Secura
A BUREAU VERITAS COMPANY

OT Cyber security

BEYOND FIREWALLS

F.Ruedisueli | CISSP, GICSP, GRID, IEC62443 Expert
Principal OT Security Consultant @ Secura

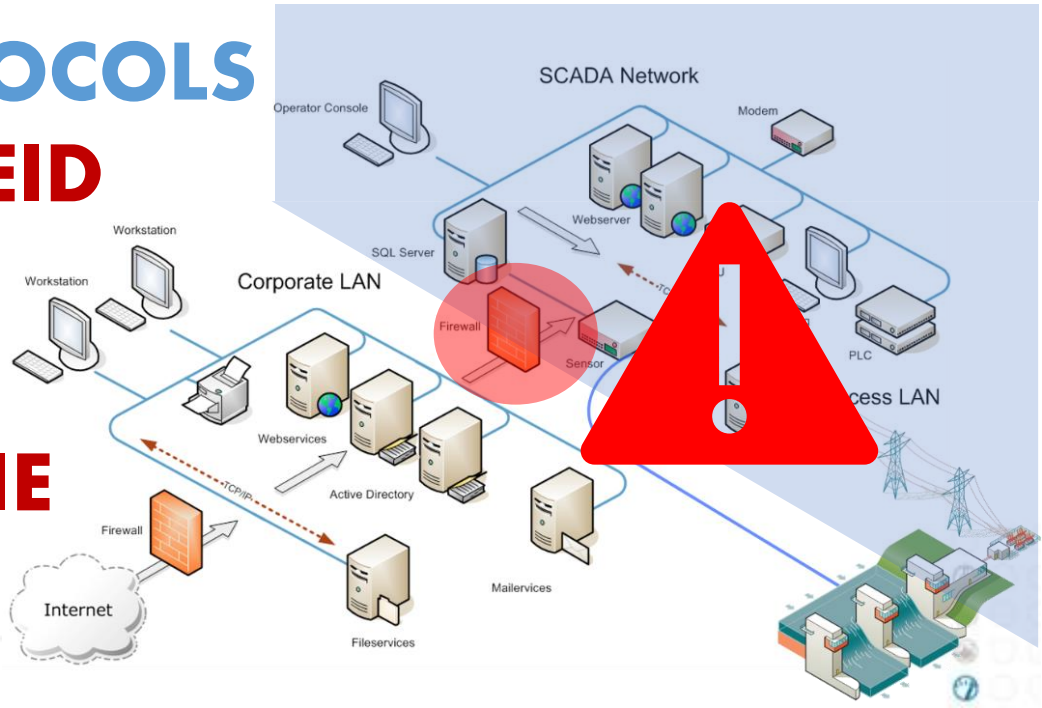
Industrial Cyber Security
10 oktober 2023 | Congrescentrum 1931, den Bosch

OT Security…..de uitdaging

SCADA
IT <> OT
VEILIGHEID
IEC62443
EIGENAARSCHAP
PATCHES
PLC
BUSINESS
CSIR
HMI
BIACS
DCS
AV & ENDPOINT SECURITY
LEGACY SYSTEMEN
OT-PROTOCOLS
NIS2
BIO
BESCHIKBAARHEID
RESTRICTIES
ISO27K
SLA
WORKSTATIONS
NIS WBNI
NIST CSF
SECURITY CONFIGURATIE

- OT Landschap
- Uitdagingen
- Normenkaders
- Verplichtingen

Industrial Cyber Security
10 oktober 2023 | Congrescentrum 1931, den Bosch



Wanneer doe je genoeg?

- Compliance is niet hetzelfde als security!
  - Normenkader als hulpmiddel
  - Doel: Beheersen van cyber security risico's

- Wanneer doe je genoeg?
  - Termen: "proportioneel", "redelijk" & "gepast"
  - Risico gedreven aanpak is nodig!

NIS 2:

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Waar begin je….???

- Doel: Verbeteren van cyberweerbaarheid

- Security is altijd een combinatie van mens, proces en techniek

Cyber security

Meer firewalls!!

Gisteren…

Kroonjuwelen?

ICT Afdeling?
Leverancier?

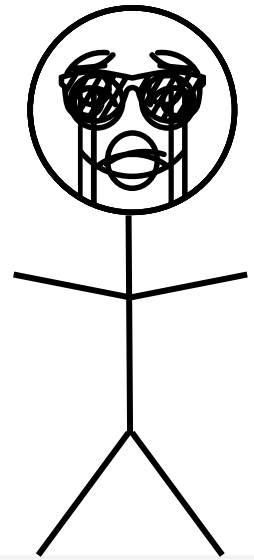
Risico’s &
Wetgeving

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

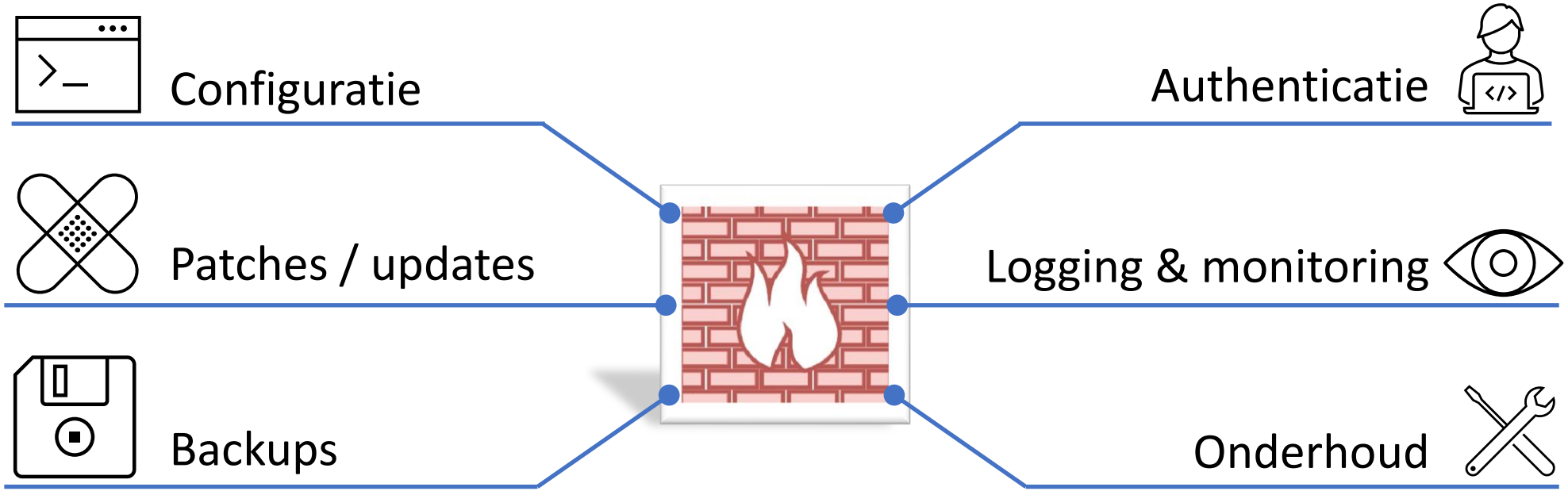
Processen

- Het maakt niet uit welke security standaard je gebruikt of aan welke set aan policies je moet voldoen, security processen staan aan de basis.
  - Zijn alle processen beschreven?
  - En worden ze ook echt in de praktijk uitgevoerd?
  - En regelmatig gecontroleerd?
  - En continu verbeterd?



Security Maturity

- Kortom, hoe volwassen is het OT security programma?
  - Want dit bepaald uiteindelijk hoe goed de “security” in de praktijk werkt.



Security Maturity

Het risico beheersproces

- Nog belangrijker: Hoe goed werkt het risico beheers proces?
  - Want alles tot 100% beveiligen is geen optie.
  - Waar zitten de grootste en onacceptabele risico's?
  - Welke risico kunnen we accepteren en hoe?

- Kortom: zonder dit **proces** is het lastig een risico gedreven aanpak te definiëren.

NIS 2:

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

Security Maturity

Verschillende niveaus van volwassenheid

Level 0. Non-Existent

Complete lack of any recognizable policy, process, control. Etc.

Level 1. Initial/Ad hoc

There are no standardized processes. Reactive and ad hoc decisions.
The overall approach to management is disorganized.

Level 2. Repeatable/Intuitive

Basic inventory of processes. Some documentation available. Processes are more regular

Level 3. Defined Process

Processes are established and defined. Formal and standardized. More consistent practices.

Level 4. Managed/Measurable

Processes measured, refined and adapted. It is integrated with communication. Management monitors and measures compliance. Processes are under constant improvement

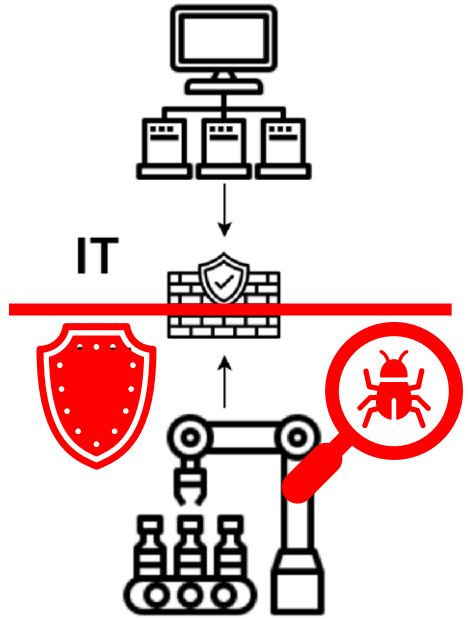
Level 5. Optimized

Processes have evolved to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Techniek

- Uitdagingen technische controls
  - Verouderde systemen, zwakke security opties, compatibiliteit, …

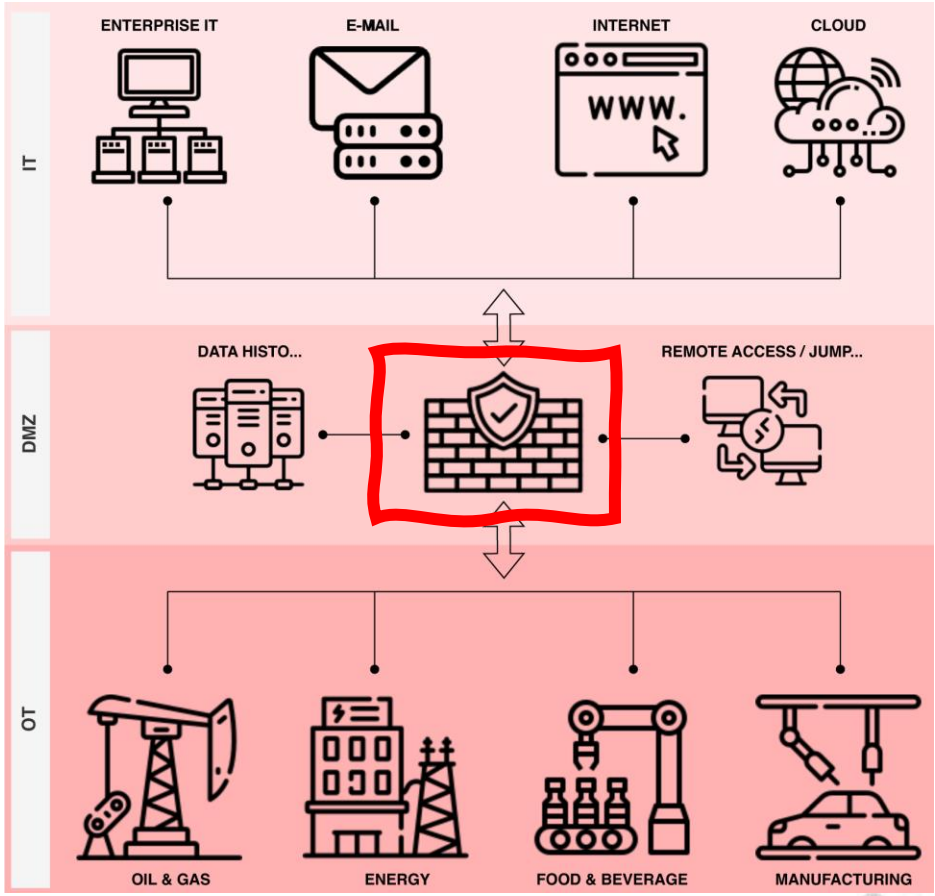
- Verschillende technische oplossingen zijn beschikbaar.
  - En alle hebben een bepaalde toegevoegde waarde
    - “Defense-in-Depth”
  - Maar als je ergens moet beginnen, start met een **betrouwbare scheiding tussen IT en OT**.
  - …en dat gaat iets verder dan alleen de firewall



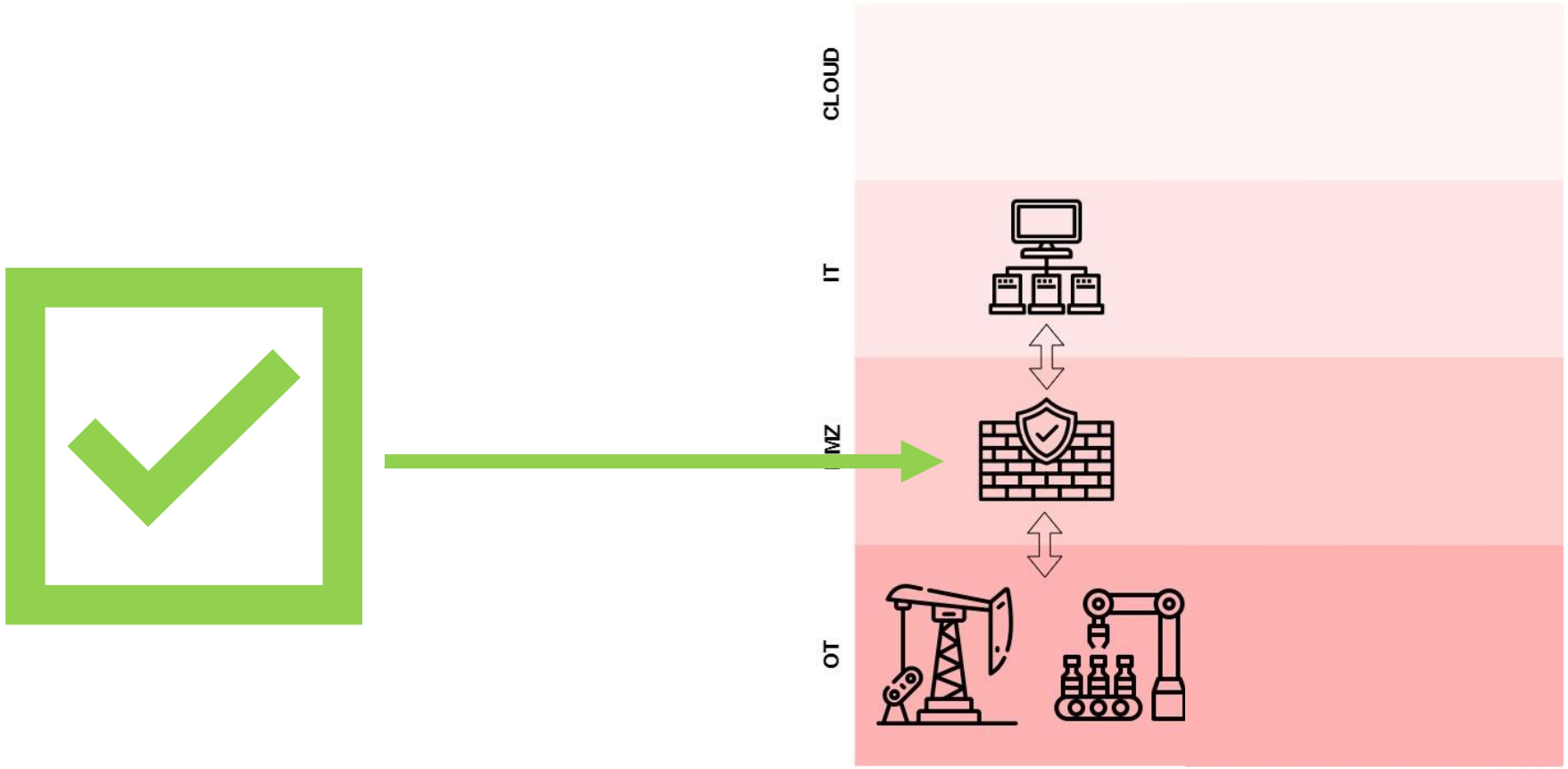
IT – OT scheidingsvlak – Stap 1

- Firewall: als technische preventieve oplossing
  - Hoe is deze geconfigureerd? (ACL).
  - Is enkel het verkeer dat nodig is, toegestaan?
  - En, dat wat nodig is, is dat veilig?
  - Worden bi-directionele ACL's gebruikt?

- Security processen firewall management
  - Log monitoring, connectiviteit scans, ACL hits.
  - Configuratie review, test, change management, security updates, etc.

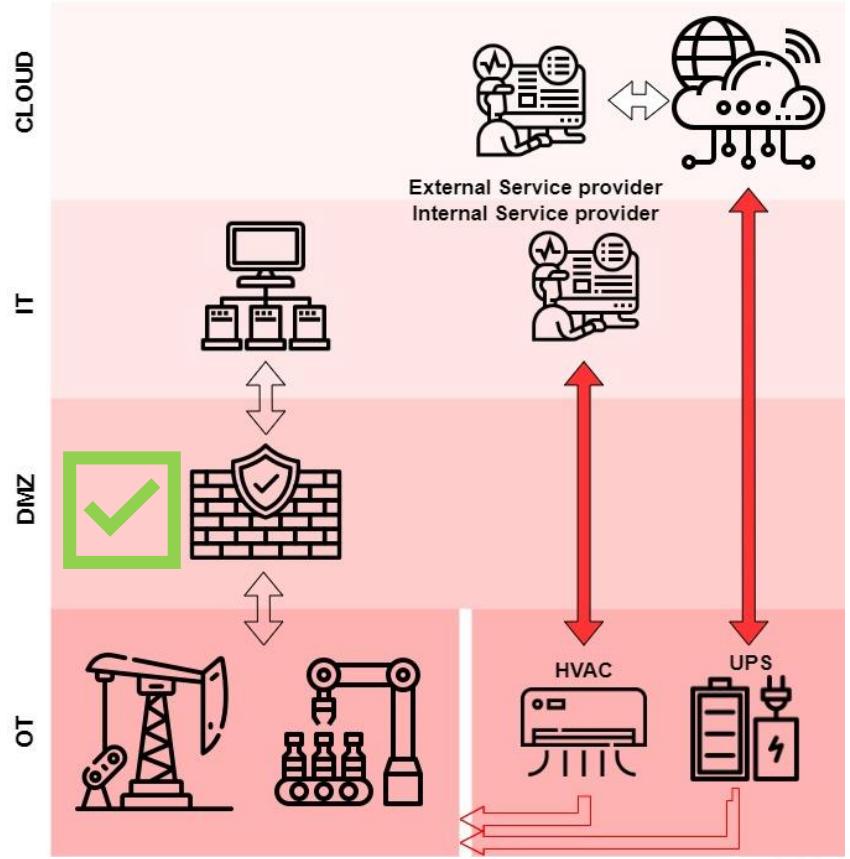


IT – OT scheidingsvlak – Stap 2



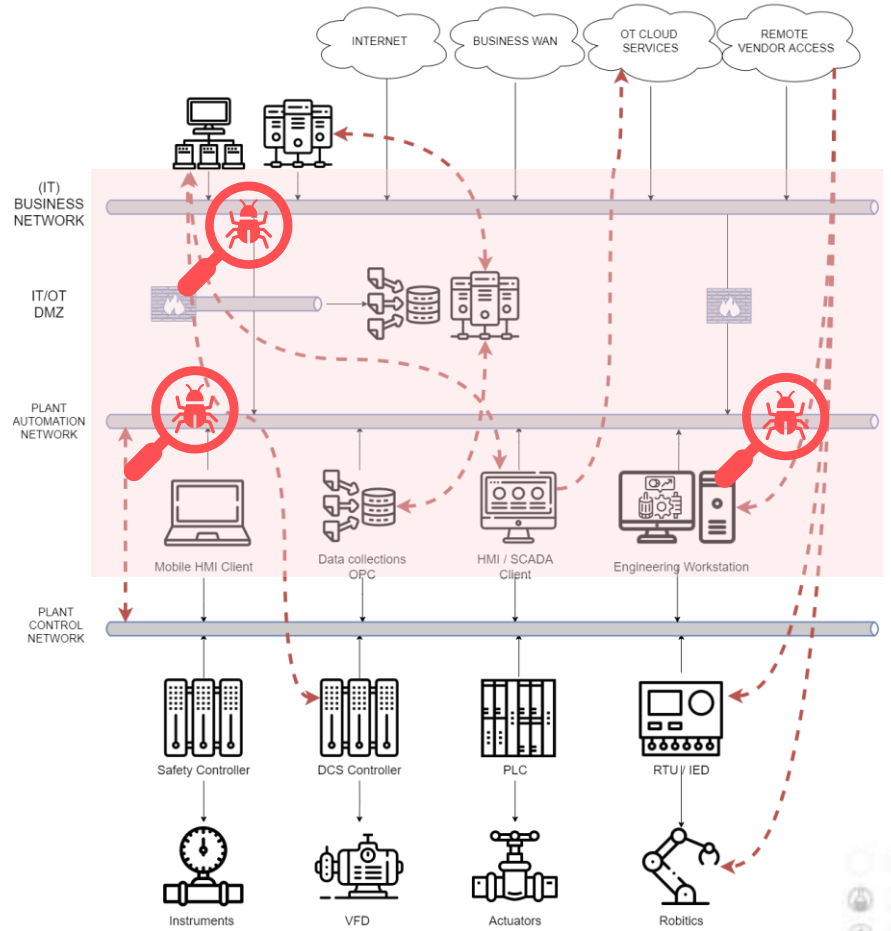
IT – OT scheidingsvlak – Stap 2

- Indirecte vormen van IT-OT connectiviteit
  - Bijvoorbeeld UPS, HVAC, toegangscontrole, BMS, ….
- “Dual homed” systemen
  - Systemen met meerdere netwerkkaarten, die mogelijk een firewall paseren
- (Onbekende) remote access mogelijkheden
  - Bijvoorbeeld (4G/5G) VPN gateways
- Draadloos
  - Bijvoorbeeld assets met extra Wi-Fi of Bluetooth opties



IT – OT scheidingsvlak – Stap 3

- Analyseren van OT netwerk verkeer
  - Voor en na de firewall, IT<> OT netwerk
  - OT focus op L3.5 (DMZ) en L3
- Detectie van:
  - Onbekende systemen
  - Onbekende communicatie stromen
  - Onveilige communicatie stromen
  - Cloud communicatie
- Maak een robuust scheidingsvlak!




Eindelijk klaar ?

Changes...

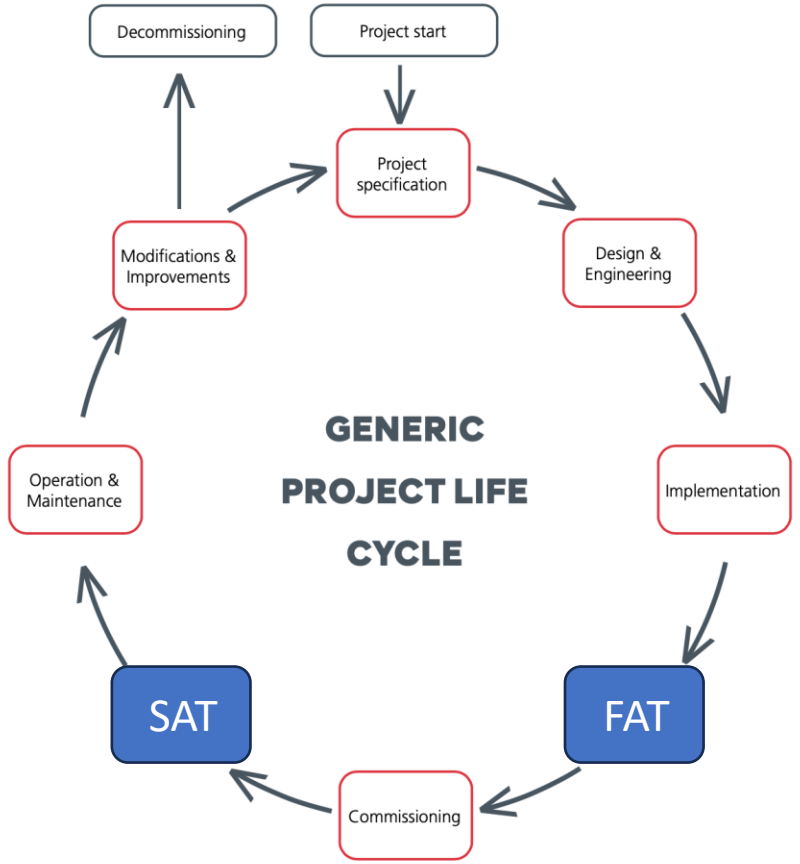
Nieuwe installaties,
Uitbreidingen, aanpassingen,
Nieuwe productie lijnen, upgrades...

Hoe om te gaan met aanpassingen?

- Hoe blijft je waarborgen dat er geen nieuwe risico's ontstaan?

- Onderdeel van de levenscyclus van projecten
  - Hoe volwassen zijn deze verander processen?
  - Vaak worden ontwerp vereisten wel getest tijdens een FAT/SAT
    maar blijft security onderbelicht

  - **Daarom een Cyber FAT & Cyber SAT**

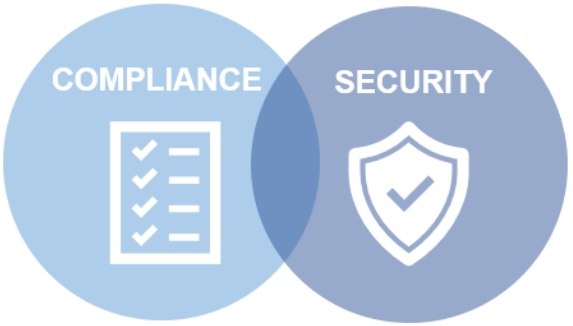


Industrial Cyber Security
10 oktober 2023 | Congrescentrum 1931, den Bosch

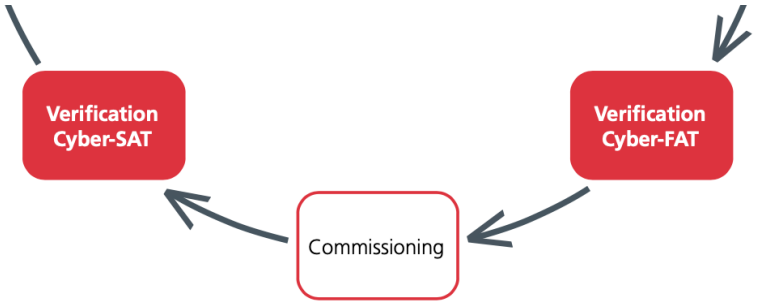
Stap 1 – Validatie

- **Compliance**
  - Is alles ontworpen, geïnstalleerd en geconfigureerd volgens de security vereisten & specificaties?
  - Programma van eisen of inkoop specificaties
    - Ontwerp moet voldoen aan….BIO/CSIR/IEC62443 en/of intern security beleid
    - Met minimale eisen als…. BBN 2, Weerstandsniveau 3, SL-T 2
  - Maar ook…
    - Risico gedreven aanpak, “best-practices”
    - Gedocumenteerde (en geaccepteerde) uitzonderingen.

Stap 2 - Verificatie



- Voldoet de **security** ook daadwerkelijk?
  - Met andere woorden: Werkt het ook zoals bedacht?
- Een FAT/SAT is de uitgelezen kans voor een actieve vulnerability scan en/of een penetration test.
  - Toetsen of bedachte maatregelen ook echt werken.
  - Zijn er misschien zaken over het hoofd gezien?
- Verbeteren voordat het in productie gaat!



Kortom…de conclusie

- OT bedreigingen en de noodzaak om deze te beheersen zijn duidelijk
  - Een **risico gedreven aanpak** is noodzakelijk
- Starten met:
  - Het in kaart brengen van **beveiligingsprocessen en het volwassenheidsniveau**
  - **Betrouwbare scheiding tussen IT en OT**
- In stand houden door:
  - Beheersen van risico's door veranderingen
  - Security reviews en penetration tests tijdens een **“CyberFAT/SAT”**
- **Conclusie: Een firewall is prima, maar geen “silver bullet”!**

Vragen?

Bezoek ons bij stand 13

Secura
A BUREAU VERITAS COMPANY

Contact:

Frank.ruedisueli@secura.com

https://www.secura.com/markets/industrial

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch