Security for Operational Technology

Use of the IEC 62443 standard by Enexis

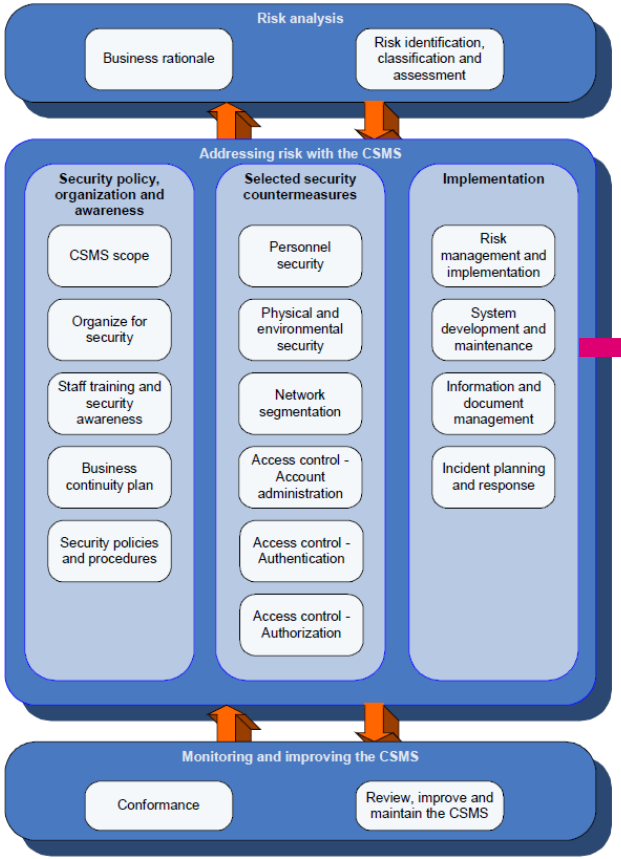
Philip Westbroek

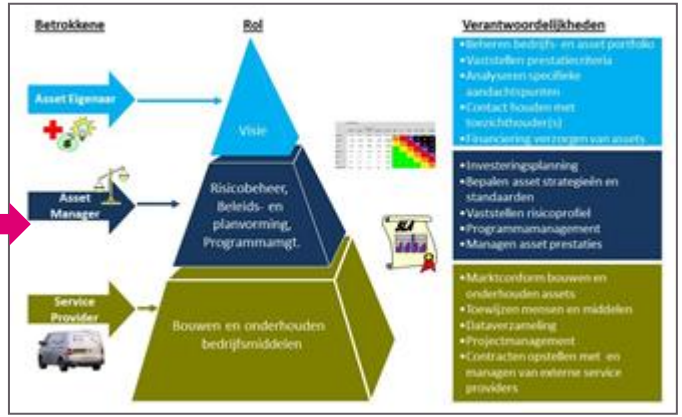
Smart Grid Forum
October 27, 2021

ENEXIS NETBEHEER

Integrating security in our asset management process

Implemented an ISMS in 2016, ISO 27001:2017 certified since 2019





ISMS based on ISO 27001 and IEC 62443

Integration in our NTA 8120- / ISO 55001-based QMS

One risk management process

OT security risk management integrated in existing risk management approach

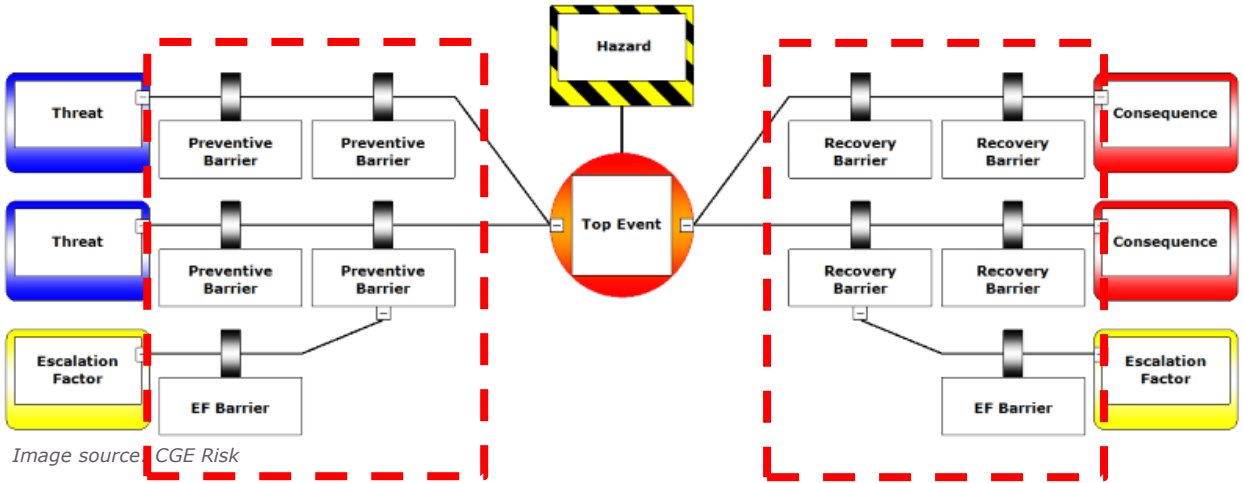


Image source: CGE Risk

One risk management process

Selecting barriers to implement

- Based on ISA99 / IEC 62443-3-3
- Control barriers (left in bowtie):
  - Between threat and top event.
- Recovery barriers (right in bowtie):
  - Between top event and consequence.

Control barriers:

Threat	Security measure examples
Social engineering	Awareness trainings
Manipulation of intercepted software before installation	Software and information integrity (SR 3.4) Digitally signing of software or firmware.
Introduction of backdoor by software vendor employees.	SR 5.1 – Network segmentation and SR 5.2 – Zone boundary protection Firewall or DMZ on an interface; blocks outbound connections. Contractual agreements with vendor, e.g. inclusion of security requirements in tenders, asking for ISMS for vendor's internal security organisation and including the right to audit the vendor's software.

Recovery barriers:

Measure	ISA 99-3-3 clause	Description
Host intrusion detection system	SR 3.2 RE (2) SR 3.4 RE (1)	The installation of a host-based intrusion detection system on computers within the domain. With this, attacker's actions can be detected.
Network intrusion detection system	-	The installation of a network-based intrusion detection system. With this, attacks can be detected.

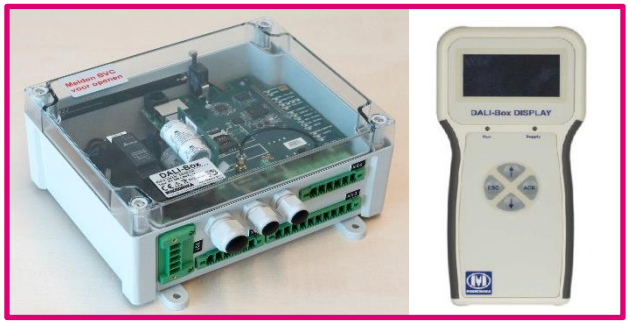
Integrating security in the procurement of components

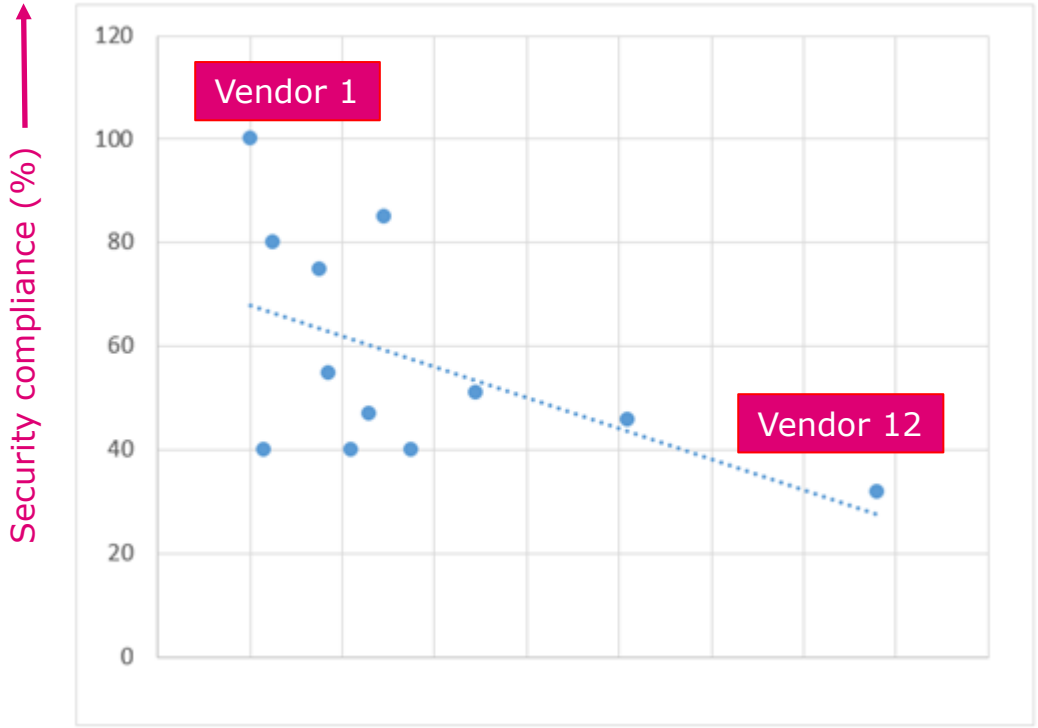
Enexis tenders grid components with formal security requirements

- Security during development and after sales:
  - Secure programming practices
  - Security testing during development
  - Vulnerability handling
  - IEC 62443-4-1
- Device security requirements:
  - User access management
  - Cryptographic algorithms and protocols
  - Logging and monitoring
  - IEC 62443-4-2
- Security improved between 2014 and now
  - All ENCS members use similar requirements
  - Successful pentest is a prerequisite for final awarding
  - More security ≠ higher TCO !

Integrating security in the procurement of components

Better cybersecurity does not always mean higher costs





OT security baseline

Mapping of security requirements (and REs) to security levels in Part 3-3, Annex B

Foundational requirement

Security levels

Security requirements and requirement enhancements

FR 1 - Identification and authentication control (IAC)
FR 2 - Use control (UC)
FR 3 - System integrity (SI)
FR 4 - Data confidentiality (DC)
FR 5 - Restricted data flow (RDF)
FR 6 - Timely response to events (TRE)
FR 7 - Resource availability (RA)

OT security baseline

Mapping of security requirements (and REs) to security levels in Part 3-3, Annex B

Foundational requirement

Security requirements and requirement enhancements

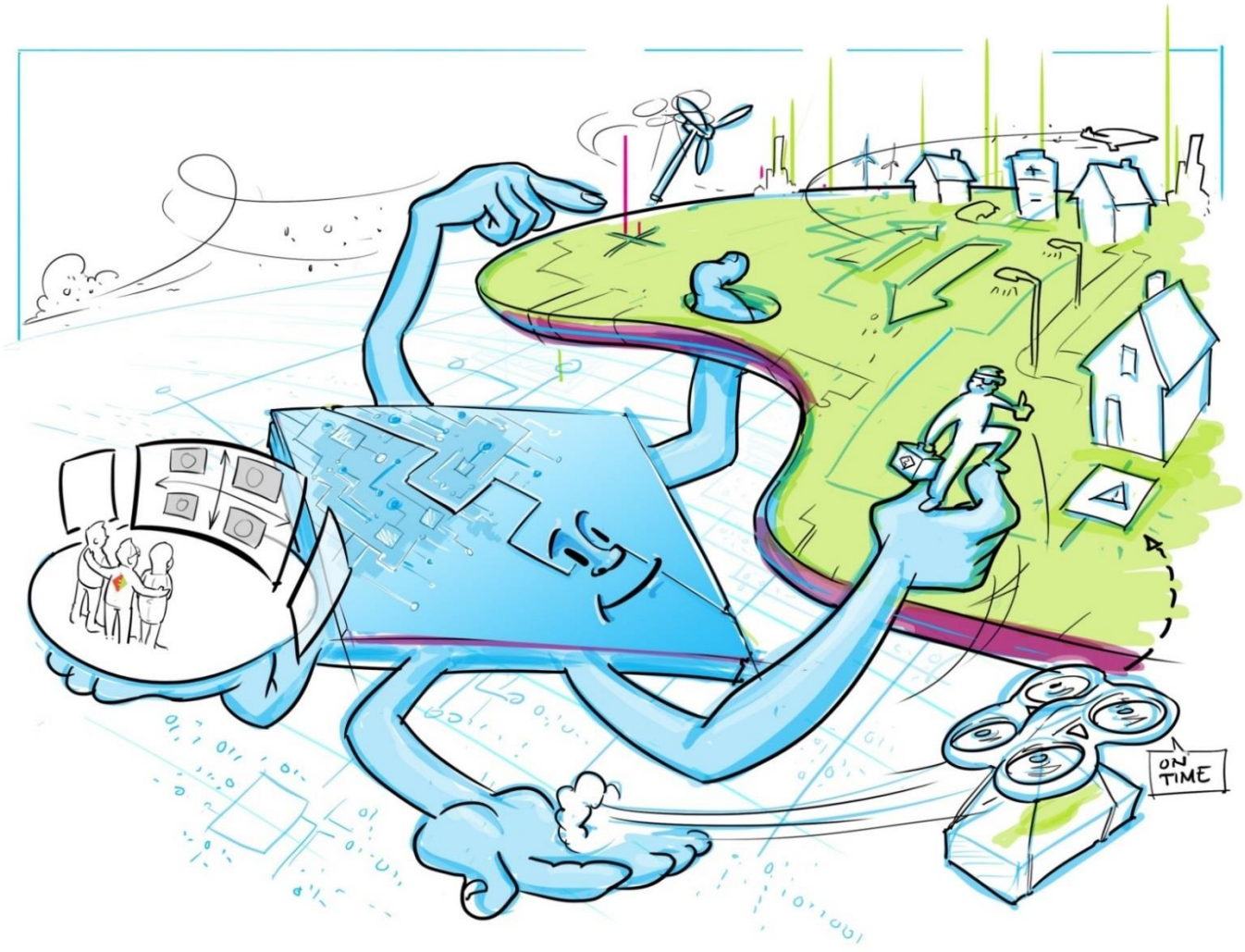
Security levels

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)					
SR 1.1 – Human user identification and authentication	5.3	✓	✓	✓	✓
SR 1.1 RE 1 – Unique identification and authentication	5.3.3.1		✓	✓	✓
SR 1.1 RE 2 – Multifactor authentication for untrusted networks	5.3.3.2			✓	✓
SR 1.1 RE 3 – Multifactor authentication for all networks	5.3.3.3				✓
SR 1.2 – Software process and device identification and authentication	5.4		✓	✓	✓
SR 1.2 RE 1 – Unique identification and authentication	5.4.3.1			✓	✓
SR 1.3 – Account management	5.5	✓	✓	✓	✓
SR 1.3 RE 1 – Unified account management	5.5.3.1			✓	✓
SR 1.4 – Identifier management	5.6	✓	✓	✓	✓
SR 1.5 – Authenticator management	5.7	✓	✓	✓	✓
SR 1.5 RE 1 – Hardware security for software process identity credentials	5.7.3.1			✓	✓
SR 1.6 – Wireless access management	5.8	✓	✓	✓	✓
SR 1.6 RE 1 – Unique identification and authentication	5.8.3.1		✓	✓	✓
SR 1.7 – Strength of password-based authentication	5.9	✓	✓	✓	✓
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users	5.9.3.1			✓	✓

OT security baseline

Difference between modern and legacy equipment and/or zones

- Legacy zone:
  - Contains equipment that can not easily be updated to modern security standards (low security level);
  - Management approval required to define legacy zone;
  - Important to minimise number of legacy zones;
  - Compensating security controls implemented to minimise risk exposure.
- Modern zone:
  - Newly implemented (security by design) or easily updated to modern security standards;
  - All other zones;
  - Highest security level.
- Select security controls for each FR



Philip Westbroek
OT security officer

Philip.westbroek@enexis.nl