Securing connection between Safety-critical systems and the cloud

UITP Report: DESIGN FOR SECURITY OF RAIL SAFETY-CRITICAL SYSTEMS

ERA_ENISA conference
December 1 & 2, 2025

REPORT OBJECTIVE, SCOPE, TARGET, AND METHODOLOGY

Objective: Provide guidelines to engineers to design secure Safety Instrumented Systems (SIL 1 to 4).

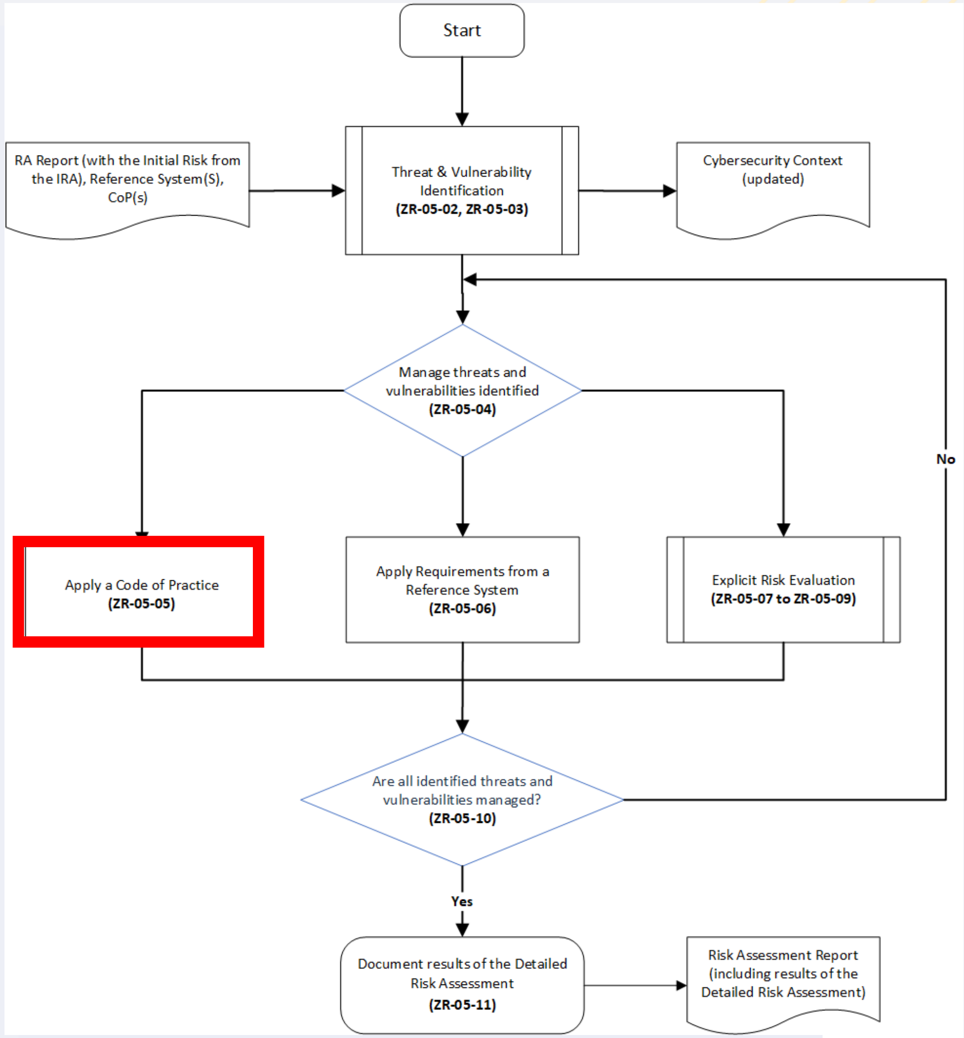
- Follow IEC 63452 recommendations, defining guidelines on how to integrate design throughout a SIS life cycle.
- Can serve as a baseline for a code of practice

Scope: Integrate best practices in terms of building synched safety and security cases.

- Provide the necessary background to understand all discussed topics.

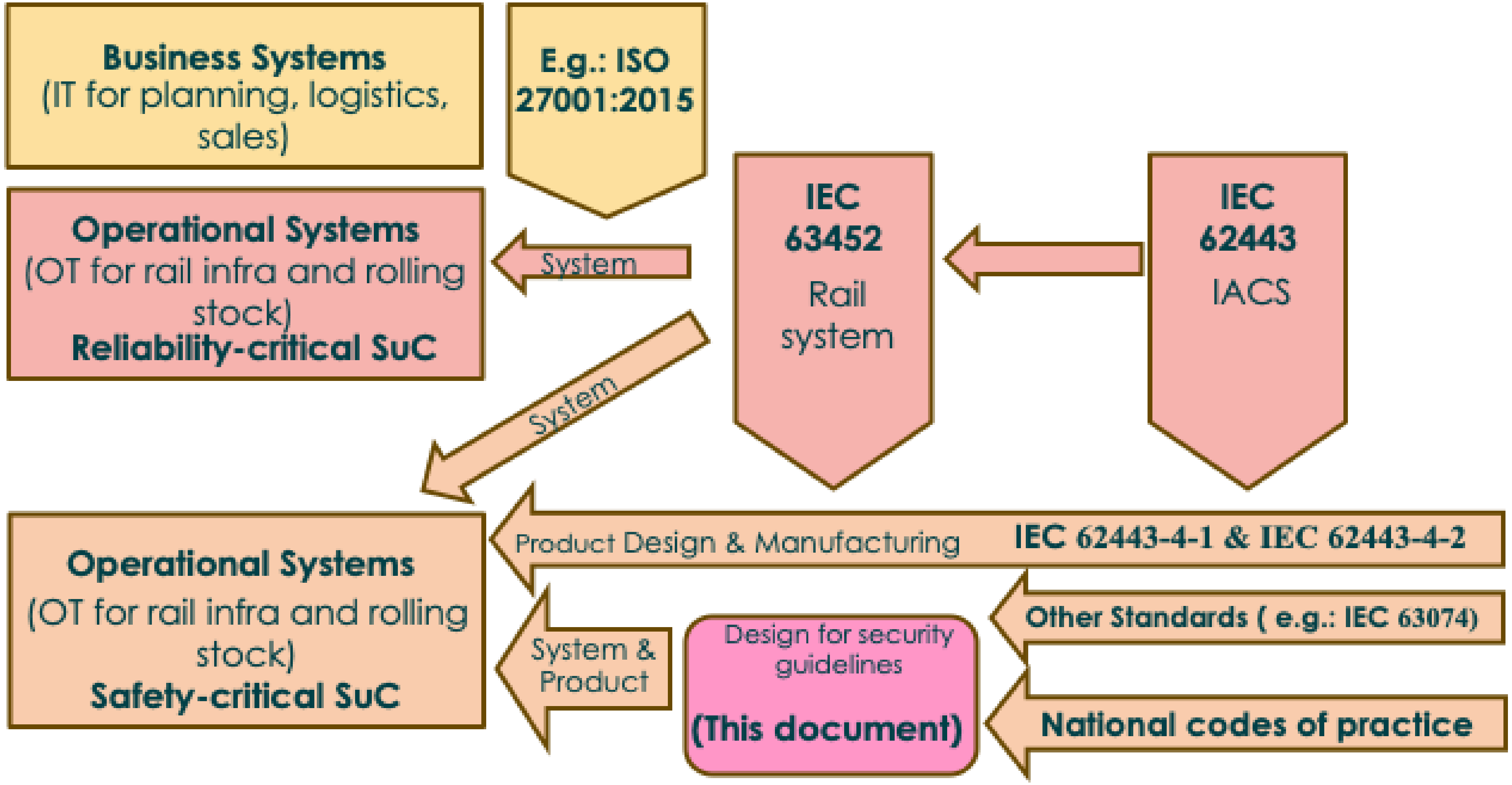
Target Audience: Aimed at safety engineers, design and cyber architectural engineers, security professionals, systems developers, and systems administrators of rail systems

Methodology: Based on 70+ Management Principles and 230+ Design Principles, applying to a SIS and relating to both Safety and Cybersecurity disciplines.



IEC 63452: SNEAK PEAK

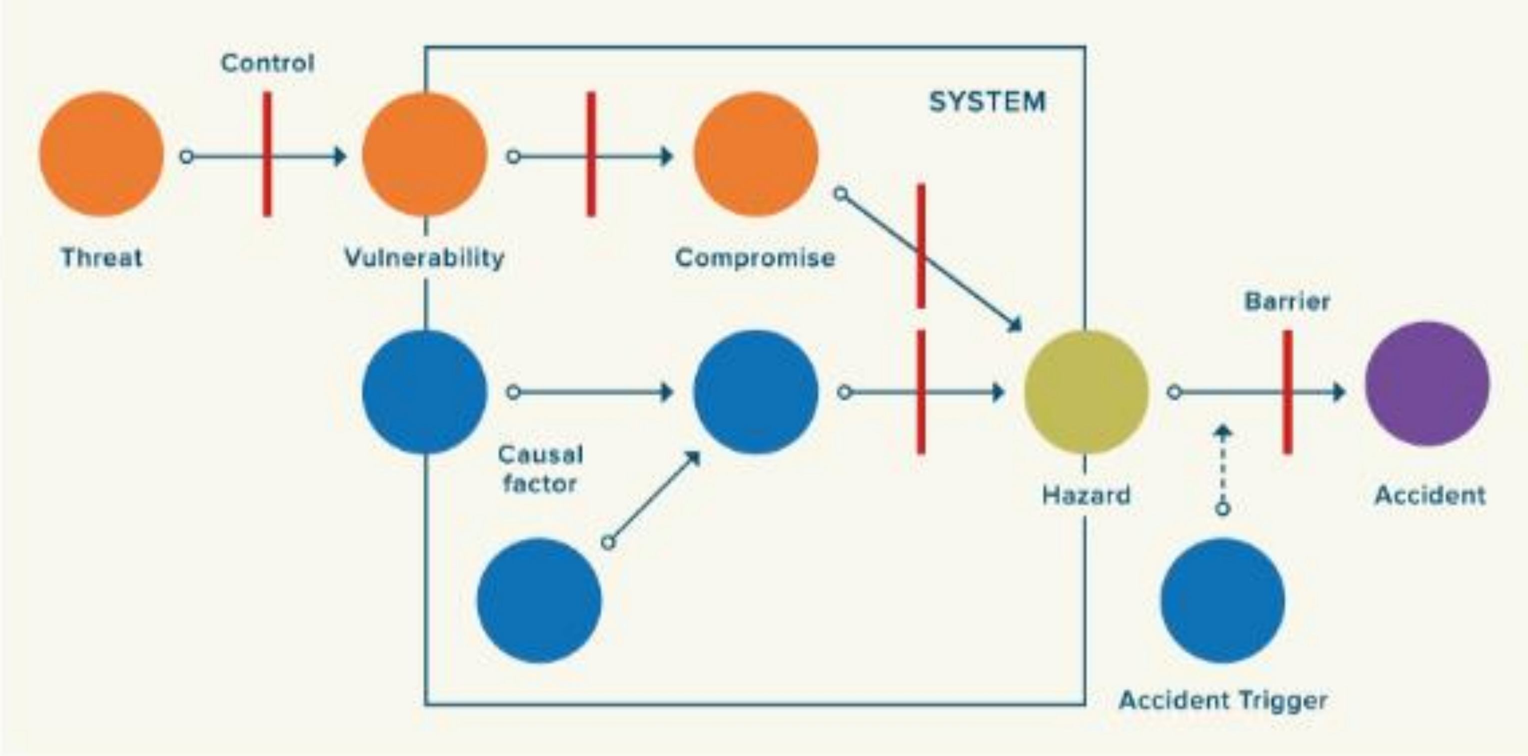
THE REPORT'S NORMATIVE ENVIRONMENT



Report positioning source: Serge Van Themsche

SIS RISK ASSESSMENT

- **Since an attack can impact a Safety Instrumented Function (SIF), a coordinated Safety/Security process for specifying, designing, implementing and validating is required**
  - Semi-quantified (Threats and Vulnerabilities) risks and (Safety causal factors) quantified risks can both generate hazards leading to an accident.



Relationship between causal factors and security, on hazards and accidents; Source UK Code of practice

THE REPORT'S STRUCTURE: 4 PARALLEL LIFE CYCLES

	System Development Lifecycle	Safety by Design Lifecycle	Product Line Lifecycle	Security by Design Lifecycle
Initiation	Concept Definition System Definition & Operational Context	Safety Planning Preliminary Hazard Assessment	Product Line Management	Security Planning Preliminary Threat Assessment
Acquisition	Tender Preparation and Evaluation	Tender Safety Requirements/ Evaluation	Product Line Proposal	Tender Security Requirements/ Evaluation
Design & Development	System Analysis Concept & Measures Architecture & SuC Requirement Definition	Detailed Safety Concept analysis Detailed Hazard and Risk Assessment Detailed Safety Architecture and SafeReq	Product Line Engineering Domain & Application Engineering Configuration Management	Detailed Security Concept Analysis Detailed Threat and Risk Assessment Detailed Security Architecture and SecReq
Manufacture or Procurement	Construction &"Whole SIS Programming" Inspection and testing plan	Safety Programmed & Developed Product Safety Testing Product Safety Certification	Program./Developed and Produced Product Testing Product Release	Security Programmed & Developed Component Security Testing Product Security Certification
Implementation	System Integration Testing	Safety Integration Testing	Product Line Verification	Security Integration Testing
System Validation	System Deployment	Safety Validation	Product Line Validation	Security Validation
System Acceptance	Commissioning	Safety Acceptance & Safety Case	Product Line Quality Assurance Update	Security Acceptance & Security Case
Op. & Maintenance	Operation & Support	Audit & Continuous Mon.	Product Updates	Audit & Continuous Mon.
Disposal	Disposal			

GUIDELINE PRINCIPLES

- **75+ Management Principles (MP):**
  - MPs drive the entire SIS development life cycle and are specific to safety and cybersecurity.
    - **MP1: Board Upper Management accountability for Safety and Security:** Depending on a Country's legislation, the PTOs board of Director or the CEO and his/her direct report are the ultimate owner(s) of these two risks.
- **230+ Design Principles (DP):**
  - DPs integrate IEC 63452 recommendations.
  - They apply to the SIS product and system development life-cycle and drive the cybersecurity network design and product manufacturing and testing.
  - They focus on issues impacting both safety and cybersecurity.
    - **DP1. Priority Principle:** Operational concepts drive safety design, which drives the cybersecurity design.
    - **DP33. SBoM safety-critical tracking principle:** the SBoM should be capable of automatic generation and the result must be machine-readable

DESIGN GUIDELINE PRINCIPLES: DETERMINISTIC ENGINEERING

- Integrating the report's Security-by-design management and design principles throughout the SIS' life cycle **shouldn't be viewed as a check list exercise.**
  - It must be understood as a global approach to **applying a deterministic cybersecurity engineering practice**.
- There is no reason why for Safety, the discipline relies on deterministic engineering methodology, while we often tolerate qualitative approaches for Security.
- The UITP cyber committee believes that whenever an SIF is involved, the cyber protection measures associated with the Capable Safety Level (SL-C) should meet or exceed the SL rate (→ i.e.: SL3 or SL4)
  - Though in theory, it is tolerated to lower the security measures.
- The great contribution of IEC 63452 = **Security case signed off by security experts.**
  - Deviations must be recorded and reviewed from time to time during the operation and maintenance phase.

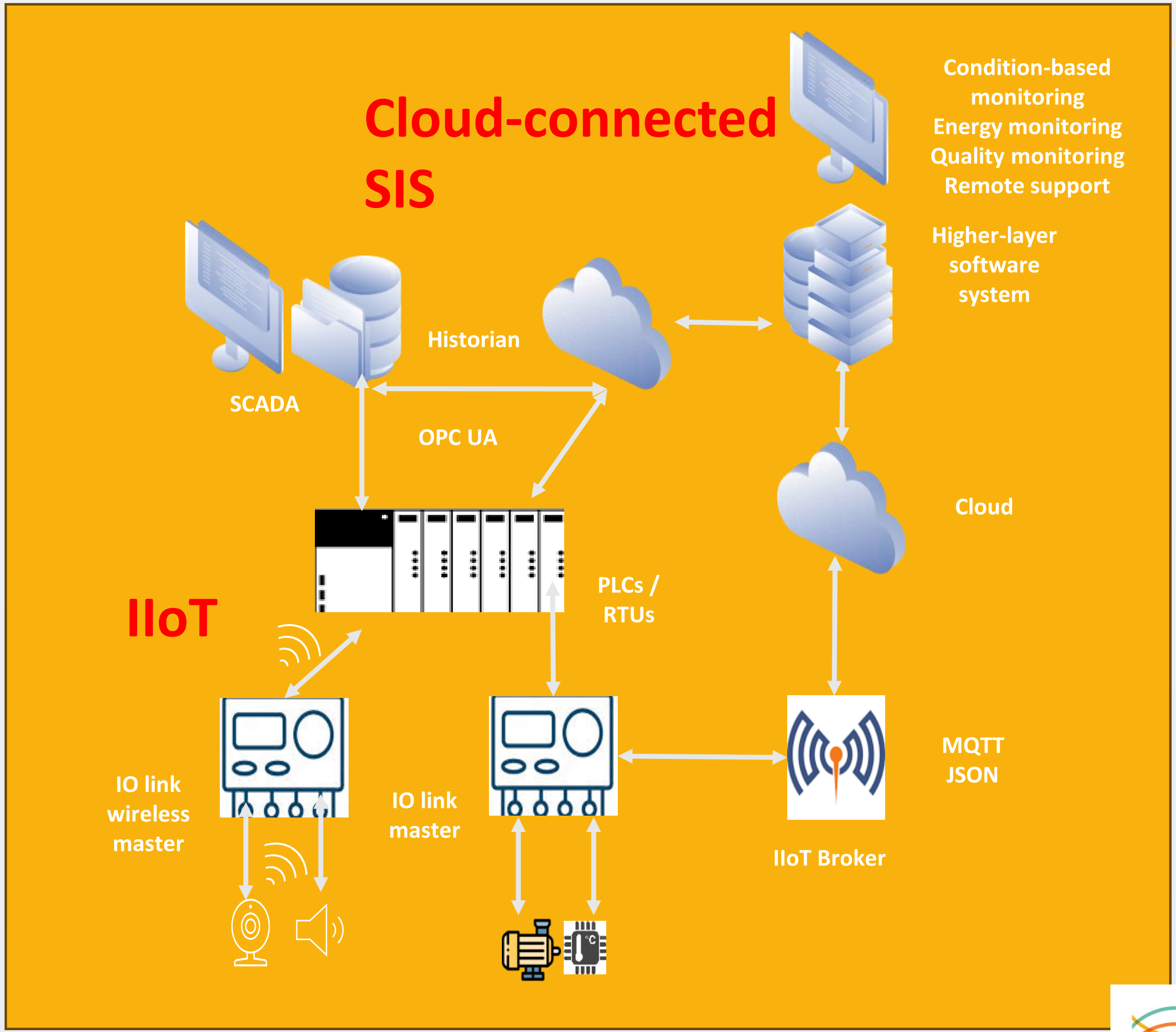
FOCUS ON SIS TO CLOUD-CONNECTION

Safety Instrumented System

- It is an independent protection layer designed to bring a process to a safe state when predetermined conditions are violated, with its reliability and performance quantified by a Safety Integrity Level (SIL 1 to 4).

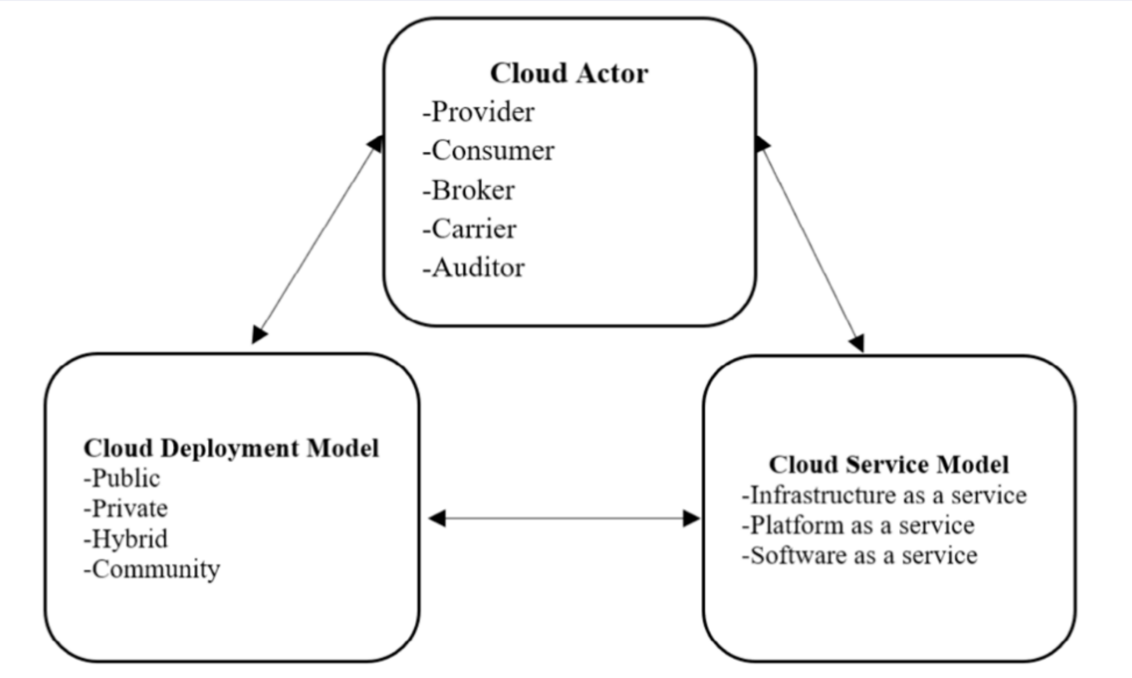
Cloud-connected SIS (OT)

- Extends traditional OT systems' functionalities by allowing data connection in the cloud and provisioning business enablement and control from the cloud.
    - IIoT allows direct connection to the cloud or to PLCs



CLOUD-CONNECTED OT RISKS: UNDERSTANDING

- The cybersecurity risk doesn't disappear miraculously with a cloud-enabled architecture. It is just shared between different stakeholders, adding complexity.
- The more off-premise activities, the more potential for new attack vectors targeting your rail on-prem. activities.
- The more open the cloud deployment and service models, the more risks.



Three-dimensional approach of NCC-SRA from NIST Cloud Computing Security Reference Architecture

CLOUD-CONNECTED OT RISKS: ATTACK TYPES

- **Rogue cloud actor**
  - **Internal attacks:** The biggest security threat, as the datacenter's own employees with access to the servers.
  - **Phishing attacks:** Obtaining employee credentials.
- **Access attacks**
  - Hackers can leverage Cloud Access Security Brokers or third-party DNS servers to get into a datacenter.
- **Cloud pivoting attacks**
  - **Application attacks:** Using infected application (e.g., control panel or customer dashboard) and vulnerable operating systems.
- **Cloud Infra attacks:**
  - **DCIM vulnerability exploit**: power DCIM (e.g., Cyber Power Panel Enterprise) and Power Distribution unit (e.g., Dataprobe iBoot, PDU), cooling system can shut down the services.
  - **Multi-site attacks**: Malicious threat actors could carry-on worldwide attacks across numerous datacenters (malware across multi-site could be leveraged for massive ransomware, DDoS, or Wiper attacks).

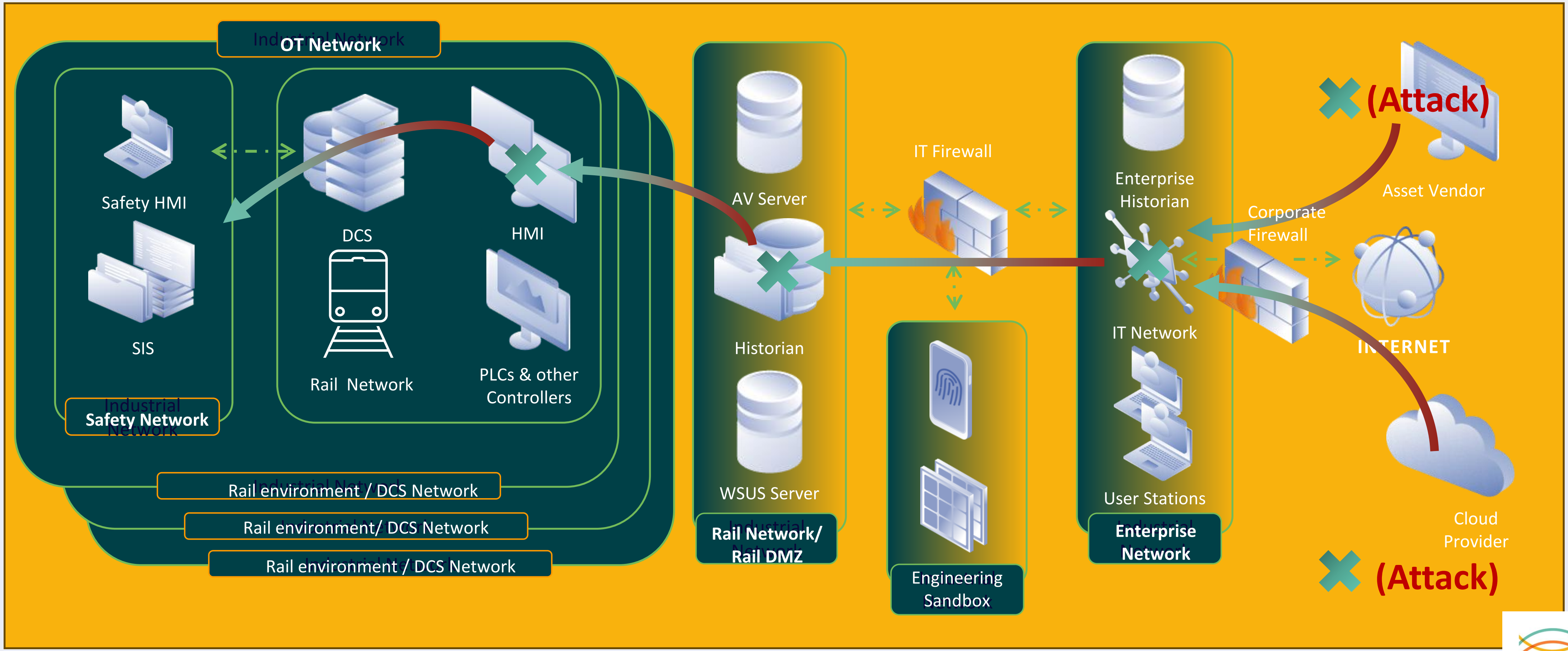
- Researchers have found over 20,000 instances of publicly exposed datacenter infrastructure management (DCIM) software that monitor devices, HVAC control systems, and power distribution units, which could be used for a range of catastrophic attacks (Source Cyble; 2022).

UITP

CLOUD-CONNECTED OT RISKS: ATTACK VECTORS

1) Top-down

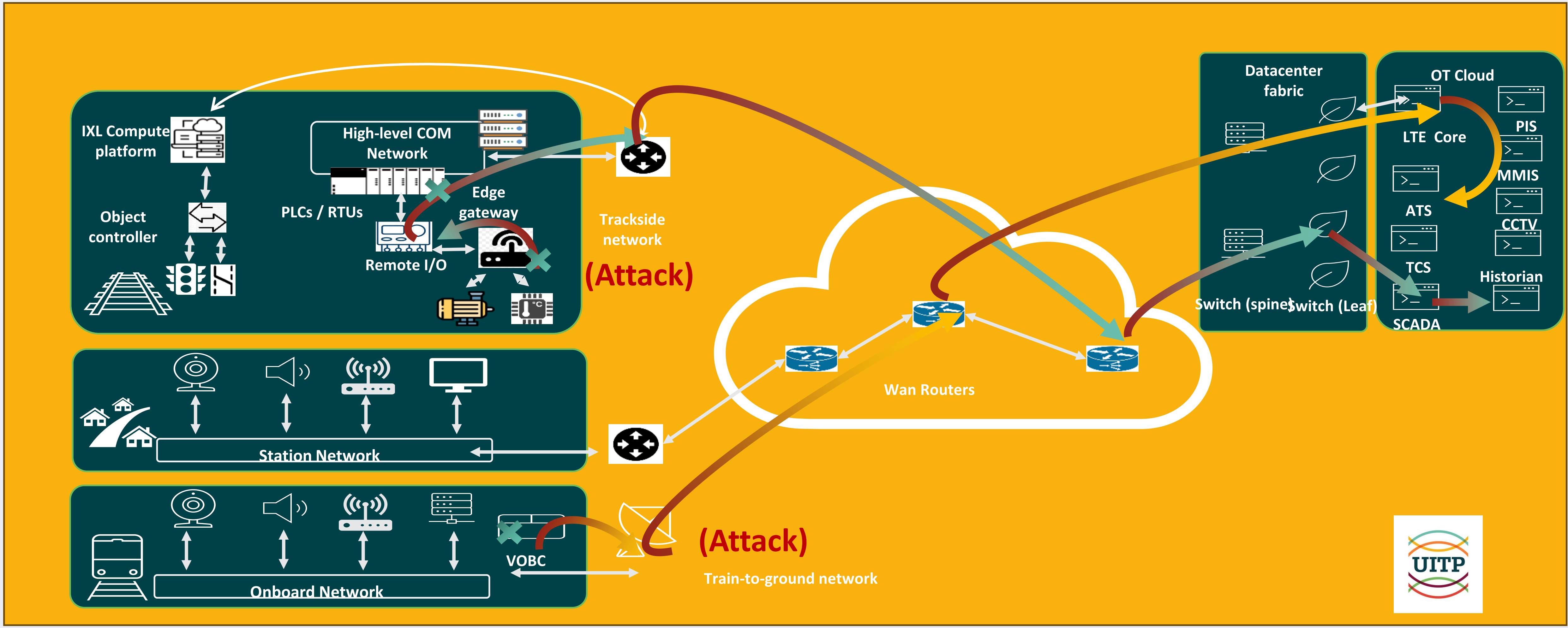
- The attack starts from the cloud and continues to take over all Rail Duty Holder's PLCs and other equipment.



CLOUD-CONNECTED OT RISKS: ATTACK VECTORS

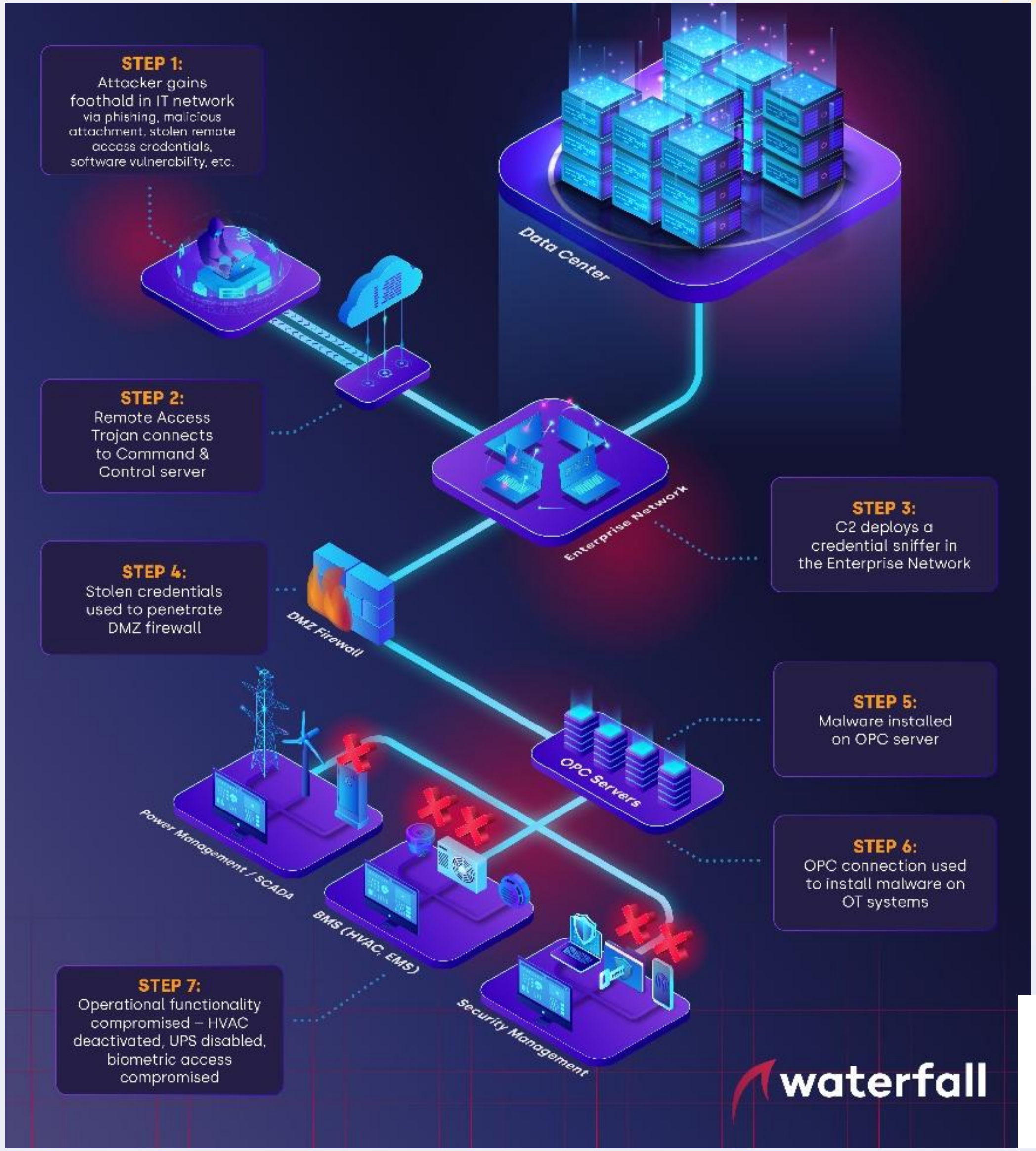
2) Bottom-up

- Starts from a component connected to a PLC and continues up to the PLCs /SCADA and then to the cloud OT



3) Infrastructure shut-down

- **Targets the datacenter infrastructure with the objective of paralyzing it (e.g.: HVAC or power)**
- **Forcing the datacenter manager to disconnect the hosted services.**



DESIGN: CLOUD-CONNECTED ARCHITECTURAL DESIGN (IEC 63452)

- **IEC 63452 cloud annex K.**
- **Whole rail system risk analysis: Security-Level measures shouldn't be established on just the cloud-connected OT systems.**
- **Dedicated access control policy: IIoT and OT cloud-connections require strict access**
  - Identity and Access Management based on: RBAC, MFA, PTO managed credentials, etc.
  - A zones and conduits should use principles of least privilege for any communication between zones.
  - Communications between zones should employ modern encryption algorithms.
  - Enforce the use of TLS/SSL with strong cipher suites.
  - Manage PKI Certificates.
  - Establish cloud security monitoring of the railway system.
- **Directionality and type of data: will drive risk and appropriate cybersecurity countermeasures.**
  - Control signals received from a cloud instance to an OT system should be filtered, authenticated, and monitored for cybersecurity anomalies.
  - Non-control signal data such as cybersecurity monitoring and telemetry data from an OT system to a cloud instance should be implemented in a uni-directional fashion.

CLOUD-CONNECTED SIS ARCHITECTURAL DESIGN (IEC 63452)

- **Communication matrix analysis**
  - Based on zone criticality for the cloud-connected OT and IIoT architecture.
    - Use guidance from IEC 63452.
    - Check what is Monitored vs Controled data.
- **Apply dataflow directionality rules**
  - Based on the PTO's risk appetite apply one the following rules:
    - "+" data flow is allowed in both directions.
    - "R": data flow is restricted to read-only (from ZC-L5 to ZC-L4) only by data diodes or similar measures which maintain unidirectional flow
    - "-": data flow is prohibited

Zone criticality and communication matrix

landside – landside

Zone criticality landside (ZC-L)	Zone Security	Example	ZC-L5s highly secure / Safety Safety: Interlocking, High Voltage	ZC-L5 highly secure / critical SCADA, ATS, central ICS/ SCADA System, platform screen doors	ZC-L4 secure Data Centre, internal DMZ, ICS/Automation	ZC-L3 medium Internal network, Office and Business network	ZC-L2 low Gateway area, External DMZ	ZC-L1 low External partner/companies	ZC-L0 none / unsecure Internet
source / from			destination / to						
ZC-L 5s	highly secure / Safety	safety: interlocking, high voltage	+	+	R	R	R	R	-
ZC-L 5	highly secure /critical	SCADA, ATS, central ICS, platform screen doors	+	+	+	R	R	R	-
ZC-L 4	secure	data centre, internal DMZ, ICS/automation	-	+	+	+	R	R	-
ZC-L 3	medium	internal network, office and business network	-	-	+	+	+	R	-
ZC-L 2	low	gateway area, external DMZ	-	-	-	+	+	+	+
ZC-L 1	low	external partner/companies	-	-	-	-	+	+	+
ZC-L 0	untrusted	Internet	-	-	-	-	-	+	+

CONCLUSION: CYBERSECURITY DETERMINISTIC DESIGN APPROACH

- **Cloud-connected OT and IIoT solutions bring many benefits but their design introduces new risks and vulnerabilities.**
  - IIoT is especially vulnerable to cyber attacks.
  - Cloud design shares the PTO's risks with other actors.
- **Specific Cloud-connected OT and IIoT risks require specific design.**
- **Use deterministic cyber design approach in cloud-environments to provide an SL3/SL4 protection to SIS (SIL 3 to 4)**
  - Around defense-in-depth principles:
    - Network segmentation using Hardware enforced protection and other technologies.

UITP

THANK YOU!

https://www.linkedin.com/in/serge-van-themsche/

https://waterfall-security.com/

waterfall