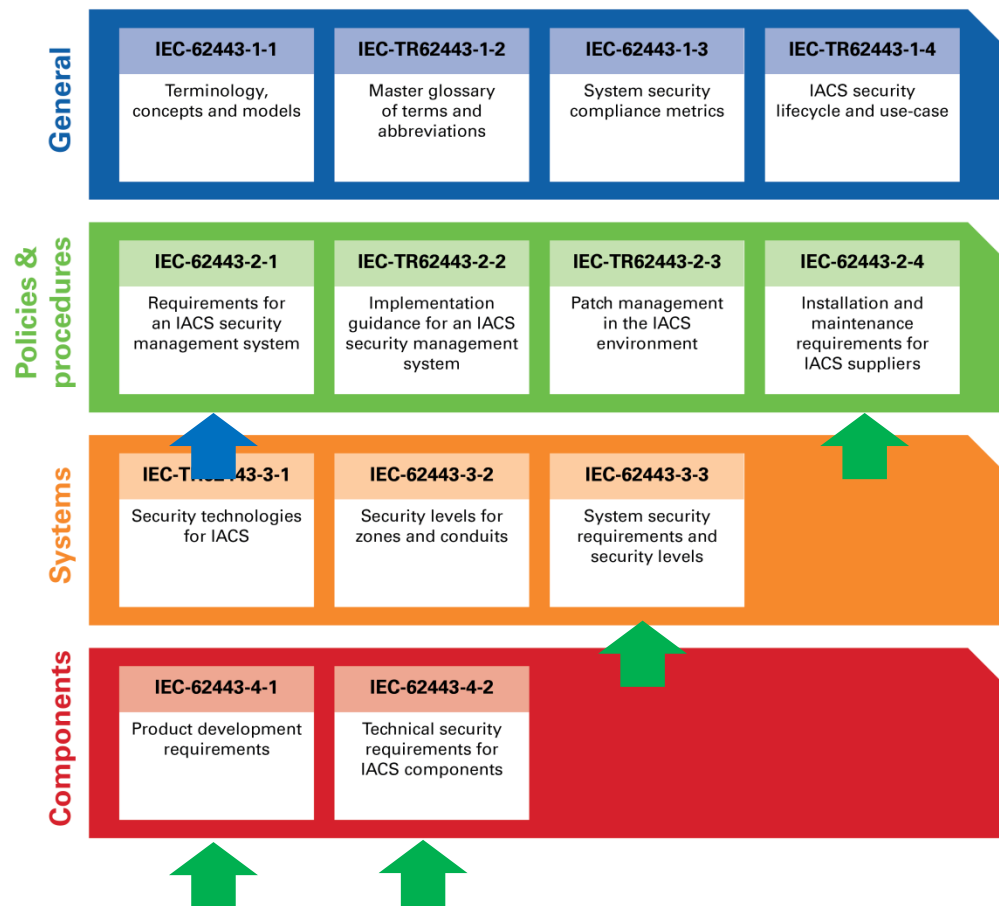


• Handvatten voor compliance:

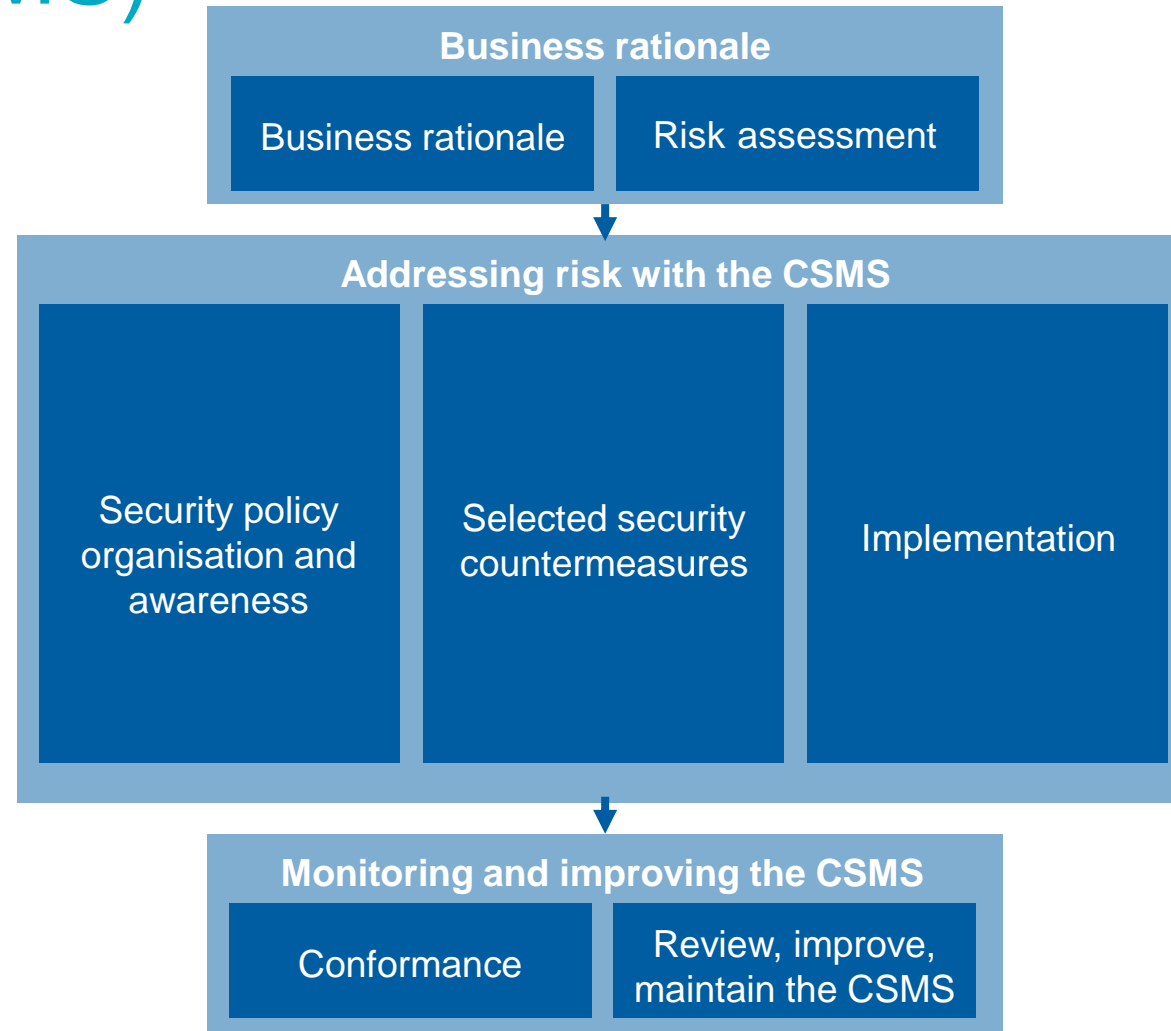
- DTC website
- ISO 27001
- IEC 62443



IEC 62443 in de keten



IEC 62443-2-1 – Cyber security management system (CSMS)



IEC 62443

Producten, systemen & installateurs



IEC 62443-4-1 & 4-2

- Security level capability van componenten en producten.
- "Security by design" in product ontwikkelings proces harde vereiste.
- Requirements uit IEC 62443-4-2 zo goed als gelijk aan requirements uit IEC 62443-3-3.

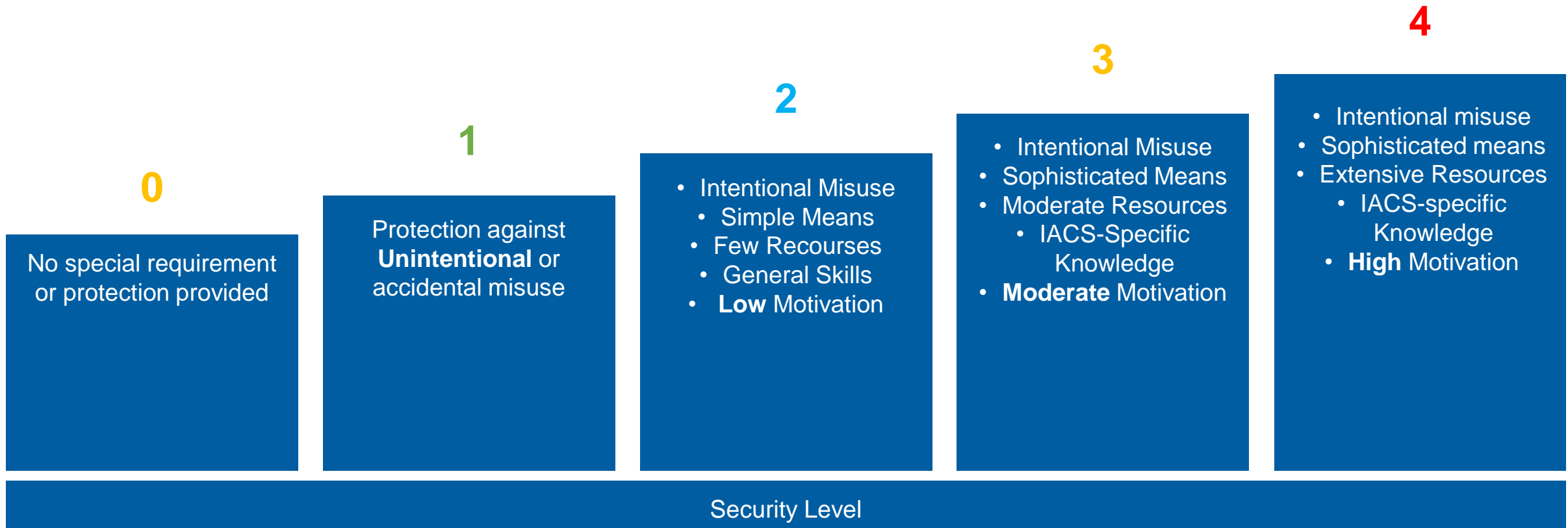


IEC 62443-3-3 & 2-4

- Maturity level van installateurs en processen.
- Netwerk architectuur: zones & conduits.
- Gebruik van IEC 62443-4-2 gecertificeerde componenten maakt behalen van security level voor systeem eenvoudiger.



IEC 62443 – Security level



IEC 62443 – Maturity level

Maturity level	Category	Organization is capable of performing a service...
1	Initial	without a documented process that is poorly controlled.
2	Managed	with a format documented process with evidence of expertise and trained personnel.
3	Defined	at maturity level 2 and demonstrates the use of defined, established and documented processes as well as defined training schemas for personnel.
4	Improving	at maturity level 3 as well as demonstration of continuous improvement.



Praktische usecase

Remote Access Remote Service for Sprinkler Pumps

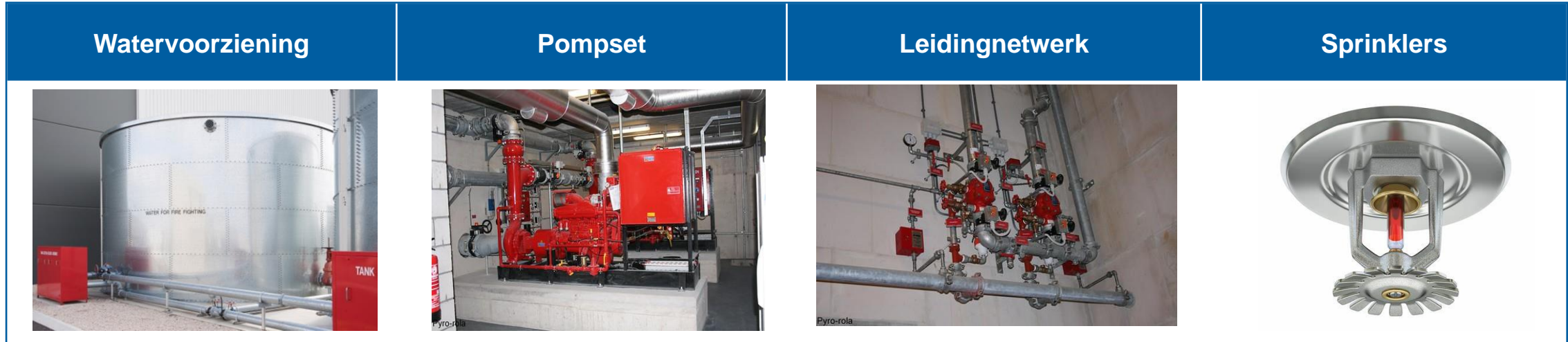


Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch








Een sprinkler systeem...sterk vereenvoudigd



- Beheerstaken (op basis van TB-80) twee wekelijks testen van pompset en diverse functionele testen (boven en onderdruk alarmkleppen, Flow etc)
- Conservatieve markt - Veelal stand-alone systemen zonder connectiviteit
- Door schaarste in arbeidsmarkt noodzaak en technologische mogelijkheden behoefte en noodzaak aan remote acces remote service (op afstand testen)
- Met toevoegen connectiviteit en “smart” sensoren introduceer je kwetsbaarheden die een bedreiging vormen voor de beschikbaarheid en integriteit van het systeem



Een sprinkler systeem... een heel nieuw “cyber secure ecosysteem”

Pompset / Smart sensors	PLC	Router	Test software (in Data Center)	Control Room
				
<ul style="list-style-type: none"> • Functionele Eisen op basis van onderhoudsvoorschriften (TB 80) • IEC 62443 4-2 op sensoren (indien radio geconnecteerd) 	<ul style="list-style-type: none"> • IEC 62443 4-2 voor component • En IEC 62443 4-1 voor producent 	<ul style="list-style-type: none"> • IEC 62443 4-2 (Radio Equipment Directive) 	<ul style="list-style-type: none"> • EN50600 \ C5 or other relevant data center standard 	<ul style="list-style-type: none"> • EN 50518 (Alarm receiving and monitoring center – CAT 2)
<p>←—————• Secure connectivity EN 50136 -1—————→</p>				



Een sprinkler systeem... een heel nieuw “cyber secure ecosysteem”

Pompset / Smart sensors	PLC	Router	Test software (in Data Center)	Control Room
 <ul style="list-style-type: none"> Functionele Eisen op basis van <u>onderhoudsvoorschriften</u> (TB 80) IEC 62443 4-2 op <u>sensoren</u> (indien radio <u>geconnecteerd</u>) 	 <ul style="list-style-type: none"> IEC 62443 4-2 voor component En IEC 62443 4-1 voor producent 	 <ul style="list-style-type: none"> IEC 62443 4-2 (Radio Equipment Directive) 	 <ul style="list-style-type: none"> EN50600 \ C5 or other relevant data <u>center</u> standard 	 <ul style="list-style-type: none"> EN 50518 (Alarm receiving and monitoring center – CAT 2)

System



Integrator



Asset owner

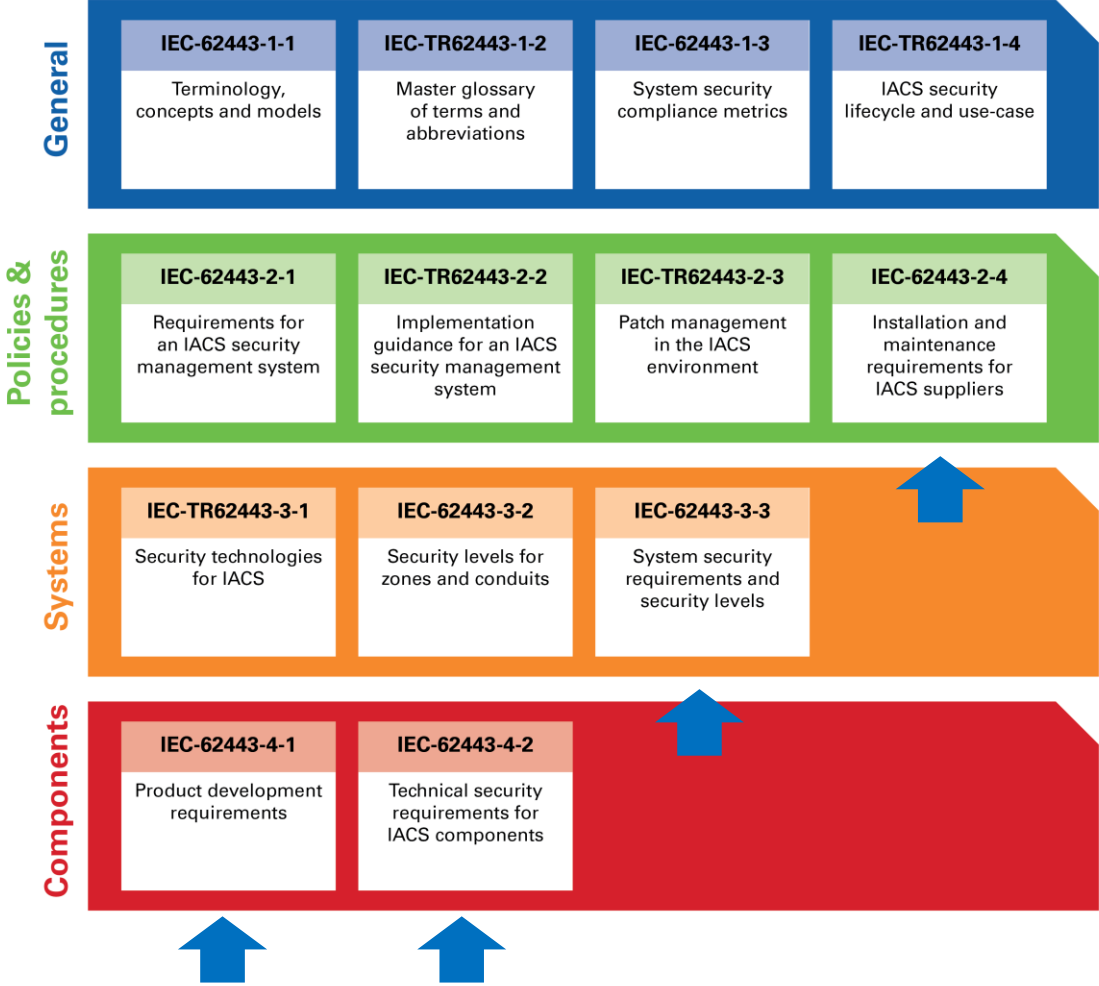


Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch



Gerelateerde IEC 62443 sub-delen.



Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch



Take aways

Bereid je voor door te kijken welke impact de NIS II heeft op uw organisatie.

Bekijk welke normenkaders er zijn en kijk welke het beste passen bij uw organisatie.

Kom naar de Kiwa stand en stel uw vragen.



Meer weten?



Bart Scholten
Commercial manager
Cyber security (IoT / OT)

E bart.scholten@kiwa.com
M +31 6 21 14 79 55

Stand 15