# OT security at Enexis

## Digital security at a regional electricity grid operator

**Philip Westbroek**
OT security officer

May 10, 2022

# Rapid digitalisation of the energy value chain

*Balancing supply and demand more difficult with increased use of renewable energy*

**Medium voltage cables**

"Put more copper in the ground"

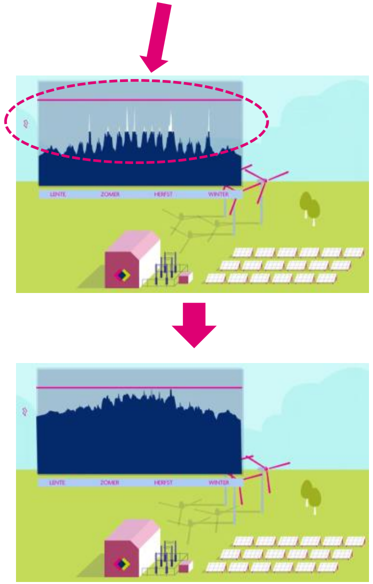
vs.

**Digital systems**

"Make smarter use of existing capacity"

# Rapid digitalisation of the energy value chain

*Prime example: curtailment*

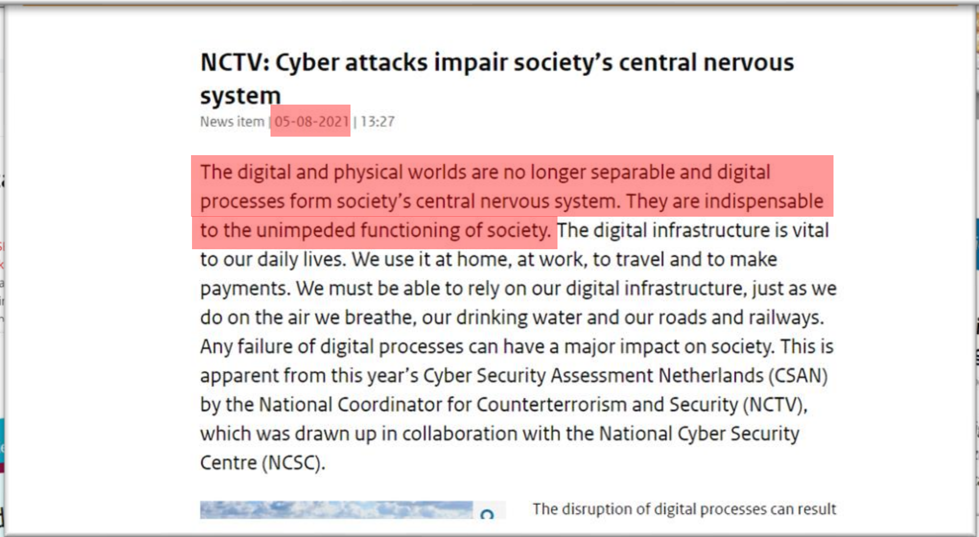


- Background:
  - The energy transition is moving fast, more and more generation by wind and solar farms;
  - At some locations (especially rural areas), the maximum capacity of the electricity grid is reached;
  - No new wind or solar farms can be connected at these locations.
- How we use digitalisation to make smarter use of existing capacity:
  - Continuous monitoring of the electricity network load;
  - From our control centers, we remotely throttle back power generation by some solar and wind farms;
  - Send commands via a data communications netwerk to equipment in the solar and wind farms.
- This way we can probably connect 30% more sustainable power generation capacity...
- ...but what about digital security:
  - *"Using this control mechanism, we limit the highest peaks in power generation by solar and wind farms";*
  - What happens if an unauthorised person can also access this control mechanism ?

[1] See https://www.youtube.com/watch?v=0D3IdEZ-AwI and https://www.enexisgroep.nl/nieuws/enexis-netbeheer-en-liander-onderzoeken-potentie-van-dimmen-zonneparken/

# Dutch coordinator for anti-terrorism and safety (NCTV):

"Cyber Attacks Impair Society's Central Nervous System"

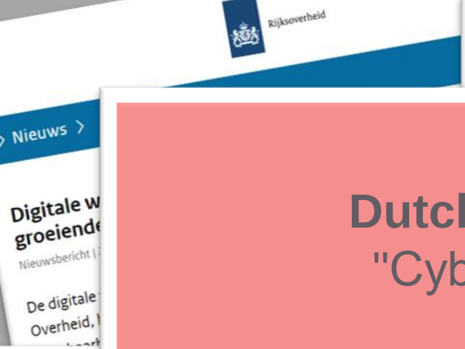


## NCTV: Cyber attacks impair society's central nervous system

News item | 05-08-2021 | 13:27

The digital and physical worlds are no longer separable and digital processes form society's central nervous system. They are indispensable to the unimpeded functioning of society. The digital infrastructure is vital to our daily lives. We use it at home, at work, to travel and to make payments. We must be able to rely on our digital infrastructure, just as we do on the air we breathe, our drinking water and our roads and railways. Any failure of digital processes can have a major impact on society. This is apparent from this year's Cyber Security Assessment Netherlands (CSAN) by the National Coordinator for Counterterrorism and Security (NCTV), which was drawn up in collaboration with the National Cyber Security Centre (NCSC).

The disruption of digital processes can result



Rijksoverheid

Nieuws

Digitale w
groeiende

Nieuwsbericht |

De digitale
Overheid,

ANDY GREENBERG SECURITY 02.03.2020 04:56 PM

Mysterious New Ransomware Targets Industrial Control Systems

'Zelfs basale cybersecurity-maatr
niet structureel

teeds

EMERCE

Home / Industry Wire / GreyEnergy groep richt zich op vitale infrastructuur

Industry Wire

Geplaatst door ESET
Woensdag 17 oktober 2018 - 12:56

GreyEnergy groep richt zich op vit
infrastructuur

17 oktober 2018 – ESI
opvolger van de Black
door ESET benoemd a
spionage en verkennin
toekomstige cybersab

CSR Cyber Security Raad

Home Over de CSR Actueel Leden CSR Publicati

Home > Actueel

'Cyberweerbaarheid IACS in Ned

'Cyberweerbaarheid IACS in Nederland onvoldoende op orde'

Nieuwsbericht | 29-4-2020 | 11:40

Rijksoverheid

ieuws

inet neemt maatregelen tegen permanente statelijke
ging

ericht | 18-04-2019 | 15:20

iging voor onze nationale veiligheid vanuit andere landen is permanent
ig. Door beïnvloeding van onze besluitvorming, digitale sabotage van
ale infrastructuur of politieke en economische spionage proberen

## US Wants To Isolate Power Grids With 'Retro' Technology To Limit Cyber-Attacks

By Security Experts July 3, 2019

1134 0

# 'Operational Technology' has some additional challenges

*Some important differences between IT and OT systems*

## Standard digital systems

### IT

- Short equipment life cycle
- Mature patching and update processes
- IT knowledge relatively easy to come by
- Easier to repair or replace, also less impact

## Digital systems for grid operators

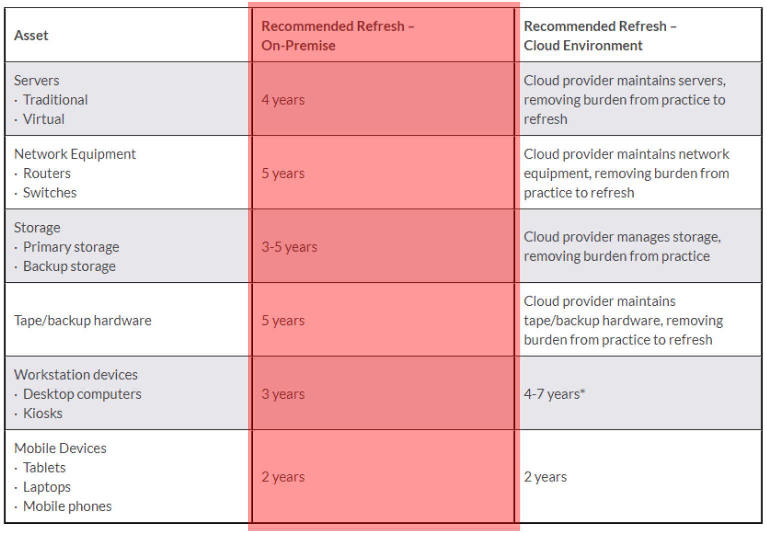
### OT

- Use of legacy equipment (e.g. Windows XP)
- Very reluctant to apply patches; 24*7 operation
- Still limited focus on cybersecurity by vendors
- Much more serious potential impact of incidents

# 'Operational Technology' has some additional challenges

*The expected lifespan of IT and OT hardware*

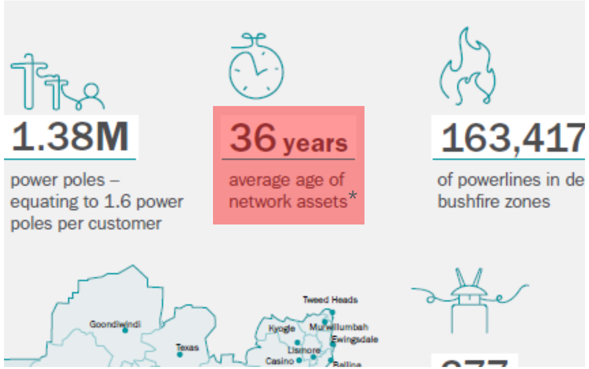
## IT[1]



| Asset | Recommended Refresh – On-Premise | Recommended Refresh – Cloud Environment |
|---|---|---|
| Servers<br>· Traditional<br>· Virtual | 4 years | Cloud provider maintains servers, removing burden from practice to refresh |
| Network Equipment<br>· Routers<br>· Switches | 5 years | Cloud provider maintains network equipment, removing burden from practice to refresh |
| Storage<br>· Primary storage<br>· Backup storage | 3-5 years | Cloud provider manages storage, removing burden from practice |
| Tape/backup hardware | 5 years | Cloud provider maintains tape/backup hardware, removing burden from practice to refresh |
| Workstation devices<br>· Desktop computers<br>· Kiosks | 3 years | 4-7 years* |
| Mobile Devices<br>· Tablets<br>· Laptops<br>· Mobile phones | 2 years | 2 years |

**Between 2-5 years**

## OT[2]



1.38M

power poles – equating to 1.6 power poles per customer

36 years

average age of network assets*

163,417

of powerlines in de bushfire zones

* Electrotechnical equipment (cables, transformers, protection relays etc), but also digital components have a much higher (expected) technical lifespan.

[1]: Source: https://netgaincloud.com/blog/whats-the-lifespan-of-hardware-and-software/

[2]: Source: Essential Energy annual report 2019-2020

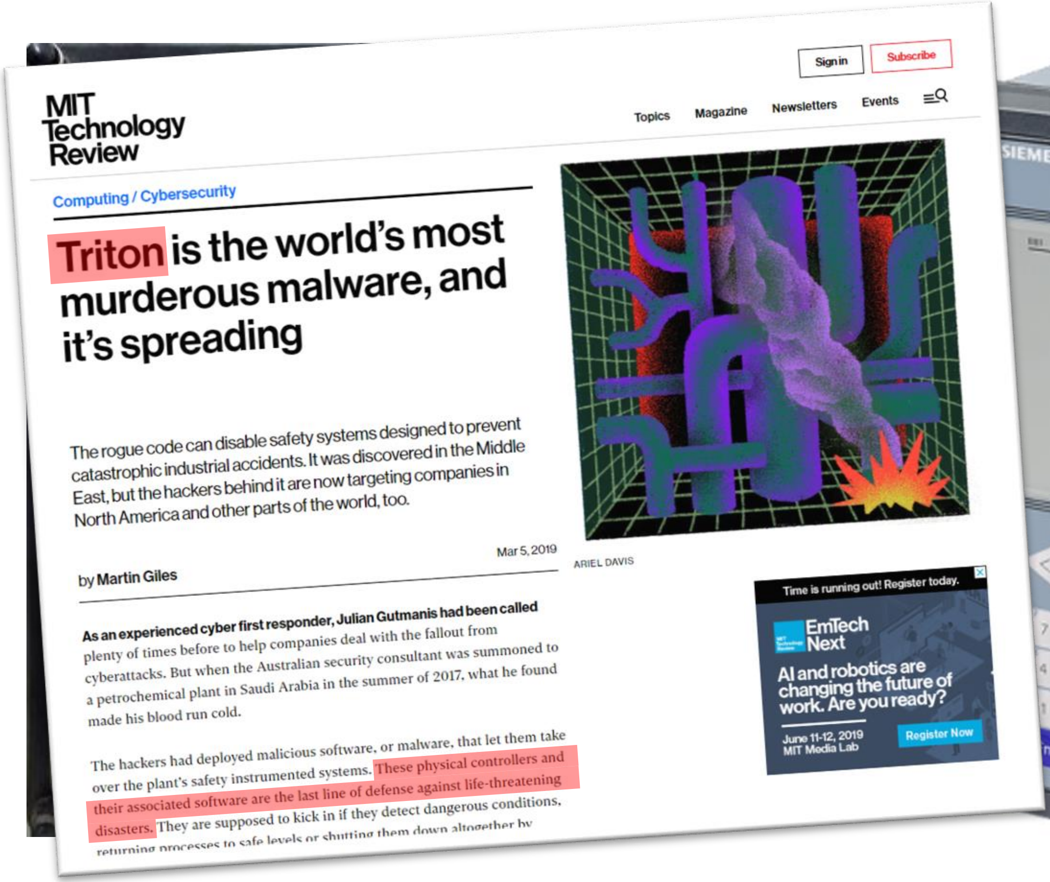
# Digitalisation is also taking place for safety systems

*Safety systems are a special kind of operational technology*

vs.

# Digitalisation is also taking place for safety systems

*Safety systems are a special kind of operational technology*



Sign in | Subscribe

MIT Technology Review

Topics | Magazine | Newsletters | Events

Computing / Cybersecurity

## Triton is the world's most murderous malware, and it's spreading

The rogue code can disable safety systems designed to prevent catastrophic industrial accidents. It was discovered in the Middle East, but the hackers behind it are now targeting companies in North America and other parts of the world, too.

by Martin Giles

Mar 5, 2019

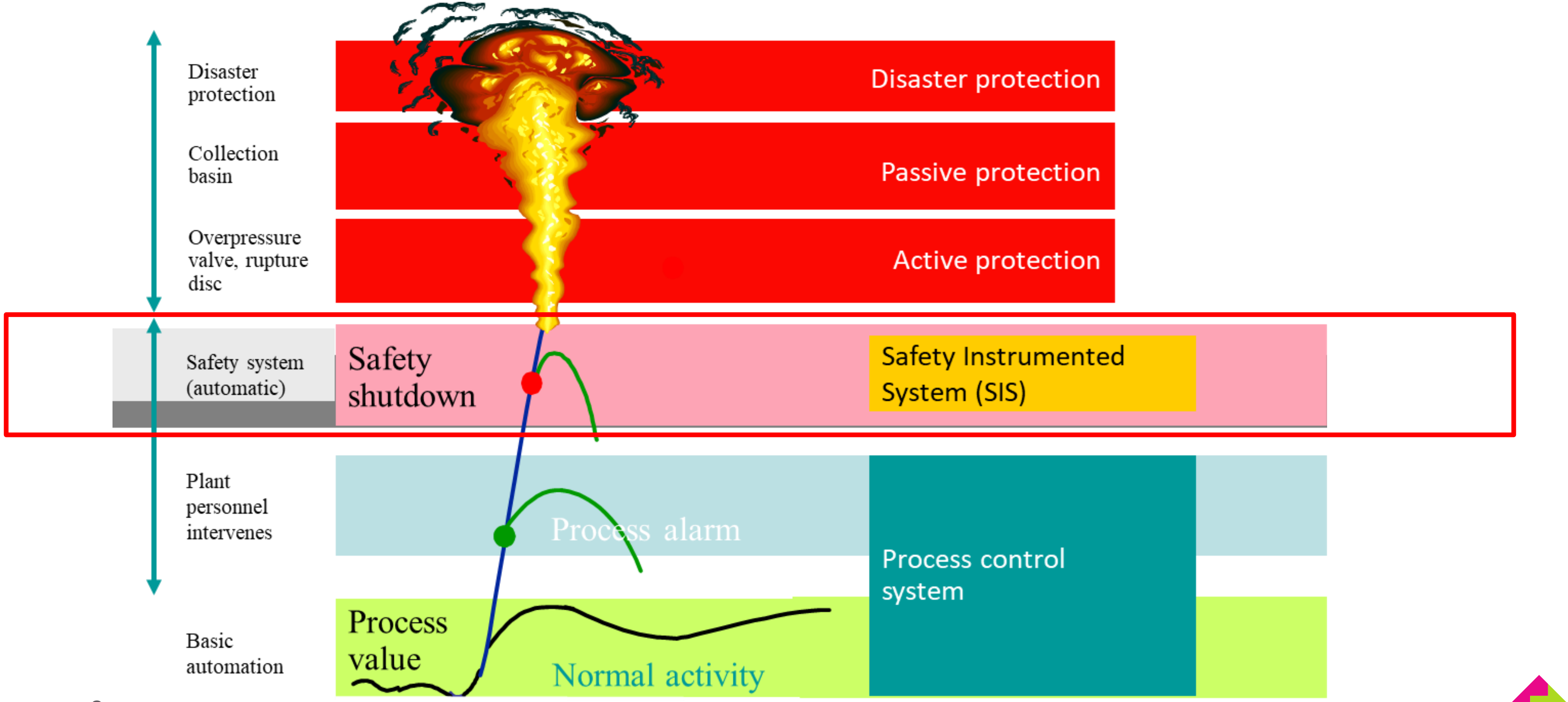
ARIEL DAVIS

**As an experienced cyber first responder, Julian Gutmanis had been called** plenty of times before to help companies deal with the fallout from cyberattacks. But when the Australian security consultant was summoned to a petrochemical plant in Saudi Arabia in the summer of 2017, what he found made his blood run cold.

The hackers had deployed malicious software, or malware, that let them take over the plant's safety instrumented systems. These physical controllers and their associated software are the last line of defense against life-threatening disasters. They are supposed to kick in if they detect dangerous conditions, returning processes to safe levels or shutting them down altogether by

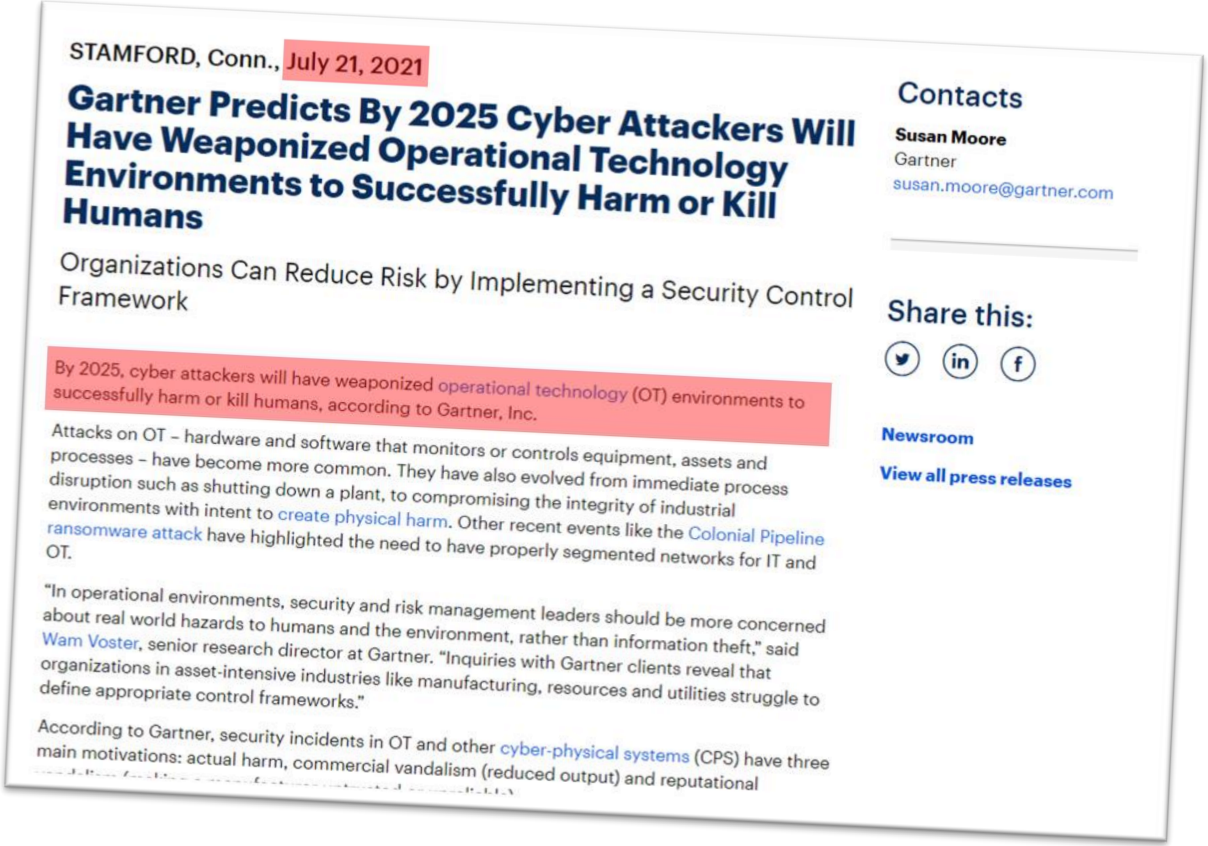
# Digitalisation is also taking place for safety systems

*Safety systems are a special kind of operational technology*



# Digitalisation is also taking place for safety systems

*Safety systems are a special kind of operational technology*



STAMFORD, Conn., July 21, 2021

## Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans

Organizations Can Reduce Risk by Implementing a Security Control Framework

By 2025, cyber attackers will have weaponized operational technology (OT) environments to successfully harm or kill humans, according to Gartner, Inc.

Attacks on OT – hardware and software that monitors or controls equipment, assets and processes – have become more common. They have also evolved from immediate process disruption such as shutting down a plant, to compromising the integrity of industrial environments with intent to create physical harm. Other recent events like the Colonial Pipeline ransomware attack have highlighted the need to have properly segmented networks for IT and OT.

"In operational environments, security and risk management leaders should be more concerned about real world hazards to humans and the environment, rather than information theft," said Wam Voster, senior research director at Gartner. "Inquiries with Gartner clients reveal that organizations in asset-intensive industries like manufacturing, resources and utilities struggle to define appropriate control frameworks."

According to Gartner, security incidents in OT and other cyber-physical systems (CPS) have three main motivations: actual harm, commercial vandalism (reduced output) and reputational

Contacts

**Susan Moore**
Gartner
susan.moore@gartner.com

Share this:

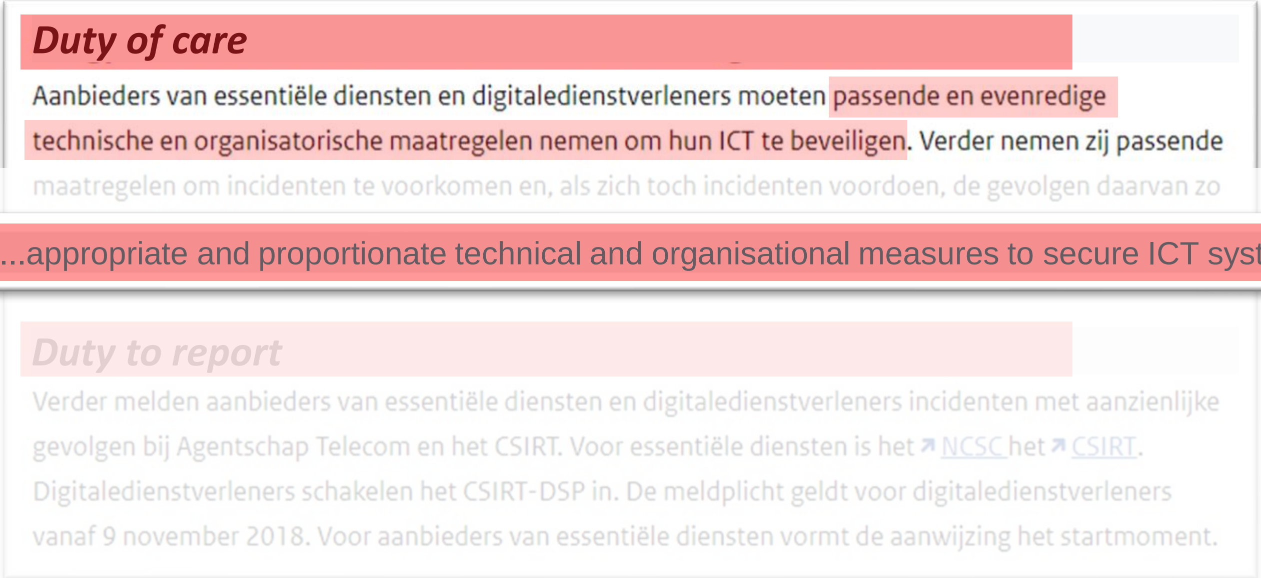
**Newsroom**

**View all press releases**

# 'Wet beveiliging netwerk- en informatiesystemen' - Wbni

*Dutch implementation of the EU NIS directive*

Agentschap Telecom
*Ministerie van Economische Zaken en Klimaat*



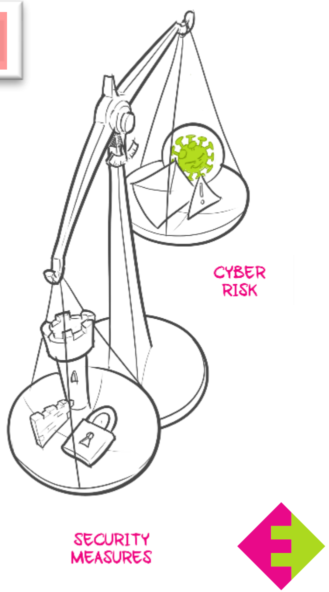
***Duty of care***

Aanbieders van essentiële diensten en digitaledienstverleners moeten passende en evenredige technische en organisatorische maatregelen nemen om hun ICT te beveiligen. Verder nemen zij passende maatregelen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo

...appropriate and proportionate technical and organisational measures to secure ICT systems.

***Duty to report***

Verder melden aanbieders van essentiële diensten en digitaledienstverleners incidenten met aanzienlijke gevolgen bij Agentschap Telecom en het CSIRT. Voor essentiële diensten is het ↗ NCSC het ↗ CSIRT. Digitaledienstverleners schakelen het CSIRT-DSP in. De meldplicht geldt voor digitaledienstverleners vanaf 9 november 2018. Voor aanbieders van essentiële diensten vormt de aanwijzing het startmoment.



# How to maximise the resilience of OT domains

*Some examples of steps we took at Enexis*

- Increase awareness on all organisation levels
- Strictly separate OT from the outside world ('air gap')
- One risk management policy and process for conventional and digital risks
- Set up an Information Security Management System (ISMS)
- Network segmentation
- Increase awareness on all organisation levels
- Include security requirements in all OT tenders
- Implement security monitoring and a security operations center (SOC); not only prevention
- Industry collaboration, both nationally and internationally (EU), facilitated by the ENCS
- Focus security investments on perimeter systems, thus relieving the 'legacy burden'
- Did I already mention increasing awareness on all organisation levels ?
- Many test activities: pentest, red teaming etc.

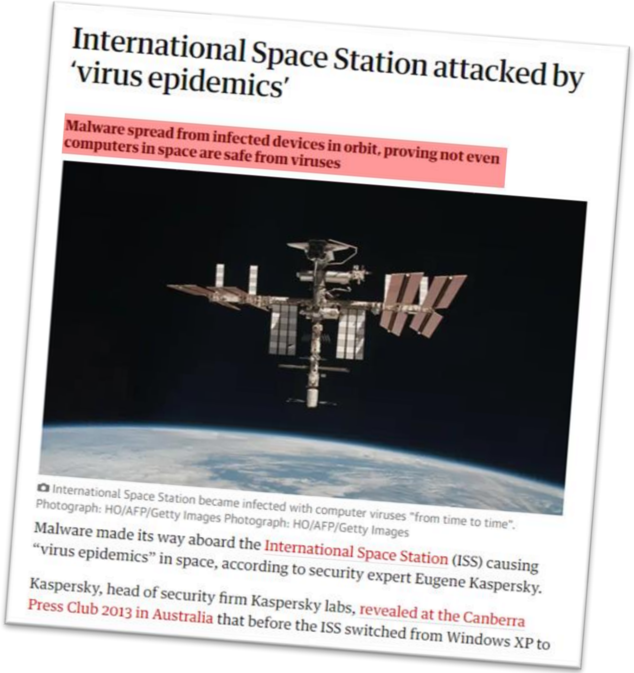
# Strictly separate OT from the outside world ('air gap')

*Easier said than done....*

- Even the ISS is not fully 'air-gapped'[1]
- US subcommittee on National Security, Homeland Defense, and Foreign Operations (May 2011 hearing):

  > "*In our experience in conducting hundreds of vulnerability assessments in the private sector,* in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network*. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network.*"[2]

- Therefore additional controls required, e.g.:
  - Increase awareness on all organisation levels;
  - Fully separated IT and OT work stations (two separate laptops);
  - Feasible policy regarding removable media (USB sticks !) and file exchange.



## International Space Station attacked by 'virus epidemics'

**Malware spread from infected devices in orbit, proving not even computers in space are safe from viruses**

International Space Station became infected with computer viruses "from time to time". Photograph: HO/AFP/Getty Images Photograph: HO/AFP/Getty Images

Malware made its way aboard the International Space Station (ISS) causing "virus epidemics" in space, according to security expert Eugene Kaspersky.

Kaspersky, head of security firm Kaspersky labs, revealed at the Canberra Press Club 2013 in Australia that before the ISS switched from Windows XP to

[1]: See https://www.theguardian.com/technology/2013/nov/12/international-space-station-virus-epidemics-malware
[2]: See https://www.youtube.com/watch?v=x1URPa1jG60 (58m30s - 59m00s) and https://www.govinfo.gov/content/pkg/CHRG-112hhrg70676/pdf/CHRG-112hhrg70676.pdf

# One risk management process

*Integrated OT security risk management in our existing process based on bowties*

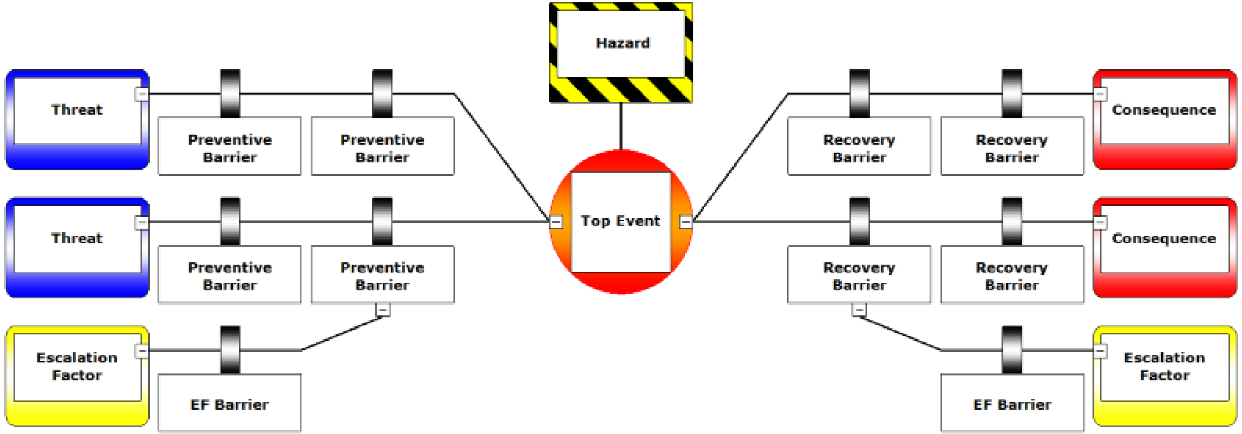


*Image source: CGE Risk*

# One risk management process

*Selecting barriers to implement*

- Based on IEC 62443-3-3 standard (ISA99)
- Control barriers (left in bowtie):
  - Between threat and top event.
- Recovery barriers (right in bowtie):
  - Between top event and consequence;
  - Minimising the impact of the top event.

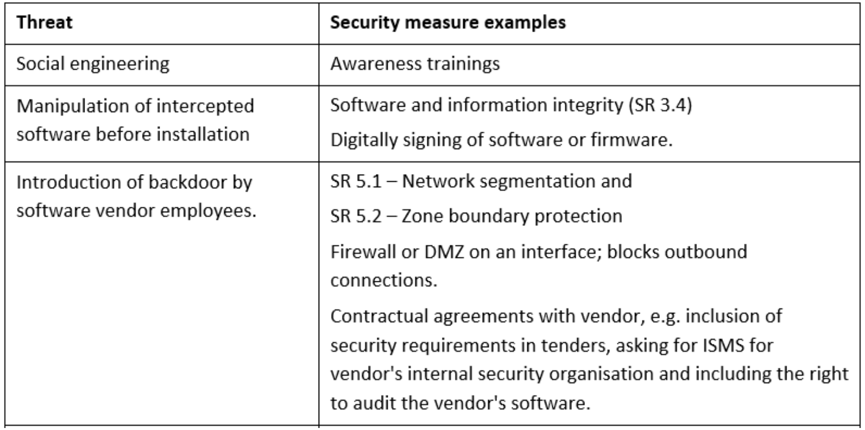
IEC 62443-3-3

Edition 1.0 2013-08

INTERNATIONAL STANDARD

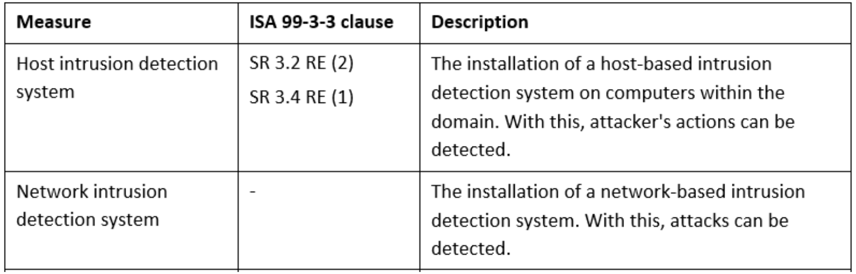
Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

Control barriers:



| Threat | Security measure examples |
|---|---|
| Social engineering | Awareness trainings |
| Manipulation of intercepted software before installation | Software and information integrity (SR 3.4)<br>Digitally signing of software or firmware. |
| Introduction of backdoor by software vendor employees. | SR 5.1 – Network segmentation and<br>SR 5.2 – Zone boundary protection<br>Firewall or DMZ on an interface; blocks outbound connections.<br>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)<br>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. |

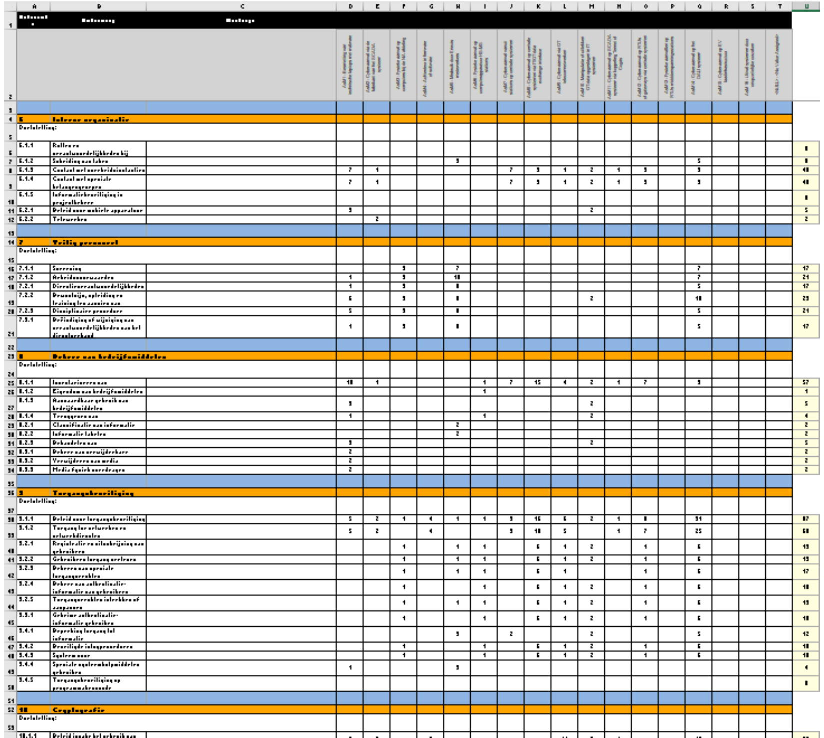
# One risk management process

*Mapping of our barriers to the ISO 27001:2017 Annex A controls (see clause 6.1.3c)*

The 114 controls of the ISO 27001:2017 Annex A

The number of times that a control is used in our bowties, easy to identify key controls

All our OT security risk categories (detailed in bowties)



| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | [illegible] | [illegible] | [illegible] | | | | | | | | | | | | | | | | | | |
| 2 | | | | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | |
| 3 | | | | | | | | | | | | | | | | | | | | | |
| 4 | 6 | Interne organisatie | | | | | | | | | | | | | | | | | | | |
| 5 | Doelstelling: | | | | | | | | | | | | | | | | | | | | |
| 6 | 6.1.1 | Rollen en verantwoordelijkheden bij | | | | | | | | | | | | | | | | | | | 0 |
| 7 | 6.1.2 | Scheiding van taken | | | | | | 3 | | | | | | | | | 5 | | | | 8 |
| 8 | 6.1.3 | Contact met overheidsinstanties | | 7 | 1 | | | | | 7 | 3 | 1 | 2 | 1 | 3 | | 3 | | | | 40 |
| 9 | 6.1.4 | Contact met speciale belangengroepen | | 7 | 1 | | | | | 7 | 3 | 1 | 2 | 1 | 3 | | 3 | | | | 40 |
| 10 | 6.1.5 | Informatiebeveiliging in projectbeheer | | | | | | | | | | | | | | | | | | | 0 |
| 11 | 6.2.1 | Beleid voor mobiele apparatuur | | 3 | | | | | | | | | 2 | | | | | | | | 5 |
| 12 | 6.2.2 | Telewerken | | | 2 | | | | | | | | | | | | | | | | 2 |
| 13 | | | | | | | | | | | | | | | | | | | | | |
| 14 | 7 | Veilig personeel | | | | | | | | | | | | | | | | | | | |
| 15 | Doelstelling: | | | | | | | | | | | | | | | | | | | | |
| 16 | 7.1.1 | Screening | | | | 3 | | 7 | | | | | | | | | 7 | | | | 17 |
| 17 | 7.1.2 | Arbeidsvoorwaarden | | 1 | | 3 | | 10 | | | | | | | | | 7 | | | | 21 |
| 18 | 7.2.1 | Directieverantwoordelijkheden | | 1 | | 3 | | 8 | | | | | | | | | 5 | | | | 17 |
| 19 | 7.2.2 | Bewustzijn, opleiding en training ten aanzien van | | 6 | | 3 | | 8 | | | | | 2 | | | | 10 | | | | 29 |
| 20 | 7.2.3 | Disciplinaire procedure | | 5 | | 3 | | 8 | | | | | | | | | 5 | | | | 21 |
| 21 | 7.3.1 | Beëindiging of wijziging van verantwoordelijkheden van het dienstverband | | 1 | | 3 | | 8 | | | | | | | | | 5 | | | | 17 |
| 22 | | | | | | | | | | | | | | | | | | | | | |
| 23 | 8 | Beheer van bedrijfsmiddelen | | | | | | | | | | | | | | | | | | | |
| 24 | Doelstelling: | | | | | | | | | | | | | | | | | | | | |
| 25 | 8.1.1 | Inventariseren van | | 10 | 1 | | | | 1 | 7 | 15 | 4 | 2 | 1 | 7 | | 3 | | | | 57 |
| 26 | 8.1.2 | Eigendom van bedrijfsmiddelen | | | | | | | 1 | | | | | | | | | | | | 1 |
| 27 | 8.1.3 | Aanvaardbaar gebruik van bedrijfsmiddelen | | 3 | | | | | | | | | 2 | | | | | | | | 5 |
| 28 | 8.1.4 | Teruggeven van | | 1 | | | | | 1 | | | | 2 | | | | | | | | 4 |
| 29 | 8.2.1 | Classificatie van informatie | | | | | | 2 | | | | | | | | | | | | | 2 |
| 30 | 8.2.2 | Informatie labelen | | | | | | 2 | | | | | | | | | | | | | 2 |
| 31 | 8.2.3 | Behandelen van | | 3 | | | | | | | | | 2 | | | | | | | | 5 |
| 32 | 8.3.1 | Beheer van verwijderbare | | 2 | | | | | | | | | | | | | | | | | 2 |
| 33 | 8.3.2 | Verwijderen van media | | 2 | | | | | | | | | | | | | | | | | 2 |
| 34 | 8.3.3 | Media fysiek overdragen | | 2 | | | | | | | | | | | | | | | | | 2 |
| 35 | | | | | | | | | | | | | | | | | | | | | |
| 36 | 9 | Toegangsbeveiliging | | | | | | | | | | | | | | | | | | | |
| 37 | Doelstelling: | | | | | | | | | | | | | | | | | | | | |
| 38 | 9.1.1 | Beleid voor toegangsbeveiliging | | 5 | 2 | 1 | 4 | 1 | 1 | 3 | 16 | 6 | 2 | 1 | 8 | | 31 | | | | 87 |
| 39 | 9.1.2 | Toegang tot netwerken en netwerkdiensten | | 5 | 2 | | 4 | | | 3 | 10 | 5 | | 1 | 7 | | 25 | | | | 68 |
| 40 | 9.2.1 | Registratie en uitschrijving van gebruikers | | | | 1 | | 1 | 1 | | 6 | 1 | 2 | | 1 | | 6 | | | | 19 |
| 41 | 9.2.2 | Gebruikers toegang verlenen | | | | 1 | | 1 | 1 | | 6 | 1 | 2 | | 1 | | 6 | | | | 19 |
| 42 | 9.2.3 | Beheren van speciale toegangsrechten | | | | 1 | | 1 | 1 | | 6 | 1 | | | 1 | | 6 | | | | 17 |
| 43 | 9.2.4 | Beheer van authenticatie-informatie van gebruikers | | | | 1 | | | 1 | | 6 | 1 | 2 | | 1 | | 6 | | | | 18 |
| 44 | 9.2.5 | Toegangsrechten intrekken of aanpassen | | | | 1 | | 1 | 1 | | 6 | 1 | 2 | | 1 | | 6 | | | | 19 |
| 45 | 9.3.1 | Geheime authenticatie-informatie gebruiken | | | | 1 | | | 1 | | 6 | 1 | 2 | | 1 | | 6 | | | | 18 |
| 46 | 9.4.1 | Beperking toegang tot informatie | | | | | | 3 | | 2 | | | 2 | | | | 5 | | | | 12 |
| 47 | 9.4.2 | Beveiligde inlogprocedures | | | | 1 | | | 1 | | 6 | 1 | 2 | | 1 | | 6 | | | | 18 |
| 48 | 9.4.3 | Systeem voor | | | | 1 | | | 1 | | 6 | 1 | 2 | | 1 | | 6 | | | | 18 |
| 49 | 9.4.4 | Speciale systeemhulpmiddelen gebruiken | | 1 | | | | 3 | | | | | | | | | | | | | 4 |
| 50 | 9.4.5 | Toegangsbeveiliging op programmabroncode | | | | | | | | | | | | | | | | | | | 0 |
| 51 | | | | | | | | | | | | | | | | | | | | | |
| 52 | 10 | Cryptografie | | | | | | | | | | | | | | | | | | | |
| 53 | Doelstelling: | | | | | | | | | | | | | | | | | | | | |
| | 10.1.1 | Beleid inzake het gebruik van | | | | | | | | | | | | | | | | | | | |

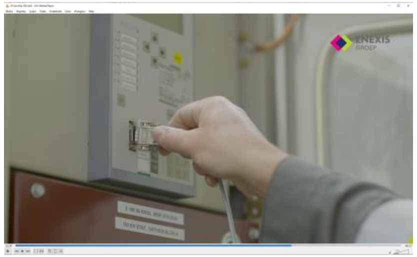
1-click xls report from our bowtie development application BowtieXP

DigiTrust
ISO 27001
MANAGEMENTSYSTEEM VOOR INFORMATIEBEVEILIGING
MGMT. SYS.
RvA C 618

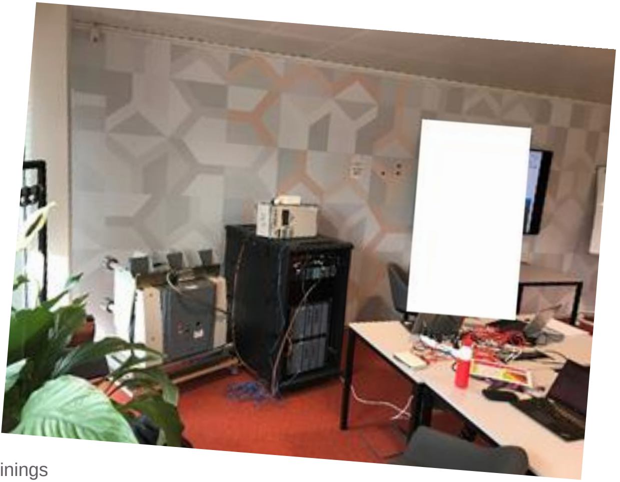
# Increase awareness on all organisation levels

*Colleagues don't always understand cyber risks and how they can influence them*

MANY demos



Movie clip about OT security risks



Red/Blue trainings

Co-financed by the Connecting Europe Facility of the European Union

Mobile OT security demo cases

See also our visualisations of OT security at Enexis: https://jamdots.nl/view/285/Enexis-OT-security

# Include security requirements in all OT tenders

*Enexis tenders grid components with formal security requirements*

ENCS

DA/SA-301-2021

Security requirements for procuring RTUs and gateways

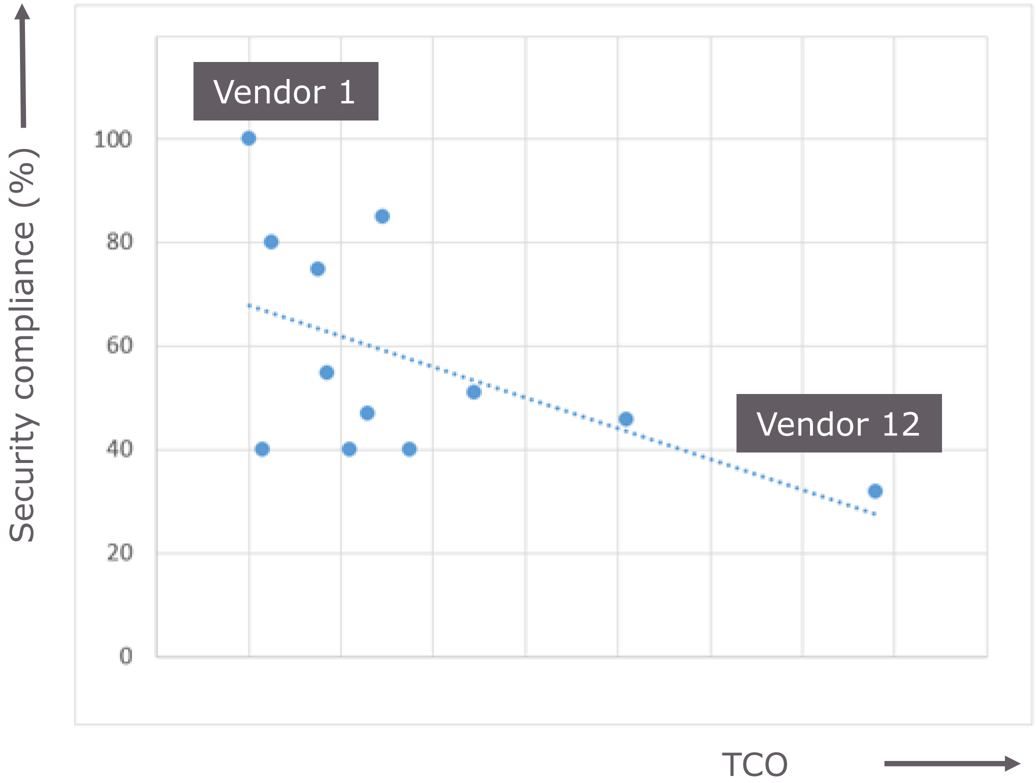
Version 2021v0.5

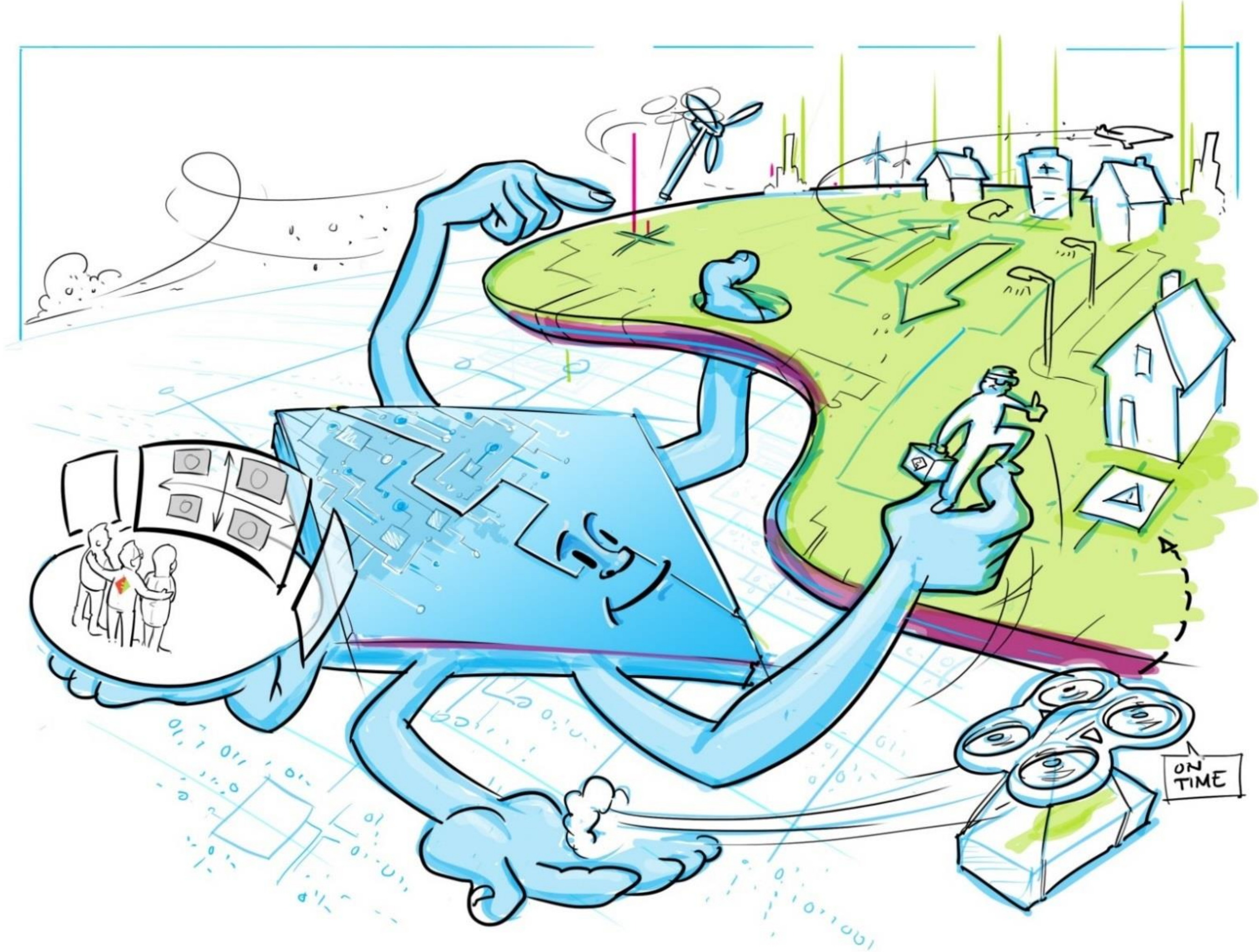
11 March 2021

- 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 !**

# Include security requirements in all OT tenders

*Results of our 2015 tender for Distribution Automation Light (DALI)*





Philip Westbroek
OT security officer

Philip.westbroek@enexis.nl

Graphics by Wilco Prinsen
www.jamvisualthinking.com