Securing Operational Technology (OT): New Kid on the Block or Familiar Risk?

A Wake Up Call for One of the Biggest Threats for Our Future

Webinar Brains4Buildings, 6 April 2023

SIEMENS

Important societal processes come to a standstill if the associated ICT systems and analog alternatives are not available.

SIEMENS

Almost all vital processes and services are completely dependent on ICT. Due to the almost complete disappearance of analog alternatives ..... socially disruptive damage.

SIEMENS

Digital disruptions affect critical processes in society. This means that they jeopardize essential services such as healthcare, payment traffic, government services and the electricity supply.

WRR, Voorbereiden op digitale ontwrichting, 2019

SIEMENS

So we seem to have a challenge, what are we going to do about it?

SIEMENS

Laws make cybersecurity a compliance issue……

2016

Network and Information Systems Directive (NIS) (EU) 2016/1148.

2023 (signed 2022, active 16 January 2023)

Network and Information Systems Directive 2 (NIS2) (EU) 2022/2555.

2018

Netwerk- en Informatiebeveiliging (NIB)
Wet beveiliging netwerk- en informatiesystemen (Wbni)
9 november 2018

2024

Netwerk- en Informatiebeveiliging (NIB2?)
Wet beveiliging netwerk- en informatiesystemen (Wbni2?)
1 oktober 2024 !

SIEMENS

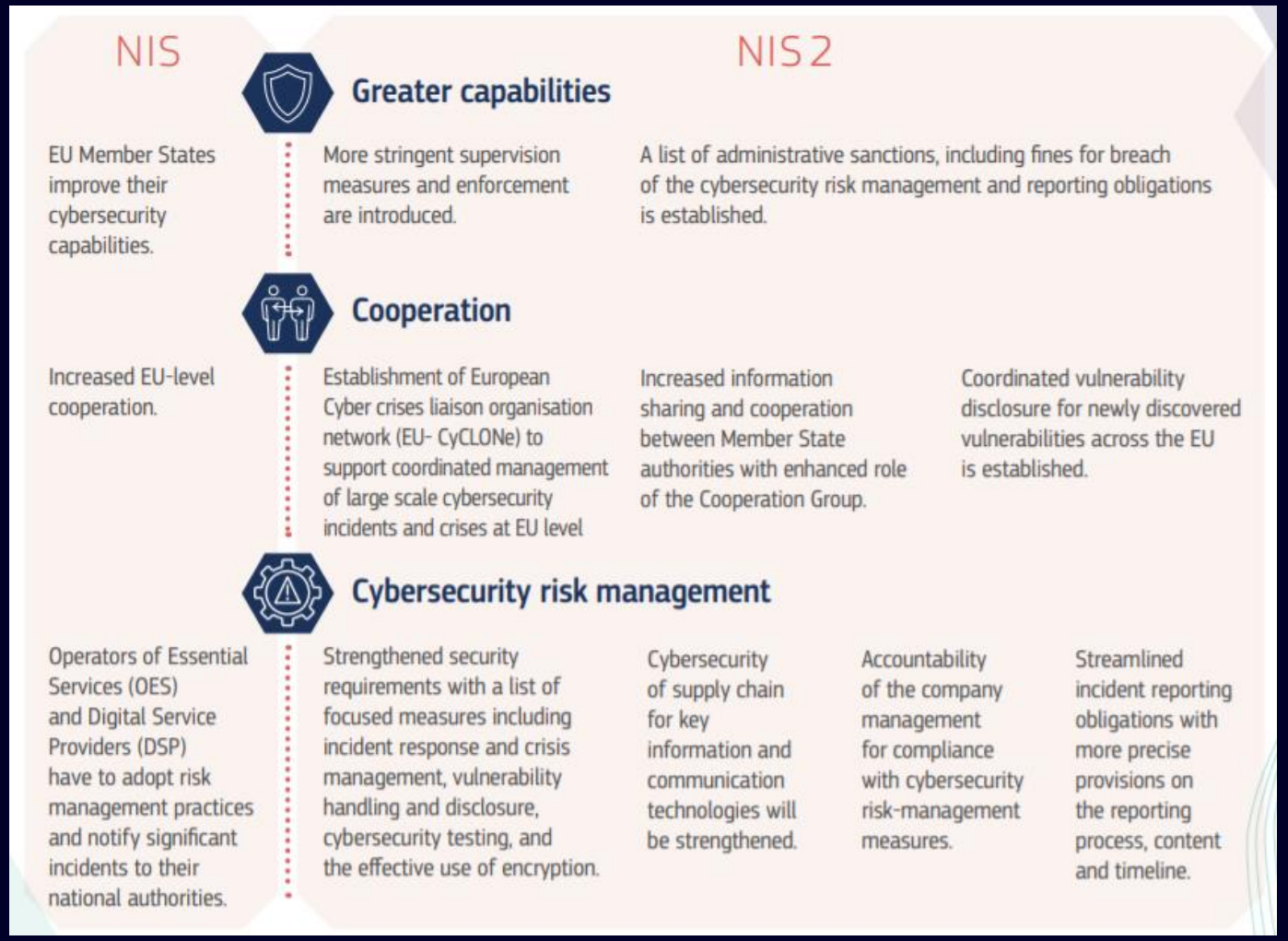
Changes in domains: expanding definition of critical infrastructure

NIS

NIS 2

SIEMENS

More requirements, more cooperation, more supervision



SIEMENS

NIS2: homework to do ?!

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Search for resources, tools, publications and more | English (en)

TOPICS | PUBLICATIONS | TOOLS | NEWS | EVENTS | ABOUT | WORK WITH ENISA | CONTACT

Details | Publications | News | Events

Supporting the implementation of Union policy and law regarding cybersecurity.

NIS Directive

On 16 January 2023, the Directive (EU) 2022/2555 (known as NIS2) entered into force replacing Directive (EU) 2016/1148. ENISA considers that NIS2 improves the existing cyber security status across EU in different ways by:

- creating the necessary cyber crisis management structure (CyCLONe)
- increasing the level of harmonization regarding security requirements and reporting obligations
- encouraging Members States to introduce new areas of interest such as supply chain, vulnerability management, core internet and cyber hygiene their national cybersecurity strategies
- bringing novel ideas such as the peer reviews for enhancing collaboration and knowledge sharing amongst the Member States
- covering a larger share of the economy and society by including more sectors which means that more entities are obliged to take measures in order to increase their level of cybersecurity.

NIS2 assigns to ENISA a number of significant new tasks such as:

- The development and maintenance of a European vulnerability registry
- The secretariat of the European Cyber Crises Liaison Organisation Network (CyCLONe)
- The publication of an annual report on the state of cybersecurity in the EU
- To support the organisation of peer reviews between member states
- The creation and maintenance of a registry for entities providing cross-border services e.g DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers and data centre service providers.

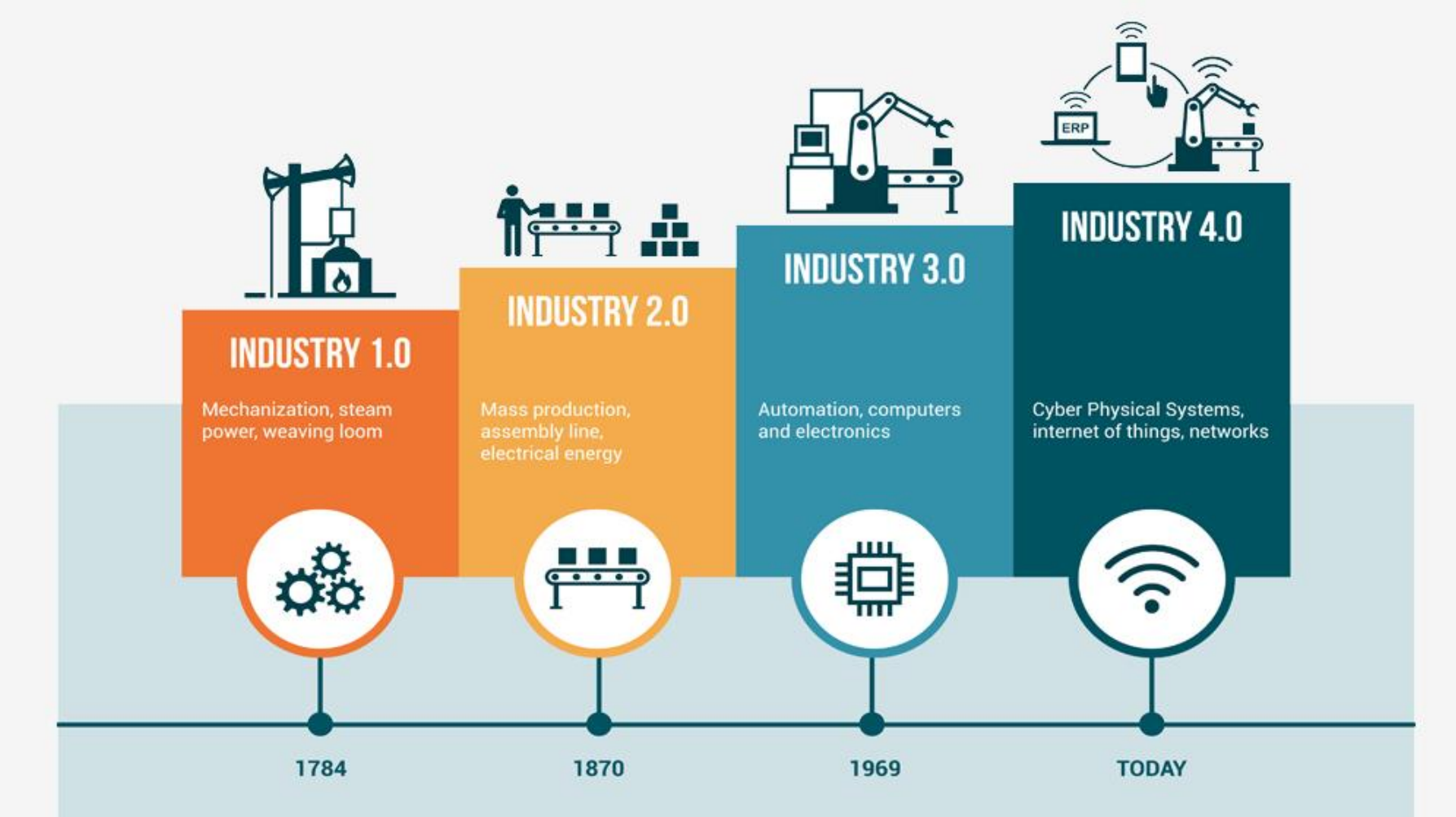
ENISA already plays a key role in the implementation of the NIS Directive by providing assistance to the Member States regarding its transposition, by supporting several working streams of the Cooperation Group with technical expertise and by providing the secretariat for the CSIRTs Network and organising the CyberEurope Exercise.

Browse the Topics

- + CSIRTs and communities
- Cyber Crisis Management
- + Cloud
- + National Cybersecurity Strategies
- + Emerging Technologies
- + Critical infrastructure
- + Incident Reporting
- + Cyber Threats
- + Standards
- + Awareness Raising
- COVID19
- Vulnerability Disclosure
- − Cybersecurity Policy
  - Policy Observatory
  - − NIS Directive
    - NIS Directive tool
  - + eIDAS
  - European Electronic communications Code
  - Data Protection
- Cryptography
- + Market
- + Research and Innovation
- + Education
- + Incident response
- Risk Management
- + Certification
- + Training and Exercises
- Foresight

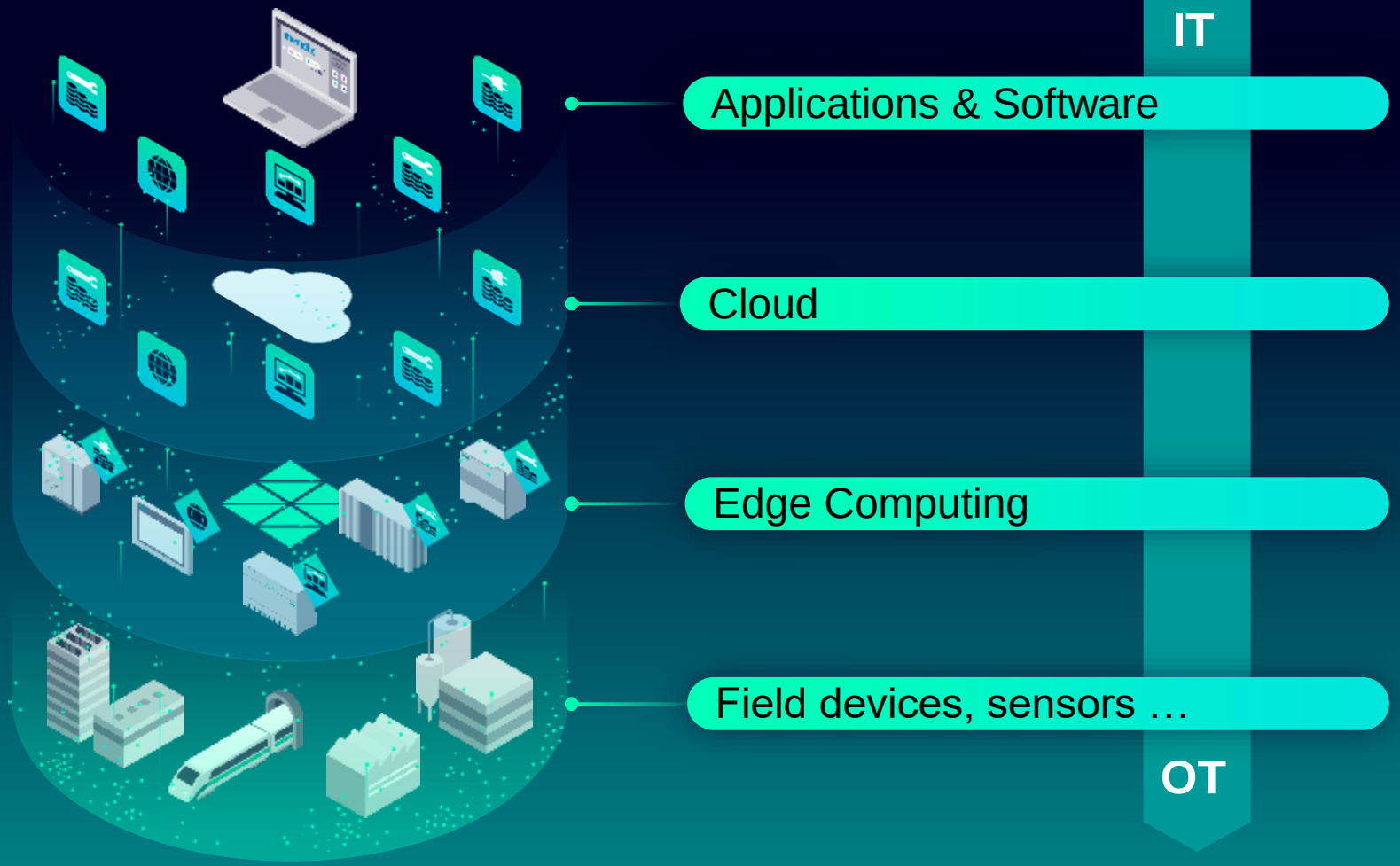
SIEMENS

Revolutions are only visible in retrospect…..



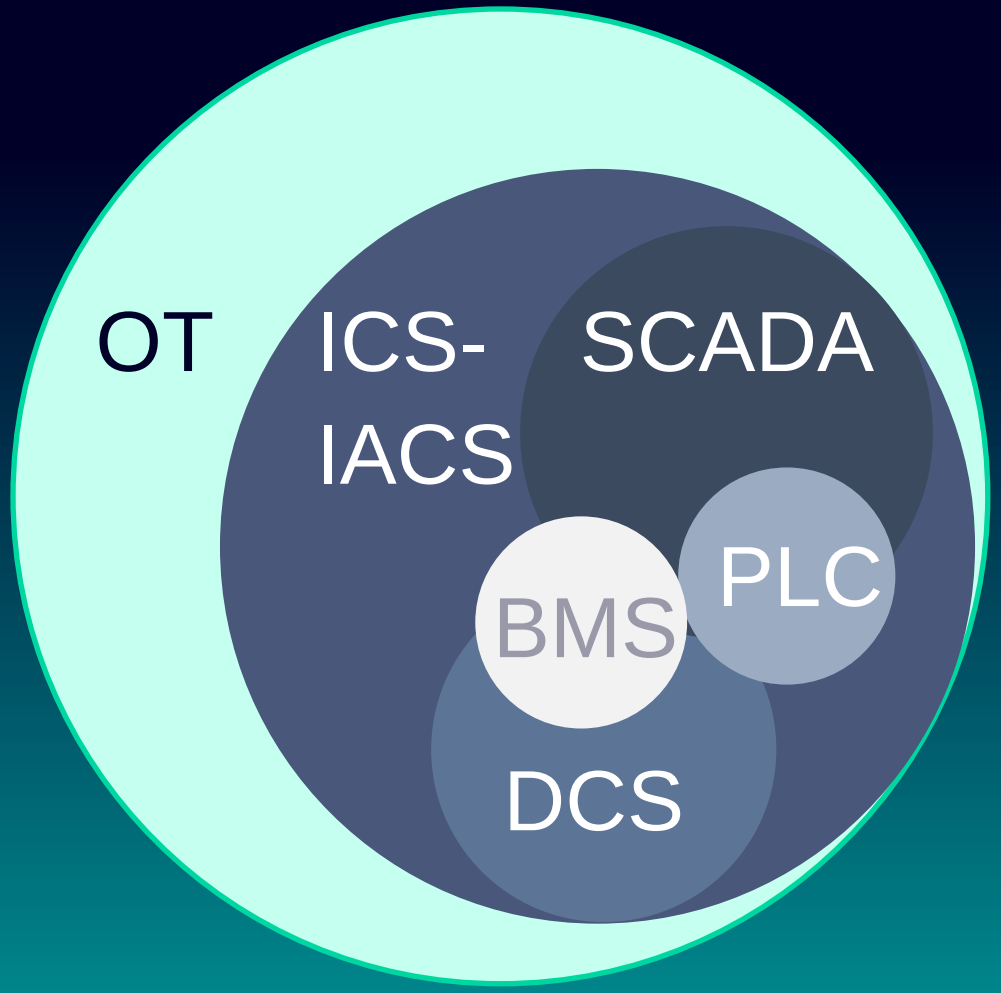
SIEMENS

The rise of Cyber - Physical systems



SIEMENS

ICS, OT, SCADA, PCS, DCS, IACS: Proces Automation



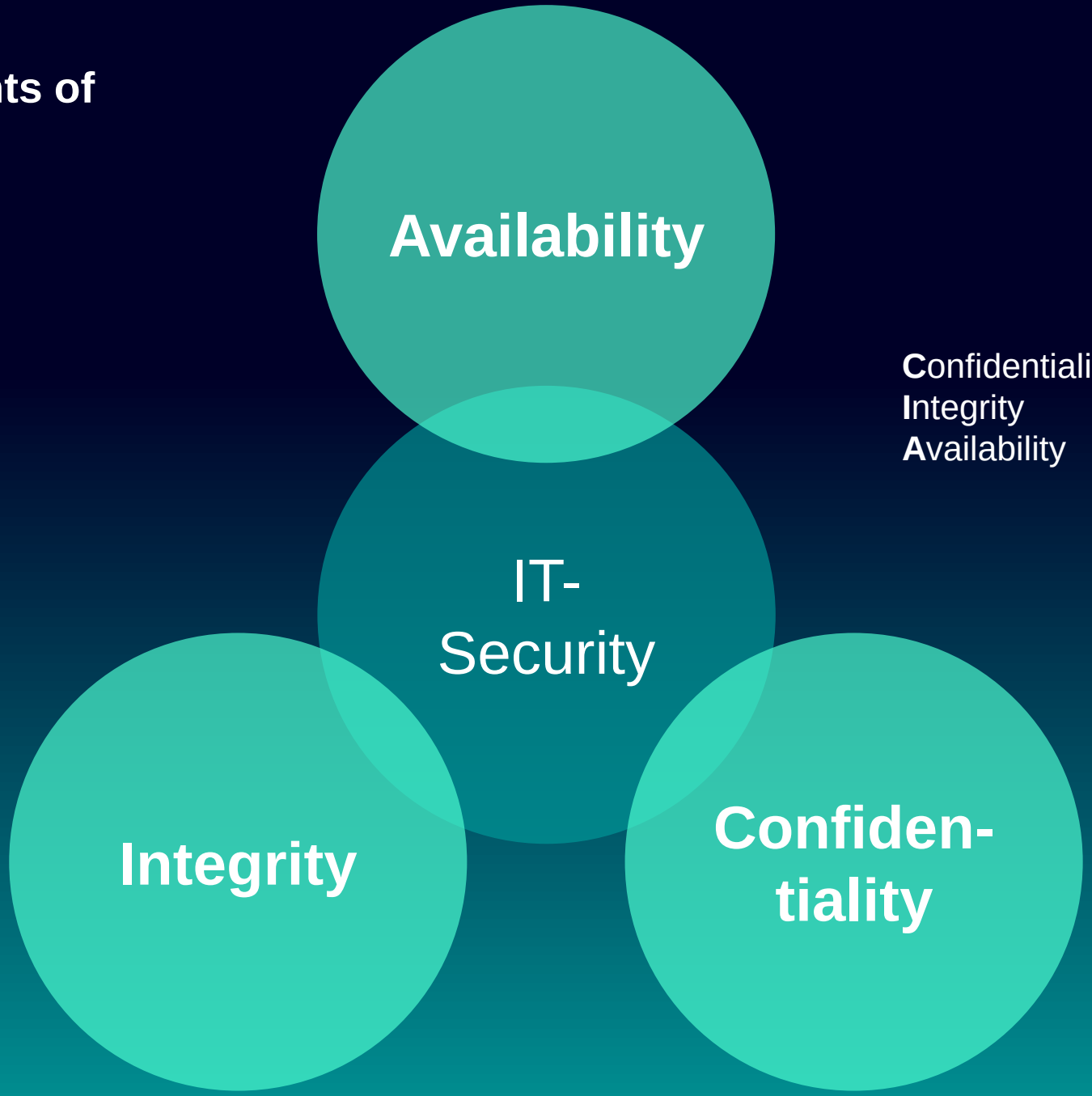
OT:	Operational Technology
ICS:	Industrial Control System
IACS:	Industrial Automation and Control System
SCADA:	Supervisory Control And Data Acquisition
DCS:	Distributed Control System
PCS:	Process Control System
PLC:	Programmable Logic Controllers
BMS:	Building Management System

SIEMENS

Cyber threats

SIEMENS

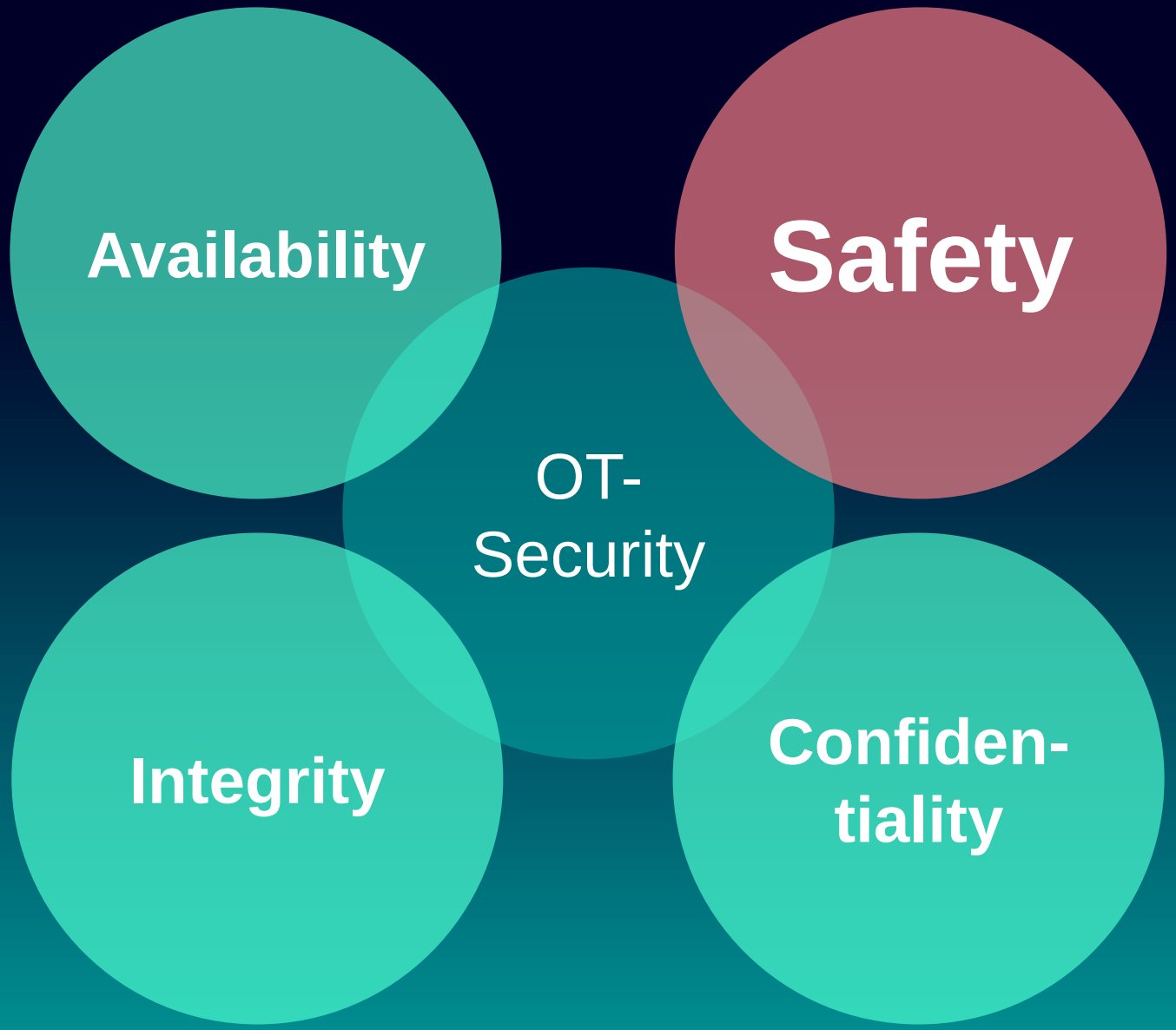
The *three* components of IT security



Confidentiality - **V**ertouwelijkheid
Integrity - **I**ntegriteit
Availability - **B**eschikbaarheid

SIEMENS

The four components of OT security



SIEMENS

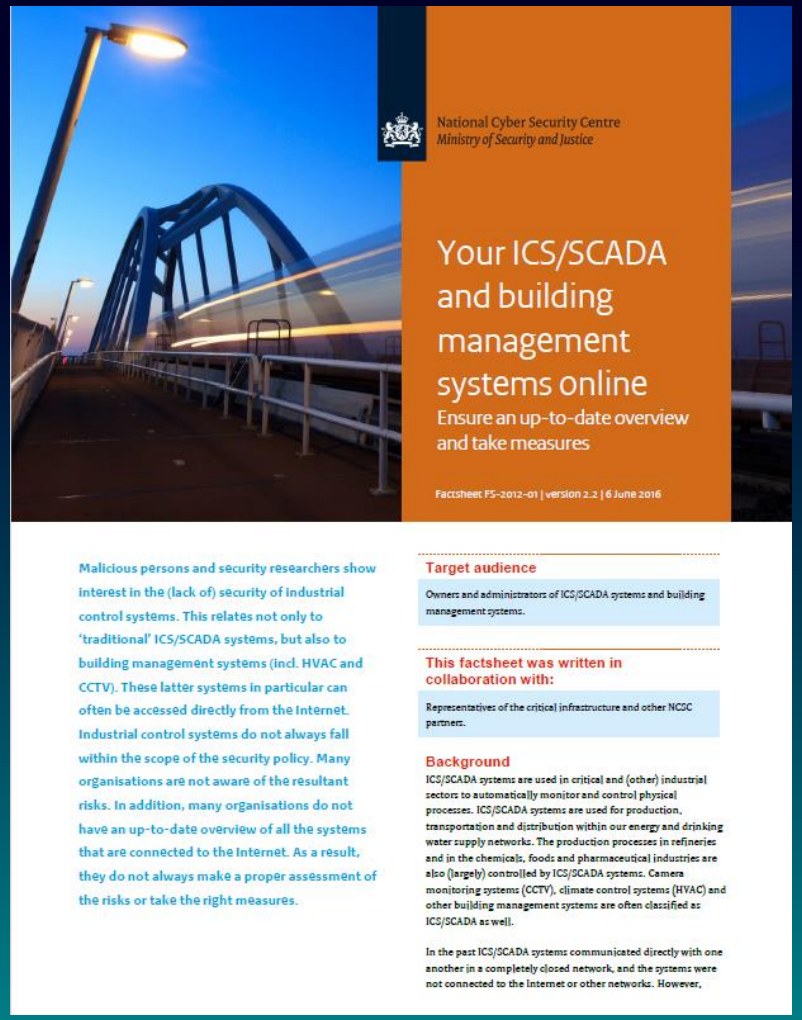
“Industrial Control Systems (ICS) and (office) IT have historically been managed by seperate organisational units.”

“ICS people do not consider their ICS to be IT.”

“ICS People lack cyber security education. The IT department, on the other hand, is unfamiliar with the peculiarities and limitations of ICS technology.”

Referentie:
TNO for GCCS 2015, Cyber Security of Industrial Control Systems, 2015

SIEMENS



National Cyber Security Centre
Ministry of Security and Justice

Your ICS/SCADA and building management systems online

Ensure an up-to-date overview and take measures

Factsheet FS-2012-01 | version 2.2 | 6 June 2016

Malicious persons and security researchers show interest in the (lack of) security of industrial control systems. This relates not only to 'traditional' ICS/SCADA systems, but also to building management systems (incl. HVAC and CCTV). These latter systems in particular can often be accessed directly from the Internet. Industrial control systems do not always fall within the scope of the security policy. Many organisations are not aware of the resultant risks. In addition, many organisations do not have an up-to-date overview of all the systems that are connected to the Internet. As a result, they do not always make a proper assessment of the risks or take the right measures.

Target audience

Owners and administrators of ICS/SCADA systems and building management systems.

This factsheet was written in collaboration with:

Representatives of the critical infrastructure and other NCSC partners.

Background

ICS/SCADA systems are used in critical and (other) industrial sectors to automatically monitor and control physical processes. ICS/SCADA systems are used for production, transportation and distribution within our energy and drinking water supply networks. The production processes in refineries and in the chemicals, foods and pharmaceutical industries are also (largely) controlled by ICS/SCADA systems. Camera monitoring systems (CCTV), climate control systems (HVAC) and other building management systems are often classified as ICS/SCADA as well.

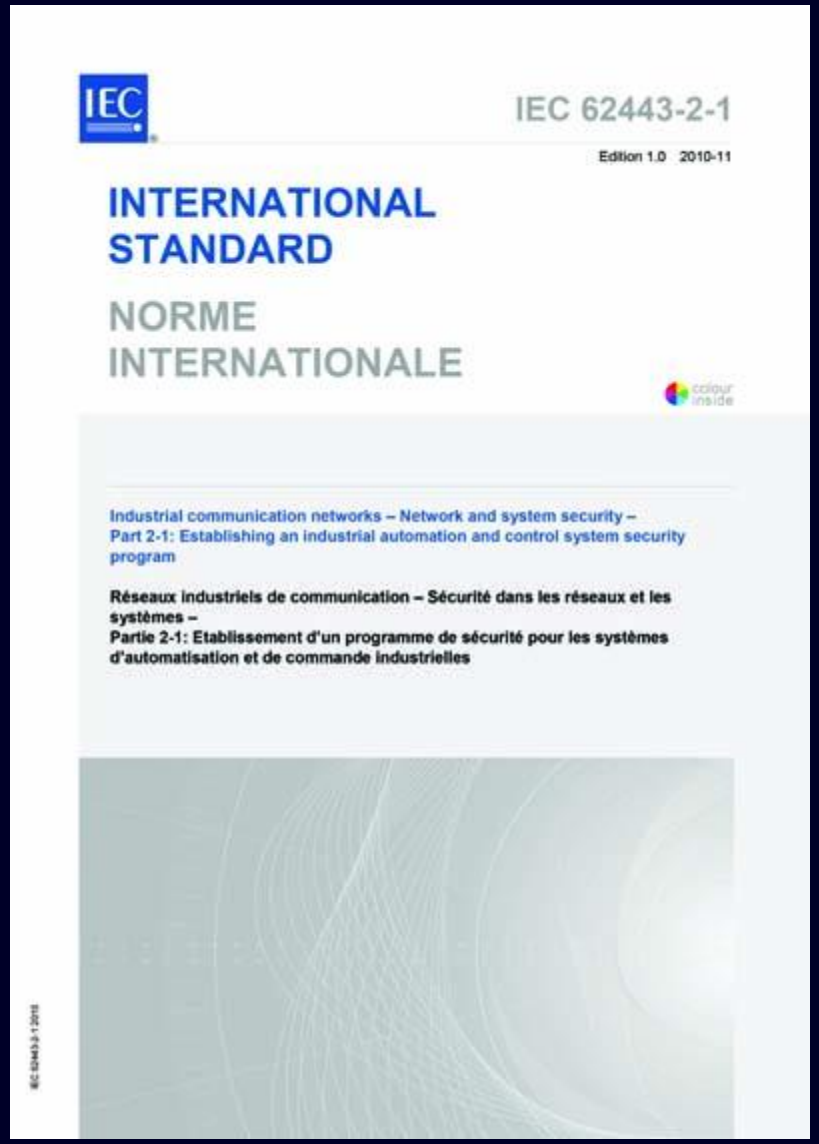
In the past ICS/SCADA systems communicated directly with one another in a completely closed network, and the systems were not connected to the Internet or other networks. However,

Malicious persons and security researchers show interest in the (lack of) security of industrial control systems. This relates not only to 'traditional' ICS/SCADA systems, but also to building management systems (incl. HVAC and CCTV). These latter systems in particular can often be accessed directly from the Internet. Industrial control systems do not always fall within the scope of the security policy. Many organisations are not aware of the resultant risks. In addition, many organisations do not have an up-to-date overview of all the systems that are connected to the Internet. As a result, they do not always make a proper assessment of the risks or take the right measures.

EMENS

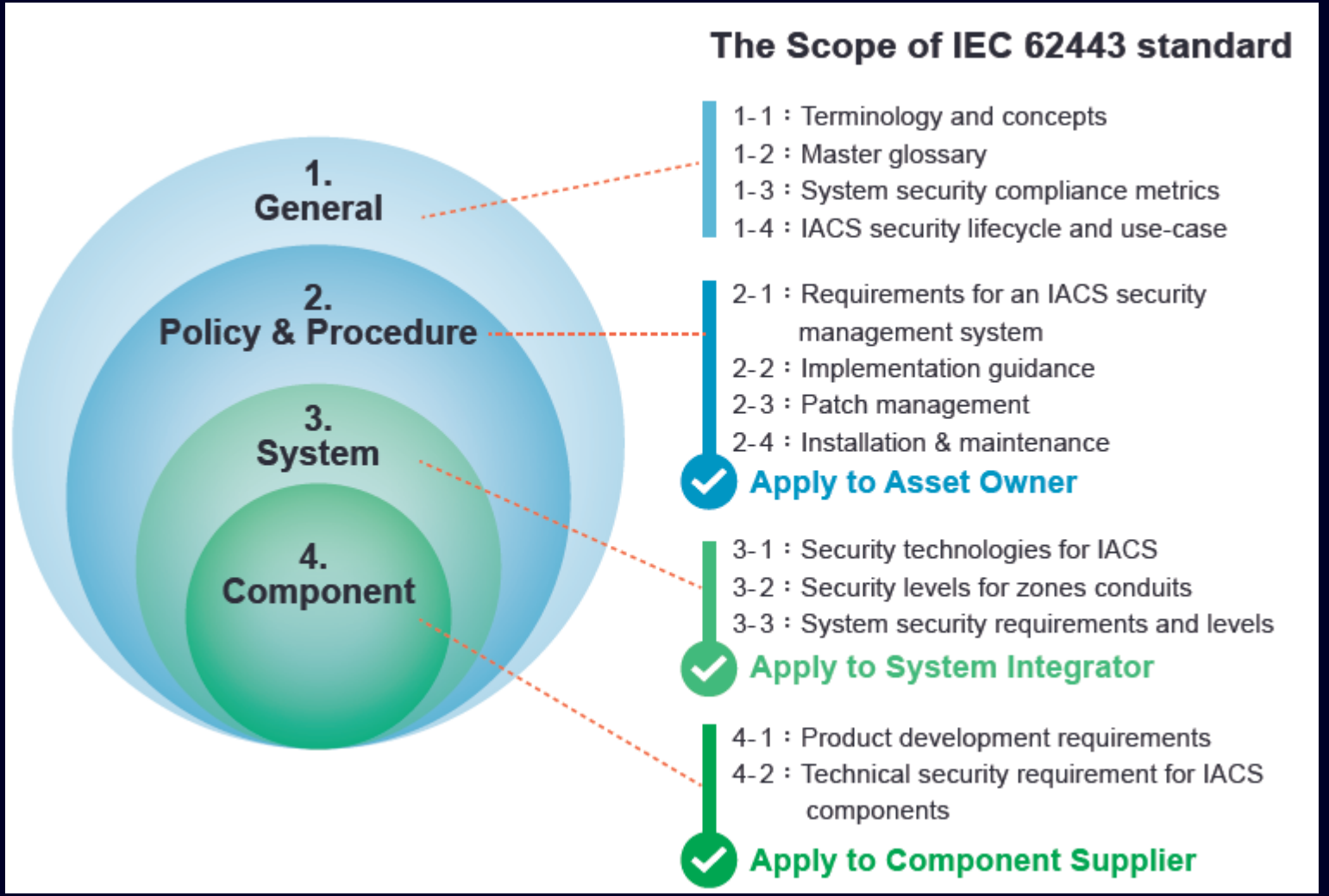
So, how do we secure OT systems?

SIEMENS


IEC 62443-2-1
Edition 1.0 2010-11
INTERNATIONAL STANDARD
NORME INTERNATIONALE
colour inside
Industrial communication networks – Network and system security –
Part 2-1: Establishing an industrial automation and control system security program
Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes –
Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles
IEC 62443-2-1:2010

SIEMENS

IEC 62443



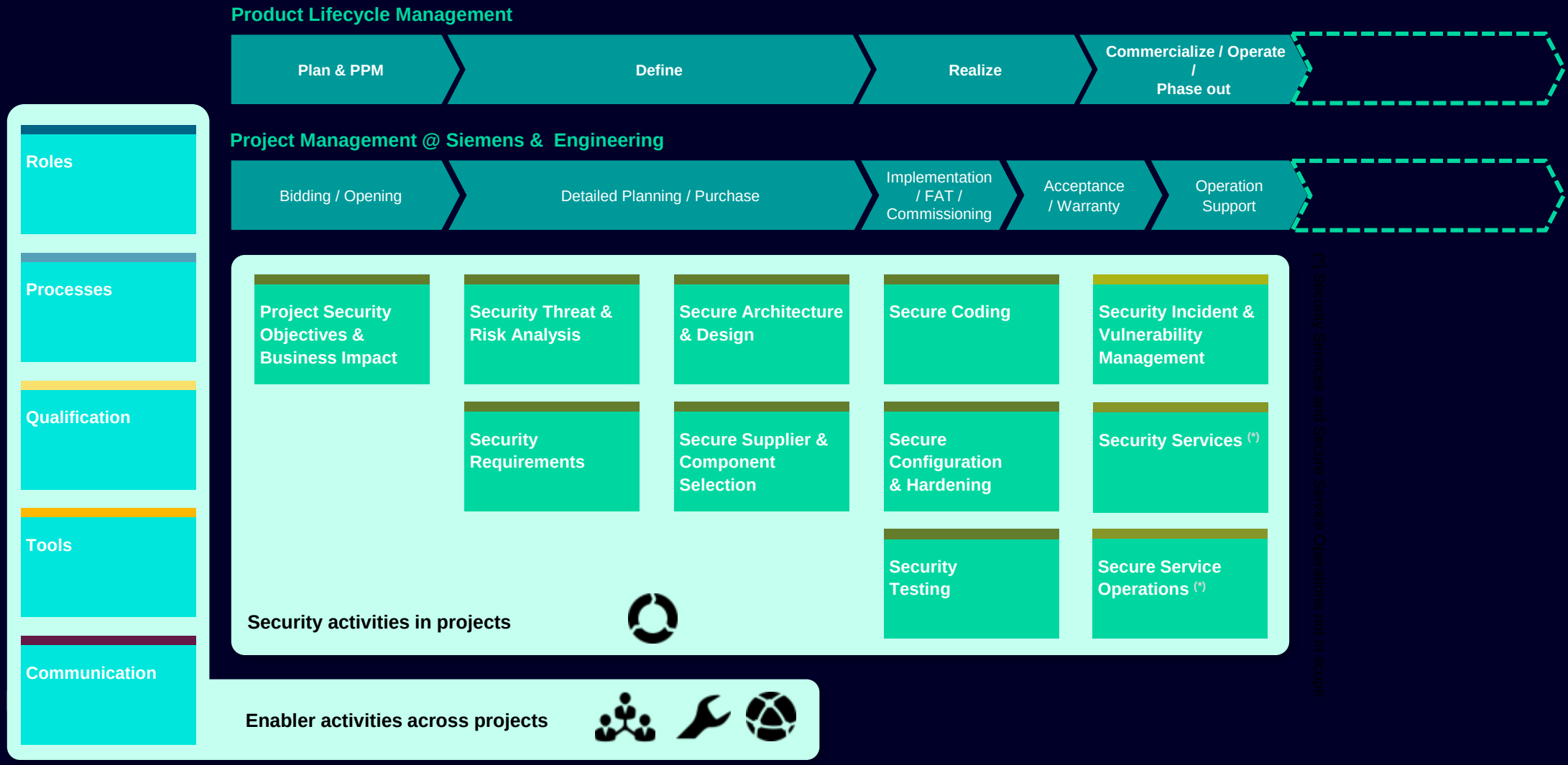
SIEMENS

IEC 62443

4 Security Level (SL)	
SL 1	Protection against **casual or coincidental** violation
SL 2	Protection against **intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation

SIEMENS

Product & Solution Security Initiative (based on IEC 62443)



SIEMENS

Cybersecurity Expert Services

End-to-end approach

Assess & Consult

Evaluation of the current security status of building system environment. Follow a clear guideline to increase your security level in OT

Services

- Health Check (engage)
- Gap Assessment
- Risk Assessment
- Penetration Testing

Outcome

Identify threats and vulnerabilities, using standard based method to give you transparency on your security level and a basis to increase your security level

Implement & Maintain

Mitigate risks through implementation and maintenance of baseline security measures

Services

- Backup services
- Patch management (SW Update/Upgrade)
- Endpoint Protection Services
- Hardening Maintenance
- Users and Account Management
- Active Directory Management
- Security Awareness Training

Outcome

Implementation and maintenance of state-of-the-art security measures closing security gaps and reduce risks

Enhance

Comprehensive long-term protection through managed services

Services

- Asset- and Vulnerability Management
- Scanning Services
- Security and log. Update and Monitoring
- Security monitoring and attack detection
- Incident Handling

Outcome

Enhance your security posture applying advanced Cybersecurity services

Our Vision:

Siemens is recognized by our customers as a leader in secure products, solutions and services

SIEMENS

Unieke publiek-private samenwerking lanceert nieuwe tool!

Cybersecurity Alliantie

VNG

NovelT

SIEMENS

Deloitte.

Programma Versterken Cyberweerbaarheid in de watersector

National Cyber Security Centre
Ministry of Security and Justice

digital trust center.

accenture

STARK NARRATIVE

ASML

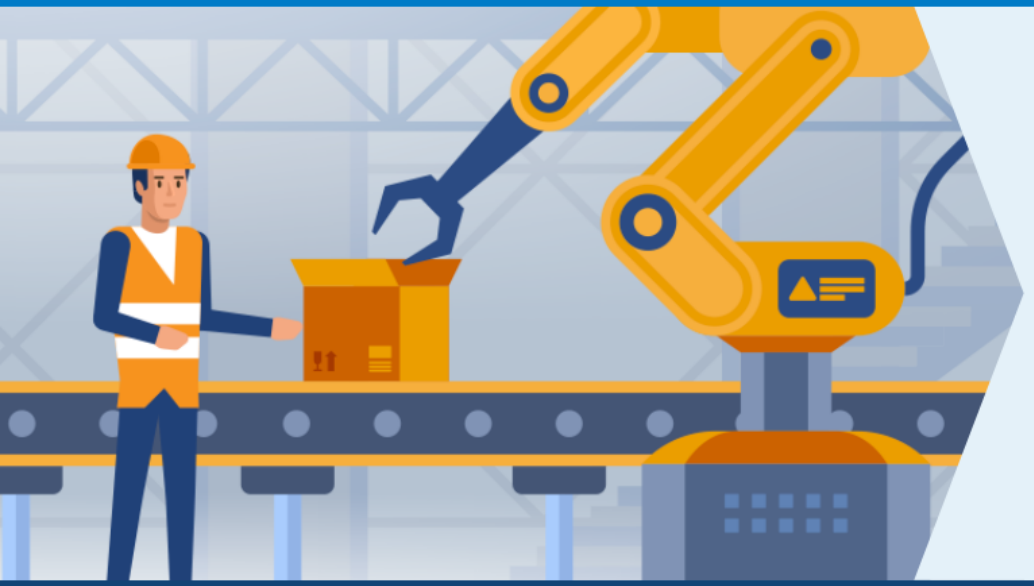
https://tools.digitaltrustcenter.nl/security-check-procesautomatisering/

digital trust center.

Ministerie van Economische Zaken en Klimaat

Home

Security Check Procesautomatisering



Hoe bescherm je de OT-omgeving van je bedrijf tegen cyberincidenten?

Met de Security Check Procesautomatisering krijg je inzicht in en advies over de beveiliging van industriële controlesystemen (ICS) in je OT-omgeving. De maatregelen die je moet treffen om beschermd te zijn, variëren per bedrijf. Doorloop daarom eerst 3 vragen om ingedeeld te worden in een categorie Hoog/Medium/Laag.

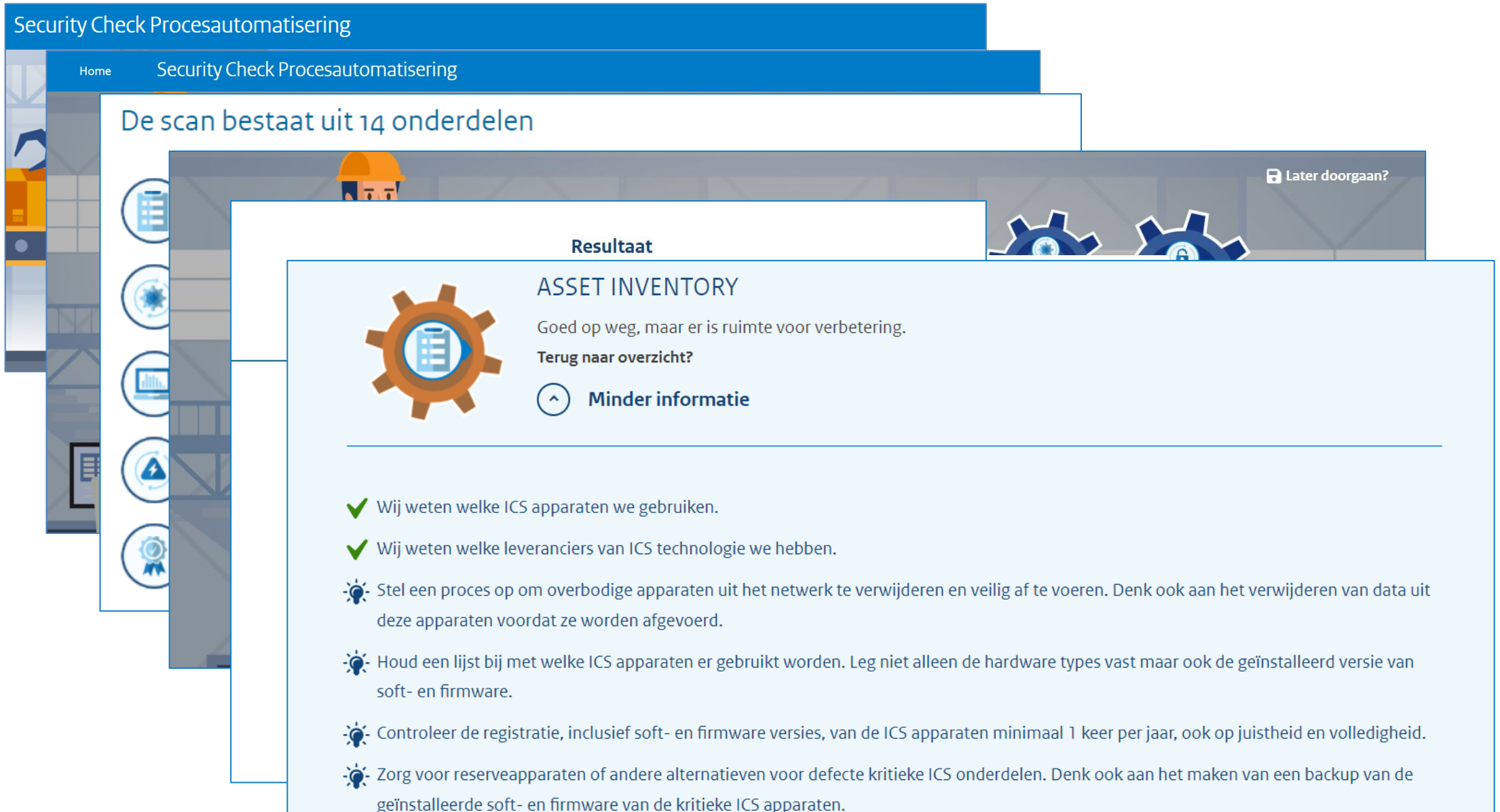
Uw mening

Start

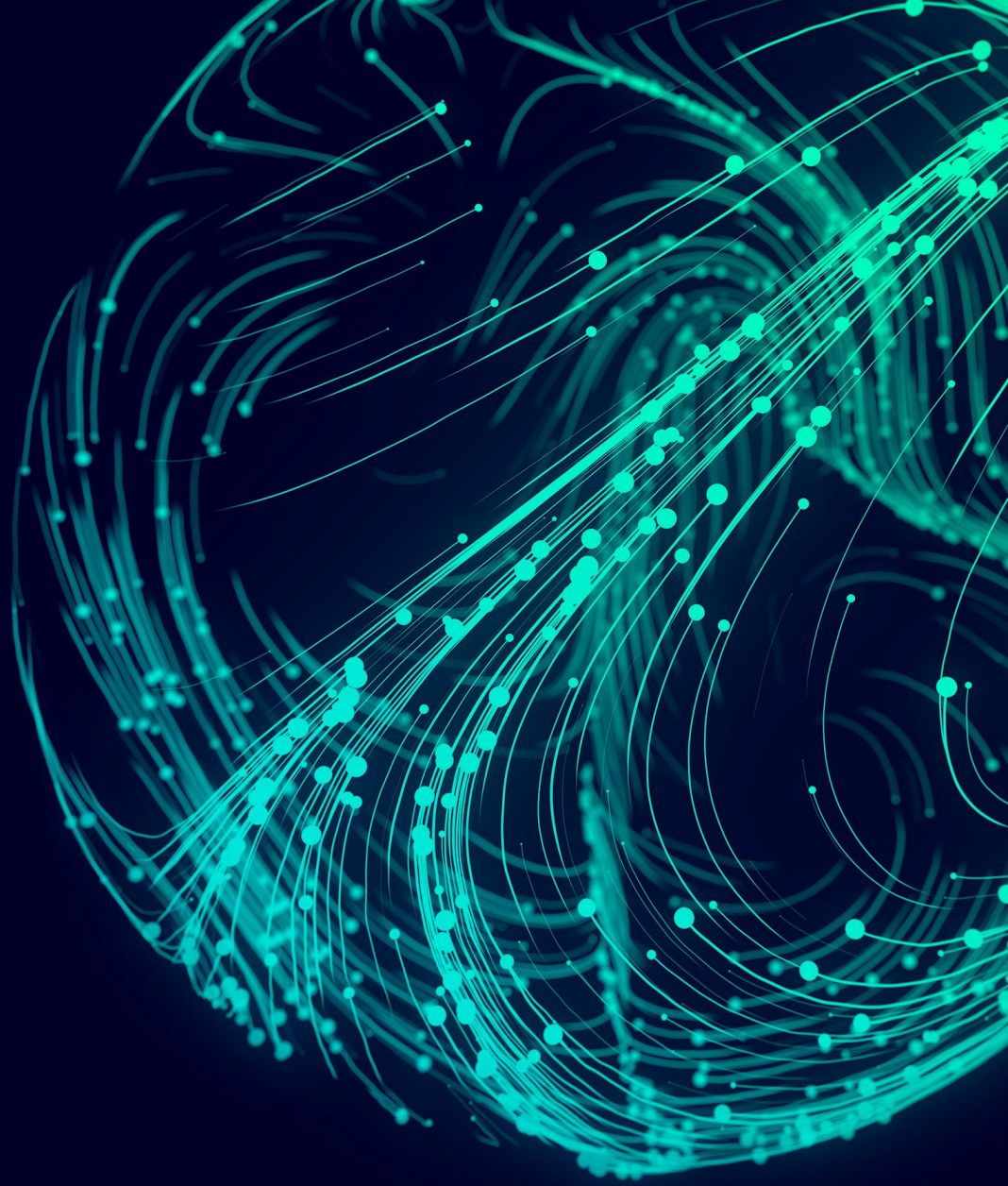
Cyberweerbaarheid van de OT-omgeving

OT, ook wel bekend als de industriële procesautomatisering van een bedrijf, is een aparte digitale omgeving. De beveiliging van de controlesystemen (ICS) vraagt om een andere aanpak dan bijvoorbeeld IT-omgevingen. Het ICS-veiligheidsbewustzijn en het bijbehorende budget zijn vaak lager dan bij traditionele IT-omgevingen. Om de juiste digitale weerbaarheidsmaatregelen te kunnen treffen, is extra aandacht vereist, op zowel strategisch als tactisch en operationeel niveau. Graag helpen we je op weg met een tool die inzicht verschaft in de betrouwbaarheid van je OT-omgeving.

Unieke publiek-private samenwerking lanceert nieuwe tool!



Sorry…



SIEMENS


There is no Smart Building without Security!
SIEMENS

Contact

Siemens Smart Infrastructure

Johan de Wit
Technical Officer Enterprise Security EMEA
The Hague
The Netherlands

Phone +31 70 333 33 33 / +31 6 55 76 60 29

E-mail: johan.de.wit@siemens.com

SIEMENS