CSA SINGAPORE | SG Passion Made Possible

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

22 – 23 AUGUST 2023

Enhancing OT Security Through Comprehensive Assessments

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

STARTING CONVERSATION WITH ASSESSMENT: SHOULD I CHOOSE ONE?

Cybersecurity Vulnerability Assessment

OT Penetration Testing

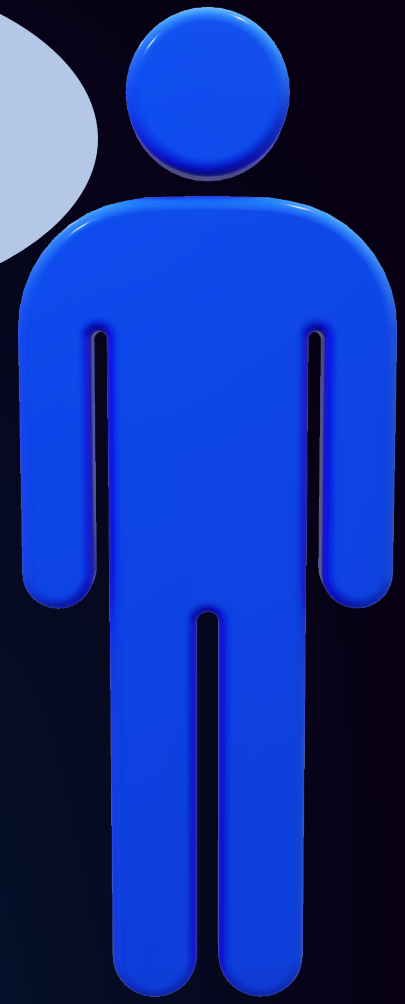
Cyber-Informed Engineering

ISA 62443

MITRE ATT&CK for ICS

Cyber-Physical Risk Assessment

Audit (compliance oriented, pass-fail outcome)



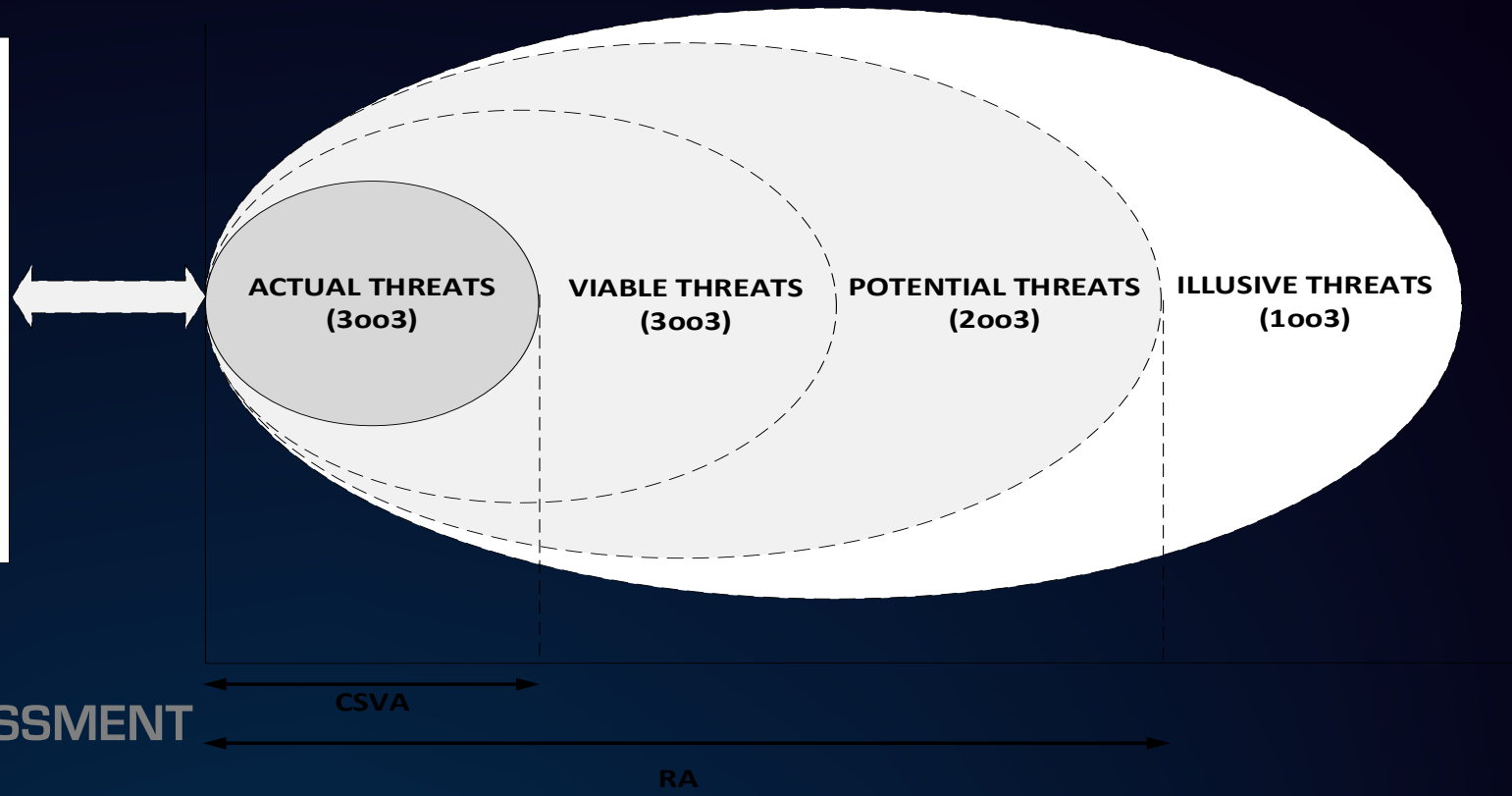
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

RISK ASSESSMENT ⇔ VULNERABILITY ASSESSMENT

RECOGNIZED THREATS

PROOF OF CONCEPT

THREATS FOR OBSERVED VULNERABILITIES



CSVA – CYBER SECURITY VULNERABILITY ASSESSMENT

RA – RISK ASSESSMENT

CYBER-PHYSICAL RISK ASSESSMENT

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

WHAT IS EXCELLENT CYBER-SECURITY?

What is excellent OT (Operational Technology) cyber-security?

Excellent OT cyber-security requires security controls that provide protection that meets plant risk criteria for loss.

What is the relationship between cyber security and process safety?

Between 40-60% of the LOPA scenarios triggered by random failures can also be caused by deliberate cyber attack causes, covering the full range of losses.

(*Results from 20+ workshops with process safety engineers*)

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

CYBER-PHYSICAL RISK AND PROCESS SAFETY RISK

THERMAL RUNAWAY REACTION

HAZARD

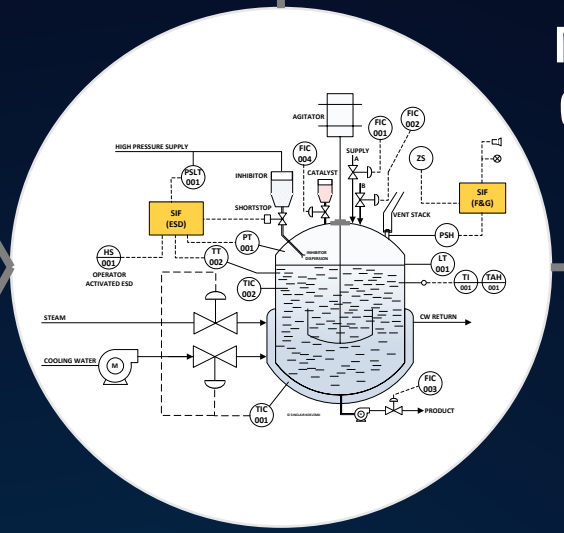
PROCESS SAFETY

COOL WATER PUMP: RANDOM FAILURE

PREVENTATIVE CONTROLS

COOL WATER PUMP: MALICIOUS SHUTDOWN

CYBERSECURITY



MITIGATIVE CONTROLS

EXPLOSION

RISK TOLERANCE: INDEPENDENT OF CAUSE

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

CYBER-PHYSICAL RISK ASSESSMENT (CSHAZOP)

Developed by industrial cybersecurity advocate (45+ years of experience in process automation) and expert **Sinclair Koelemij (Honeywell)**

Cyber-physical risk assessment extends the cybersecurity risk of a process automation system to the physical domain of the production process/process installation. It connects the cyber security of the process automation functions with the process security of the entire production installation and thus forms the link between deaths/injuries of individuals or society, environmental

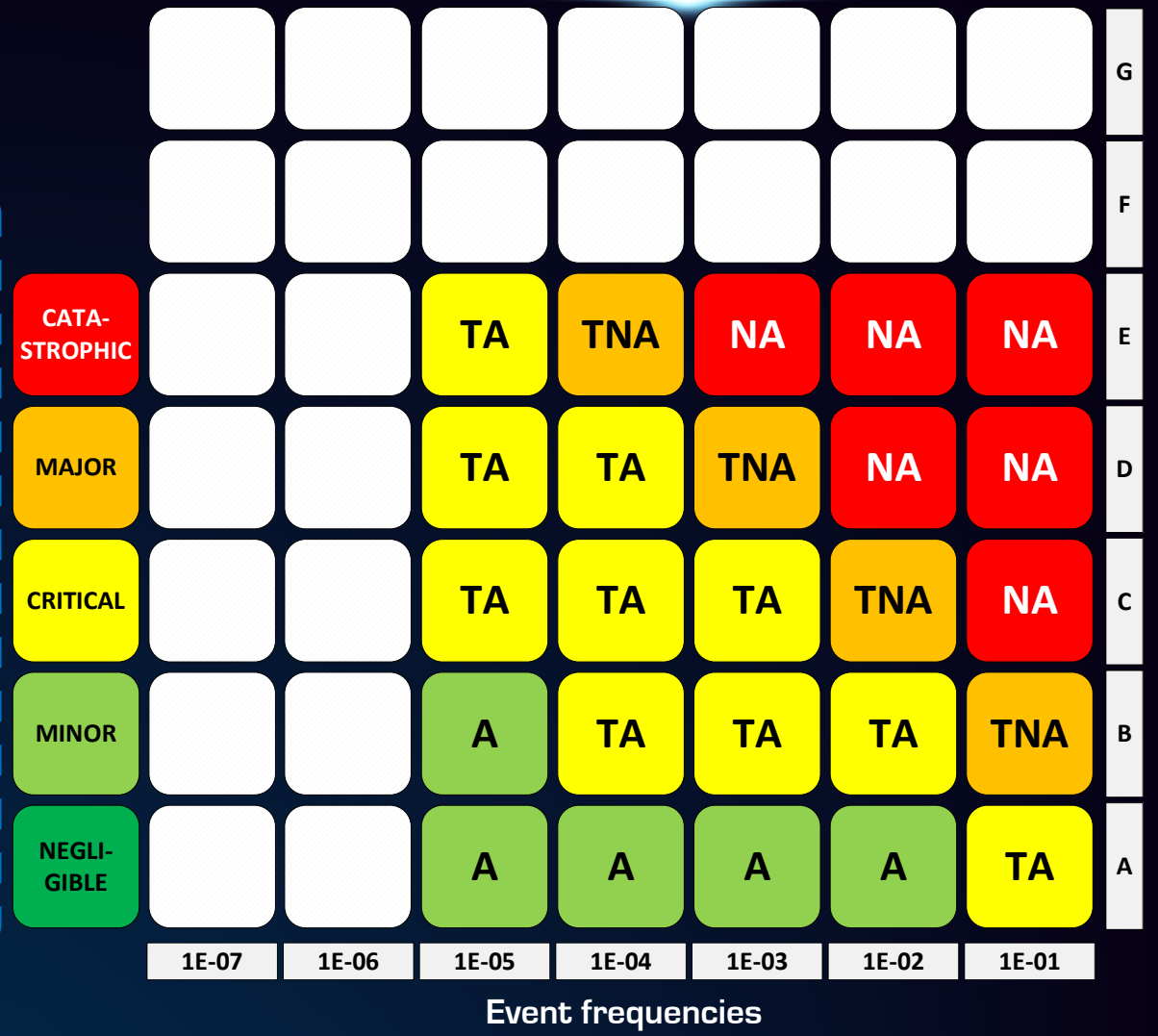
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

QUANTITATIVE PLANT CRITERIA

Risk tolerance level
Target mitigated event likelihood (TMEL)

PERSONNEL	TMEL	COMMUNITY	TMEL	ENVIRONMENT	TMEL	FINANCE	TMEL
Fatality	1E-05	Major injury	1E-06	Environmental disaster	2.0E-03	>= € 20.000.000	1E-05
Multiple major injuries	1E-04	Moderate injury	1E-05	Major damage	2.5E-03	< € 20.000.000 >= € 2.000.000	1E-04
Moderate injuries plus single major injury	1E-03	Minor injury	1E-04	Moderate damage	1.0E-02	< € 2.000.000 >= € 100.000	1E-03
Single injury	1E-02	Smell, noise	1E-03	Low impact	2.5E-02	< € 100.000 >= € 10.000	1E-02
Minor injury	1E01	No impact	1E-02	No impact	1.0E-01	< € 10.000	1E-01

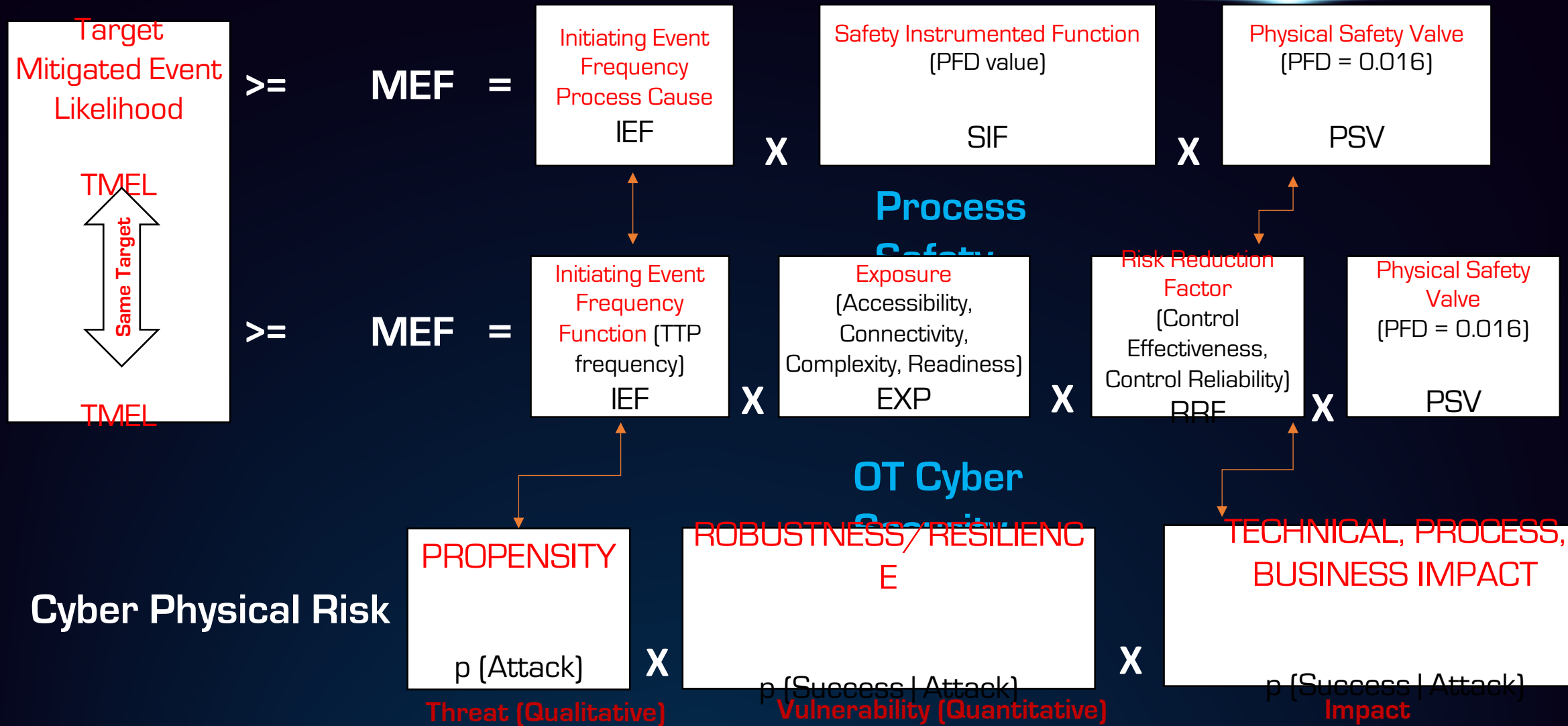
Numeric criteria



Event frequencies

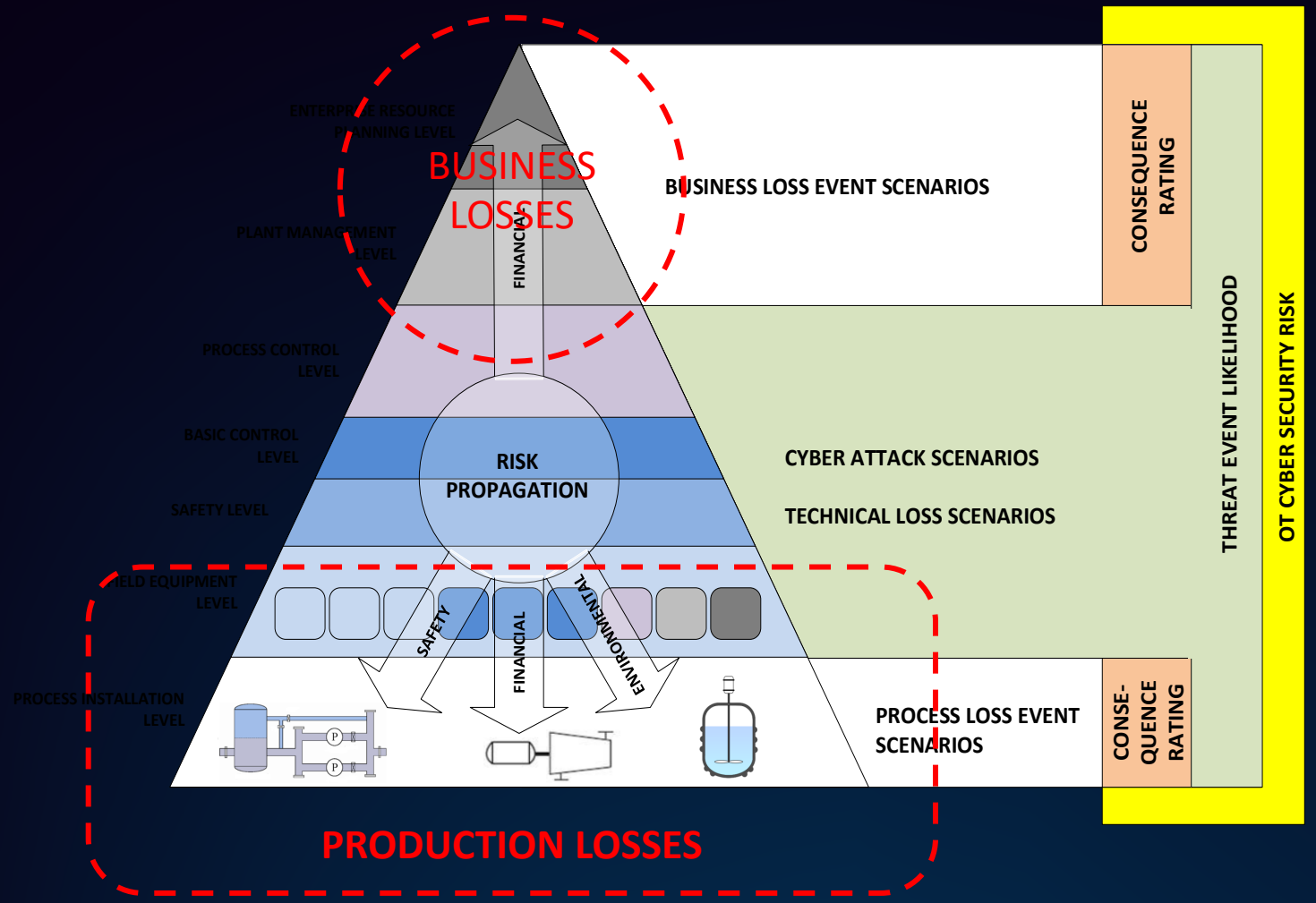
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

ESTIMATION OF CYBER-PHYSICAL RISK



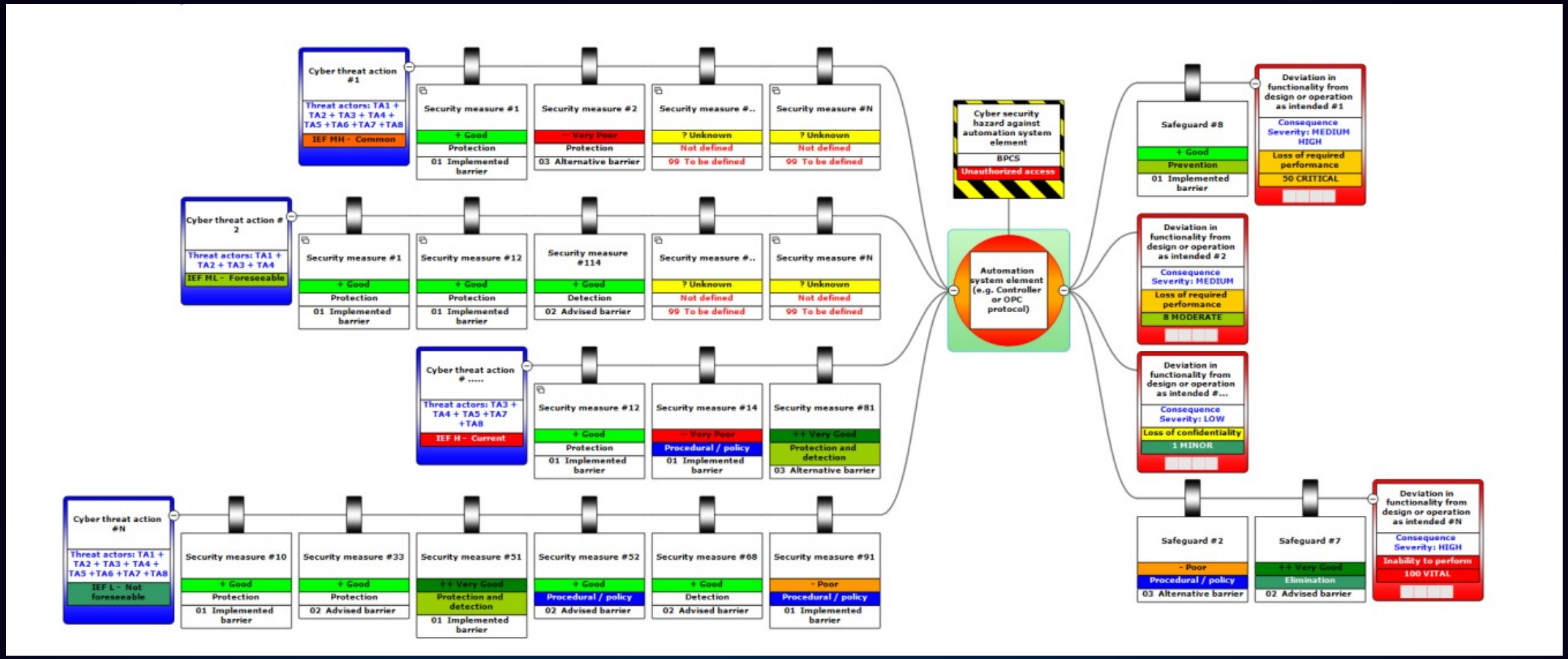
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

PROCESS SAFETY RISK ASSESSMENT



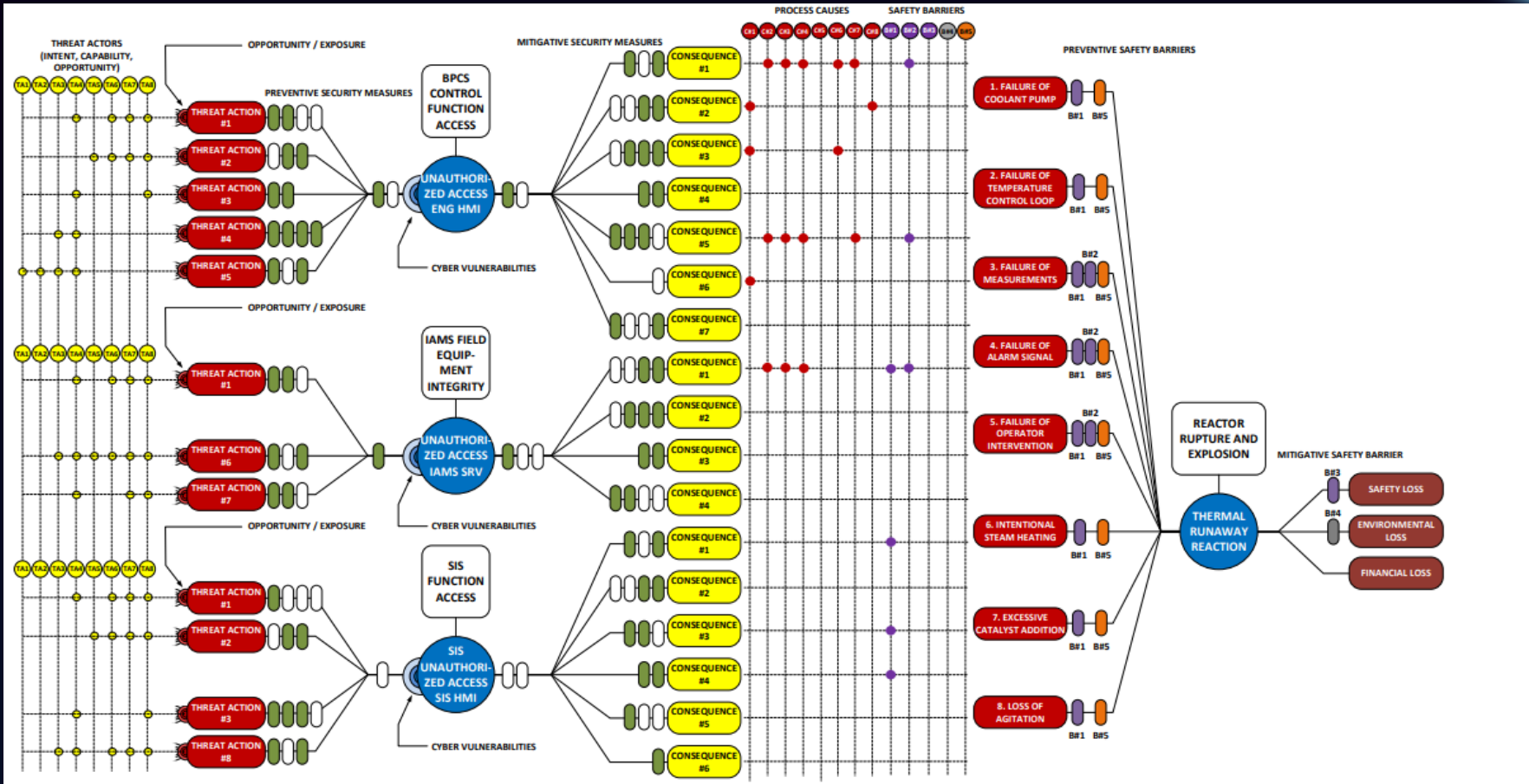
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

EXAMPLE OF ATTACK SCENARIO/CYBERSECURITY HAZARD



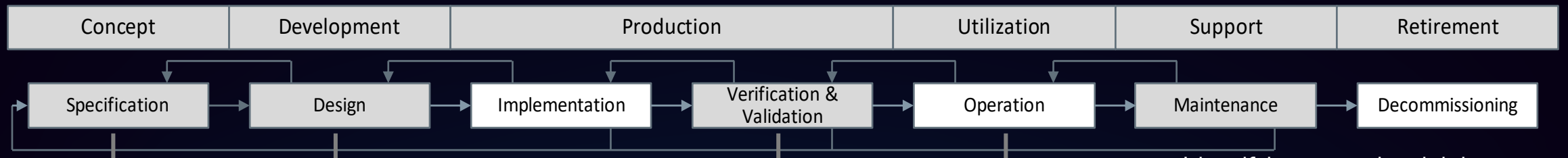
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

RELATIONSHIP WITH LOSS SCENARIOS



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

WHERE DO PLANTS USE CYBER-PHYSICAL RISK ASSESSMENT?



- Identifying security risk in a changing threat landscape
- Verify security measures still cover threats

- Used for validating security risk against a formal level:
  - Target Mitigated Event likelihood
  - IEC 62443 security level

- Used for detailed level of specifying and / or selecting security measures
- Detailed information on selected automation products is available
- HAZOP or LOPA has been executed
- Level of cyber resilience can be compared with TMEL

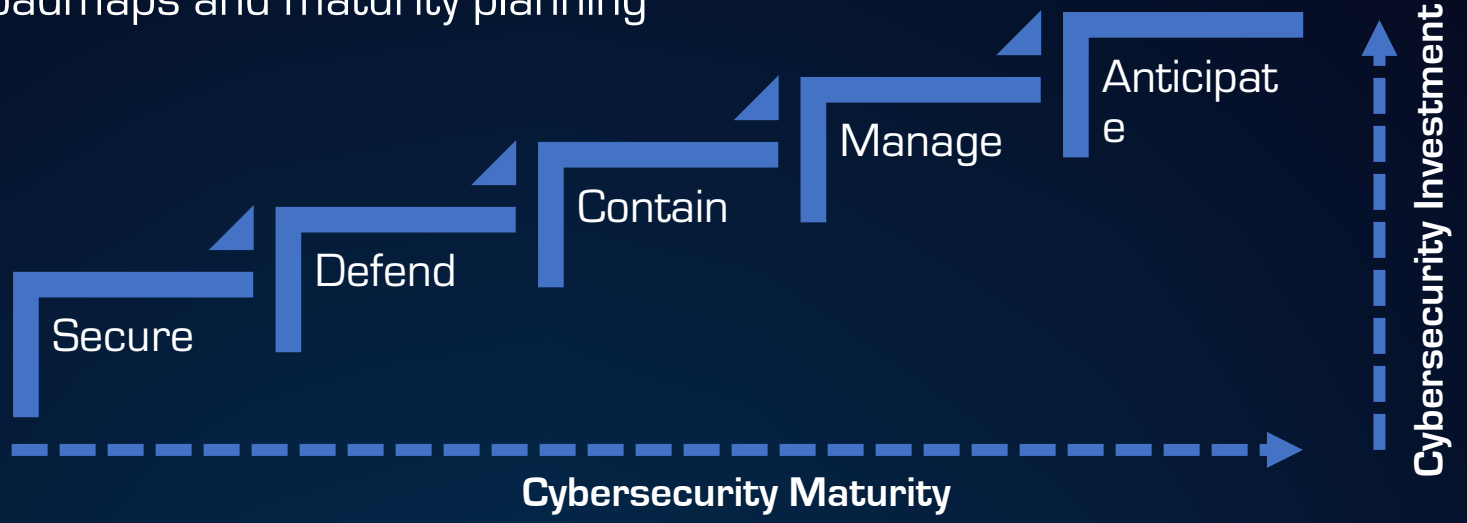
- High level specifying security requirements
- However detailed information is not available
- HAZOP or LOPA have not been executed

CYBERSECURITY VULNERABILITY ASSESSMENT

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

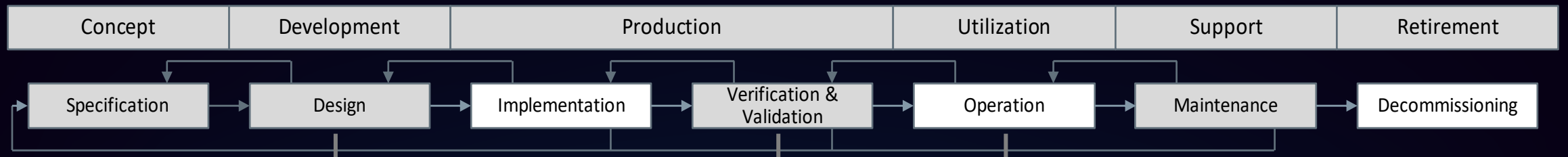
HOW TO SECURELY EXECUTE A VULNERABILITY ASSESSMENT AND SCOPE

- CSVA recommended to run according to best practice frameworks such as ISA 62443, NIST and most important to vendor security guidelines (e.g., Honeywell's Process Control Network Security Guidelines)
- CSVA scope minimum includes security policies & procedures, physical security, security architecture, network architecture, cyber access control, cyber security management.
- Usually, it is done doing site infrastructure survey, interviews of OT and IT personnel to ascertain security practices, the collection and review of written policy and procedural documentation and the collection of configuration information to complete an operational technical assessment of the deployed security infrastructure.
- For cybersecurity roadmaps and maturity planning



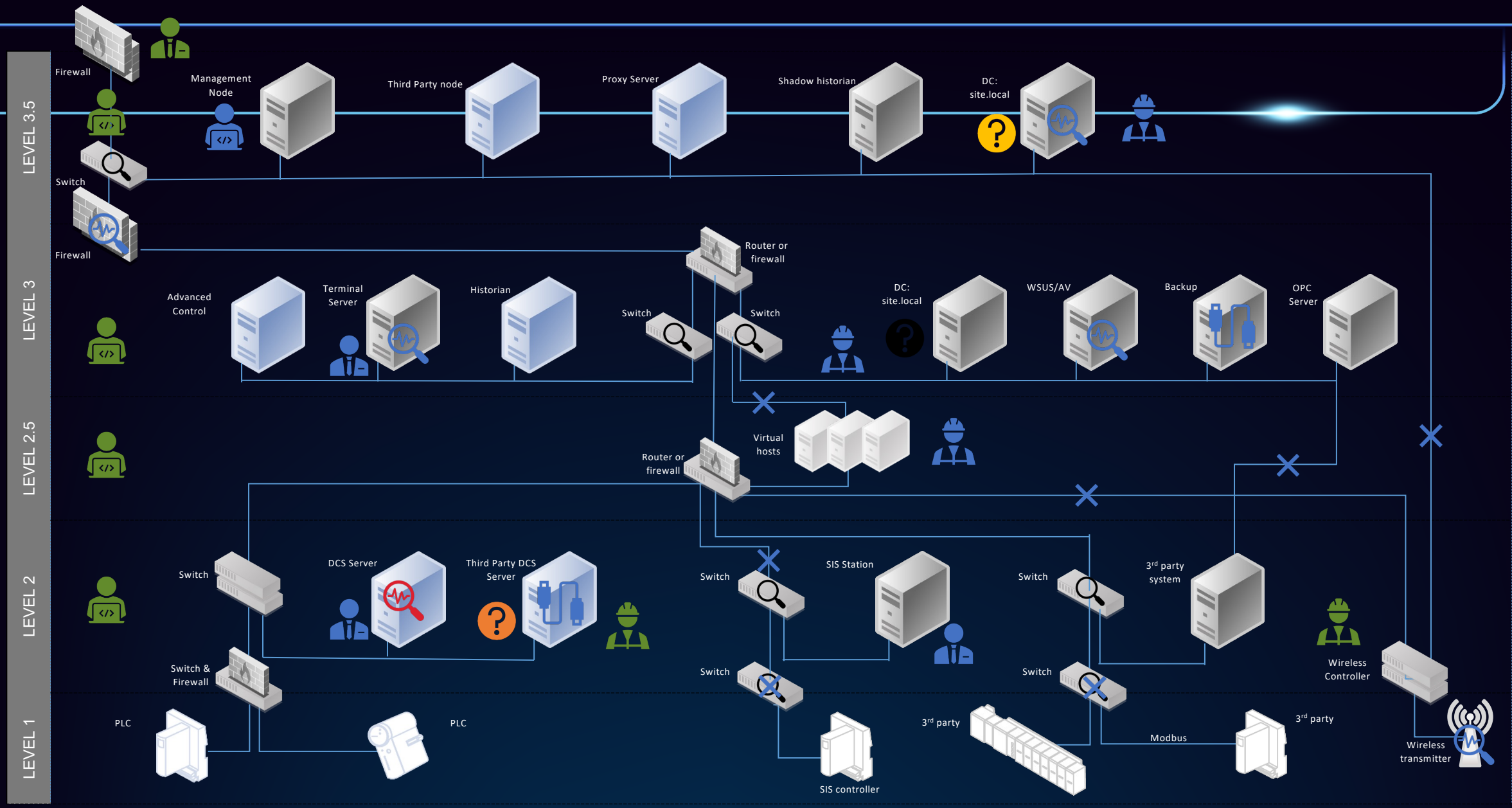
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

WHEN AND HOW OFTEN TO DO CSVA?



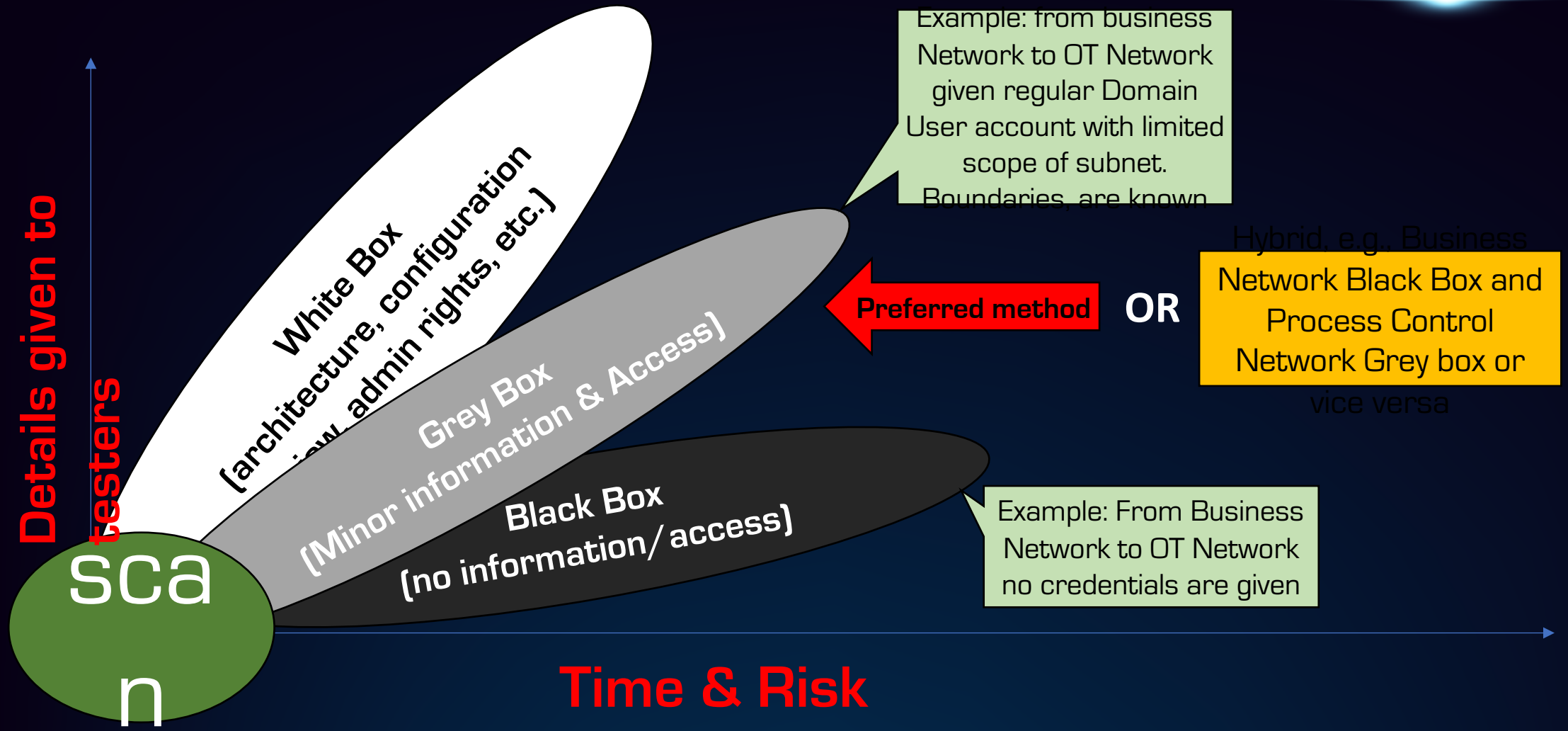
- After FAT (Factory Acceptance Testing)
- Before Ready for Operation
- Once a year for mature stable environments
- After every major change cyber journey just started
- At the end of projects and migrations
- In between, rely on automated, continuous monitoring

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023



OT PENETRATION TESTING

WHAT REALLY IS AN OT PENTEST?



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

BREAKING OT PENETRATION TEST INTO PHASES

1. External Phase (L5 → L4)

- The purpose of the external Penetration Test is to establish a foothold on IT networks leveraging social engineering, spear-phishing, USB drops, or exploitation of remote services including provided user access to company web portals.

2. Perimeter Phase (L4 → L3.5)

- The perimeter Penetration Test will assess the OT footprint on IT networks and can include enumeration of various information sources like SQL Servers, remote access, file transfer, historians, emails, documentation, and shared credentials. The primary objective of the perimeter Penetration Test is to pivot from IT network to OT DMZ network.

3. Process Phase (L3.5 → L3 / L2)

- Assess potential exploitation chains to establish a foothold on OT Control networks. On the OT Control network, as most systems are critical, the engagement will closely follow the parameters set by site during the pre-engagement phase. This can include privilege escalation on designated in-scope systems or establishing a network level session to a specific system or application.

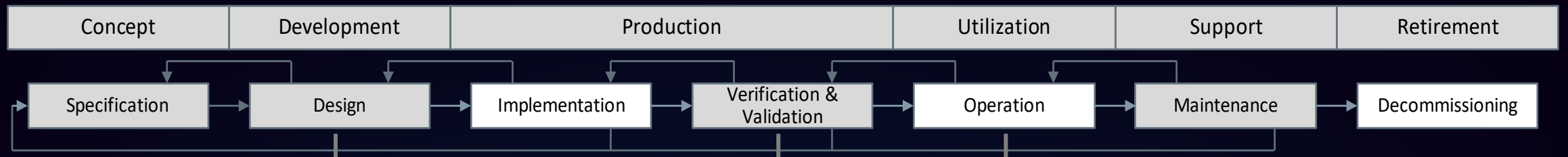
Table 19: Payload Testing

Payload	Threat Level	Target System	Detection?	Carbon Black	AV
Metasploit (Msfvenom)	Low	-	-	-	-
Core Impact	Moderate	Various	Yes	Yes	No
Obfuscated Powershell Payload	Moderate	Various	Yes	Yes	Yes
Covenant C2 with LOLBAS	High	Various	Yes	Yes	No
Mimikatz	Low	[redacted]	-	**Monitoring Mode**	No
Bloodhound	Low	[redacted]	-	**Monitoring Mode**	No

Endpoint malware protection is not present on the Production systems. Windows defender was found as well as McAfee Agent and CarbonBlack Protection was found on the system. Whitelisting is always a superior solution to block any type of execution which includes in-memory execution as this can be used in bypassing basic AV protection.

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

WHEN AND HOW OFTEN TO DO AN OT PENTEST?



- Limited “Penetration Testing”
- After FAT/SAT

- Post SAT/Commissioning before Ready for Operation (RFO)

- Once a year for mature stable environments
- After every major change cyber journey just started
- At the end of projects and migrations
- In between, rely on automated scanning (with dedicated ICS Product)

CONCLUSION AND KEY TAKEAWAYS

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

TAKEAWAYS

- **Cyber-Physical Risk Assessment (csHAZOP) - defines the security design requirements (looks at all possible threats)**

  Identifies cybersecurity threats and residual risk related to business loss using viable cybersecurity threats against the projected automation functions to determine whether residual risk meets the asset owner's risk criteria based on the Target Mitigated Event Likelihood (TMEL)

- **Cybersecurity vulnerability assessments - Checks if these requirements are properly implemented. (Looks at threats directly linked with the system's implementation)**

  Assess at the entire integrated industrial control system to identify weaknesses – people, processes, technologies

  For all stages of your cybersecurity journey

- **OT penetration testing - "Proof of the pudding is in the eating" (Attempts to find one or more threats not properly defended against)**

  Targeted approach to test your existing defenses in real-life scenarios, looks for "loopholes"


OTCEP
2023
OPERATIONAL TECHNOLOGY
CYBERSECURITY EXPERT PANEL FORUM 2023

THANK YOU