



IACS & CYBERSECURITY CONFERENCE



April 15th 2025 • Amersfoort • The Netherlands



Risicomanagement in OT

Beheer de dreigingen, bescherm de operatie



Agenda

- Eerste 10 minuten – Theoretische context van OT Security Risico.
- Vervolgens 20 minuten – Toepassing van tools en voorbeelden.
- Daarna 15 minuten – Gelegenheid voor vragen.



De (meest gebruikte) industrie standaarden voor security risico management in OT omgevingen

IEC 62443 serie

- Een internationale standaard voor beveiliging van Industrial Automation and Control Systems (IACS). Richt zich op defense-in-depth, risicogebaseerde benaderingen en veilig systeemontwerp.

Specifieke standard over risico: IEC 62443:3-2

Belangrijkste kenmerken:

- OT-specifiek: is sterk gericht op de behoeften van operationele technologie.
- Zones en conduits: maakt gebruik van de concepten van zones en conduits om netwerken te segmenteren.
- Beveiligingsniveaus: biedt een methode om beveiligingsniveaus te definiëren voor verschillende delen van het OT-netwerk.

ISO 27000 serie

De ISO 27000 serie biedt aanbevelingen voor best practices op het gebied van informatiebeveiligingsbeheer: het beheer van informatierisico's door middel van maatregelen (controls).

Specifieke standard over risico: ISO 27005

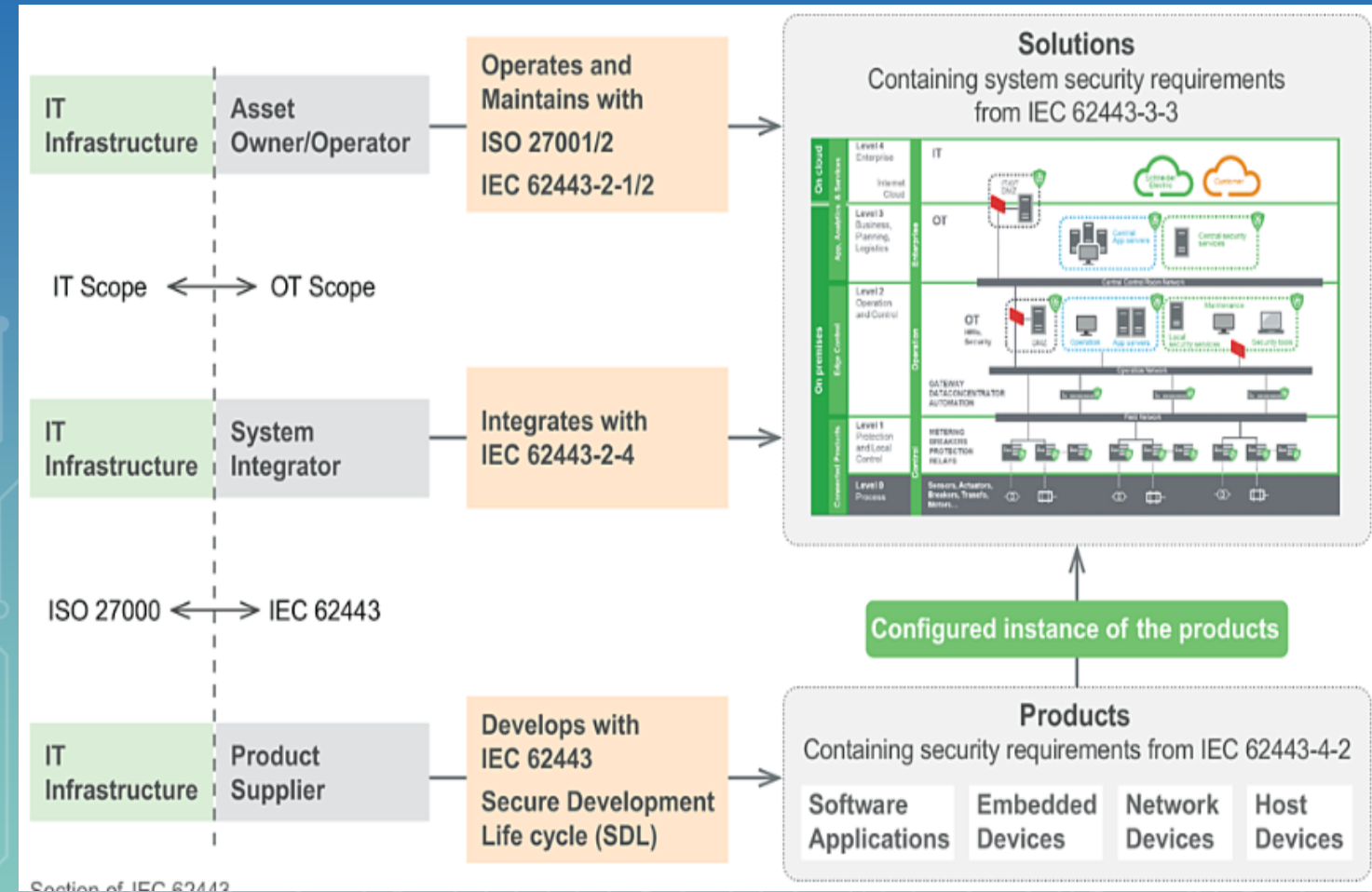
Belangrijkste kenmerken:

- IT/OT Algemeen: toepasbaar op cloud-, IT- als OT-omgevingen.
- Breed toepassingsgebied: ontworpen voor cloud, IT en OT assets en data (privacy).
- Risicomanagementkader: structuur voor risicobeheer



Verschillen en overwegingen bij gebruik

- IEC 62443-3-2 kan worden gezien als een gespecialiseerde uitbreiding van ISO 27005 voor OT-omgevingen.
- U kunt ISO 27001 en 27005 gebruiken als overkoepelend raamwerk voor het risicomanagement van uw organisatie en vervolgens IEC 62443-3-2 toepassen voor de gedetailleerde risicobeoordeling van het IACS, IEC 62443 geeft daarbij OT-specifieke tools.



Section of IEC 62443

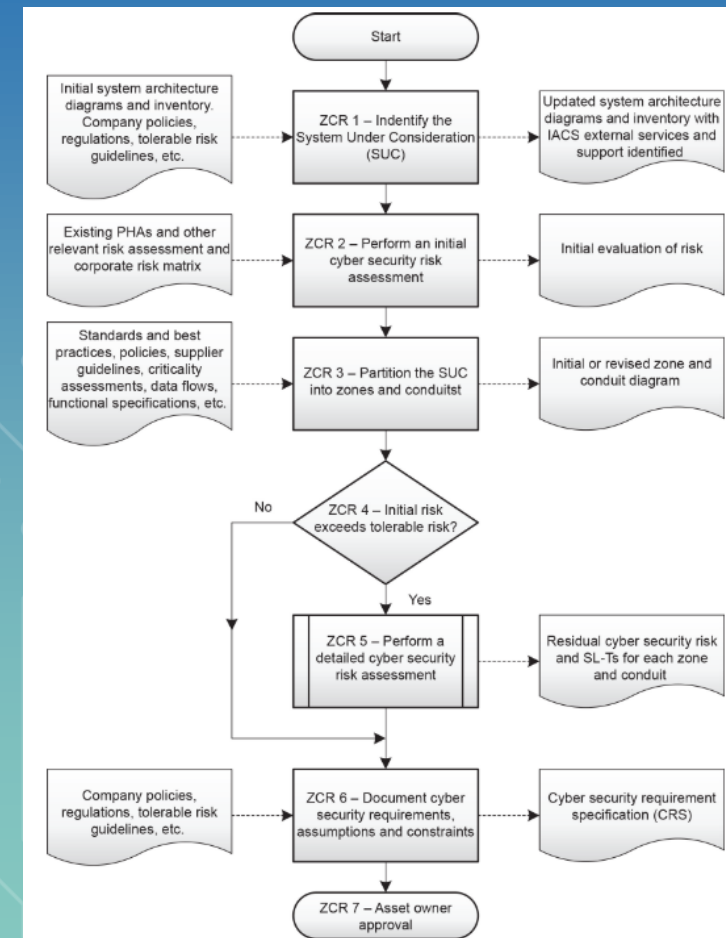


De high level risico beoordeling/initial risk assessment

Hiermee kunt u op relatief snelle wijze de grootste risico's binnen een automatiseringssysteem bepalen.

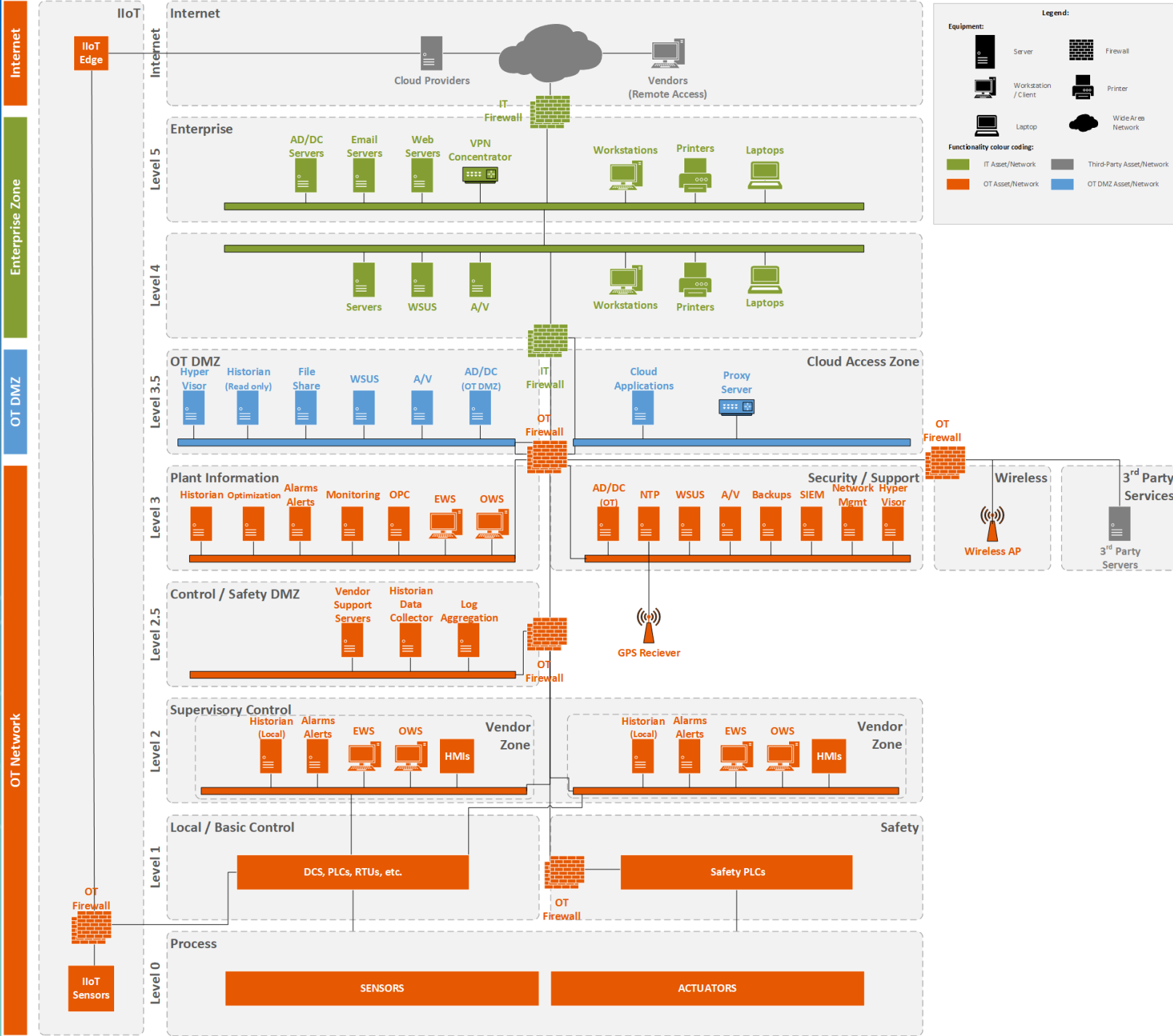
Activiteiten:

- Identificeer het system under consideration (SuC)
- Doe een hoog over risico analyse
 - BIA, worst case incident scenario:
 - Maximale impact
 - Threat likelihood (kans) = 1 -> "Assume breach"
- Pas het principe van zones en conduits toe op het het SuC o.b.v.
 - Risico en target security levels.
 - Functionele en technische design specificaties van het systeem
 - Geografisch/lokatie van systeem componenten
- Is het risico groter dan het geaccepteerde risico?
 - Check de RAM
 - Doe dan een detail risico beoordeling



Identificeer het systeem under consideration (SuC)

Voorbeeld van een Netwerk topologie / referentie architectuur





Enkele aandachtspunten

1. Zorg voor **consistentie** met het bestaande risico beleid.

Gebruik:

- Business impact criteria (voor de BIA).
- Criteria voor het weergeven van kans.
- Risico matrix en risico acceptatie criteria.

Maar let op:

1-op1 **hergebruik** is vrijwel onmogelijk.

- Berekening van kans vaak vertaald vanuit functional safety waarbij:
 - functional safety/SIL = Kwantitatief
 - cybersecurity = Kwalitatief
- De impact is te hoog, want gebaseerd op enterprise risk.

SIL Level	Probability of Failure on Demand (PFD)	Risk Reduction Factor (RRF)
SIL 1	10^{-1} to 10^{-2}	10 to 100
SIL 2	10^{-2} to 10^{-3}	100 to 1,000
SIL 3	10^{-3} to 10^{-4}	1,000 to 10,000
SIL 4	10^{-4} to 10^{-5}	10,000 to 100,000

		Consequence				
		Minor Problem easily handled by normal day to day processes	Some Disruption Possible (e.g., damage between \$500K and \$1 Million)	Significant Time & Resources Required (e.g., damage between \$1 Million and \$10 Million)	Operations Severely Damaged (e.g., between \$10 Million and \$25 Million)	Business Survival is at Risk (e.g., damage > \$25 Million)
Likelihood	Almost Certain (e.g., Greater than 90%)	High	High	Extreme	Extreme	Extreme
	Likely (e.g., Between 50% and 90%)	Moderate	High	High	Extreme	Extreme
	Moderate (e.g., Between 10% and 50%)	Low	Moderate	High	Extreme	Extreme
	Unlikely (e.g., From 3% to 10%)	Low	Low	Moderate	High	Extreme
	Rare (e.g., < 3% Chance)	Low	Low	Moderate	High	High



Voorbeelden van kans matrices

	A	B	C	D	E
Nominale frequentie [incidenten per jaar]	3×10^{-1} (0,3)	3×10^{-2} (0,03)	3×10^{-3} (0,003)	3×10^{-4} (0,0003)	3×10^{-5} (0,00003)
Kans op een cyberincident	Zeer waarschijnlijk. > 90%	Waarschijnlijk. <90%	Matig waarschijnlijk. <50%	Zeer onwaarschijnlijk. <10%	Bijna onmogelijk, < 3%

Likelihood	Almost certain	Likely	Possible	Unlikely	Rare
Technical skills	Opportunistic script kiddie / malicious insider	Skilled individual	Moderately skilled team / Hactivist	Cybercriminals	State-sponsored actors
Discoverability	Connected to internet	Connected to internet	Connected to internet	Separated / segmented network or physical	Separated / segmented network or physical
Accessibility	No access control / shared accounts	Simple access control	Role based access control	Mature access controls	Mature access controls
Vulnerability	Multiple vulnerabilities. Public exploits.	Multiple vulnerabilities. Public exploits.	Vulnerabilities. Crafted exploits.	No public vulnerabilities. Crafted exploits.	No public vulnerabilities. Zero-day exploits.
Funding	None	Little	Some	Substantial	Substantial
Time	Days	Weeks	Months	Years	Decades

duidelijkheid



Detail risico beoordeling

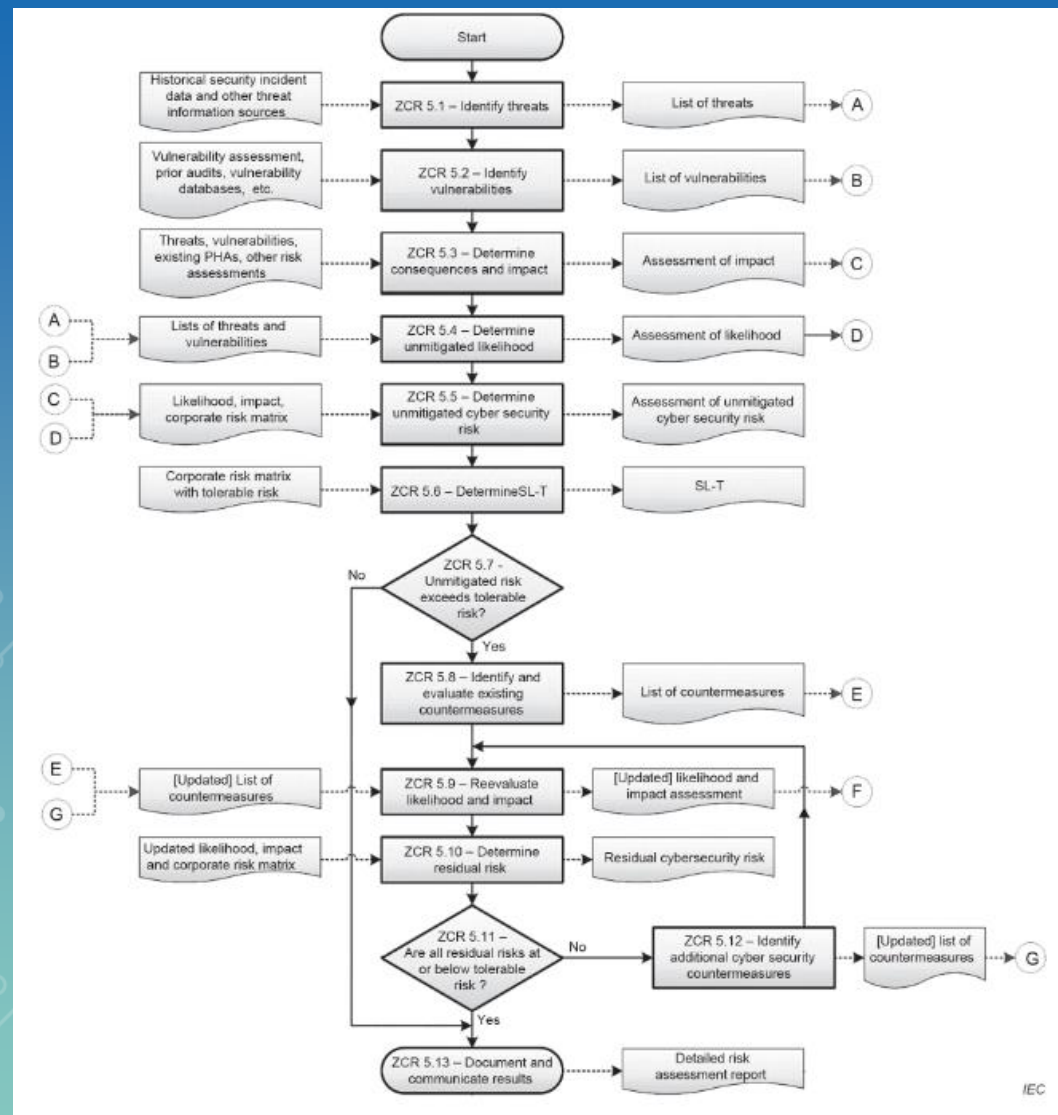
Verkrijg inzicht in het huidige risiconiveau binnen een automatiseringssysteem, rekening houdend met potentiële dreigingsvectoren en bestaande/geplande tegenmaatregelen.

Beoordeel voor elke zone, conduit en externe verbinding (!):

- Dreiging
- Kwetsbaarheden (voor alle componenten...)
- Impact/verstoring bij een incident
- Bereikte security level (SL-A) en effectiviteit van maatregelen

Onderwerpen:

- Secure netwerk architectuur
- Conduits (firewalls, netwerk inrichting)
- Externe verbindingen





De detail risico beoordeling in de praktijk...

✓ High level risico beoordeling

Een volledige detail risico beoordeling:

Is erg kostbaar en tijdrovend.

Is lastig omdat ICS netwerken door de asset owner soms worden beschouwd als een black box waarbij de OEM de verantwoordelijkheid heeft voor het onderhoud.

Maar, gebruik de principes van een detailed risk assessment om zwakke plekken in te identificeren:

- Threat modeling / cyber kill chain. Risico gezien vanuit perspectief van de dreigings actoren.
- Pentesten en kwetsbaarheidsbeheer



Het beoordelen van de kans....

Cyber dreiging

- Motivatie/motief van de actor: financieel gewin, terrorisme/ordeverstoring, status.
- Mogelijkheden: vaardigheden en de beschikbare middelen van de aanvallers.

Voorbeelden van dreigings actoren:

- Criminelen, inlichtingendiensten, statelijke actoren, opportunisten.
- Insider threats, supply chain risks.



Kwetsbaarheden

- Bekende kwetsbaarheden in hard- en software.
- Onveilige inrichtingen/configuraties.
- Mitigerende maatregelen die niet bewezen effectief zijn.

Voorbeelden van kwetsbaarheden:

- Ongepatchte software
- Zwakke authenticatie
- Blootstelling van het netwerk

Dit is geen exacte wetenschap...



Hoe verbeter je de beoordeling van kans

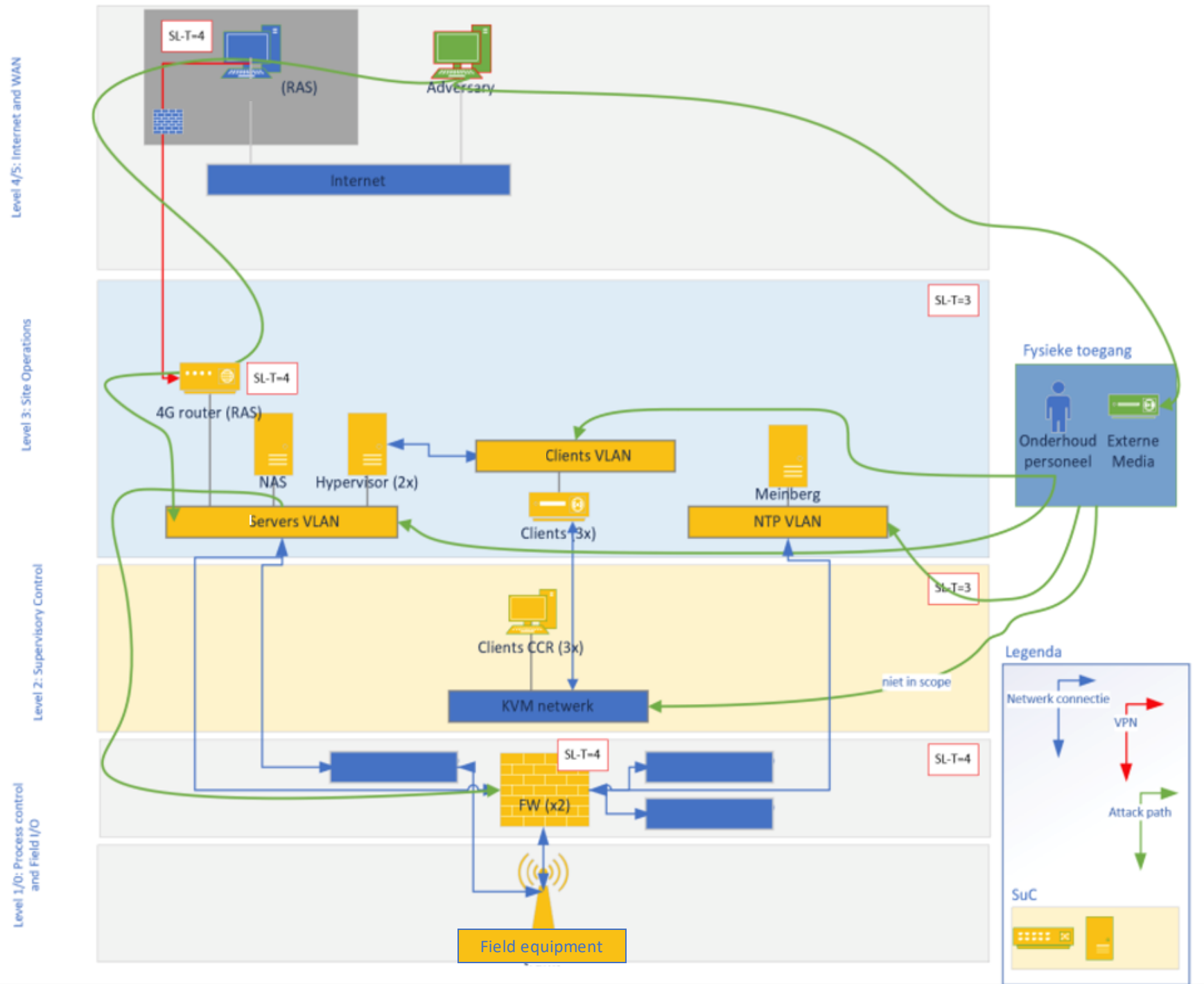
Om de betrouwbaarheid van het beoordelen van de waarschijnlijkheid te vergroten, moeten organisaties overwegen om het volgende te gebruiken:

- Werk in een multidisciplinair team met verschillende expertises.
- Gebruik (externe) incident rapportages, threat intel, CVE publicaties en de publicaties van NCSC.
- Wees realistisch. Security incidenten gebeuren dus de kans is eerder 1x per 3 jaar dan 1x per 10 jaar, laat staan 1x per 100 jaar.
- Maak het risico visueel en gebruik 'tools'

In de volgende slides gaan we dieper in op de tools:

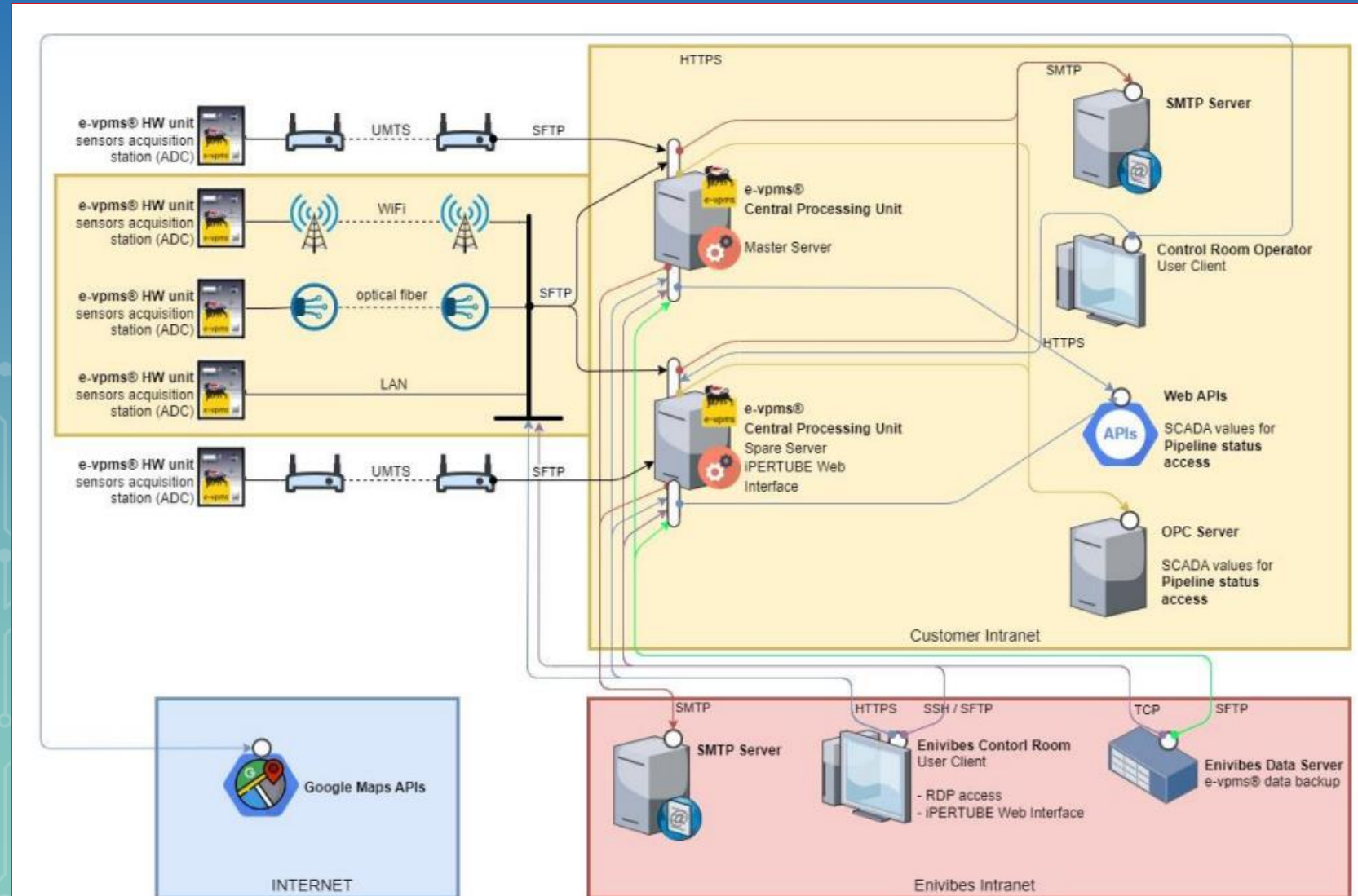
- Visualisatie van:
 - SuC, zones en security levels.
- Kansbeoordeling:
 - NCSC Inschalingsmatrix
- Cyber dreiging:
 - Threat modeling.
 - Mitre ATT&CK for ICS.
- Maatregelen en kwetsbaarheden:
 - Bowtie analyse.

Visualiseer SuC, zones en security levels (voorbeeld 1)



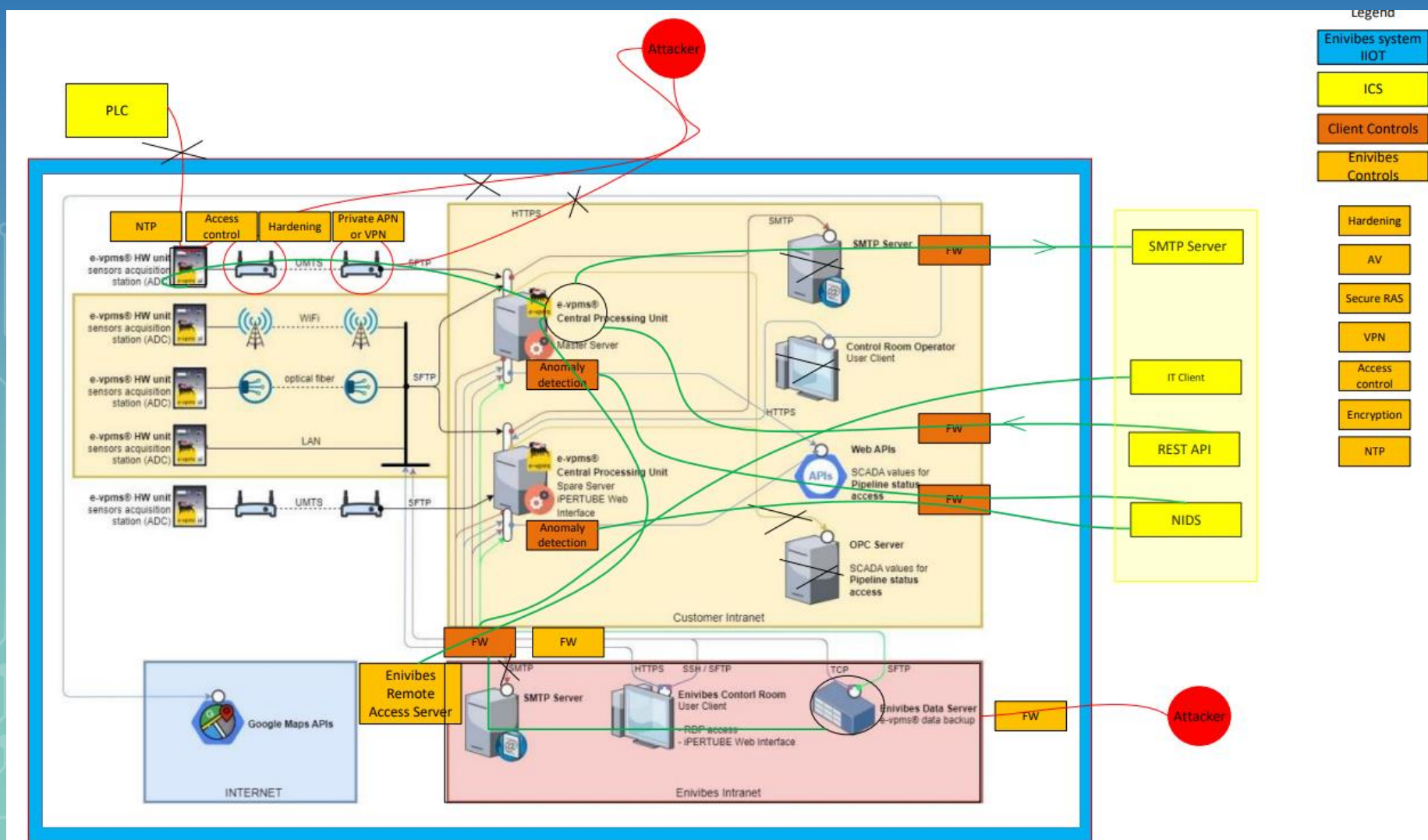


Visualiseer SuC (voorbeeld 2)



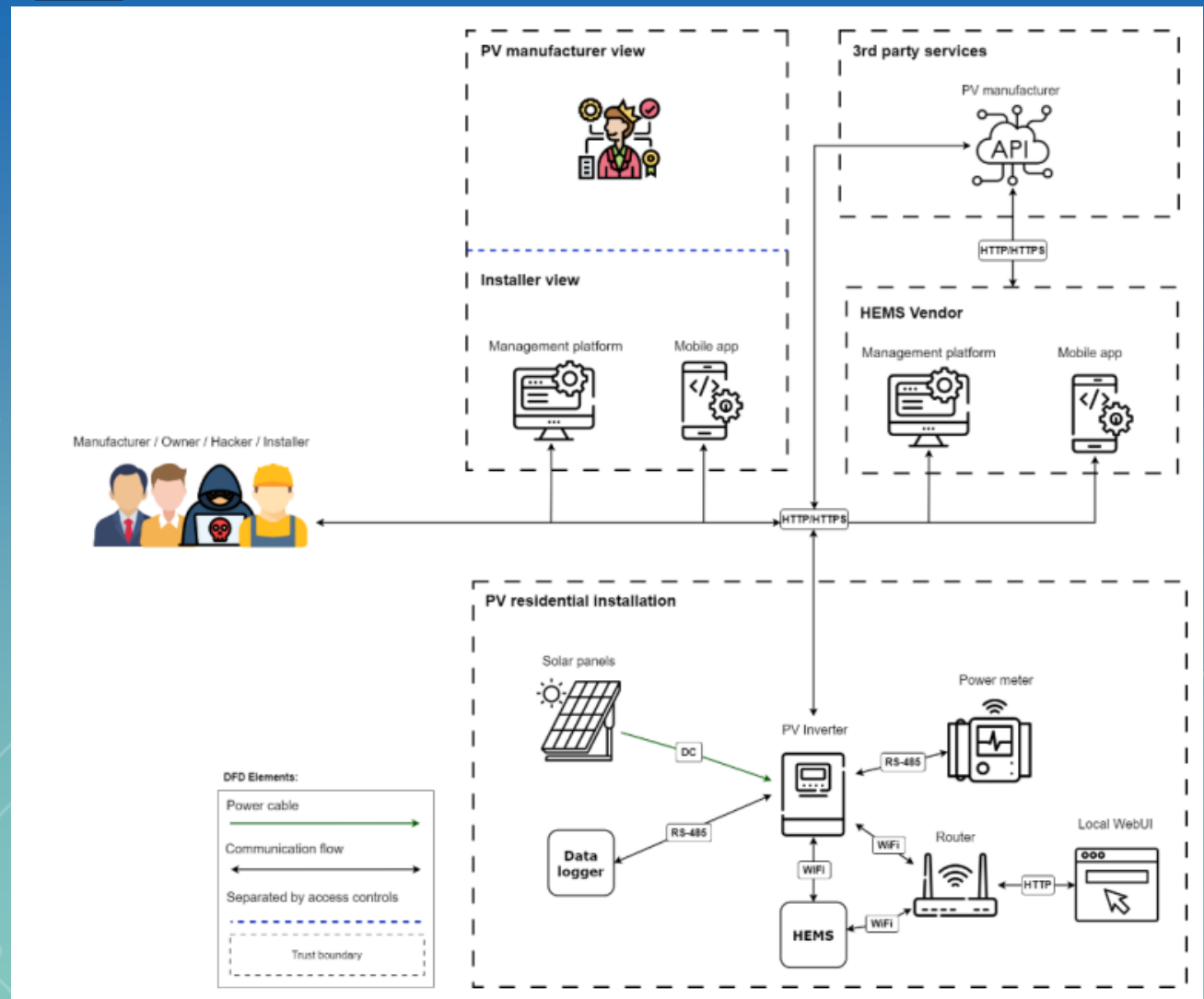


Visualiseer SuC en dreigingsvlak (voorbeeld 2)





Hoogover visualisatie SuC (voorbeeld 3)





Risico beoordelen dmv dreigings scenarios en threat modeling

- Bewustwording en inlevingsvermogen vergroten: “oh ja” en “ah ok”
- Gebruik de visualisatie van het SuC.
- Je beperkt je tot de scenarios die relevant zijn. Andere gooi je weg.
- Uitwerken van de relevante scenarios of toevoegen van subscenarios.



Risico beoordelen d.m.v. scenarios en threat

Scenario	Interne/Externe Actor	Threat Actor	Dreigingsnivo Mogelijkheden, motivatie en kunde	SL-T	Relevant scenario	Mogelijkheid van initiatie ***	Beoordeling van conduits	OT Attack TTP's Detecteren en blokkeren *****
Een engineer introduceert onbedoeld een virus via verwijderbare media (USB) of een externe verbinding.	Interne	Werknemer/Contractor	LAAG-LAAG-HOOG	SL-T=2	Indien een scenario niet relevant is hoeft het ook niet uitgewerkt te worden	Gebruik de NCSC inschalingsmatrix om de waarschijnlijkheid van de aanval te bepalen. Alle scenario's met een waarschijnlijkheid van > "1 Remote" worden overwogen.	Zijn de conduits, mits veilig geconfigureerd, effectief in het voorkomen en detecteren van de actor TTP?	Beoordeel OT/ICS TTP's en detectiemogelijkheden met Mitre Att@ck of Bowtie
Een hacker introduceert malware via een social engineering aanval bij een ICS toeleverancier/dienstverlenende partij. De toeleverancier infecteert het ICS netwerk tijdens het uitvoeren van onderhoud.	Interne	Hacker - criminele groep via Werknemer/Contractor	MED-HOOG-HOOG	SL-T=3	JA	3-Probable	Bijv: FWs, RAS	
Criminele groep infecteert het ICS met ransomware via bestaande connectiviteit tussen de IT-omgeving en de OT-omgeving.	Externe	Hacker - criminele groep	HOOG-HOOG-MED	SL-T=3				
Een criminele groep hackt het IT-netwerk en infecteert een voor het ICS kritieke server (bijv. planning, finance) met malware.	Externe	Hacker - criminal group	MED-HOOG-MED	SL-T=2				

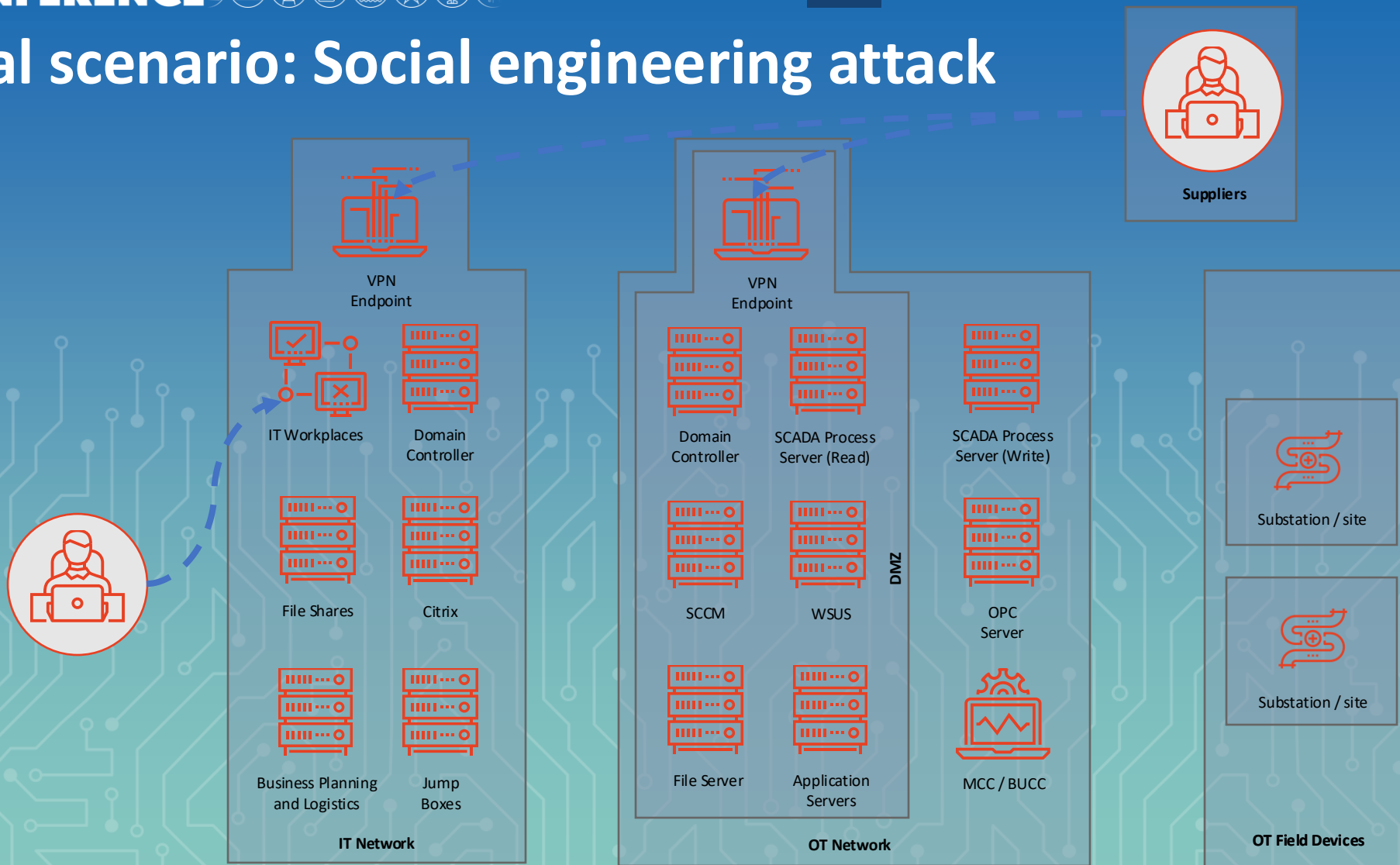
Security Level	Target	Skills	Motivation	Means	Resources
SL1	Casual or coincidental violations	No Attack Skills	Mistakes	Non-intentional	Individual
SL2	Cybercrime, Hacker	Generic	Low	Simple	Low (Isolated Individual)
SL3	Hackivist, Terrorist	ICS Specific	Moderate	Sophisticated (Attack)	Moderate (Hacker Group)
SL4	Nation State	ICS Specific	High	Sophisticated (Campaign)	Extended (Multi-disciplinary Teams)

Geen standaardwaarden, niet voor elk ICS hetzelfde (een DCS vergt bijv hoger kennisnivo dan een PV managementplatform)



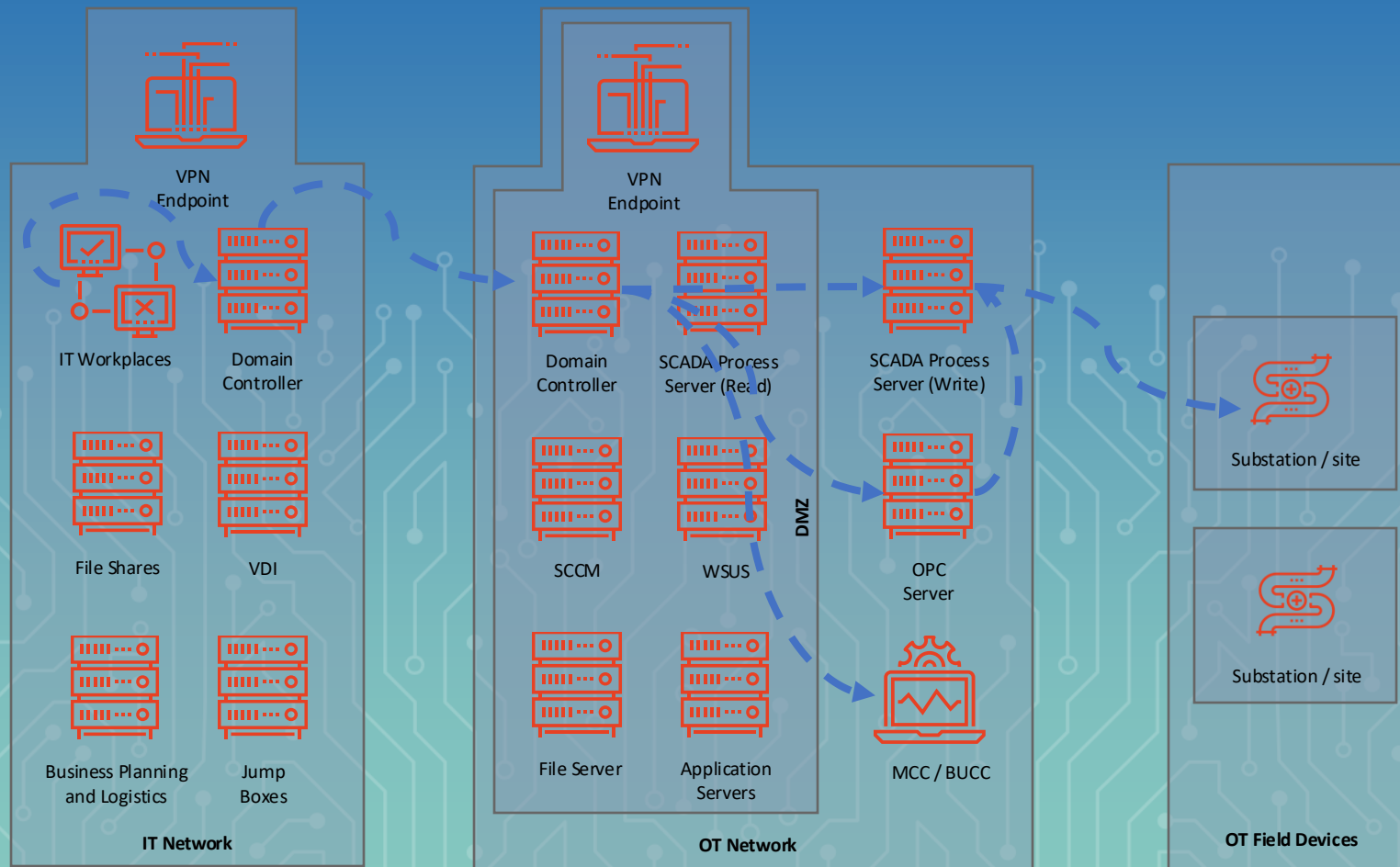


Visual scenario: Social engineering attack





Visual scenario: laterale beweging icm DC trust



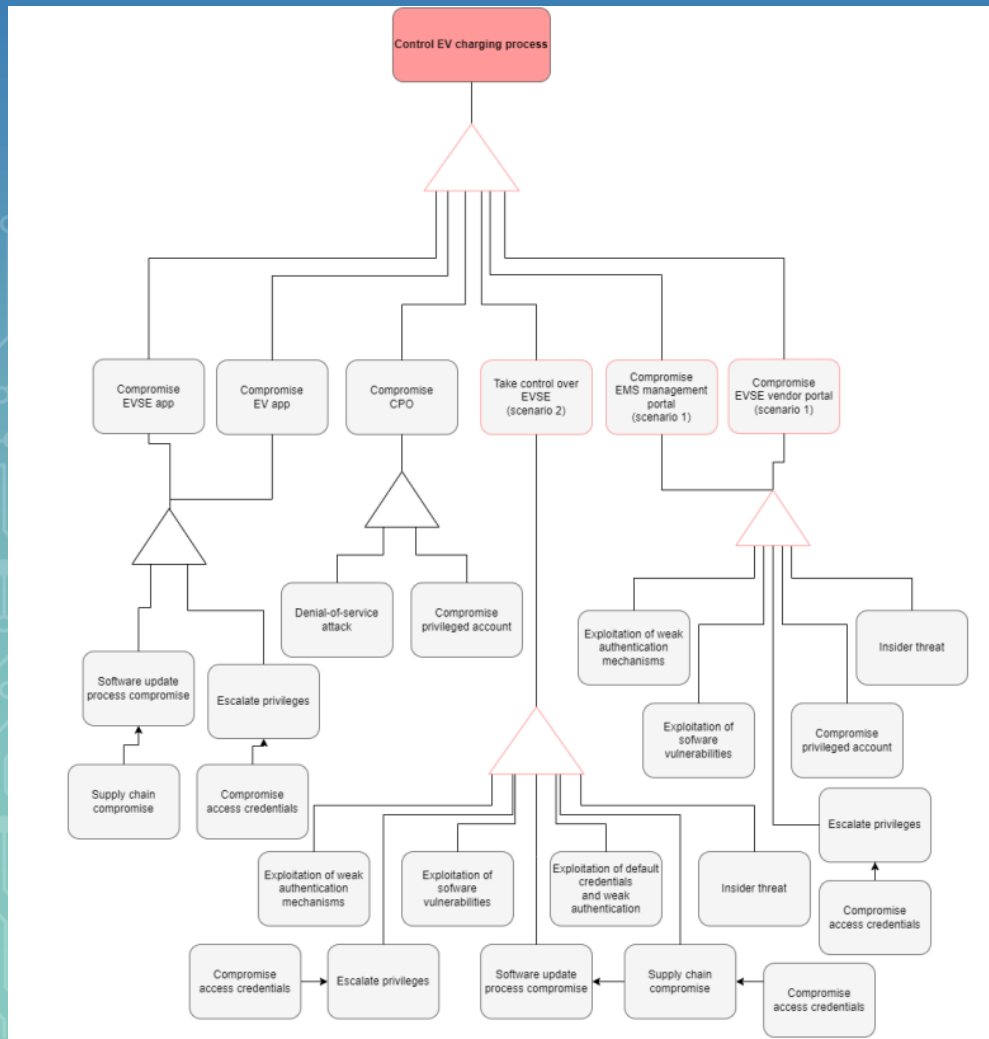


NCSC Inschalingsmatrix

Question		Option 1		Option 2		Option 3		Value	
Vulnerability default present		No	1	x	Not sure/Yes	3		3	✓
Is code available to exploit		None	1		Concept	4	x	6	✓
Are technical details available		None	1		Some	2	x	3	✓
Required access	x	Physical	1		LAN	4		6	✓
Needed credentials	x	Admin	1		User	2		4	✓
Complexity to exploit		Complex	1	x	Average	2		3	✓
User interaction required		Complex	1	x	Simple	3		4	✓
Is vulnerability being exploited		Yes	1		Limited	2	x	3	✓
Is an exploit expected	x	None	1		Yes	3		1	✓
Patch available	x	> 2 months	1		<= 2 months	2		3	✓
								24	
This is based on the "inschalingsmatrix" (Dutch for "classification matrix") from the Dutch National Cyber Security Institute: https://www.ncsc.nl/documenten/publicaties/2019/juli/02/inschalingsmatrix						3 Probable			
Scale 3-Probable 2-Occasional 1-Remote									



Attack vector & TTPs weergegeven in een attack tree



Scenarios

Attack scenario	Impact	Likelihood	Risk level
Gain Unauthorized Access to the Management Platform	Moderate	Likely	High
Exploit vulnerabilities to remotely access and control EVSE	Minor	Likely	Medium
Gain Unauthorized Access to the EMS Platform	Minor	Likely	Medium
Compromising EVSE app	Moderate	Possible	Medium
Compromising EV app	Minor	Possible	Medium
Compromising CPO	Moderate	Unlikely	Medium

Attack paths

Likelihood	Attack Path
Likely	Exploitation of Weak Authentication Mechanisms
Likely	Exploitation of Software Vulnerabilities
Likely	Compromise of Privileged Account
Likely	Privilege Escalation
Possible	Insider Threat

IACS & CYBERSECURITY CONFERENCE



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact - ICS
The adversary is trying to get into your ICS environment.	The adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way.	The adversary is trying to maintain their foothold in your ICS environment.	The adversary is trying to gain higher-level permissions.	The adversary is trying to avoid security defenses.	The adversary is locating information to assess and identify their targets in your environment.	The adversary is trying to move through your ICS environment.	The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.	The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe condition.	The adversary is trying to manipulate, disable, or damage physical control processes.	The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment.
Data Historian Compromise T0817 Drive-by Compromise	Change Program State Command and Scripting Interpreter	Account Manipulation BITS Jobs	Abuse Elevation Control Mechanism Access Token Manipulation	Abuse Elevation Control Mechanism Access Token Manipulation	Account Discovery Application Window Discovery	T0812 Default Credentials T0868 Exploitation of Remote	Archive Collected Data Audio Capture	T0863 Standard Application Layer T0885 Commonly Used Port	Activate Firmware Update Mode T0878 Alarm Suppression	Brute Force I/O Change Program State	Damage to Property T0813 Denial of Control
Engineering Workstation Compromise Exploit Public-Facing Application	T0807 Command-Line Interface Execution through API	Boot or Logon Autostart Execution Boot or Logon Initialization Sequence	Boot or Logon Autostart Execution Boot or Logon Initialization Sequence	BITS Jobs Deobfuscate/Decode Files or Information	Browser Bookmark Discovery Control Device Identification	External Remote Services Internal Spearphishing	T0802 Automated Collection Clipboard Data	Communication Through Remote Access Connection Proxy	T0803 Block Command Messages T0804 Block Reporting Messages	Masquerading Modify Control Logic	T0815 Denial of View Loss of Availability
T0822 External Remote Services Hardware Additions	Exploitation for Client Execution T0823 Graphical User Interface	Browser Extensions Compromise Client Software	Create or Modify System Process Event Triggered Execution	Direct Volume Access Execution Guardrails	Domain Trust Discovery File and Directory Discovery	Lateral Tool Transfer Program Organization Units	T0811 Data from Information Resources Data from Local System	Data Encoding Data Obfuscation	Block Serial COM Data Destruction	T0836 Modify Parameter T0839 Module Firmware	Loss of Control Loss of Productivity and Revenue
Internet Accessible Device	Inter-Process Communication	Create Account	T0890 Exploitation for Privilege Escalation	Exploitation for Defense Evasion	I/O Module Discovery	Remote File Copy	Data from Network Shared Drive	Dynamic Resolution	Denial of Service	Program Download	Loss of Safety
Phishing T0847 Replication Through Remote	Man in the Middle Native API	Create or Modify System Process Event Triggered Execution	Group Policy Modification Hijack Execution Flow	File and Directory Permissions Modification Group Policy Modification	T0840 Network Connection Enumeration Network Service Scanning	Remote Service Session Hijack T0886 Remote Services	Data from Removable Media Data Staged	Encrypted Channel Fallback Channels	T0816 Device Restart/Shutdown Manipulate I/O Image	Rogue Master Device Service Stop	T0829 Loss of View Manipulation of Control
T0862 Supply Chain Compromise Trusted Relationship	Program Organization Units Project File Infection	External Remote Services Hijack Execution Flow	Process Injection Scheduled Task/Job	Hide Artifacts Hijack Execution Flow	Network Share Discovery T0842 Network Sniffing	Replication Through Remote Access T1072 Software Deployment Tools	Detected Operating Mode Detect Program State	Ingress Tool Transfer Multi-Stage Channels	T0838 Modify Alarm Settings Modify Control Logic	T0856 Spoof Reporting Messages T0855 Unauthorized Command	T0832 Manipulation of View T0882 Theft of Operational Information
Valid Accounts Wireless Compromise	Scheduled Task/Job Scripting	T0874 Hooking T0857 System Firmware	Valid Accounts T0874 Hooking	Impair Defenses T0872 Indicator Removal on Host	Password Policy Discovery Taint Shared Content	Use Alternate Authentication Material T1615 Group Policy Discovery	Email Collection I/O Image	Non-Application Layer Protocol Non-Standard Port	Program Download Rootkit		T0837 Loss of Protection
T0886 Remote Services T0865 Spearphishing Attachment	Shared Modules Software Deployment Tools	Office Application Startup Pre-OS Boot	Indirect Command Execution T0843 Masquerading	Indirect Command Execution T0843 Masquerading	Process Discovery Query Registry	T0859 Valid Accounts	Input Capture Location Identification	Protocol Tunneling Proxy	T0857 System Firmware Utilize/Change Operating Mode		
T0864 Transient Cyber Asset for	System Services T0863 User Execution	Program Download Project File Infection	Modify Authentication Process Modify Registry	Modify Authentication Process Modify Registry	Remote System Discovery T0888 Remote System Information Discovery		Man in the Browser Man-in-the-Middle	Remote Access Software Standard Application Layer Protocol			
	Windows Management Instrumentation T0821 Modify Controller Tasking	Scheduled Task/Job Server Software Component	Obfuscated Files or Information Pre-OS Boot	Obfuscated Files or Information Pre-OS Boot	Software Discovery System Information Discovery		Monitor Process State Point & Tag Identification	Traffic Signaling Web Service			
		Traffic Signaling T0859 Valid Accounts	Process Injection Rogue Domain Controller	Process Injection Rogue Domain Controller	System Network Configuration Discovery Rogue Master Device		Program Upload Role Identification				
			T0851 Rootkit Signed Binary Proxy Execution	T0851 Rootkit Signed Binary Proxy Execution	System Network Connections Discovery System Owner/User Discovery		T0852 Screen Capture Video Capture				
			Signed Script Proxy Execution T0856 Spoof Reporting Message	Signed Script Proxy Execution T0856 Spoof Reporting Message	System Service Discovery System Time Discovery						
			Subvert Trust Controls Template Injection	Subvert Trust Controls Template Injection	Virtualization/Sandbox Evasion						
			Traffic Signaling	Traffic Signaling							
			Trusted Developer Utilities Proxy Execution Use Alternate Authentication Material	Trusted Developer Utilities Proxy Execution Use Alternate Authentication Material							
			Utilize/Change Operating Mode	Utilize/Change Operating Mode							
			Valid Accounts	Valid Accounts							
			Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion							
			XSL Script Processing	XSL Script Processing							
			T0858 Change Operating Mode	T0858 Change Operating Mode							

Legenda
TTP in OT
TTP in IT @ Employee/Contractor scenarios

Per TTP kun je aangeven wat de events zijn die moeten worden vastgelegd tbv event detectie en respons.

- host en netwerk detectie
- Incident playbooks
- IT/OT SIEM en SOC

Tactic ID	Detection ID	Source eventdata	Event type to log
T0847	Replication Through Rem	DS0016	Drive Creation
T0847	Replication Through Rem	DS0022	File Access
T0847	Replication Through Rem	DS0022	File Creation
T0847	Replication Through Rem	DS0009	Process Creation
T0822	External Remote Services	DS0015	Application Log Content
T0822	External Remote Services	DS0028	Logon Session Metadata
T0822	External Remote Services	DS0029	Network Traffic Flow
T0807	Command-Line Interface	DS0017	Command Execution
T0807	Command-Line Interface	DS0011	Module Load
T0807	Command-Line Interface	DS0009	Process Creation
T0807	Command-Line Interface	DS0012	Script Execution
T0823	Graphical User Interface	DS0029	Network Traffic Content
T0823	Graphical User Interface	DS0029	Network Traffic Flow



APT DragonFly 2.0 voorbeeld

Dragonfly 2.0 (G0074)

selection controls layer controls technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
Drive-by Compromise External Remote Services Spearphishing Attachment Spearphishing Link Valid Accounts Exploit Public-Facing Application Hardware Additions Replication Through Removable Media Spearphishing Supply Chain Trusted Relationships	Command-Line Interface PowerShell Scheduled Task Scripting User Execution AppleScript CMSTP Compiled HTML File Control Panel Items	Account Manipulation Create Account External Remote Services Registry Run Keys / Startup Folder Scheduled Task Shortcut Modification Valid Accounts Web Shell	Scheduled Task Valid Accounts Web Shell Access Token Manipulation Accessibility Features AppCert DLLs AppInit DLLs Application Shim	Disabling Security Tools File Deletion Indicator Removal on Host Masquerading Modify Registry Scripting Template Injection Valid Accounts	Account Manipulation Brute Force Credential Dumping Forced Authentication Bash History Credentials in Files Credentials in Registry Event Viewer Logs and Auditing	Account Discovery File and Directory Discovery Network Share Discovery Permission Groups Discovery Query Registry Remote System Discovery System Network Configuration Discovery	Remote Desktop Protocol Remote File Copy AppleScript Application Deployment Software Distributed Component Object Model Exploitation of Remote Services	Data from Local System Data Staged Email Collection Screen Capture Audio Capture Automated Collection Clipboard Data Data from Information	Commonly Used Port Remote File Copy Standard Application Layer Protocol Communication Through Removable Media Connection Proxy Custom Command and Control Protocol Custom Cryptographic	Data Compressed Automated Exfiltration Data Encrypted Data Transfer Size Limits Exfiltration Over Alternative Protocol Exfiltration Over Command and Control Channel Exfiltration Over Other	Data Destruction Data Encrypted for Impact Defacement Disk Content Wipe Disk Structure Wipe Endpoint Denial of Service Firmware Corruption Host System Recovery Denial of Service Resource Hijacking Service Stop Data Manipulation Data Removal Data Submission

Valid Accounts

T1086
Score: 1
Comment: Dragonfly 2.0 used PowerShell scripts execution.

Web Shell

T1074
Score: 1
Comment: Dragonfly 2.0 added the registry to the Registry to establish persistence.

Account Manipulation

Remote Desktop Protocol

T1076
Score: 1
Comment: Dragonfly 2.0 moved laterally via RDP.

Data from Local System

Data Staged

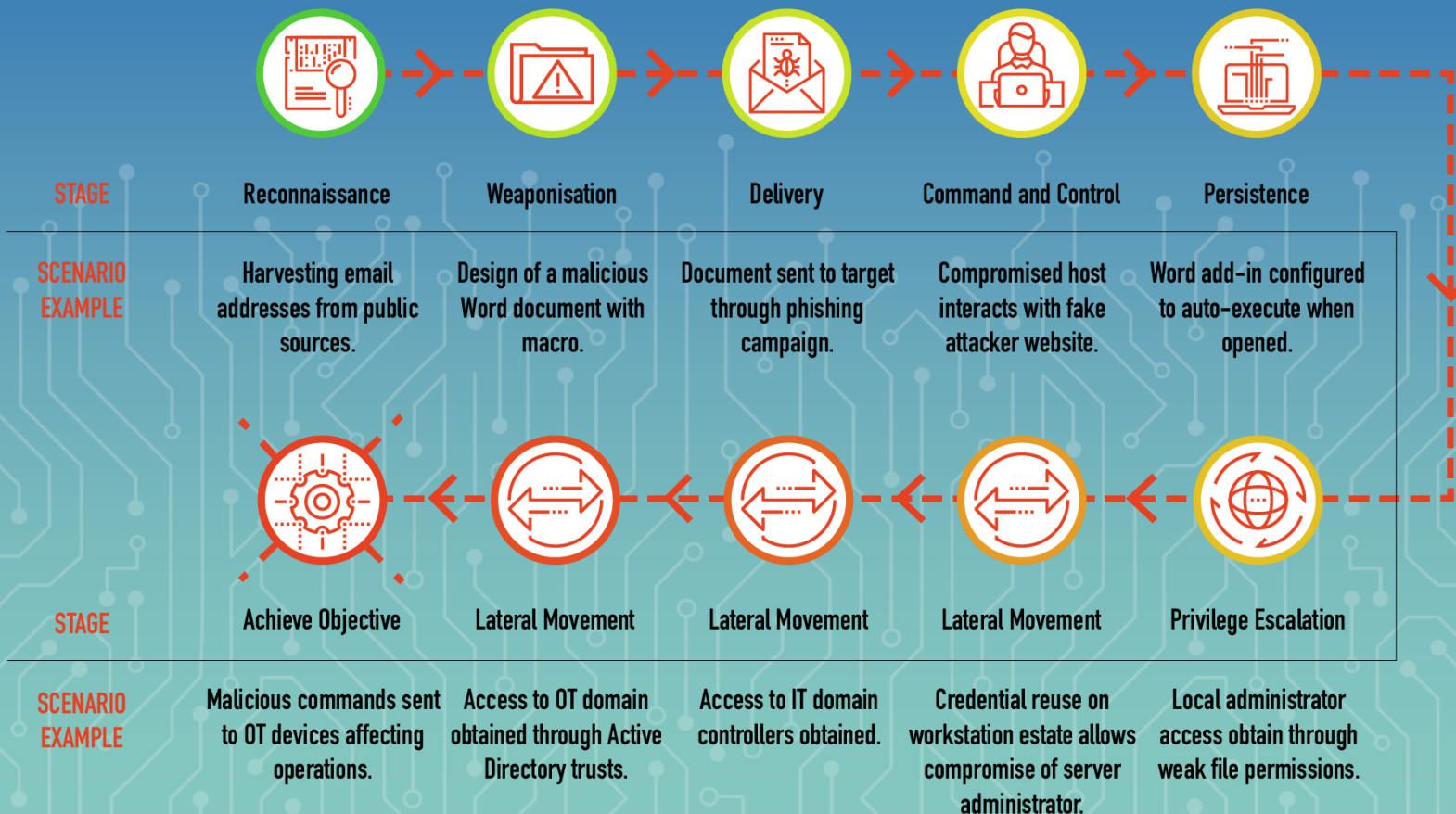
T1074
Score: 1
Comment: Dragonfly 2.0 created a directory named "out" in the user's %AppData% folder and copied files to it.

Remote File Copy

T1043
Score: 1
Comment: Dragonfly 2.0 used SMB over ports 445 or 139 for C2. The group also established encrypted connections over port 443.



ICS Cyber Kill Chain als alternatief voor Mitre Att@ck



Dutch Authority for Digital Infrastructure
Ministry of Economic Affairs

National Cyber Security Centre
Ministry of Justice and Security





Maatregelen en kwetsbaarheden beoordelen: Bowtie

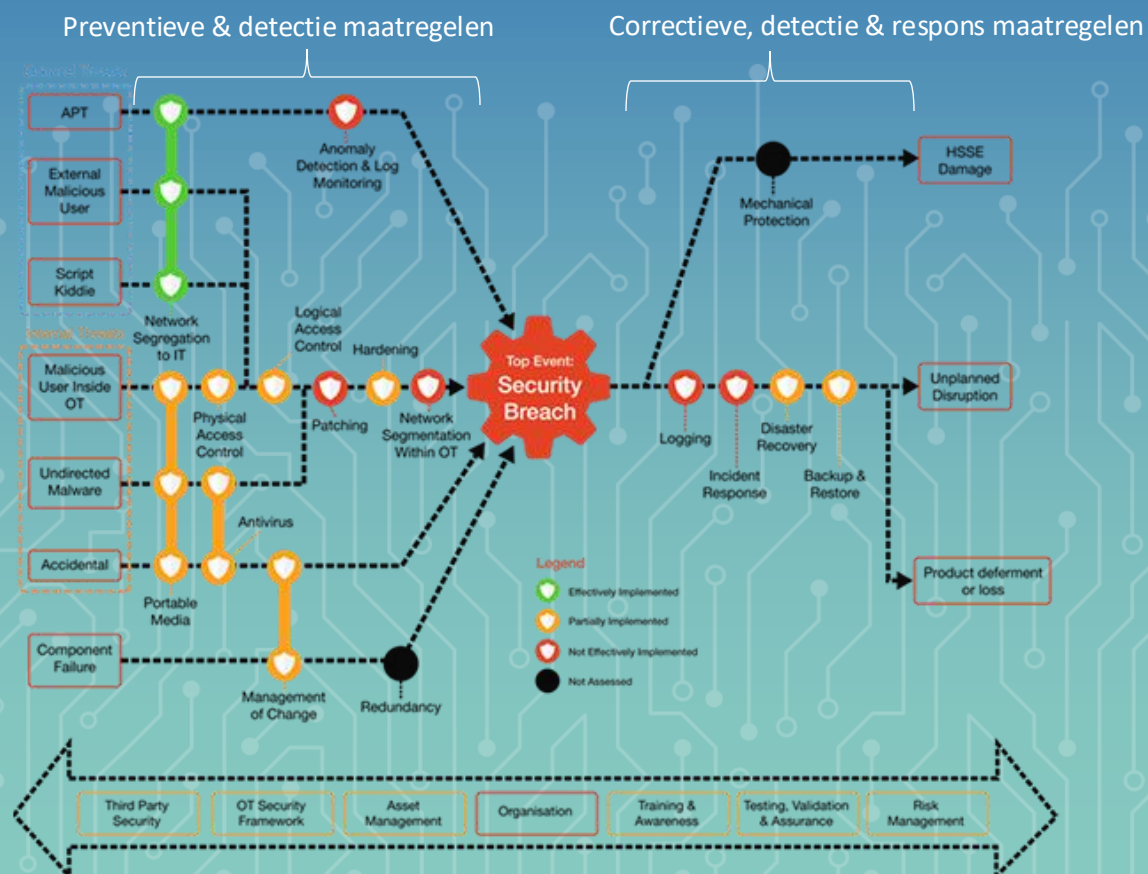


Diagram 2: The Bow Tie Assessment

Je kunt een bowtie per scenario opstellen of één voor alle relevante scenarios.

Informatie nodig van:

- System custodians
- OEM engineers
- Technische review
- Review van tool rapportages
- Pentest
- (Kwetsbaarheidsscan)

IACS & CYBERSECURITY CONFERENCE



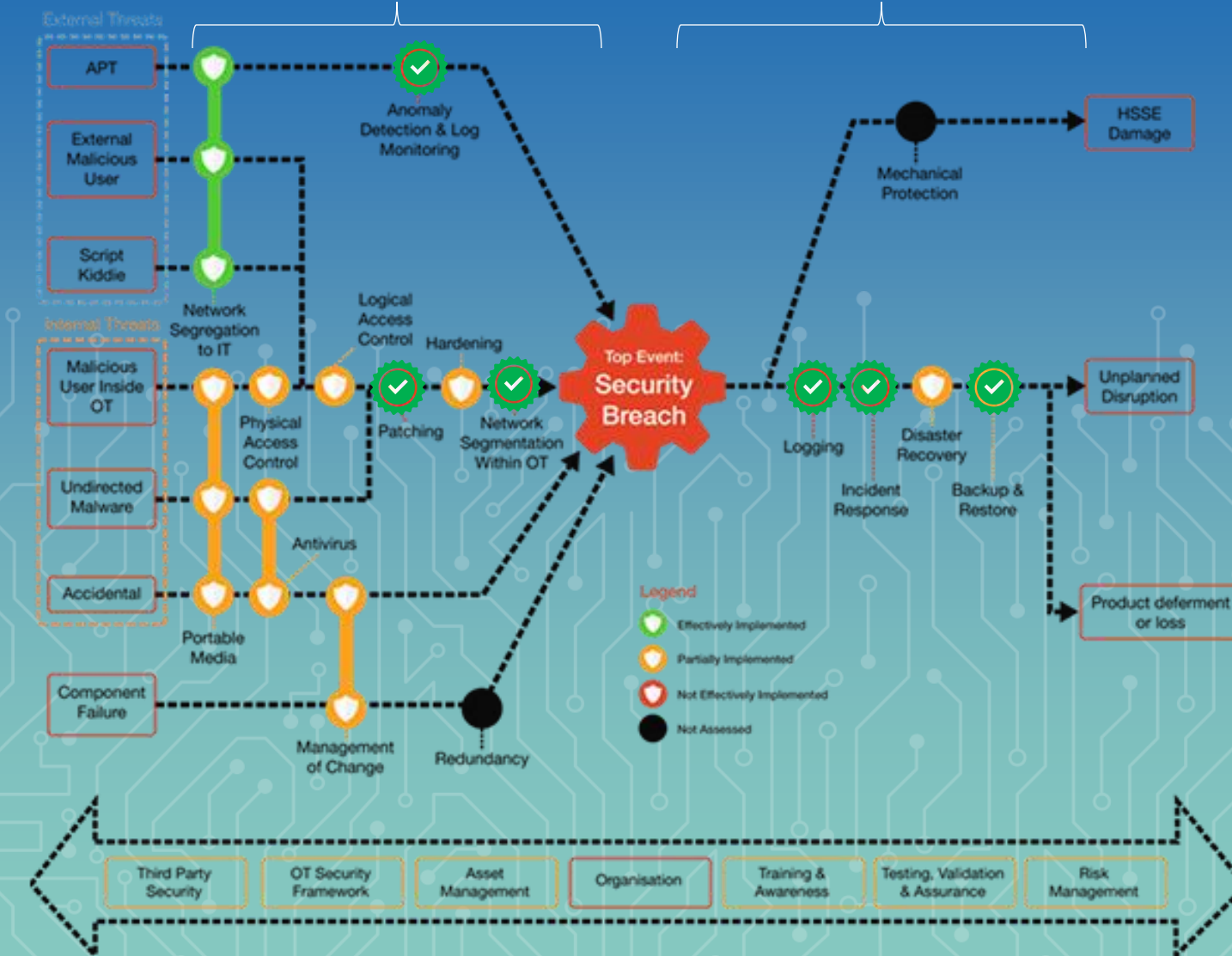
Foundational Requirement IEC62443:3-3	#	Security Requirements	Applicable OT components	Security level	Selected controls	Security level Requirement	Testing the security requirement
FR - 5 - Restricted Data Flow	SR 5.1	Network segmentation	PLC, switch, router, firewall	1	yes	The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.	Demonstrate that a probe placed in one network segment cannot be reached from another (to be separated) segment. Depending on the technology used for segmentation, use a probe and connection initiator as appropriate.
				2	yes	The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.	
				3	yes	The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.	
				4	yes	The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.	
	SR 5.2	Zone boundary protection	Router, firewall	1	no	The device providing boundary protection shall be capable of filtering and monitoring traffic.	Verify that component has functionality to configure blocking and monitoring of a given network stream traversing it.
				2	no	The component shall by default deny all network traffic crossing the zone boundary and permit only traffic by exception.	Verify that direct connections to the protected network are disabled by default.
				3	yes	The component shall be able to work in an "island mode" where no traffic can cross the boundary. The component shall respond to failures in the boundary protection in a fail-safe manner, i.e. it shall revert to island mode. The control system shall provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close).	Verify firewalling capability by performing the following steps as a minimum: - Full scan of all TCP/UDP ports, including IP fragmentation scan. - ACL mapping by fire-walking from both insecure and secure zones. - Test tunneling from the secure side, using e.g. ICMP, DNS, SSH, or HTTP. If it is possible to configure the component with an invalid configuration (e.g. delete all ACL rules), verify that all connections through the device are denied in a failure state. - Verify advanced firewalling capability at least testing with ICMP, or DNS, or HTTP tunneling.
				4			
	SR 5.3	User content filtering	Router, firewall	1	yes	The gateway shall provide capabilities for identifying and blocking communication violating security policies, e.g. social media content, transfer of images, etc.	Verify that sites violating security policies, e.g. common social media sites, can be blocked.
				2			
				3	no	The control system shall provide the capability to prevent both transmission and receipt of general purpose person-to-person messages.	
				4			
	SR 5.4	Application partitioning	Endnode, switch, router, firewall	1	yes	The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.	
				2			
				3			
				4			
FR - 6 - Timely response to events	SR 6.1	Audit information accessibility	PLC, Endnode, switch, router, firewall	1	yes	Audit records required by [2.8] shall be accessible on read-only basis, subject to authorization.	Verify that manual read-only access to audit logs is available (and subject to authorization).
				2			
				3			
				4	no	It shall be possible to access audit records using an application programming interface (API) for analysis and other event management purposes.	Demonstrate access to audit logs using the vendor's API. Verify that API access is not possible without using the appropriate credentials.
	SR 6.2	Continuous monitoring	PLC, router, firewall	1	N.A	Not applicable	Not applicable
				2	yes	It shall be possible to continuously monitor security mechanisms which are provided by a component. Such monitoring may be performed e.g. by a dedicated intrusion detection system (IDS) or intrusion prevention system (IPS).	Manufacturer shall document and/or demonstrate that all implemented security mechanisms are continuously monitored or can be continuously monitored e.g. by event recording or dedicated devices.
				3			
				4			



Preventieve & detectie maatregelen

Correctieve, detectie & respons maatregelen

Hebben de extra maatregelen het risico verminderd?



Informatie nodig van:

- System custodians
- OEM engineers
- Technische review
- Review van tool rapportages
- Pentest
- (Kwetsbaarheidsscan)

Diagram 2: The Bow Tie Assessment



Herbeoordeel het risico

Is het risico veranderd door de nieuwe/verbeterde maatregelen?

- ✓ Is de kans van initiatie verminderd?
- ✓ Is de snelheid van detectie en respons verhoogd?
- ✓ Is de impact van het incident verminderd?

Zorg ervoor dat de maatregelen bijgewerkt worden tijdens preventief onderhoud.

- Aanpassing Service agreement
- Plannen preventief onderhoud
- Checklists van de onderhouds activiteiten

		Consequence				
		Minor Problem easily handled by normal day to day processes	Some Disruption Possible (e.g., damage between \$500K and \$1 Million)	Significant Time & Resources Required (e.g., damage between \$1 Million and \$10 Million)	Operations Severely Damaged (e.g., between \$10 Million and \$25 Million)	Business Survival is at Risk (e.g., damage > \$25 Million)
Likelihood	Almost Certain (e.g., Greater than 90%)	High	High	Extreme	Extreme	Extreme
	Likely (e.g., Between 50% and 90%)	Moderate	High	High	Extreme	Extreme
	Moderate (e.g., Between 10% and 50%)	Low	Moderate	High	Extreme	Extreme
	Unlikely (e.g., From 3% to 10%)	Low	Low	Moderate	High	Extreme
	Rare (e.g., < 3% Chance)	Low	Low	Moderate	High	High



Ketenrisico

De waarde van certificeringen

ISO 27001 (ISMS)

- Aantoonbaar en systematisch beheren van informatiebeveiligingsrisico's binnen een organisatie.
- Verhoogt vertrouwen en geloofwaardigheid.
- Maar: De scope is bepalend voor de toepassing van security bij klanten.

IEC 62443-4-1 (secure development)

IEC 62443-4-2 (component security)

- Embedded devices en componenten
- Voornamelijk: SL-C=1 en SL-C=2.

IEC 62443:3-3 (system security):

Voornamelijk: SL-C=1.

Picture	Supplier	Type	Model	Version	Certificate	Certification Date
	ABB	System	Ability System 800xA	6.1.1.x	SSA 4.0.0 Level 1	4/26/2022
	Emerson Automation Solutions	System	DeltaV DCS and SIS	15.LTS	SSA 4.0.0 Level 1	12/22/2022
	Emerson Automation Solutions	System	DeltaV DCS and SIS	14.3	SSA 2.0.0 Level 1	3/7/2019
	Honeywell Process Solutions	System	Experion PKS	R510.1	SSA 2.0.0 Level 1	12/30/2019

Security Level	Target	Skills	Motivation	Means	Resources
SL1	Casual or coincidental violations	No Attack Skills	Mistakes	Non-intentional	Individual
SL2	Cybercrime, Hacker	Generic	Low	Simple	Low (Isolated Individual)
SL3	Hackivist, Terrorist	ICS Specific	Moderate	Sophisticated (Attack)	Moderate (Hacker Group)
SL4	Nation State	ICS Specific	High	Sophisticated (Campaign)	Extended (Multi-disciplinary Teams)



Vragen?

Michael Noorlander

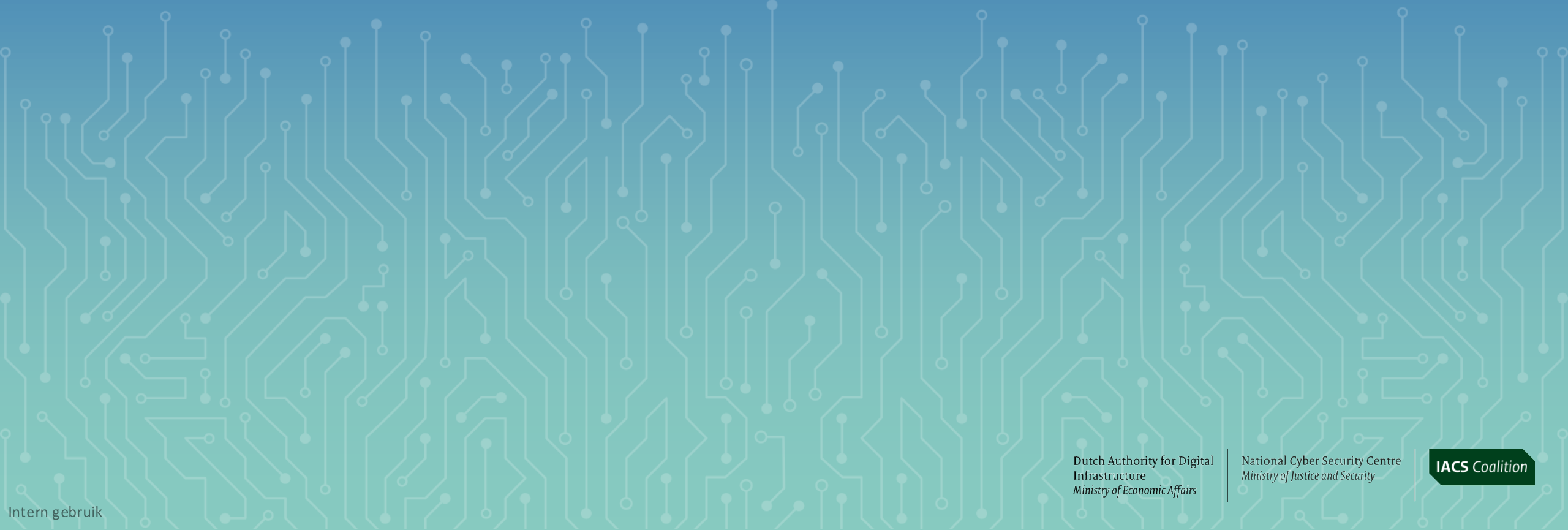
Michael.Noorlander@dnv.com

Dutch Authority for Digital
Infrastructure
Ministry of Economic Affairs

National Cyber Security Centre
Ministry of Justice and Security

IACS Coalition

IACS & CYBERSECURITY CONFERENCE



Dutch Authority for Digital
Infrastructure
Ministry of Economic Affairs

National Cyber Security Centre
Ministry of Justice and Security

IACS Coalition

IACS & CYBERSECURITY CONFERENCE



IACS & CYBERSECURITY CONFERENCE



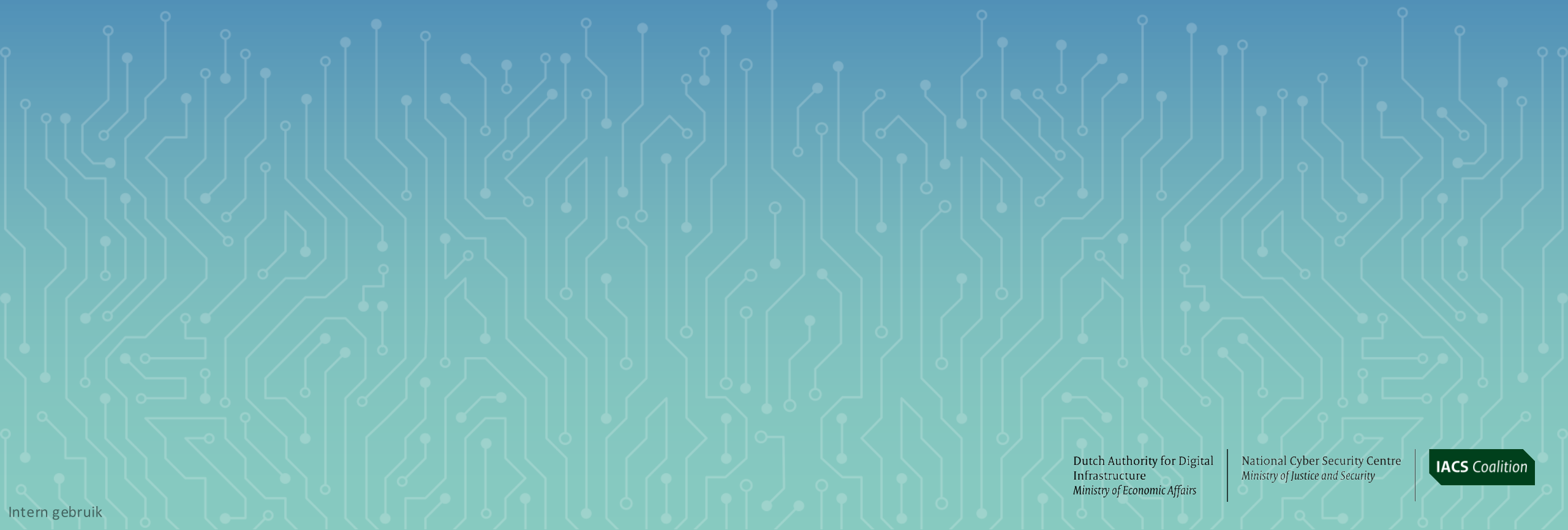
IACS & CYBERSECURITY CONFERENCE



IACS & CYBERSECURITY CONFERENCE



IACS & CYBERSECURITY CONFERENCE



Dutch Authority for Digital
Infrastructure
Ministry of Economic Affairs

National Cyber Security Centre
Ministry of Justice and Security

IACS Coalition