OT security bij Enexis

PvIB themabijeenkomst 10 februari 2022

Philip Westbroek
OT security officer

10 februari 2022

ENEXIS

Informatie vs. Operationele Technologie (IT vs. OT)

Enkele noemenswaardige verschillen

Informatie Technologie (IT)

- Data en informatiestromen
- Belangrijkste IT risico's:
  - Vertrouwelijkheid, integriteit en/of beschikbaarheid van data gecompromitteerd.
- Prioriteit voor B-I-V:
  1. Vertrouwelijkheid
  2. Integriteit
  3. Beschikbaarheid
- Over het algemeen up-to-date software

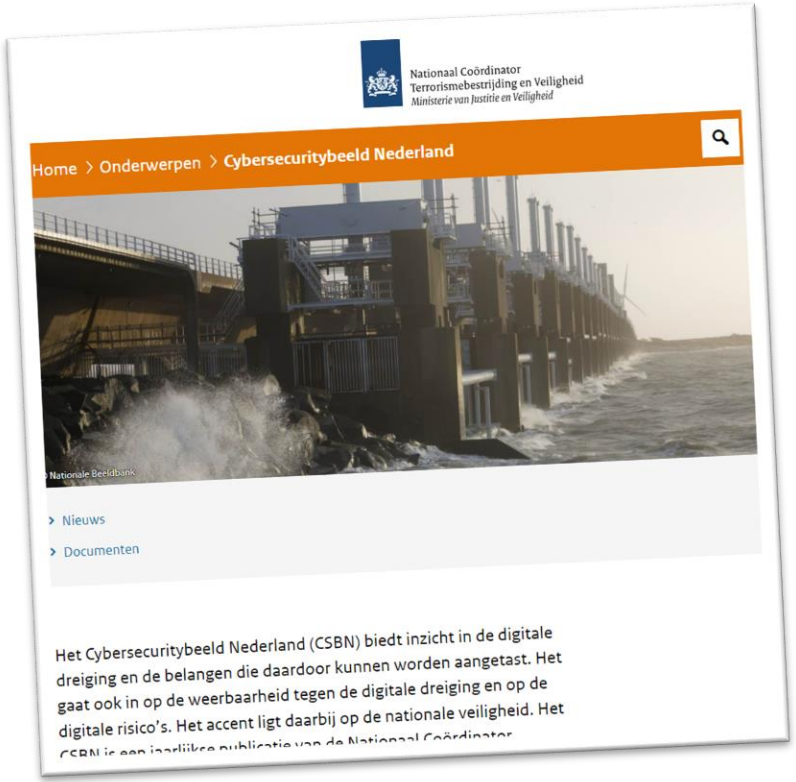
Operationele Technologie (OT)

Procesautomatisering (PA)
Industrial Control Systems (ICS)

- Aansturing van een fysiek (productie)proces
- Belangrijkste OT risico's:
  - Persoonlijke veiligheid gecompromitteerd;
  - Productieverlies omdat systemen niet beschikbaar zijn.
- Prioriteit voor B-I-V:
  1. Beschikbaarheid
  2. Integriteit
  3. Vertrouwelijkheid
- Veel gebruik legacy apparatuur en software *(patching is lastig vanwege o.a. downtime)*

Toenemende digitalisering in de maatschappij

Het Cybersecuritybeeld Nederland (CSBN) van 2021



Enkele interessante statements uit het CSBN 2021[1]:

- *"Digitale processen vormen het 'zenuwstelsel' van de maatschappij, omdat ze onmisbaar zijn voor het ongestoord functioneren daarvan."*
- *"Er zijn amper nog processen zonder digitale component."*
- *"De digitale en de fysieke wereld zijn niet meer van elkaar te onderscheiden."*

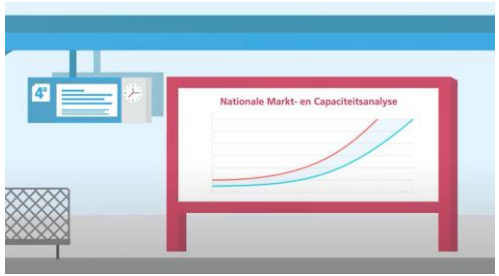
Twee sprekende voorbeelden op OT gebied:

1. Treindigitalisering bij NS en ProRail
2. Curtailment in elektriciteitsnetwerken

[1] Zie https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland

Toenemende digitalisering in de maatschappij

OT voorbeeld 1: treindigitalisering bij NS en ProRail[1]



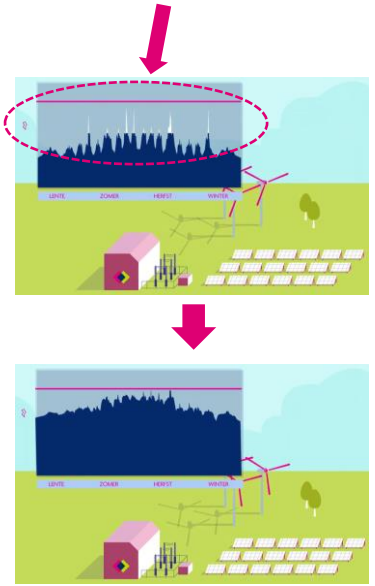
- Aanleiding:
  - Het huidige beveiligingssysteem uit de jaren '60 is aan vervanging toe;
  - Het aantal reizigers wordt in de komende jaren fors hoger;
  - Meer en efficiënter rijden op bestaande infrastructuur.
- Wat houdt deze digitalisering concreet in:
  - De technologie verplaatst van het spoor naar een computer in de trein;
  - Onderhoud en uitbreiding verschuiven naar het digitale domein;
  - *“Treinen worden steeds meer een soort rijdende computers”.*

- Dit resulteert in verbeterde betrouwbaarheid, punctualiteit en veiligheid voor reizigers...
- ...maar hoe zit het met digitale veiligheid:
  - *"Zo kunnen remweg en snelheid nauwkeuriger en automatisch worden bepaald."*
  - *"In plaats van naar buiten te kijken* [naar seinen]*, ziet een machinist voortaan op een scherm in de trein wat hij kan en mag."*

[1] Zie https://www.prorail.nl/programmas/ertms en https://werkenbijns.nl/nieuws/treindigitalisering-hoe-techniek-treinreizen-nog-veiliger-en-comfortabeler-maakt/

Toenemende digitalisering in de maatschappij

OT voorbeeld 2: curtailment in elektriciteitsnetwerken[1]



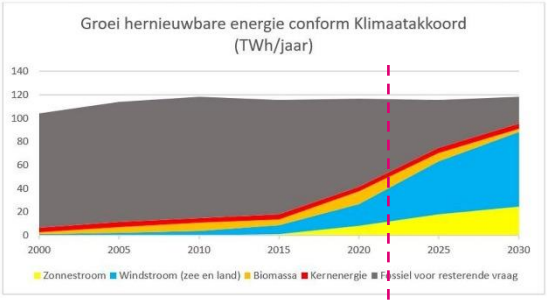
- Aanleiding:
  - De energietransitie gaat snel, steeds meer opwekking van stroom door windmolens en zonnepanelen;
  - Op sommige plaatsen is de maximale belasting van het elektriciteitsnetwerk bereikt;
  - Op die plaatsen kunnen niet direct nieuwe zonne- of windparken worden aangesloten.
- Wat houdt deze digitalisering concreet in:
  - Continu monitoren van de belasting van het elektriciteitsnetwerk;
  - Vanuit bedrijfsvoeringscentrum aansturen van zonne- of windpark om tijdelijk minder energie te leveren;
  - Via datacomverbinding commando's naar apparatuur in het zonne- of windpark.
- Zo kan naar verwachting tot 30% meer capaciteit aan duurzame opwek worden aangesloten...
- ...maar hoe zit het met digitale veiligheid:
  - *"Met deze sturing worden de hoogste pieken afgetopt door de productie van de opwekinstallaties te dimmen";*
  - Wat gebeurt er als een onbevoegd persoon toegang krijgt tot deze stuurmogelijkheid ?

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

Toenemende digitalisering in de maatschappij

Deze digitalisering introduceert nieuwe risico's

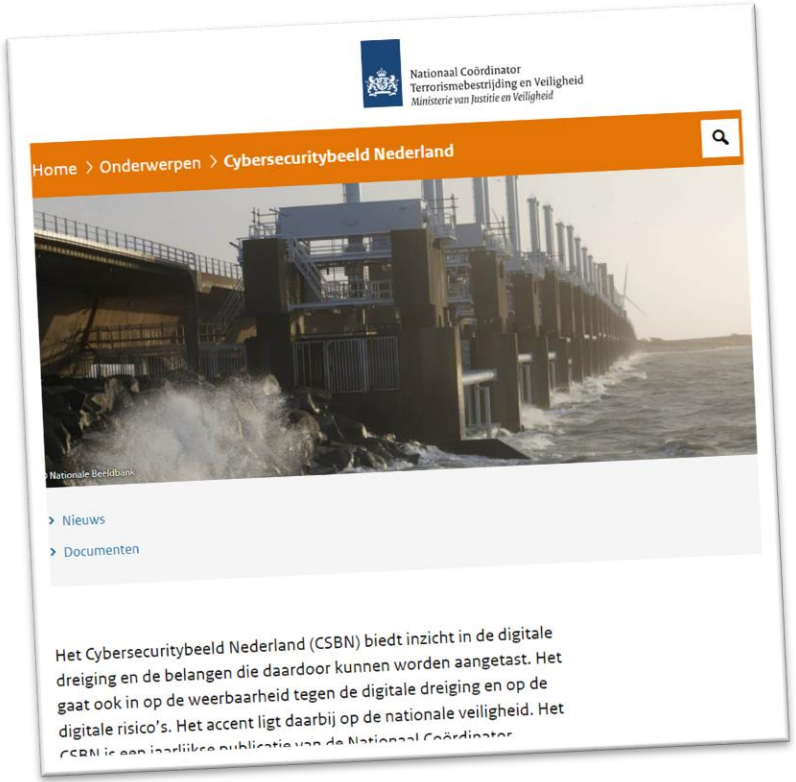
- Voor deze en veel andere voorbeelden van digitalisering geldt:
  - Het zorgt voor efficiëntere inzet van bestaande fysieke infrastructuur en daarmee maatschappelijke besparingen;
  - Ze zijn daarom deels onvermijdelijk; het is niet wenselijk of zelfs onmogelijk om die digitalisering volledig achterwege te laten;
  - Als je digitale beveiliging (in dit geval OT security) niet goed regelt, kan dat zeer grote gevolgen hebben.
- Nog heel veel andere voorbeelden van digitalisering bij netbeheerders ('smart grids'), zoals:
  - Op afstand meten en sturen van apparatuur in onderstations, bv. om storingstijden te minimaliseren;
  - Slim laden van elektrische auto's om extra piekbelasting te voorkomen.
- Belang wordt groter vanwege de 'elektrificatie van het energieverbruik'



Bron: Energeia

Toenemende digitalisering in de maatschappij

Wat betekent dit voor digitale veiligheid bij netbeheerders ?



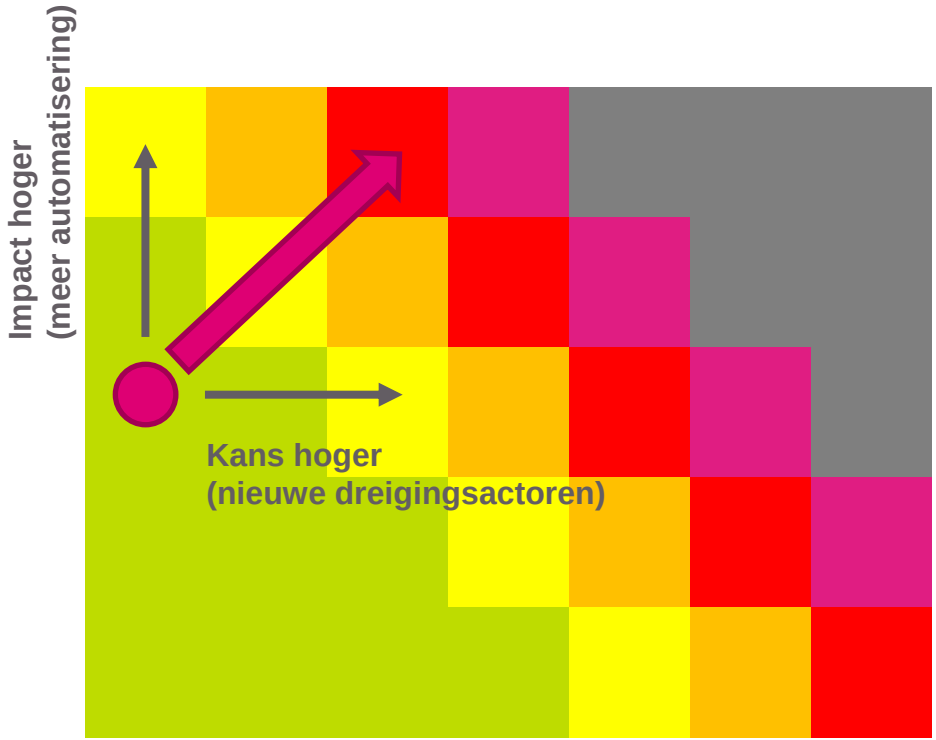
Nog enkele statements uit het CSBN 2021[1]:

- *"Uit het meest recente CSBN 2021 blijkt dat cyberaanvallen dit zenuwstelsel van de maatschappij aantasten."*
- *"Uit verschillende rapporten blijkt dat de weerbaarheid in vitale processen in Nederland soms tekortschiet."*
- *"Het afgelopen jaar zijn opnieuw wereldwijd vitale processen in de sectoren elektriciteit, water, olie & gas, chemie, voedsel, transport en de zorg doelwit geweest van digitale aanvallen door criminele groepen."*

[1] Zie https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland

OT (én IT) security risico's nemen toe

Dit geldt voor zowel de impact- als de kanscomponent van deze risico's



Geavanceerde aanvalscapaciteiten laagdrempelig toegankelijk

Cybersecuritybeeld Nederland 2019 [1]

Offensief cyberprogramma

Een ideaal businessmodel voor staten

AIVD, 2019 [2]

[1] Zie https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019/CSBN2019.pdf
[2] Zie https://www.aivd.nl/actueel/nieuws/2019/06/27/offensief-cyberprogramma-een-ideaal-businessmodel-voor-staten

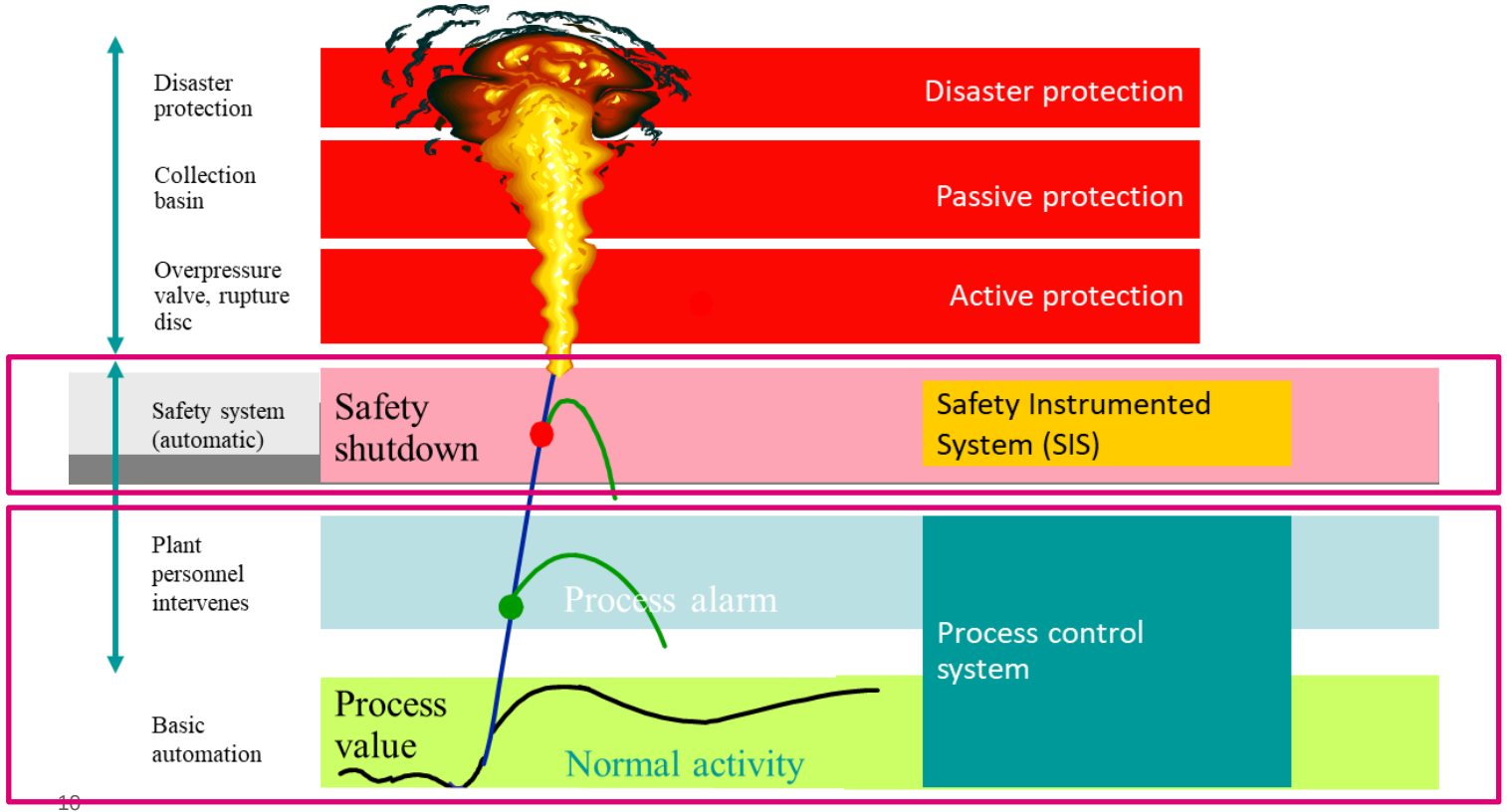
Safety systemen, een speciale categorie OT

In elektriciteitsnetwerken: beveiligingsrelais die bv. overbelasting van kabels voorkomen

vs.

Safety systemen, een speciale categorie OT

Als safety systemen niet meer werken, gebeuren er hele nare dingen



Safety systemen

'Standaard' OT

Safety systemen, een speciale categorie OT

Ook safety systemen worden actief aangevallen (Saudi Aramco in 2017)

MIT Technology Review

Sign in | Subscribe

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

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 triggering things like shutoff valves and pressure-release mechanisms.

[1] Zie https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

Safety systemen, een speciale categorie OT

Volgens Gartner wordt de dreiging nog veel groter[1]

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:

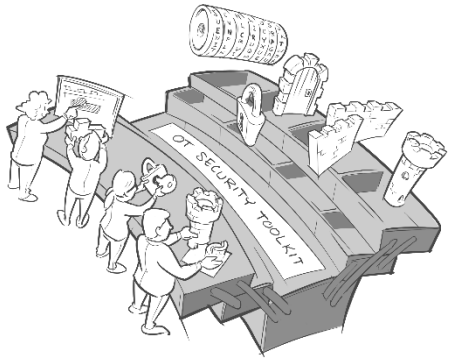
Newsroom

View all press releases

[1] Zie https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

Hoe houd je OT omgevingen zo weerbaar mogelijk ?

Voorbeelden van stappen die we bij Enexis hebben gezet



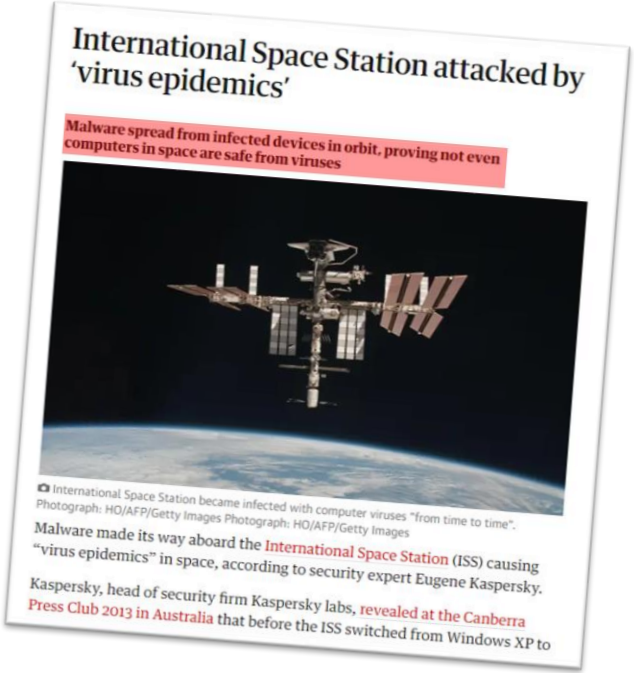
- Verbeteren awareness op alle organisatieniveaus
- OT strikt scheiden van de buitenwereld ('air gap')
- Eén risicomanagementproces voor conventionele én digitale risico's
- Opzetten van een ISMS
- Security-eisen structureel meenemen in aanbestedingen
- Verbeteren awareness op alle organisatieniveaus
- Netwerkzonering
- Inrichten van security monitoring, niet alleen richten op preventie
- Intensieve samenwerking in de sector, op NL en EU niveau (gefaciliteerd door het ENCS)
- Focus op digitale veiligheid van componenten aan de randen van systemen (want veel *legacy*)
- Had ik het verbeteren van awareness op alle organisatieniveaus al genoemd ?
- Véél testen: pentesten, red teaming enz.

OT strikt scheiden van de buitenwereld ('air gap')

Makkelijker gezegd dan gedaan...

- Zelfs het ISS is niet volledig 'air-gapped'[1]
- US subcommittee on National Security, Homeland Defense, and Foreign Operations (hoorzitting in mei 2011):

  "*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]
- Daarom aanvullende maatregelen nodig zoals:
  - Bewust maken van collega's op alle organisatieniveaus van de risico's;
  - Volledig gescheiden IT en OT werkplekken (dus twee aparte laptops);
  - Afspraken rondom verwijderbare media (USB sticks !) en bestandsuitwisseling.



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

Eén risicomanagementproces

OT security risicomanagement geïntegreerd in het bestaande proces met bowties

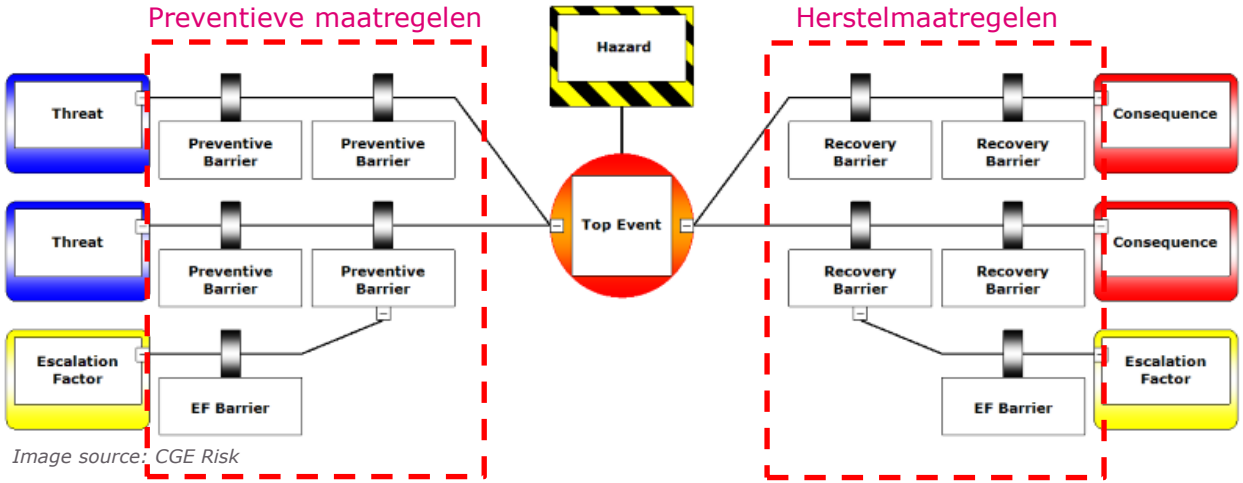


Image source: CGE Risk

Eén risicomanagementproces

Het selecteren van maatregelen voor risicomitigatie

- Gebaseerd op IEC 62443-3-3
- Preventieve maatregelen (links in de bowtie):
  - Tussen dreiging en kerngebeurtenis.
- Herstelmaatregelen (rechts in de bowtie):
  - Tussen kerngebeurtenis en consequentie;
  - Minimaliseren van de impact van de kerngebeurtenis.

Preventieve maatregelen:

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.

Herstelmaatregelen:

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.

Security-eisen structureel meenemen in aanbestedingen

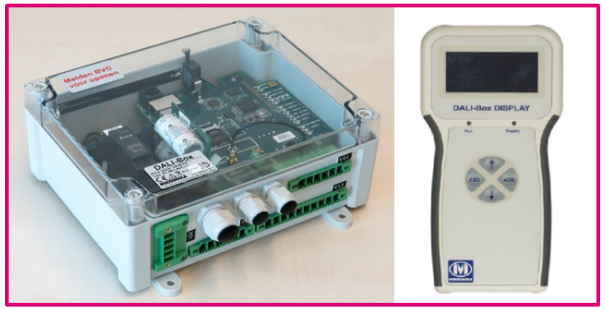
Digitale veiligheid is een vast onderdeel van alle aanbestedingen voor OT componenten

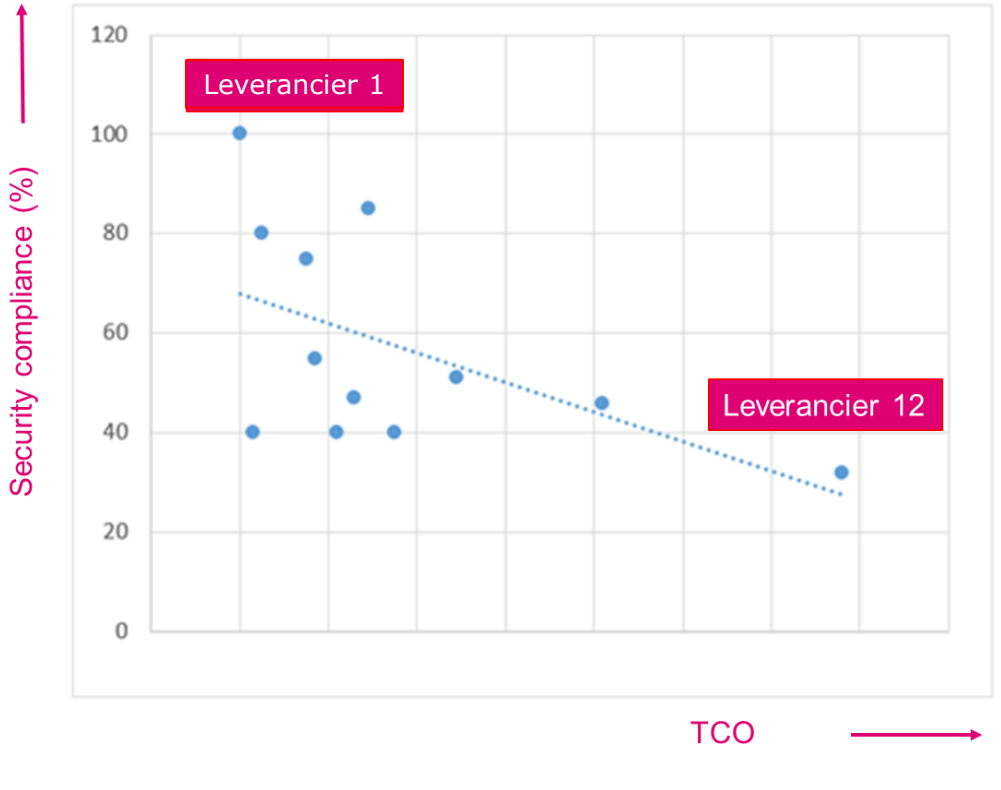
- Eisen aan ontwikkel- en supportproces leverancier:
  - Secure programming practices;
  - Security testing tijdens ontwikkeling;
  - Vulnerability management;
  - Hiervoor gebruiken we de IEC 62443-**4-1**.
- Eisen aan het product zelf:
  - Gebruikersauthenticatie en -autorisatie;
  - Cryptografische algoritmes en protocollen;
  - Logging en monitoring;
  - Hiervoor gebruiken we de IEC 62443-**4-2**.
- Digitale veiligheid fors verbeterd sinds 2014:
  - Alle ENCS leden gebruiken (bijna) identieke eisen in tenders;
  - Succesvol afronden pentest noodzakelijk om tender te winnen;
  - Betere digitale veiligheid ≠ hogere TCO !

Security-eisen structureel meenemen in aanbestedingen

Betere digitale veiligheid betekent niet altijd automatisch hogere kosten (tender 2015)

ENCS

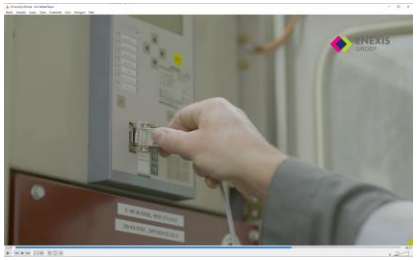




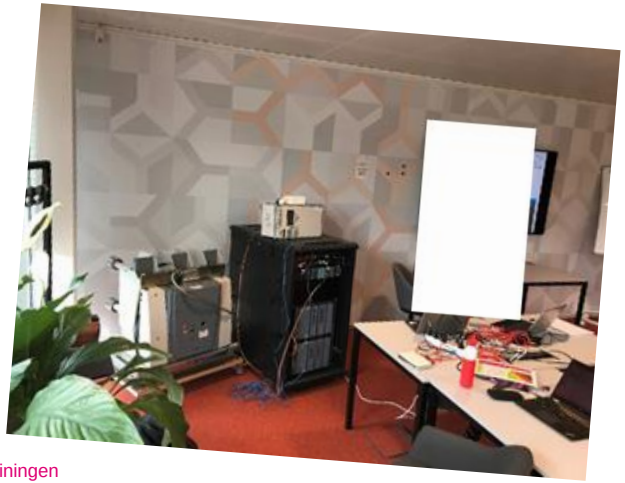
Verbeteren awareness op alle organisatieniveaus

Veel collega's begrijpen OT security risico's en hun invloed daarop onvoldoende

VEEL demo's



Filmpje over OT security risico's



Red/Blue trainingen

Mobiele OT security demokoffers

Zie ook onze visualisatie van OT security bij Enexis: https://jamdots.nl/view/284/Enexis-OT-security

Wat je zeker niet moet doen

Enkele mythes en gevaarlijke aannames rondom OT security

- *"We hebben geen verbinding met het internet"*
  - Is dat écht wel zo (nog steeds veel OT via Shodan zoekmachine[1]);
  - En is er ook geen indirecte verbinding, bv. via laptops, USB sticks of Teamviewer.
- *"Bij een digitale aanval zullen onze safety systemen de grootste impact voorkomen"*
  - Zie Triton/Trisis.
- *"Wij zijn geen doelwit, waarom zouden 'ze' ons willen aanvallen"*
  - Zie WannaCry/NotPetya; meeste getroffen bedrijven waren *collatoral damage*;
  - Het is voor criminelen een logische vervolgstap om op OT systemen gerichte ransomware te ontwikkelen.
- *"Hackers hebben geen verstand van OT systemen"*
  - Malware / Hacking / Ransomware as a Service;
  - Steeds meer OT-specifieke malware beschikbaar via internet (bv. BlackEnergy, Industroyer).

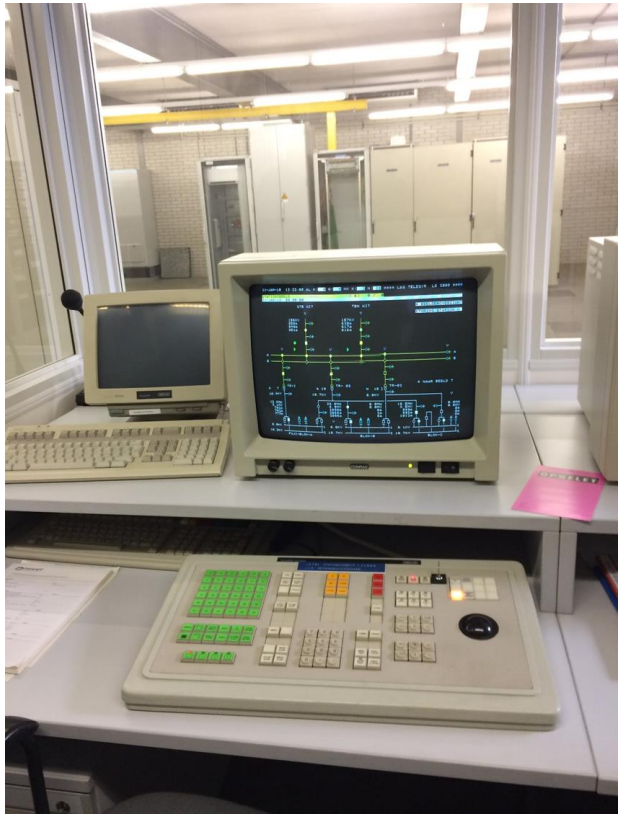
BLACK ENERGY

INDUSTROYER

[1] Zie https://www.shodan.io/

Wat je zeker niet moet doen

"Hackers hebben geen verstand van OT systemen": proprietary systemen vs. COTS



vs.

Siemens SIPROTEC

Twee voorbeelden van waar het fout is gegaan

Wereldwijd de eerste aanvallen op netbeheerders

Oekraïne, december 2015 en 2016

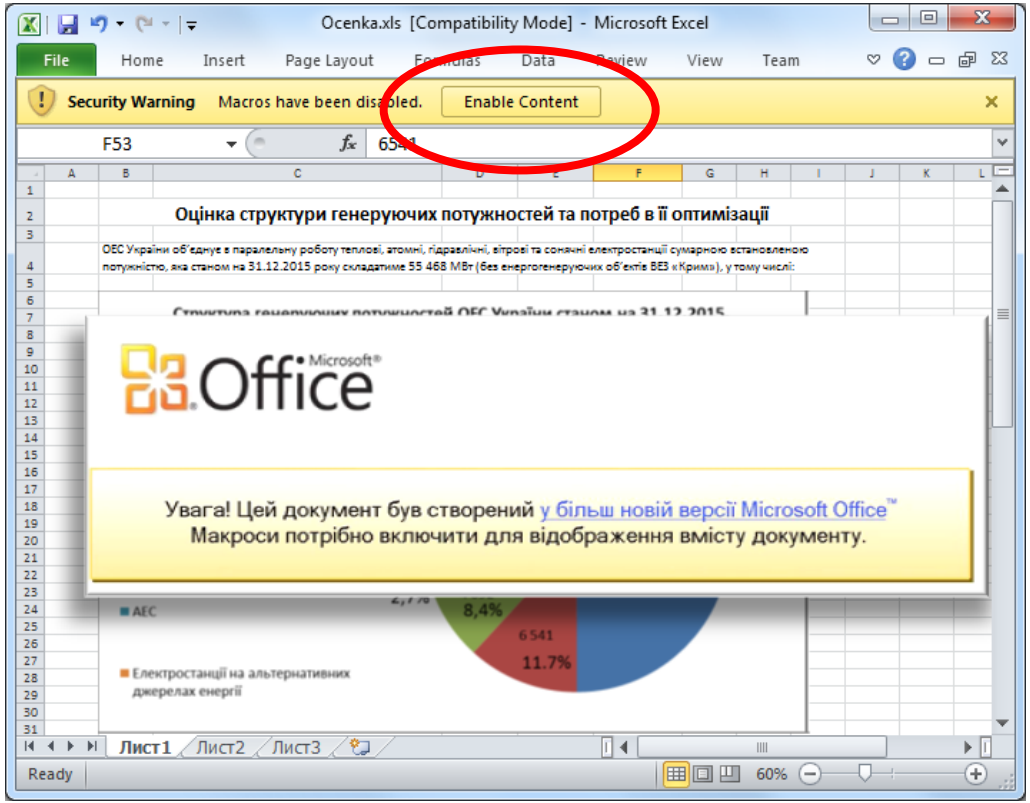
- Phishing mails
- Overname van SCADA
- Overschrijven van RTU firmware
- Stuurcommando's naar 30 stations
- DoS aanval callcenter

Geen elektriciteit bij 230.000 huishoudens gedurende ~6 uur[1].

[1] Zie https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Twee voorbeelden van waar het fout is gegaan

Wereldwijd de eerste aanvallen op netbeheerders



Twee voorbeelden van waar het fout is gegaan

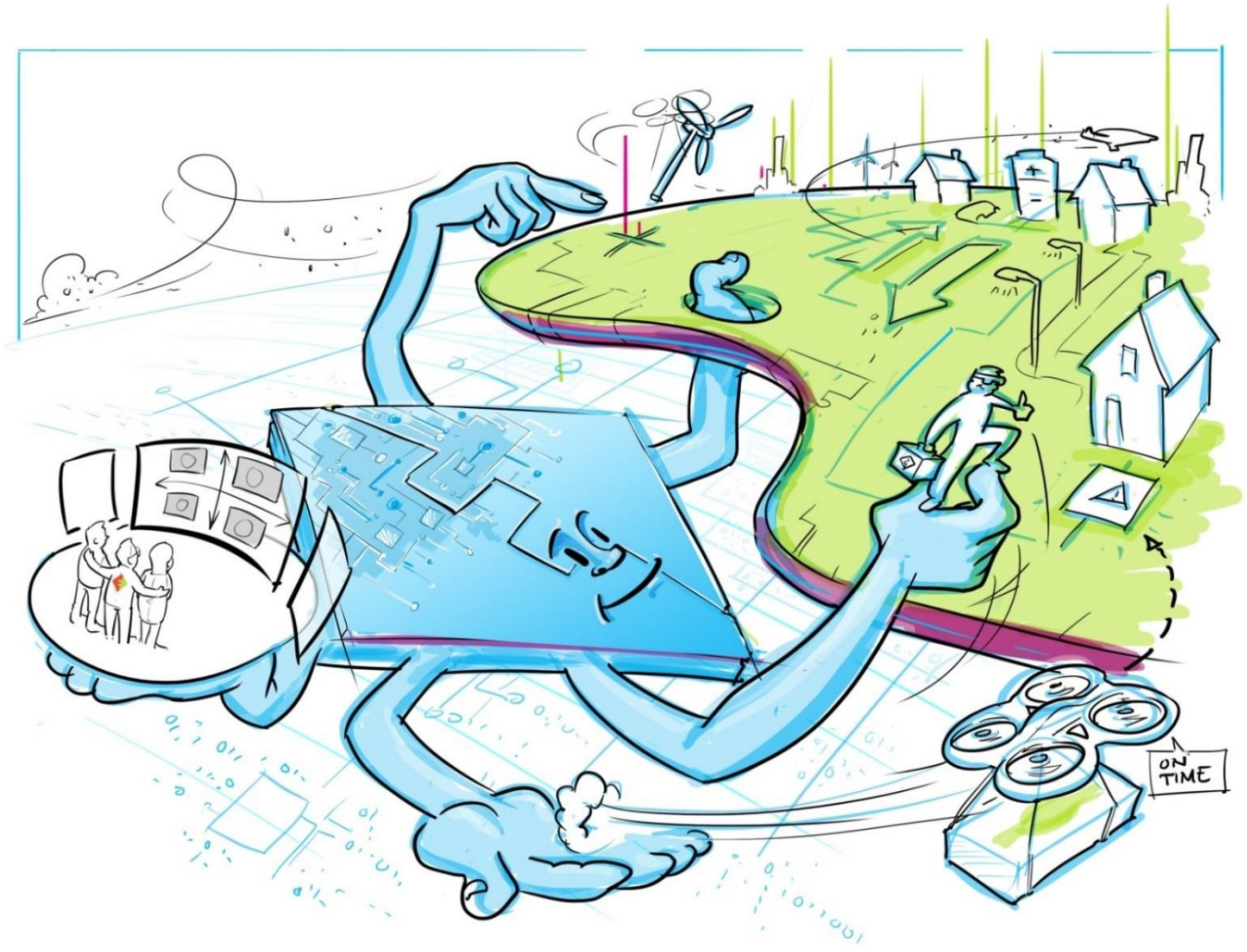
Colonial Pipeline in mei 2021

Het zuidoosten van de VS, mei 2021

- Eigenlijk een IT security incident; OT systemen niet geraakt
- Ransomware aanval
- Colonial Pipeline Company heeft de operatie stilgelegd
- Hackergroep DarkSide heeft ~100GB aan data gestolen
- Losgeld (deels) teruggehaald door de FBI

Tekort aan brandstof en hogere prijzen[1].

[1] Zie https://edition.cnn.com/2021/05/08/politics/colonial-pipeline-cybersecurity-attack/index.html



Philip Westbroek
OT security officer
Philip.westbroek@enexis.nl

Graphics by Wilco Prinsen
www.jamvisualthinking.com

Bijlagen

'Wet beveiliging netwerk- en informatiesystemen' - Wbni

Nederlandse implementatie van de EU NIS Directive

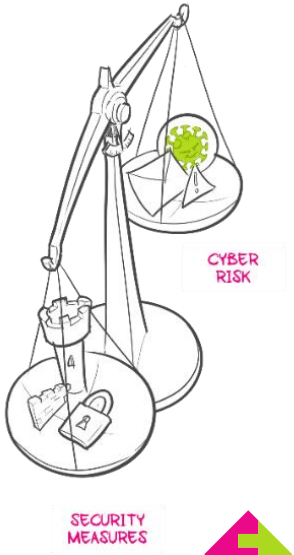
Zorgplicht: incidenten voorkomen en maatregelen nemen

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 veel mogelijk te beperken.

Meldplicht: incidenten melden

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.

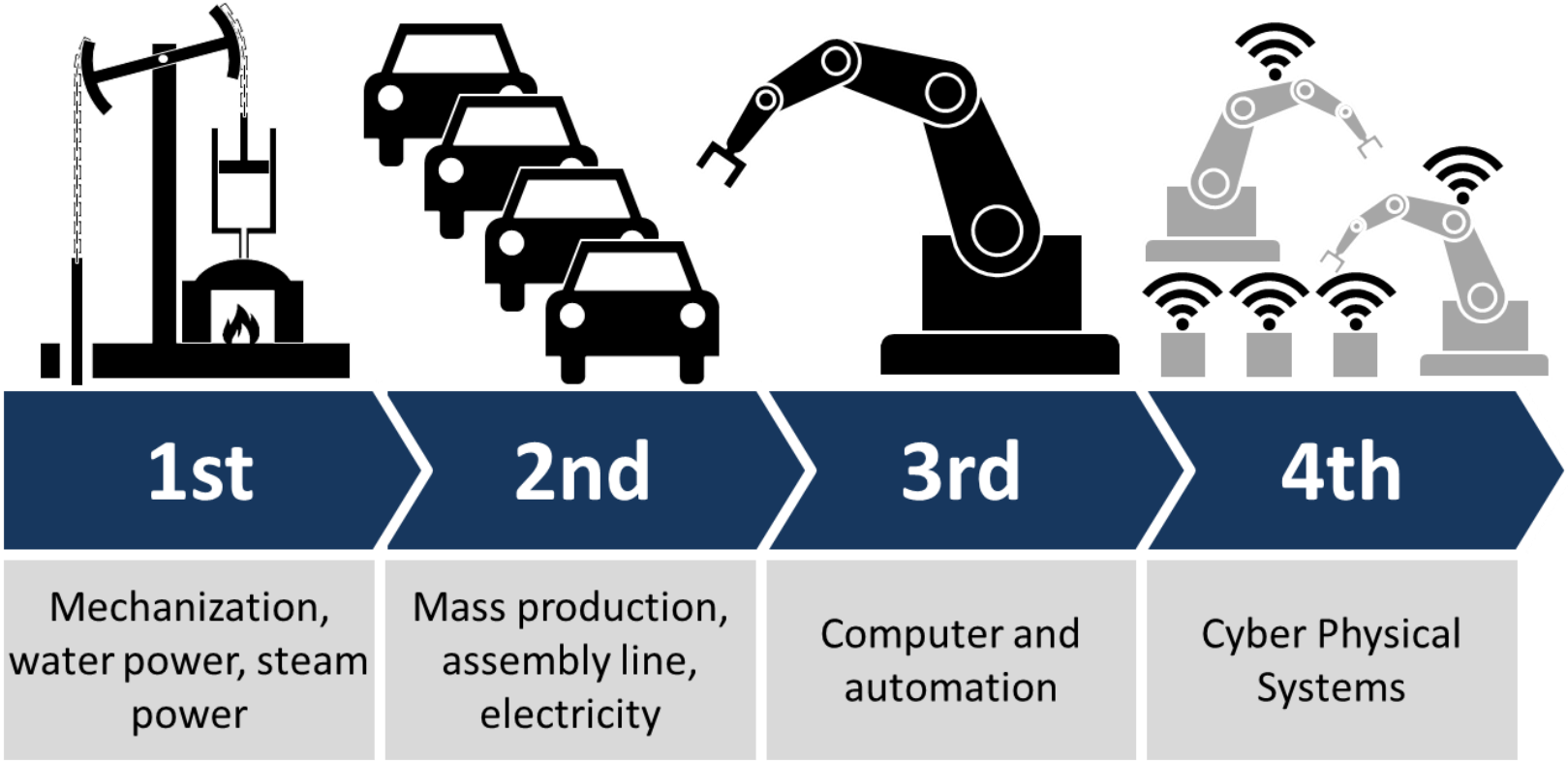
Agentschap Telecom
Ministerie van Economische Zaken en Klimaat



[1] Zie https://www.agentschaptelecom.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen

OT security risico’s nemen toe

Industry 4.0 zal deze situatie nog eens verergeren



Industry 4.0 / Image by Christoph Rosser; Source: AllAboutLean.com via Wikipedia Commons, licensed under Creative Commons Attribution-Share Alike International 4.0

Improving cybersecurity in Europe

Directive on security of network and information systems (NIS directive[1])

- The NIS Directive is the first piece of EU-wide legislation on cybersecurity.
- It provides legal measures to boost the overall level of cybersecurity in the EU.
- Boost the overall level of cybersecurity in the EU by ensuring:
  - Member States' preparedness;
  - Cooperation among all the Member States;
  - A culture of security across sectors that are vital for our economy.
- Operators of essential services identified by member states

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

[1] Zie https://digital-strategy.ec.europa.eu/en/policies/nis-directive

Improving cybersecurity in Europe

Latest developments - NIS2[1]

- Revised NIS directive (NIS2):
  - Improved version of the NIS directive;
  - Expanded scope; new sectors will be added based on their criticality for the economy and society;
  - Distinction between operators of essential services and digital service providers will be eliminated;
  - Security of supply chains and supplier relationships;
  - Improve the level of joint situational awareness.

[1] Zie https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2021)689333

Improving cybersecurity in Europe

Latest developments - Network code on cybersecurity (contents)

NIS directive	***Network code***
Take appropriate measures to manage risks	Risk management cycle *(Art 29)* Cybersecurity controls *(Art 30)* Management system *(Art 32)* Verification *(Art 33)*
Notify authority on incidents	Security operations center *(Art 38)* Reporting of incident, vulnerabilities, threats *(Art 38)* Incident response and crisis management *(Art 39 - 41)* Exercises at entity, national, regional level *(Art 43 - 45)*

Bron: European Network for Cybersecurity (ENCS)

Improving cybersecurity in Europe

Latest developments - Network code on cybersecurity (entities in scope)

Companies in the electricity sector	Markets & electricity associations	Government agencies
• TSO • DSO • Producer • Aggregator • Suppliers • Storage • Others	• NEMOs • Digital market platforms • ENTSO-E • EU DSO entity • RCC	• ACER • ENISA • NRA • CS-NCA • CSIRT

Bron: European Network for Cybersecurity (ENCS)