

IACS & CYBERSECURITY CONFERENCE



Marcel Jutte

OT Cybersecurity expert, IPCS
(Industrial Platform Cyber Security)



Johan Assies

OT Security Consultant, IPCS
(Industrial Platform Cyber Security)



IACS & CYBERSECURITY CONFERENCE



April 15th 2025 • Amersfoort • The Netherlands



Industrieel Platform Cyber Security

Publiek / private samenwerking

Johan Assies

Voorzitter IPCS

johan.assies@securitydelta.nl

Marcel Jutte

Vicevoorzitter IPCS

marcel.jutte@securitydelta.nl



Bio Marcel Jutte

Marcel is een senior cybersecurityspecialist met meer dan 35 jaar ervaring in operationele technologie (OT). Hij is gepassioneerd, betrokken en communicatief vaardig. In zijn carrière heeft hij verschillende functies gehad, van operationeel tot C-level, in vitale sectoren zoals olie & gas, defensie, drinkwater- en waterbehandeling, procesindustrie en voedingsmiddelenindustrie. Met zijn ervaring brengt Marcel creativiteit, structuur en innovatie om organisaties beter bestand te maken tegen digitale incidenten. Hij is o.a. bestuursvoorzitter van ISA (Netherlands Section), lid adviesraad CyberSec Netherlands, vice-voorzitter/woordvoerder van het Industrial Platform Cyber Security (IPCS), mentor/coach bij start- en scaleUp's, Tech Investor en als onafhankelijk adviseur bij verschillende (internationale) organisaties in zowel de private als de publieke sector.



Bio Johan Assies

Johan Assies is sinds 1997 actief in de IT- en OT-sector. Meer dan 23 jaar werkte hij bij een productiebedrijf, waar hij uiteindelijk de verantwoordelijkheid droeg voor zowel de IT- als de OT-omgeving. In deze rol kreeg OT-security een steeds grotere betekenis. Sinds 2021 is Johan werkzaam als OT Security Consultant bij Routz, waar hij dagelijks diverse klanten ondersteunt bij uiteenlopende OT-securityvraagstukken. Zijn klantenkring omvat zowel de vitale sector als de industrie. Daarnaast is hij expert op de IEC 62443-norm, een internationale standaard voor OT-security. In 2015 sloot Johan zich aan bij het kort daarvoor opgerichte IPCS. Sinds 2018 is hij voorzitter van dit platform.





De noodzaak van OT Cybersecurity

- Operationele Technologie (OT): De ruggengraat van vitale infrastructuren en industriële processen.
- Toenemende digitalisering en convergentie van IT en OT vergroten het aanvalsoppervlak.
- De impact van cyberaanvallen op OT kan catastrofaal zijn (veiligheid, milieu, economie).
- Een proactieve en gecoördineerde aanpak is essentieel.



IEC 62443

De Internationale Standaard voor OT Cybersecurity

“Cyber Security for Industrial Automation & Control Systems (IACS)”

Stond aan de basis van de oprichting van Industrial Platform
Cyber Security



IEC 62443: De ontwikkeling

- Eind jaren '90 / Begin 2000: Erkennen van de groeiende cybersecurityrisico's in industriële omgevingen.
- 2002: ISA (International Society of Automation): Speelde een cruciale initiële rol met de ISA-99 standaard.
- 2010: IEC (International Electrotechnical Commission): Nam de ontwikkeling over om een wereldwijde standaard te creëren.





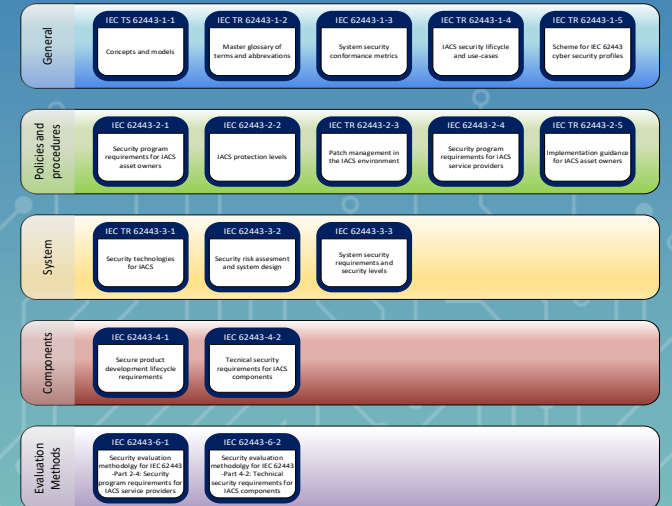
IEC 62443: Huidige betrokken Organisaties

- **IEC TC65/SC65E:** De technische commissie binnen IEC verantwoordelijk voor de IEC 62443-serie.
- **ISA Security Compliance Institute (ISCI):** Ondersteunt de adoptie en certificering van de standaard.
- **Nationale Standaardisatie Organisaties:** (NEN in Nederland) dragen bij aan de implementatie en interpretatie.
- **Industriële Consortia en Werkgroepen:** Diverse sectoren en organisaties leveren expertise en use-cases.



IEC 62443: De Internationale Standaard voor IACS

- Een reeks open standaarden, technische rapporten en werkproducten.
- Adresseert cybersecurity voor “Industrial Automatisering & Control Systems”(IACS).
- Een holistische benadering die de gehele levenscyclus van OT-systemen omvat.
- Biedt een framework voor risicomangement, beveiligingsniveaus en implementatieguidelines.
- Geschikt voor fabrikanten, systeemintegrators en asset owners.





IEC 62443: De Kracht van de Standaard

- **Gemeenschappelijke Taal:** Biedt een uniform framework en terminologie voor OT cybersecurity.
- **Risicogebaseerde Aanpak:** Stelt organisaties in staat beveiligingsmaatregelen te prioriteren op basis van risico.
- **Verbeterde Veiligheid:** Helpt bij het implementeren van effectieve technische en organisatorische maatregelen.
- **Verhoogd Vertrouwen:** Faciliteert vertrouwen tussen leveranciers, integrators en eindgebruikers.
- **Compliance en Regulering:** Ondersteunt de naleving van (toekomstige) wet- en regelgeving.
- **Levenscyclusbenadering:** Integreert beveiliging in elke fase van het OT-systeem.





Oprichting IPCS

- De complexiteit van OT-omgevingen vereist een gezamenlijke inspanning.
 - De publieke sector: Vitale infrastructuur
 - Drinkwater, Energievoorziening, Waterschappen
 - De private sector beschikt over specifieke expertise en operationele inzichten.
 - Fabrikanten, Systeemintegrators, Asset owners.
- Samenwerking versnelt de ontwikkeling en implementatie van effectieve beveiligingsoplossingen.
- 2014: Oprichting IPCS (Industrieel Platform Cyber Security) door NEN





PPS: Industrial Platform Cyber Security

- Initiatief van de NEN in 2014
- Sinds 2024 wordt het secretariaat gevoerd door Security Delta (HSD): Het nationale veiligheidscluster van Nederland.
- Doel: Het versterken van de cybersecurity van de Nederlandse industriële sector.
- Betrokken Partijen: Overheid (nationaal en regionaal), kennisinstellingen, consultancybedrijven, technologieleveranciers, industriële eindgebruikers.
- Focus: Kennisdeling, bewustwording, ontwikkeling van expertise, informatievoorziening en innovatie.
- Voorbeelden van activiteiten: Werkgroepen, themabijeenkomsten, sitevisits, delen van best practices, etc.
- Borgen van kwaliteit door strenge toelatingseisen
- Sinds 2025 onderdeel van de IACS Coalitie



IACS Coalition



De meerwaarde van IPCS

- **Versnelde Adoptie van Best Practices:** Door gezamenlijke ontwikkeling en deling van kennis.
- **Verhoogd Bewustzijn:** Publicaties en evenementen richten zich op het vergroten van de cybersecurity awareness binnen de OT-sector.
- **Gedeelde Expertise en Talentontwikkeling:** Samenwerking met bijvoorbeeld organisaties als CVNL, HSD, Onderwijsinstellingen leidt tot beter gekwalificeerd personeel.
- **Sterkere Collectieve Weerbaarheid:** Een gecoördineerde aanpak maakt de Nederlandse industrie als geheel beter bestand tegen cyberaanvallen.



Kenmerken IPCS



- Eén OT-expertgroep met groeiend aantal leden uit publieke en private sector
- Platform OT Subject Matter Experts (SME's)
- Sparringspartner voor overheid en bedrijfsleven over IACS/OT cybersecurity (o.a. IACS Coalitie)
- Actieve deelname leden aan werkgroepen
- Kwaliteitsborging door strenge selectie bij beoogd lidmaatschap
- Toezien op naleving van gedragsregels
- Praktijk: Minimaal twee sitevisits per jaar



Site Visits





2015-11 RWS – Oosterscheldekering





2018-3 Gasunie



gasunie



2020-4 en 11 Online wegens Covid-19





2022-04 Elaad





2023-04 Royal Swinkels





2024-05 Security Delta





2024-11 Thales



THALES

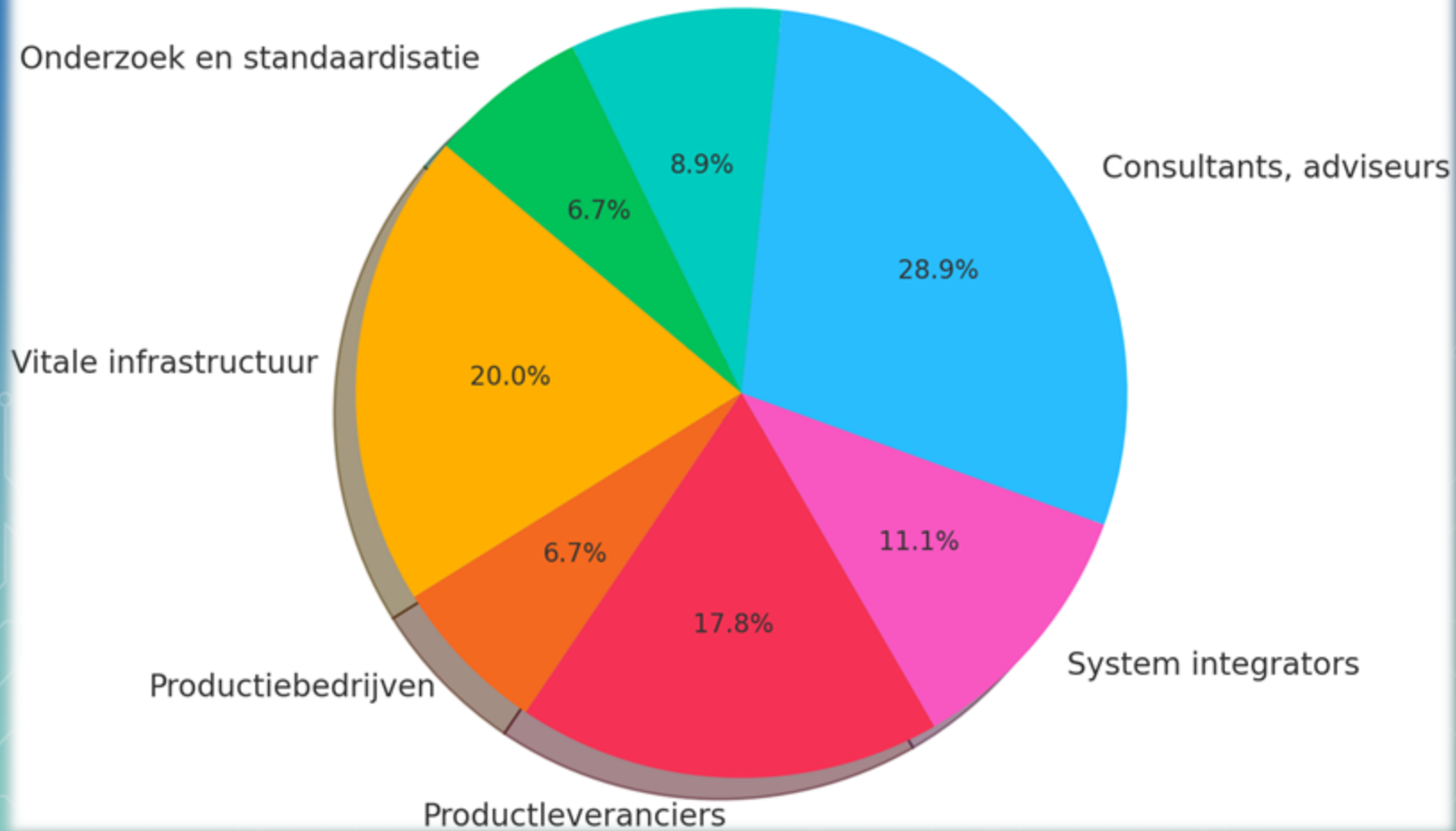


Leden

- Actieve community met > 45 OT-security experts vanuit verschillende publieke en private sectoren:
 - 9 x Vitale infrastructuur
 - 3 x Productiebedrijven
 - 8 x Productleveranciers
 - 5 x System integrators
 - 13 x Consultants, adviseurs
 - 4 x Engineering
 - 3 x Onderzoek en standaardisatie



Verdeling OT-security experts per sector



IACS & CYBERSECURITY CONFERENCE



Logos included in the grid:

- accenture
- ACTEMIUM
- avite SECURITY TOOLS
- BiFINGER
- BDO
- CCV
- croonwolver&dros | TBI
- duurzaam energie perspectief
- EKB
- ENEXIS NETBEHEER
- enode INDUSTRIAL NETWORKS
- Compumatica SECURE NETWORKS
- gasunie crossing borders in energy
- Elaadnl
- Hoogheemraadschap van Rijnland
- EQUANS EMPOWERING TRANSITIONS
- kader
- HIMS
- HIGHBERG
- TICT GROUP
- ROUTZ
- KH Engineering
- RambiCo
- PWN
- Rijkswaterstaat Ministerie van Infrastructuur en Waterstaat
- Royal HaskoningDHV
- PHILIPS Innovation Services
- SECNET
- TNO
- TUVNORD
- Royal Swinkels family brewers
- PHOENIX CONTACT
- THALES Building a future we can all trust
- TATA CONSULTANCY SERVICES tcs
- Vialis
- WELP
- uni per
- YOKOGAWA Co-innovating tomorrow



Werkgroepen





Werkgroepen

- Verschillende werkgroepen waarin whitepapers worden uitgewerkt en gepubliceerd:
 - Scantools en CMDB
 - Guidelines voor het vaststellen van een Target Security Level voor een eindgebruiker
 - Werkbaar maken van een High Level Risico Inventarisatie
 - IIoT IEC 62443-1-6 / Toepassen van IIoT binnen OT / OT afhankelijk van cloud
 - OT in de cloud
 - NIS2



Publicaties van het IPCS

- Publicaties met als doel om kennis over IACS/OT-security binnen Nederland te verspreiden.
- Publicaties zijn geschreven door leden van het IPCS.
- Doelgroep zijn zowel eindgebruikers als productleveranciers. Iedereen met interesse in IACS/OT-security.



Publicaties van het IPCS: Enkele voorbeelden

- **Elevator pitch “board level” – Beveiliging van industriële automatisering voor het topmanagement**
 - *In deze one pager staat beschreven hoe OT-security onder de aandacht te brengen van het management van het bedrijf. Hierbij gebruik makend van de IEC 62443-normenreeks.*
- **Elevator pitch “leveranciers” - Beveiliging van industriële automatisering**
 - *In twee pagina's staat beschreven waarom het belangrijk is dat leveranciers cyberveilige producten en diensten leveren. Hierbij gebruik makend van de IEC 62443-normenreeks.*



Publicaties van het IPCS: Enkele voorbeelden

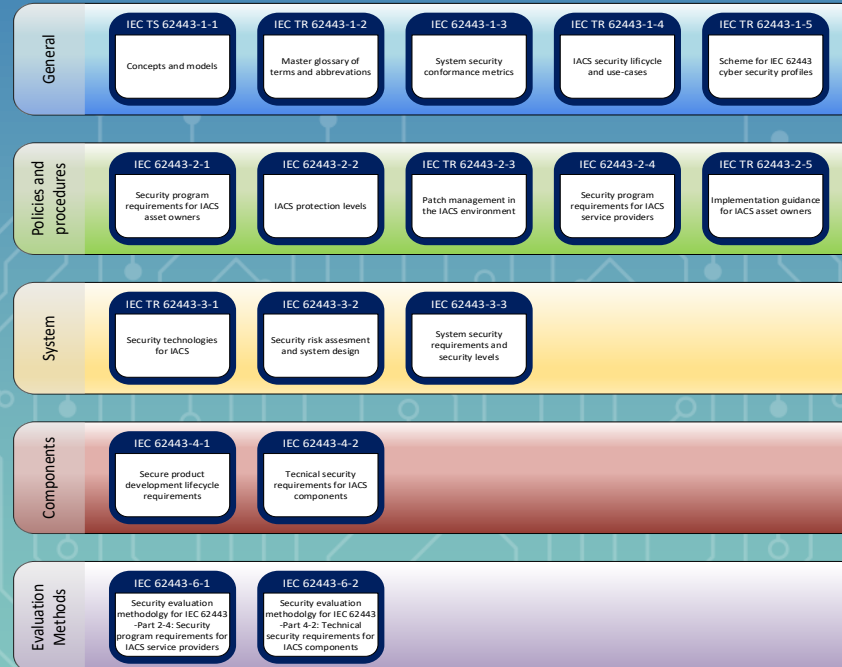
- **Korte beschrijving van de IEC 62443**
 - *Dit document geeft inzicht in de inhoud en structuur van de IEC 62443 en kan helpen bij het selecteren van de juiste normdelen.*
- **Starten met de IEC 62443**
 - *In dit document staat beschreven hoe de IEC 62443 kan helpen om te beginnen met het beveiligen van de OT-omgeving binnen de organisatie.*
- **Waarom certificeren op de IEC 62443**
 - *Dit document beschrijft de eventuele noodzaak, de meerwaarde en de rol van certificering op de IEC 62443 voor de organisatie.*

Publicaties van het IPCS: Enkele voorbeelden

- **Incident response en recovery**
 - *Dit document is bedoeld om bedrijven te helpen zich voor te bereiden op cybersecurity incidenten.*
- **Handleiding Security Level Target**
 - *Een praktische handleiding om het Security Level Target te bepalen.*
- **Cybergevoeligheid van tijd**
 - *Dit document beschrijft het belang van het aspect 'tijd' in OT-omgevingen.*



IEC 62443





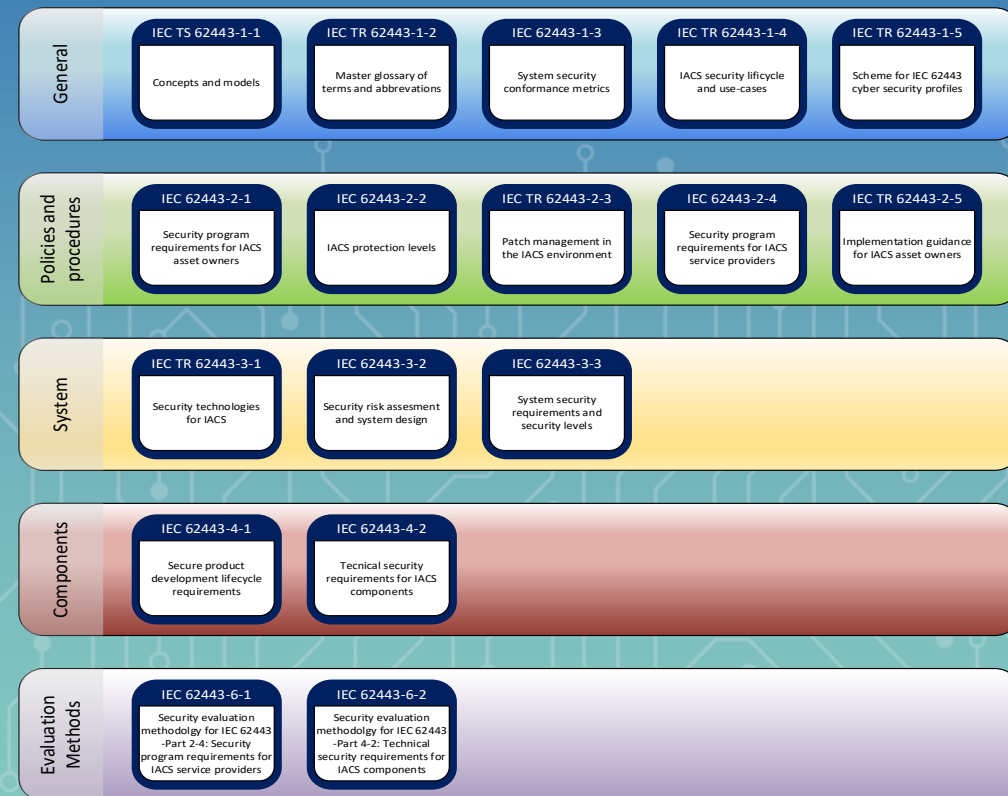
IEC 62443 als Fundament voor Publiek-Private OT Cybersecurity

- IEC 62443 biedt een gemeenschappelijk referentiekader voor samenwerking.
- Publiek-private initiatieven zoals IPCS kunnen de adoptie en implementatie van IEC 62443 faciliteren.
- Gezamenlijke interpretatie en toepassing van de standaard door verschillende stakeholders verhoogt de effectiviteit.
- Samenwerking kan leiden tot sectorspecifieke implementatieguidelines op basis van IEC 62443.

Wat is de IEC 62443

De IEC 62443 bestaat uit meerdere delen, verdeeld over de volgende categorieën:

- 1. General
- 2. Policies & Procedures
- 3. System
- 4. Component
- 5. Profiles (toekomstig)
- 6. Evaluation methods





Waarvoor wordt de IEC 62443 gebruikt?

- Waarborgen van de cybersecurity van industriële automatiserings- en controlesystemen (IACS).
- De IEC 62443 biedt richtlijnen en best practices voor het beveiligen van industriële netwerken en systemen tegen cyberaanvallen en andere beveiligingsrisico's.



Specifieke toepassingen van de IEC 62443

- Beveiliging van industriële netwerken
- Risicoanalyse en –beheer
- Ontwikkeling van veilige producten
- Implementatie van beveiligingsmaatregelen
- Bewustwording en training

De IEC 62443 is essentieel voor bedrijven in sectoren zoals energie, waterbeheer, transport, en productie, waar de beveiliging van operationele technologie van cruciaal belang is.



Voor wie is de IEC 62443?

- Eindgebruikers van IACS systemen
- System Integrators
- Productleveranciers

Publicatiedatums per deel 1/2

Deel	Laatste publicatie	Geplande publicatie / start herziening in
IEC 62443-1-1	2009-8	2024
IEC 62443-1-2	Nog niet gepubliceerd	Onbekend
IEC 62443-1-3	Niet gepubliceerd	Niet (werk aan de huidige draft is gestopt)
IEC 62443-1-4	Nog niet gepubliceerd	Onbekend (draft is nog niet beschikbaar)
IEC 62443-1-5	1.0 2023-09	Onbekend
IEC 62443-2-1	2.0 2024-08	Onbekend
IEC 62443-2-2	2025-03	Onbekend
IEC 62443-2-3	2015-07	2025
IEC 62443-2-4	2017-08	2023
IEC 62443-2-5	Nog niet gepubliceerd	Onbekend



Publicatiedatums per deel 2/2

Deel	Laatste publicatie	Geplande publicatie / start herziening in
IEC 62443-3-1	2009-08	2025
IEC 62443-3-2	2020-06	2025
IEC 62443-3-3	2013-08	2025
IEC 62443-4-1	2018-02	2025
IEC 62443-4-2	2019-03	2025
IEC 62443-6-1	2024-03	Onbekend
IEC 62443-6-2	2025-01	Onbekend



1. General

Deel	Omschrijving
IEC 62443-1-1	Dit normdeel introduceert de concepten en modellen zoals deze in de gehele norm worden gebruikt. Het scheidt daarmee een gemeenschappelijke basis.
IEC 62443-1-2	Dit normdeel vormt het centrale overzicht van begrippen en afkortingen zoals deze in de gehele norm worden gebruikt. Het scheidt daarmee een gemeenschappelijke basis.
IEC 62443-1-3	Oorspronkelijke doelstelling voor dit normdeel was “[to specify] the requirements to be addressed by a comprehensive set of metrics for the ISA-62443 series”. Het werk aan de huidige draft is gestopt; de inhoud wordt opgenomen in delen 2-1, 2-4 en 3-3.
IEC 62443-1-4	Oorspronkelijke doelstelling voor dit technical report is het geven van een gedetailleerde beschrijving van de onderliggende cyber security lifecycle voor IACS, alsook enkele use cases voor verschillende toepassingen. Een draft is op dit moment nog niet beschikbaar.
IEC 62443-1-5	Deze technische specificatie beschrijft de vereisten voor het definiëren van beveiligingsprofielen. Toepassingsgebieden kunnen zijn b.v. specifieke producten, operationele omgeving, of het toepassingsdomein.

2. Policies & Procedures

Deel	Omschrijving
IEC 62443-2-1	Dit normdeel beschrijft de vereisten voor een IACS security management system, ofwel een Information Management System (ISMS). Het gaat vooral in op dat zaken belegd moeten zijn. CISO's of COSO's bij end-users kunnen dit deel gebruiken voor het implementeren van een CSMS binnen hun organisatie.
IEC 62443-2-2	Dit normdeel beschrijft de effectiviteit van een security program middels een Security Program Rating. Hierbij worden security levels gekoppeld aan maturity levels.
IEC 62443-2-3	Dit technical report beschrijft best practices en geeft handvatten voor het opzetten van een patch management programma binnen IACS.
IEC 62443-2-4	Dit normdeel helpt end-users om de juiste security vereisten te stellen aan hun System Integrator. Het helpt System Integrators om de cybersecurityvereisten van hun klanten te begrijpen. Het normdeel biedt beiden partijen een gemeenschappelijk platform om vereisten op gebied van cybersecurity en verwachtingen ten aanzien van de System Integrator te bespreken.
IEC 62443-2-5	Doelstelling van dit technical report is het geven van handvatten voor implementatie van een securityprogramma of CSMS. Dit rapport bestaat alleen nog in conceptfase.



3. System

Deel	Omschrijving
IEC 62443-3-1	Dit technical report beschrijft en evalueert een aantal security technologieën voor IACS. Het geeft handvatten hoe deze technologieën toe te passen.
IEC 62443-3-2	Dit normdeel helpt end-users en system integrators bij het opstellen van een risico gedreven Zone & Conduit model, en het vastleggen van securitylevels voor het (design van de) proces control omgeving.
IEC 62443-3-3	Dit normdeel helpt end-users en system integrators bij het selecteren en implementeren van de juiste technische maatregelen volgens de gewenste security levels. Het helpt end-users daarnaast ook om te bepalen wat het securitylevel is van een bestaande infrastructuur.



4. Component

Deel	Omschrijving
IEC 62443-4-1	Dit normdeel beschrijft de cyber security vereisten voor de product development lifecycle voor IACS producten. Het normdeel geeft handvatten hoe aan de vereisten te voldoen.
IEC 62443-4-2	Dit normdeel helpt gebruikers en system integrators bij het stellen van security requirements aan componenten van leveranciers. Het helpt leveranciers om aan te geven wat de security capabilities zijn van hun componenten. Daarnaast helpt het om te bepalen wat de security capabilities zijn van een component. Wat de 3-3 doet op systeemniveau, doet de 4-2 op componentniveau.



6. Security Evaluatiemethoden

Deel	Omschrijving
IEC 62443-6-1	Deze technische specificatie beschrijft hoe evaluaties van beveiligingsprogramma's ten opzichte van de IEC 621443-2-4 op reproduceerbare wijze kunnen worden uitgevoerd. Daarbij wordt voor elke vereiste uit de IEC 62443-2-4 de acceptabele criteria en bewijslast voor evaluatie vastgelegd.
IEC 62443-6-2	Deze technische specificatie beschrijft hoe evaluaties van beveiligingsprogramma's ten opzichte van de IEC 621443-4-2 op reproduceerbare wijze kunnen worden uitgevoerd. Daarbij wordt voor elke vereiste uit de IEC 62443-4-2 het acceptabele evaluatieproces en bewijslast voor evaluatie vastgelegd.



Afronding

Trends in de sector

- Nieuwe wet- en regelgeving (NIS2, Cbw, CRA, RED)
- OT in de cloud
- Meer behoefte aan data en sturing vanuit management
- Assetmanagement wordt steeds belangrijker
- Live Digital Twins
- Post-Quantum Computing / Post-quantum cryptografie
- Geopolitieke omstandigheden vereisen grotere slagkracht
- Artificial Intelligence in relatie tot OT Cybersecurity
- MEGA





Conclusie: Samenwerken = Veiligere OT-Toekomst



- OT cybersecurity is van cruciaal belang in een steeds meer gedigitaliseerde wereld.
- IEC 62443 biedt een essentieel framework voor het beveiligen van industriële systemen.
- Publiek-private samenwerking is onmisbaar om de complexe uitdagingen in OT cybersecurity aan te pakken.
- Initiatieven zoals IPCS en IACS Coalitie tonen de concrete voordelen van deze samenwerking.
- Een gezamenlijke en gestandaardiseerde aanpak is de sleutel tot een duurzaam en veerkrachtig OT-ecosysteem.

Take-away

Bouw mee aan een veerkrachtig netwerk.

Samen staan we sterker!



Wij nodigen u uit om naar de Main Stage te gaan voor de plenaire afsluiting