FHI INDUSTRIËLE AUTOMATISERING

OT Beveiliging in de Productiesector

Trends en Drijfveren voor Verandering

Thomas Vasen, BusDev NetSec

thova@hms.se / www.linkedin.com/in/tvasen

Productie Proces Automatisering

25 januari 2024 | Van der Valk Hotel, Vianen

Even voorstellen

> 1997

go:teborg

99,999%

> 2023 Anybus® BY HMS NETWORKS

Business Development Network Security

Wij creëren producten waarmee industriële apparatuur kan communiceren en informatie kan delen.

FHI INDUSTRIËLE AUTOMATISERING

Agenda

Status van CyberSecurity in (proces)productie

Reis door het OT Security landschap

Drijfveren voor verandering

Status van CyberSecurity in (proces)productie

- Het ziet er niet rooskleurig uit...

FHI INDUSTRIËLE AUTOMATISERING

France's Renault hit in worldwide 'ransomware' cyber attack

Issued on: 12/05/2017 - 17:31 Modified: 14/05/2017 - 15:20

Honda factory forced to close due to WannaCry virus

Posted on 23 Jun 2017 by Michael Cruickshank

Hydro

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday, March 19, 2019, impacting operations in several of the company's business areas.

APPLIED MATERIALS®

February 17th, 2023

Semiconductor industry giant says ransomware attack on supplier will cost it $250 million

German Autoparts Specialist, the Bilstein Group, Confirms Cyberattack

June 28, 2023

Cyberattack at SAF-Holland Causes Three Month Production Backlog

June 28, 2023

Toyota to resume plant operations from Wednesday, following system failure at a domestic supplier

MARCH 01, 2022

Ransomware attack temporarily shuts down Dole production, disrupts food supplies

FEBRUARY 23, 2023

Productie Proces Automatisering

25 januari 2024 | Van der Valk Hotel, Vianen

HMS

FHI INDUSTRIËLE AUTOMATISERING

WORLD ECONOMIC FORUM

TECH AND INNOVATION

Manufacturing is the most targeted sector by cyberattacks. Here's why increased security matters

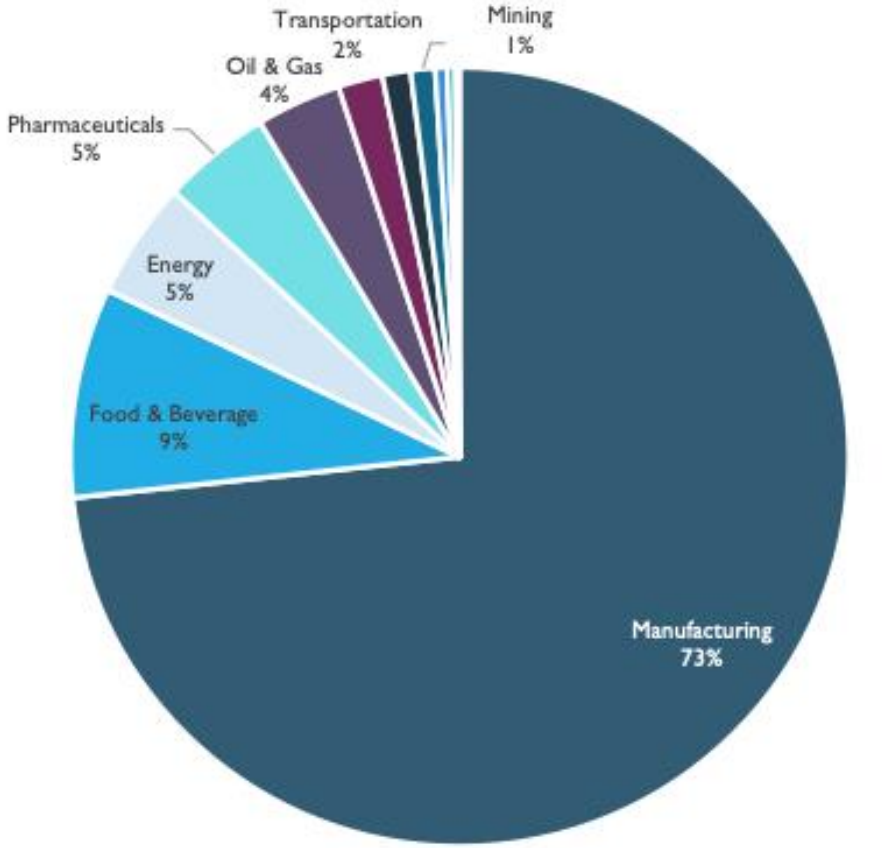
Mar 27, 2023

Hoewel de digitalisering de productiesector ten goede is gekomen, kunnen de voordelen teniet worden gedaan door de risico's, aangezien de productiesector het meest doelwit is van cyberaanvallen.

Er bestaat geen overkoepelende "gouden standaard voor cyberbeveiliging" voor fabrikanten in verschillende sectoren en landen, die rekening houdt met de onderlinge afhankelijkheid van de sector.

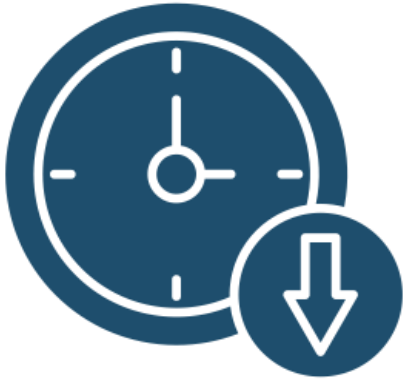
HMS

Ransomware is het grootste probleem…



DRAGOS

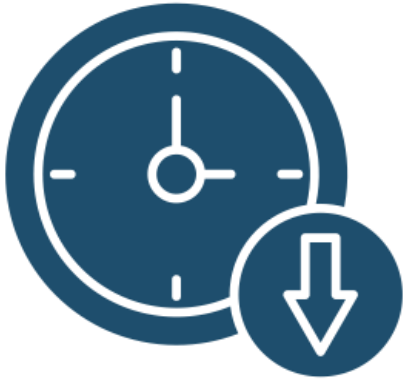
Veroorzaakt downtime en kost veel €€€



comparitech

Since 2018, ransomware attacks on the manufacturing industry cost the world economy $46bn in downtime alone

Maar OT-aanvallen zullen resulteren in erger!



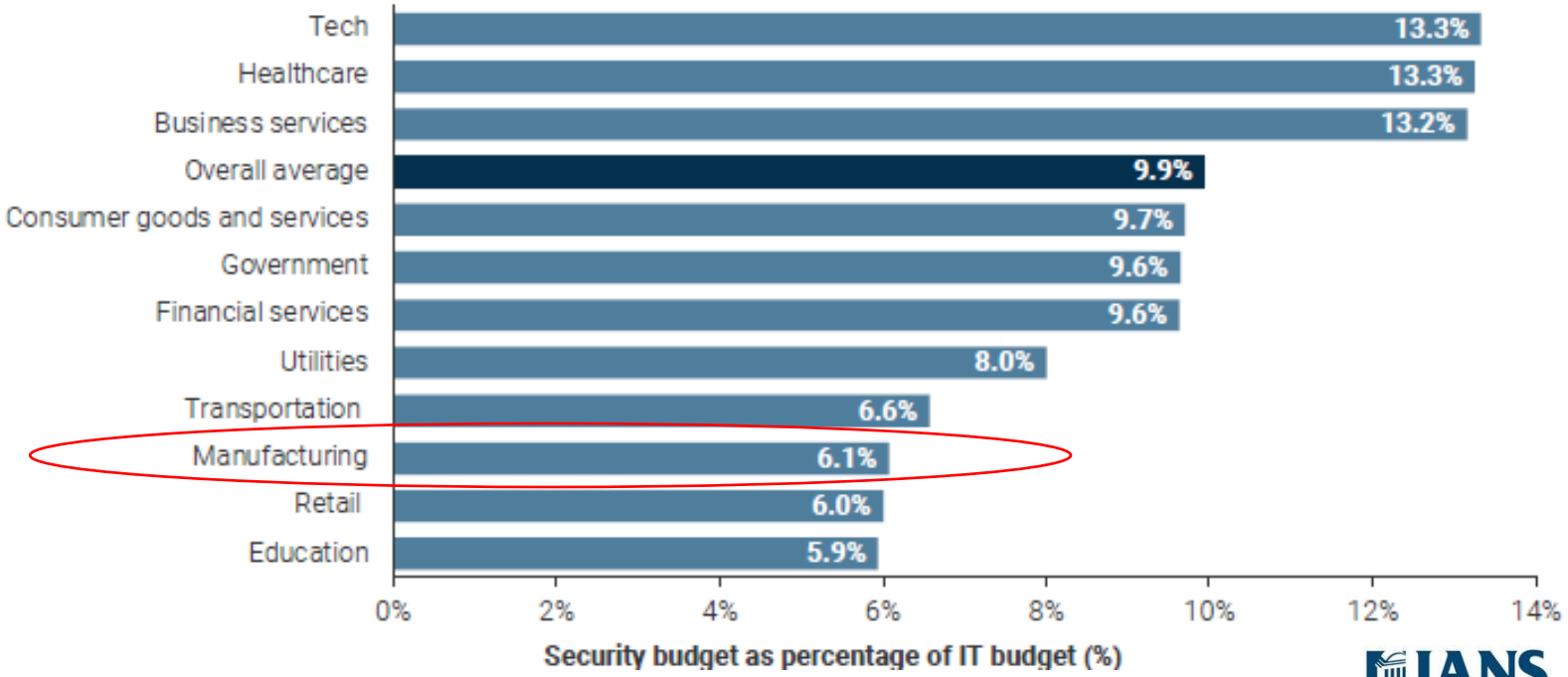
Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans

Waarom wordt de productie zo zwaar getroffen?

1. De CVSS-scores van de productie liggen 33% hoger dan het mondiale gemiddelde.

(CVSS = Common Vulnerability Scoring System, wat de ernst van bekende kwetsbaarheden betekent)

2. Beveiligingsbudget als percentage van het IT-budget is minder dan de helft...



IANS

Wat moeten we doen?

- Reis door het OT Security landschap

FHI INDUSTRIËLE AUTOMATISERING

Reis door het industriële cyberbeveiligingslandschap:

Consultancy & Training

AV/EDR/XDR solutions

OT/IT Separation firewalls

Remote Access Solutions

Asset Discovery & Vulnerability Management

Secure Authentication Solutions

Industrial Firewalls

Configuration Backup & Version Control

Threat Detection / Monitoring

SIEM / SOC / SOAR & Governance tools

USB scanning & management

Intrusion Protection Systems

Micro Segmentation / ZTNA / SDN

Data Diodes

Deception / Honeypots

HMS

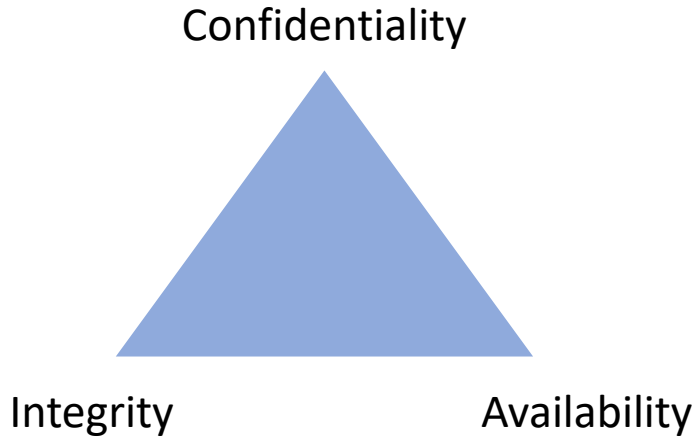
Afzonderlijke domeinen:

IT versus OT

CISO

1. **C**onfidentiality
2. **I**ntegrity
3. **A**vailability

Begroting

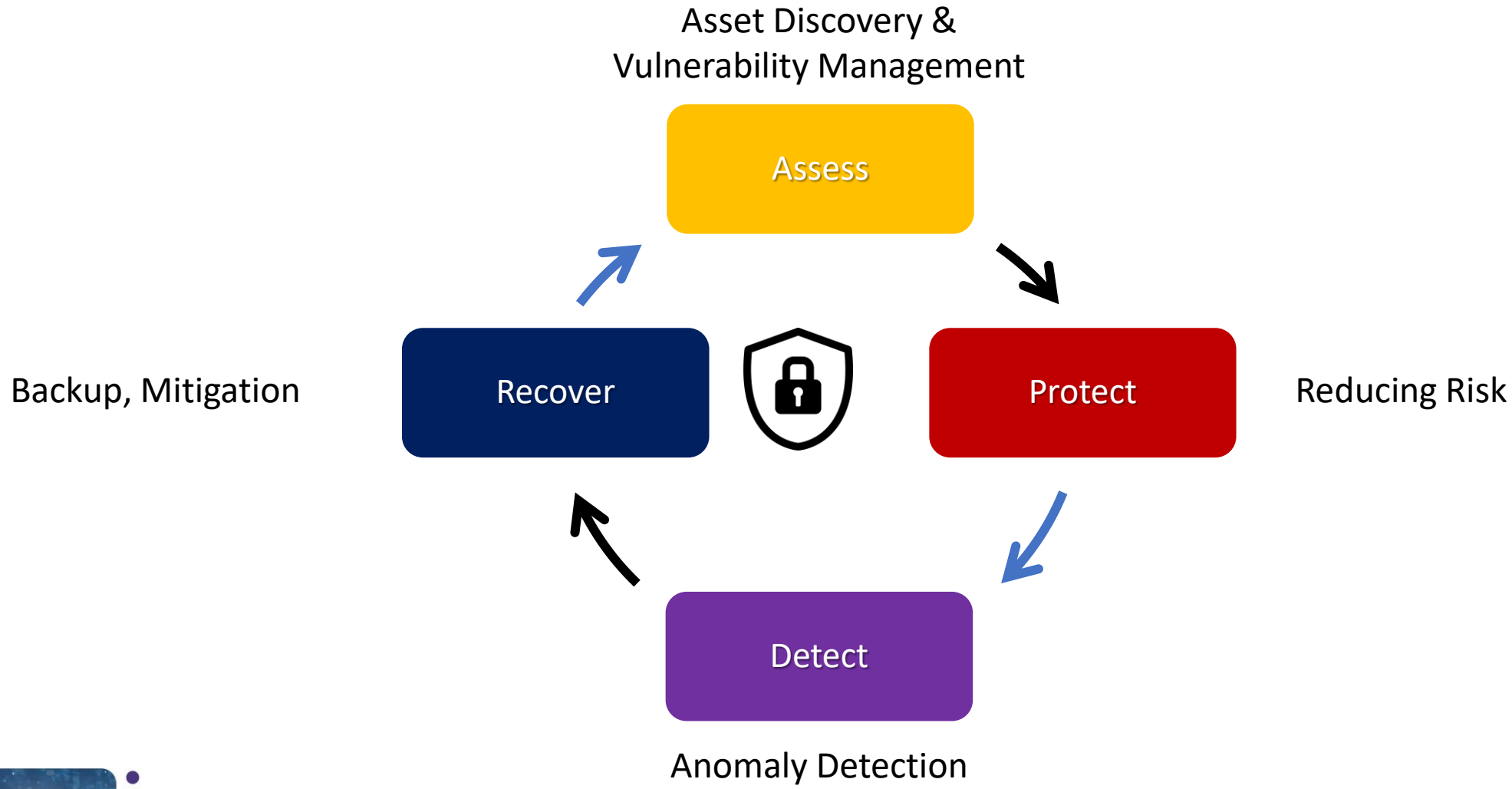


Operations Manager

1. **A**vailability
2. **I**ntegrity
3. **C**onfidentiality

Verantwoordelijkheid

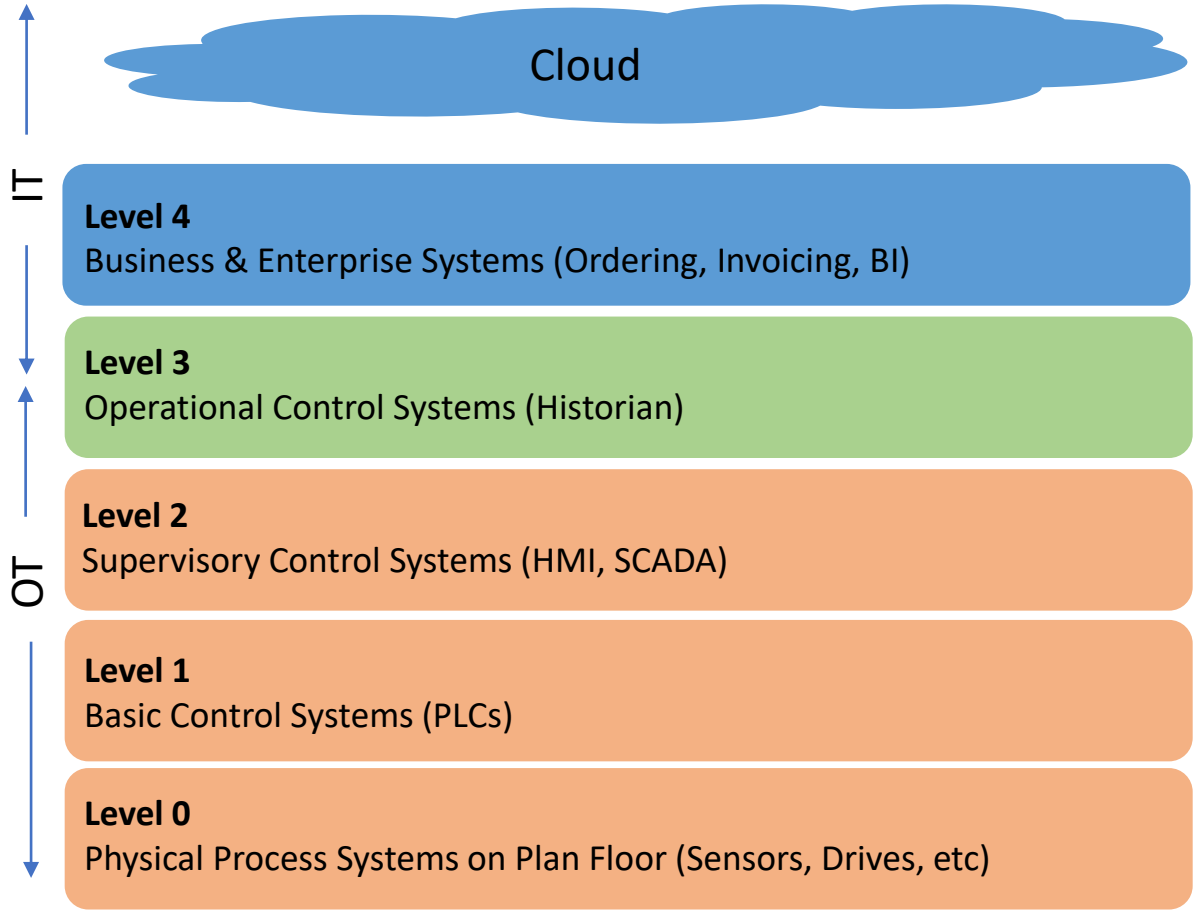
Vereenvoudigd – OT-beveiligingsprocessen:



Architectuur:
Purdue-model

- Gelaagd model om de toegang tot "OT" ver weg te houden
- 'Gemakkelijk' om toegangscontroles tussen lagen af te dwingen zonder het bedrijfsleven te hinderen

- Realiteit: Aantal lagen hangt sterk af van de volwassenheid
- Ook geen rekening houdend met de omvang en complexiteit van de "OT"-kant



Wat drijft verandering?

- Behalve een incident...
- Regelgeving & Standaardisatie

FHI INDUSTRIËLE AUTOMATISERING

Regelgeving en standaards/normen

1. NIS2 Direcitve

- Preppen, monitoren en rapporteren

2. ISA/IEC62443

- Segmentatie in zones en verharding van activa

EU Cyber Resillience Act

- Verharden & Weten

SBOM

- Weten, monitoreren

NIST SP 800-82

- Identificeren, beschermen, detecteren, reageren, herstellen

Machinery Directive

- Bescherming tegen manipulatie

HMS

1. NIS2 Directive

- **Doel:**
  - Een sterker en veerkrachtiger Europa
  - Uitgebreide reikwijdte van NIS1 – meer industrieën en sub leveranciers
- **Tijdlijn:**
  - Vervangt NIS1-richtlijn met harde deadline oktober 2024
  - Lokale voorstelen voor herziening verwacht in februari 2024 – maar zal niet lichter zijn
- **Impact:**
  - Boetes zoals in GDPR mogelijk
  - Leidinggevenden persoonlijk verantwoordelijk
- **Wat?**
  - Educatie, adequate bescherming, inspecties, incidentmelding, MFA, beleid, plannen, etc.
  - ISO27001 dekt het grootste deel, *maar niet binnen OT*

OTHER CRITICAL SECTORS

5. Manufacturing	(a) Manufacture of medical devices and *in vitro* diagnostic medical devices
	(b) Manufacture of computer, electronic and optical products
	(c) Manufacture of electrical equipment
	(d) Manufacture of machinery and equipment n.e.c.
	(e) Manufacture of motor vehicles, trailers and semi-trailers
	(f) Manufacture of other transport equipment

- **Vereist:**
  - Tools die zichtbaarheid en detectie bieden
  - Segmentatie ”best practices”
  - Educatie, processen, …

2. ISA/IEC 62443

- **Doel:**
  - Standaardisatie van processen, procedures en architectuur om meer cyberveilige industriële omgevingen te creëren.
  - Vermindering van de impact op inbreuk/incident

- **Wat?**
  - Deel 3-3: Architectuurverharding
  - Deel 4-1: Veilig ontwikkelingsproces
  - Deel 4-2: Productverharding

- **Tijdlijn:**
  - Gestart na 9/11
  - 62443-4-2 v1.0 gepubliceerd in 2019

- **Handhaving?**
  - Overname door branche specifieke organisaties
  - Landen nemen REQ's als nationaal richtlijn aan
  - Meestal klantgericht

IEC International Electrotechnical Commission

ISA GLOBAL CYBERSECURITY ALLIANCE

- **Vereiste:**
  - Beveiligingsmaatregelen, afhankelijk van de risicoanalyse
  - Operationele risico analyse
  - Architectuur met meer segmentatie

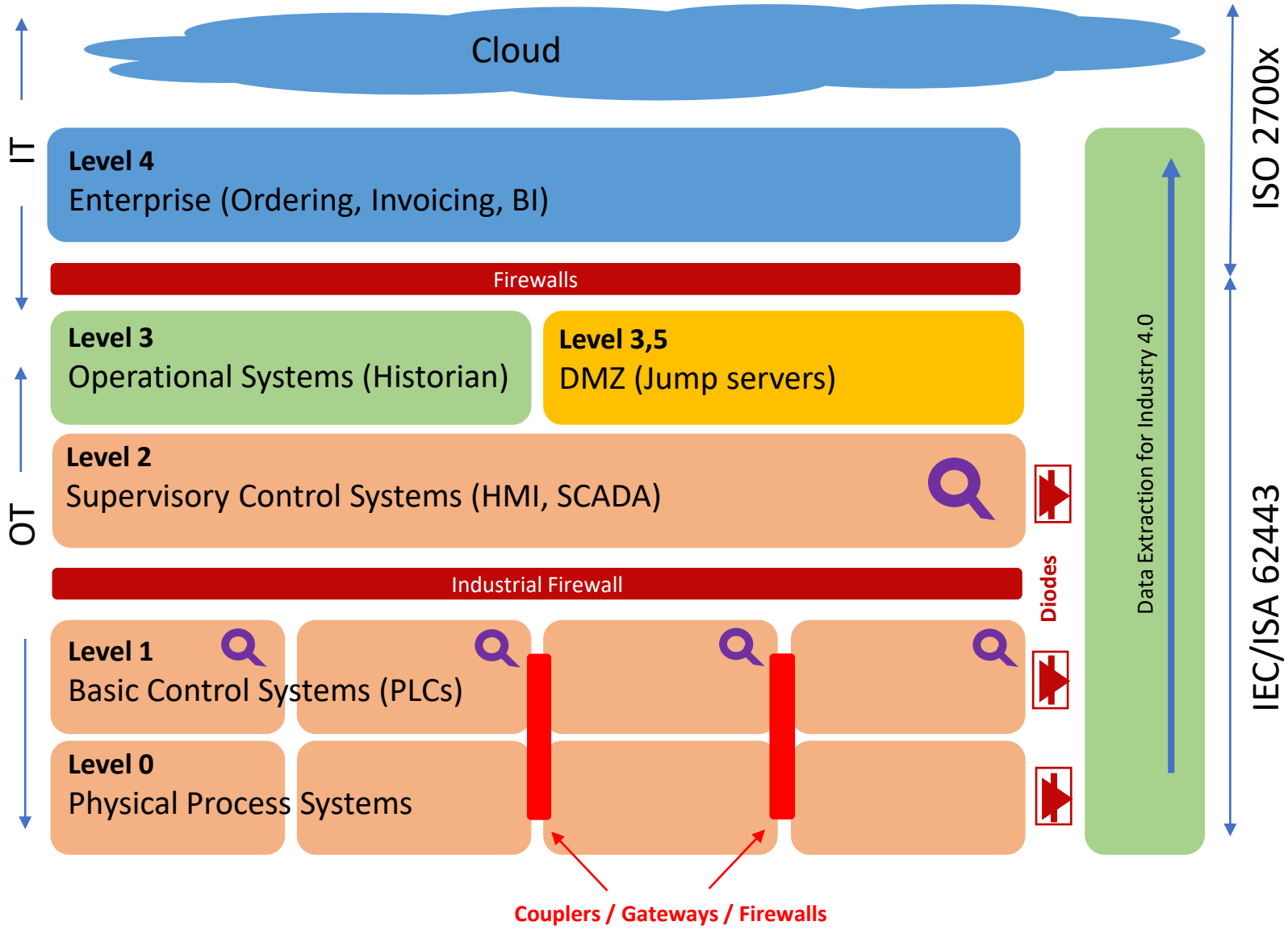
Beveiligingsarchitectuur:
Evolved Model

In operationele controle zones:

- Focus op activabeheer en dreigingsdetectie (NIS2)

Binnen proces domein:

- 62443 voegt Zones en Conduits toe aan deze architectuur
- Conduits zijn firewalls die apparatuur scheiden die in verschillende beveiligingsniveaus is ingedeeld
- Beheren het verkeer en verminderen het risico op zijdelingse bewegingen bij een inbreuk/incident
- Optioneel: Diodes om veilig data weg te sluizen



Conclusies

- **De bedreigingen nemen snel toe**
  → impact zal verschuiven van € alleen naar veiligheidsrisico's
- **Er bestaan oplossingen, maar het aanbod en de implementaties zijn complex**
  → samenwerking tussen IT en OT is de sleutel tot succes
- **Regelgeving en standaarden/normen helpen**
  → Maar…

ABIresearch®
THE TECH INTELLIGENCE EXPERTS

"As neither IEC 62443 nor other standards are mandated, it is ultimately down to choice. "

PHIL SEALY
Research Director

Hardware Meets Software™

thova@hms.se

LinkedIn

Stay Connected!

www.hms-networks.com