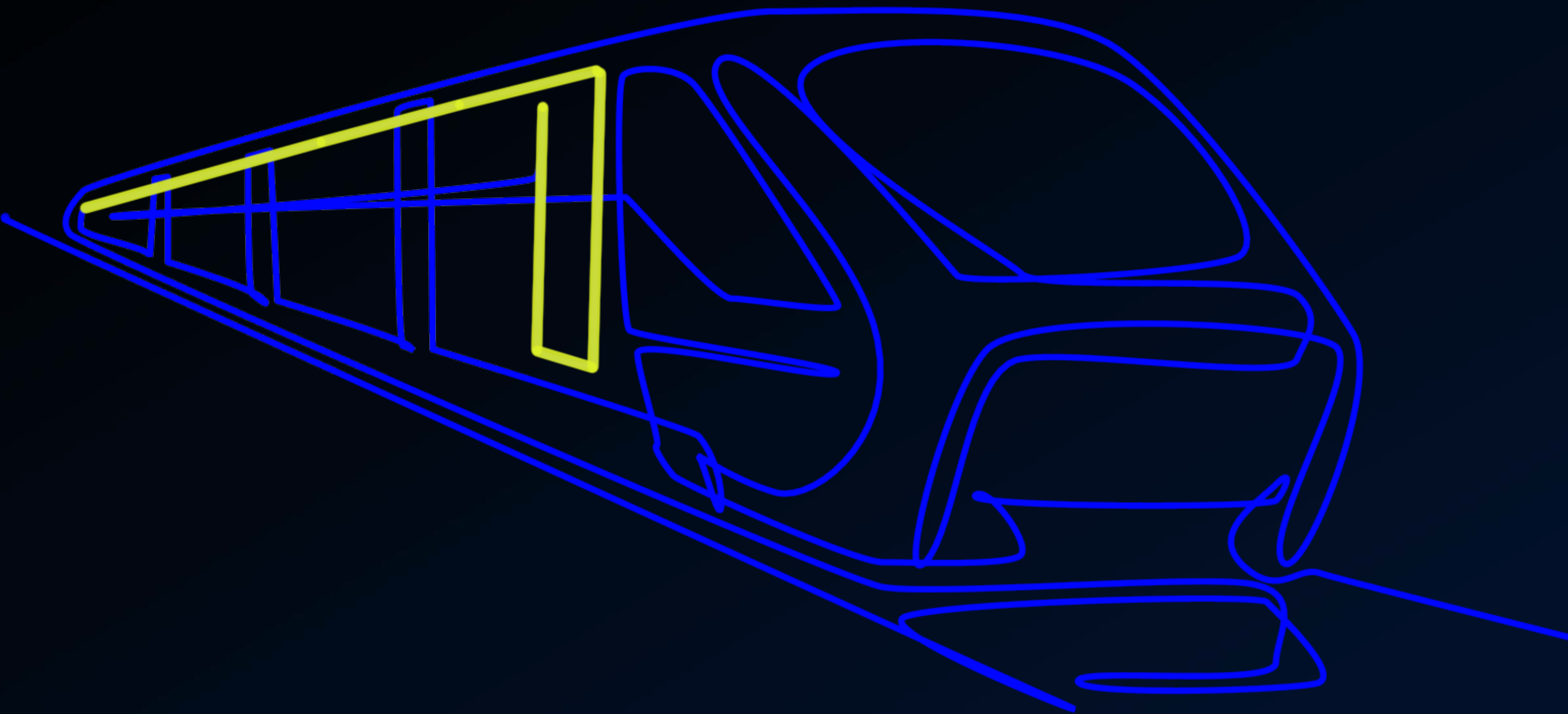
Radiflow

Securing Railway Operations from OT Cyberattacks

The Radiflow Cybersecurity Team
March 2022



1. Introduction

Railway systems – both inter-city and inner-city light rail and metro systems – are considered among the most critical national infrastructure operations in many countries where the bulk of passenger and goods transport is done by rail. And while we have seen in recent years debilitating attacks (primarily ransomware attacks, for extorting a cash ransom) on railway companies' IT systems, an attack on a railway's OT networks, e.g. on its signaling system, could lead to loss of life, damage to tracks, trains and transported goods, as well as environmental damages in the case of hauling hazardous materials.

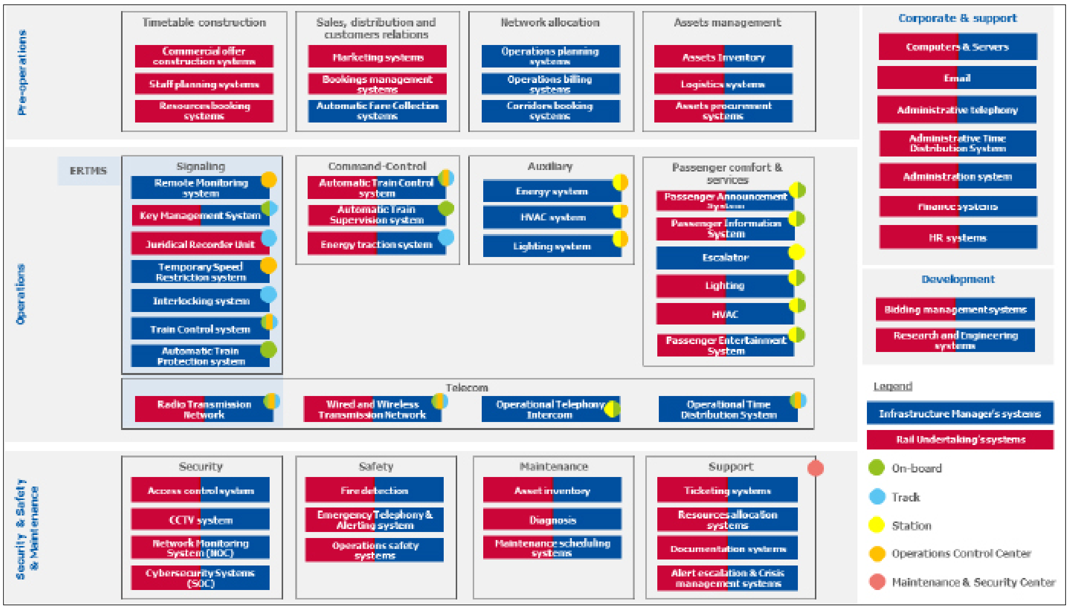
Railway companies' communications and operations networks are, as in other traditional industrial settings, divided roughly between the IT and OT sides (even though the boundaries between the two have blurred over the years).

On the IT side, much of the protected information is managed by the Passenger Information System (PIS), which encompasses all customer service, ticketing and online operations.

The OT side controls a number of critical systems, which manages (among many other functions):

- Railways power management and safety systems
- Various building management system (BMS) operations at stations and train depots, e.g. power, air conditioning (HVAC) and elevators
- The railway signaling system (both onboard trains and track signaling), which controls track shifting and emergency braking. These systems typically connect and transmit data to a central command & control center via both wired and wireless transmission networks.

In addition, OT operations controls various physical security systems such as access control and video surveillance, at stations and onboard trains.



Pre-operations
Timetable construction
Commercial offer construction systems
Staff planning systems
Resources booking systems
Sales, distribution and customers relations
Marketing systems
Bookings management systems
Automatic Fare Collection systems
Network allocation
Operations planning systems
Operations billing systems
Corridors booking systems
Assets management
Assets Inventory
Logistics systems
Assets procurement systems
Operations
ERTMS
Signaling
Remote Monitoring system
Key Management System
Juridical Recorder Unit
Temporary Speed Restriction system
Interlocking system
Train Control system
Automatic Train Protection system
Command-Control
Automatic Train Control system
Automatic Train Supervision system
Energy traction system
Auxiliary
Energy system
HVAC system
Lighting system
Passenger comfort & services
Passenger Announcement System
Passenger Information System
Escalator
Lighting
HVAC
Passenger Entertainment System
Telecom
Radio Transmission Network
Wired and Wireless Transmission Network
Operational Telephony Intercom
Operational Time Distribution System
Security & Safety & Maintenance
Security
Access control system
CCTV system
Network Monitoring System (NOC)
Cybersecurity Systems (SOC)
Safety
Fire detection
Emergency Telephony & Alerting system
Operations safety systems
Maintenance
Asset inventory
Diagnosis
Maintenance scheduling systems
Support
Ticketing systems
Resources allocation systems
Documentation systems
Alert escalation & Crisis management systems
Corporate & support
Computers & Servers
Email
Administrative telephony
Administrative Time Distribution System
Administration system
Finance systems
HR systems
Development
Bidding management systems
Research and Engineering systems
Legend
Infrastructure Manager's systems
Rail Undertaking's systems
On-board
Track
Station
Operations Control Center
Maintenance & Security Center

A listing of OT functions in typical railway systems (Source: ENISA Railway Security Report, 2020)

2. Unique Risk Factors

To make things worse, railways face a unique combination of factors that exacerbate their exposure to cyber-threats:

- Increased connectivity to reporting and traffic management systems (such as the U.S. Positive Train Control aimed at preventing train collisions)
- Broad device-vendor mix throughout the railway network, which introduces a myriad of vendor- and device-specific threats
- Widely dispersed systems, ranging across different counties, states and even countries adds complexity to the transmission of network data from remote locations (often over low-bandwidth networks) for security monitoring and analysis
- As railway systems are often state-owned and/or subsidized, they are often under-funded by local or federal governments, leaving tighter budgets for OT security

In addition, at this time of heightened geopolitical tensions and military conflicts, railways, as a national critical infrastructure, may be especially targeted by state-sponsored attackers seeking to wreak havoc on both military and civilian transport using various hacking methods (we have already witnessed a ransomware attack on Belarus' state-run railway's computer system , aimed at preventing the transport of Russian troops and artillery to the country, in anticipation of an attack on Ukraine).

3. Emerging Government Regulations

US TSA's security directive 1580-21-01

The above risk factors, as well as the distributed ownership of the American railway infrastructure which has shown to inhibit the reporting of cyber-attacks and cross-operator cooperation in railway security, were the driving force behind the US TSA's security directive 1580-21-01 for enhancing railway security.

- The new TSA's directive aims at creating a uniform system across the American railway industry for reporting and managing security incidents. This includes:
- Requiring that each ground carrier designate a point person opposite the TSA and the DHS' Cybersecurity and Infrastructure Security Agency (CISA) to coordinate the implementation of cybersecurity practices and reporting of incidents
- Mandatory development of Cybersecurity Incident Response Plans to reduce the risk of operational disruption in case of an attack
- Conduct a cybersecurity vulnerability assessment, including assessing security practices and technologies; identifying cybersecurity gaps; and identifying remediation measures to rectify cybersecurity vulnerabilities and gaps.

ENISA's 2020 Railway Security Directive

The concerns and recommended security measures listed in the TSA directive echo those listed in its European counterpart issued a year earlier, the November 2020 Railway Cybersecurity report issued by ENISA (the EU central cybersecurity agency)

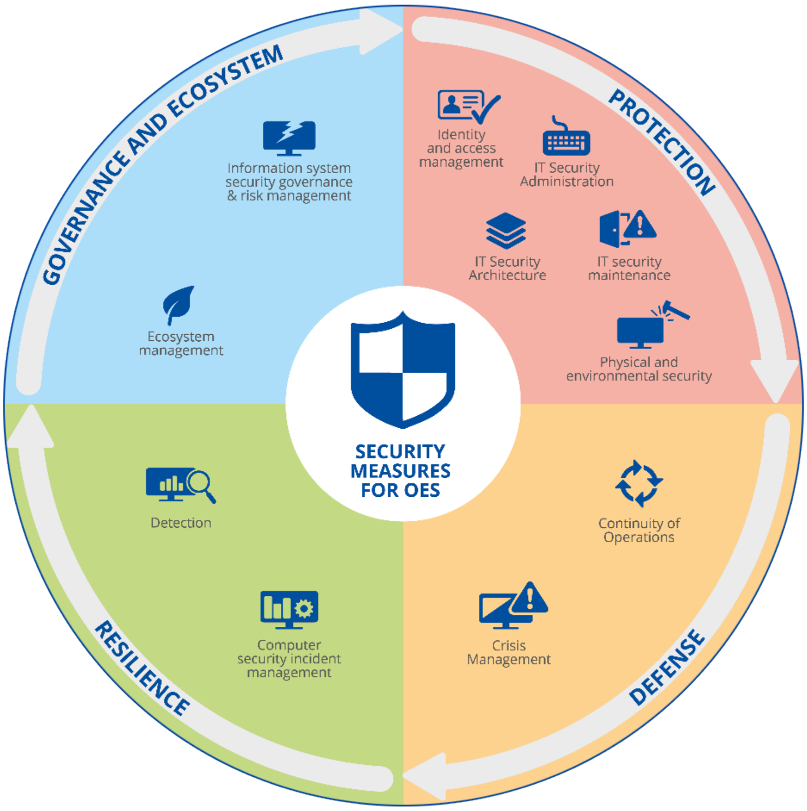
The ENISA directive defines the four domains that make up railway operations and the security measures associated with each:

- Governance, risk management and ecosystem management
- Protection: including identity & access management; IT security administration, architecture & maintenance; and physical & environmental security
- Defense: including continuity of operations and crisis management
- Resilience: including detection and incident management

Noteworthy among the security measures indicated in the ENISA directive is the strong recommendation to apply (the relatively new) risk-based approach to OT security, using risk management solutions designed for today's OT security space, such as Radiflow's own automated industrial risk assessment and management platform.

To this end ENISA published a guide for arranging the OT network logically into Zones and Conduits for railway operations, as specified on the IEC 62443 standard.

Applying a risk-based methodology to OT security enables optimizing OT security operations by quantitatively calculating the actual risk the Railway OES may incur following a cyberattack, accounting for the impact of an attack on each and every business unit, as well as for the risk tolerance of the organization.


GOVERNANCE AND ECOSYSTEM
Information system security governance & risk management
Ecosystem management
PROTECTION
Identity and access management
IT Security Administration
IT Security Architecture
IT security maintenance
Physical and environmental security
SECURITY MEASURES FOR OES
Continuity of Operations
Crisis Management
DEFENSE
Detection
Computer security incident management
RESILIENCE

Security measures for railway operators defined as operators of essential services (OES)

4. Radiflow's Solutions for Protecting Railway Systems' OT Networks

Radiflow's OT-security suite has been successfully implemented in a number of major ground transportation carriers worldwide.

Radiflow's multi-prong solution provides anomaly detection and threat monitoring on the OT part of the Railway infrastructure (railway energy provision and BMS) to ensure the detection of breach attempts originating from the IT network. The Radiflow solution further improves network oversight by providing full visibility (via network "maps") into the OT network, including all and device properties, vulnerabilities, communication protocols and possible intra-network attack vectors.

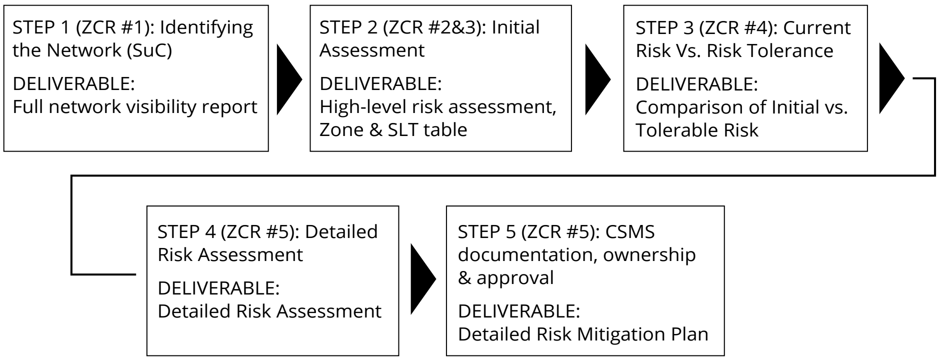
Once discovered, assets are grouped into Zones (connected by Conduits) to facilitate IEC 62443-compliant risk assessment & management, as per ENISA's guide to Zones & Conduits.

Using multiple data feeds for newly-discovered threats and vulnerabilities, as well as rich contextual information received from signaling and other equipment vendors for cybersecurity analysis, Radiflow's threat detection and monitoring solution provides operators full control over anomaly alerting and incident handling.

The Radiflow system connects to the railway operator's enterprise SOC where all incident, event analysis and cyber risk management is performed, and allows for instant access to each and every intrusion detection system in the carriers network. The Radiflow system also integrates with dedicated railway signaling security providers as well as a large array of IT security players, for context enrichment and better threat detection, as well as for easily implementing Radiflow solution within a wide range of data and asset management platforms.

As a renowned compliance enabler, Radiflow accompanies its OT-operator customers through the cyber risk assessment process, in accordance to leading standards, such as IEC 62443 and the new TSA directive for ground transportation.

The different steps in the process, which progresses from network discovery to assessment to risk remediation, are defined in both the ENISA guidelines and IEC 62443 as ZCRs (Zone and Conduit Requirements), as follows:



STEP 1 (ZCR #1): Identifying the Network (SuC)
DELIVERABLE:
Full network visibility report

STEP 2 (ZCR #2&3): Initial Assessment
DELIVERABLE:
High-level risk assessment, Zone & SLT table

STEP 3 (ZCR #4): Current Risk Vs. Risk Tolerance
DELIVERABLE:
Comparison of Initial vs. Tolerable Risk

STEP 4 (ZCR #5): Detailed Risk Assessment
DELIVERABLE:
Detailed Risk Assessment

STEP 5 (ZCR #5): CSMS documentation, ownership & approval
DELIVERABLE:
Detailed Risk Mitigation Plan

Radiflow's risk assessment process follows the ZCR methodology used in both IEC 62443 and the ENISA guidelines for railway and other OT organizations

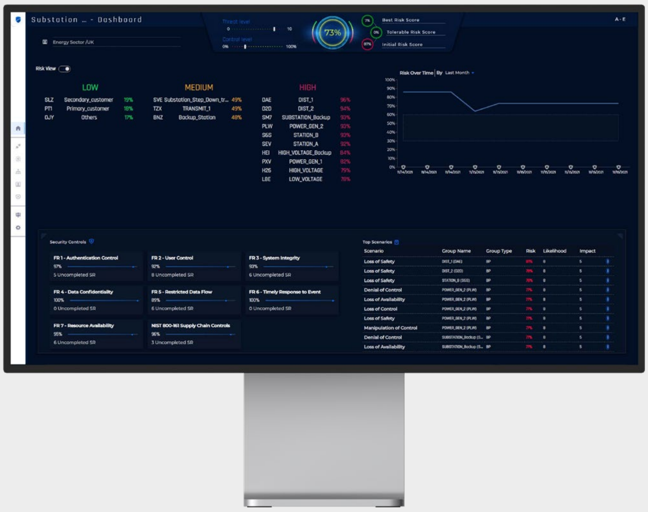
Going beyond threat detection, network visibility and security assessment, Radiflow's risk management platform empowers users to optimize their cybersecurity expenditure by prioritizing the threats that pose the most risk to the organization as a whole (accounting for the impact of a debilitating attack on each zone/business unit) and subsequently the mitigation measures best suited to reducing the most risk, toward increasing the ROI of the entire cybersecurity operation.

Radiflow's risk assessment process involves analyzing thousands of data points for network and asset properties, threat intelligence and impact calculation, toward providing various KPIs and full reports for the network's risk state:

- Network and asset properties: using non-intrusive self-learning of the OT network, Radiflow creates a complete digital image of the network with all network, communications and assets properties and vulnerabilities.

  The digital image serves as the baseline activity model for assessing risk and OT cybersecurity planning. Additional properties include the sector and region the SuC (System under Consideration) operates in, to de-prioritize threat tactics that aren't relevant to the SuC. Other information may be provided by the SuC owner, such as threat mitigation measures already in place.
- Threat intelligence: newly-detected threats and threat players' capabilities are analyzed and published by a number of dedicated agencies (e.g. MITRE ATT&CK) as well as by others, including Radiflow's own research.
- Zone impact & criticality, risk tolerance and other considerations: assets and business processes are grouped into zones with different levels of criticality and security needs (e.g. processes linked to "Safety" are assigned high criticality and a higher target security level).

  The SuC owner also provides the quantified impact of debilitating attacks on different business units, as well as other considerations, such placing partial focus on closing certification gaps vs. hardening critical processes only.



Substation ... - Dashboard

Energy Sector /UK

Threat level 0 – 10

Control level 0% – 100%

73%

7% Best Risk Score

0% Tolerable Risk Score

87% Initial Risk Score

A - E

Risk View

LOW			MEDIUM			HIGH		
SLZ	Secondary_customer	19%	SVE	Substation_Step_Down_tr...	49%	DAE	DIST_1	96%
PT1	Primary_customer	18%	TZX	TRANSMIT_1	49%	D2D	DIST_2	94%
DJY	Others	17%	BNZ	Backup_Station	48%	SM7	SUBSTATION_Backup	93%
						PLW	POWER_GEN_2	93%
						S6S	STATION_B	93%
						SEV	STATION_A	92%
						HEI	HIGH_VOLTAGE_Backup	84%
						PXV	POWER_GEN_1	82%
						H26	HIGH_VOLTAGE	79%
						LBE	LOW_VOLTAGE	78%

Security Controls

FR 1 - Authentication Control
97%
5 Uncompleted SR

FR 2 - User Control
92%
8 Uncompleted SR

FR 3 - System Integrity
93%
6 Uncompleted SR

FR 4 - Data Confidentiality
100%
0 Uncompleted SR

FR 5 - Restricted Data Flow
89%
6 Uncompleted SR

FR 6 - Timely Response to Event
100%
0 Uncompleted SR

FR 7 - Resource Availability
95%
6 Uncompleted SR

NIST 800-161 Supply Chain Controls
96%
3 Uncompleted SR

Top Scenarios

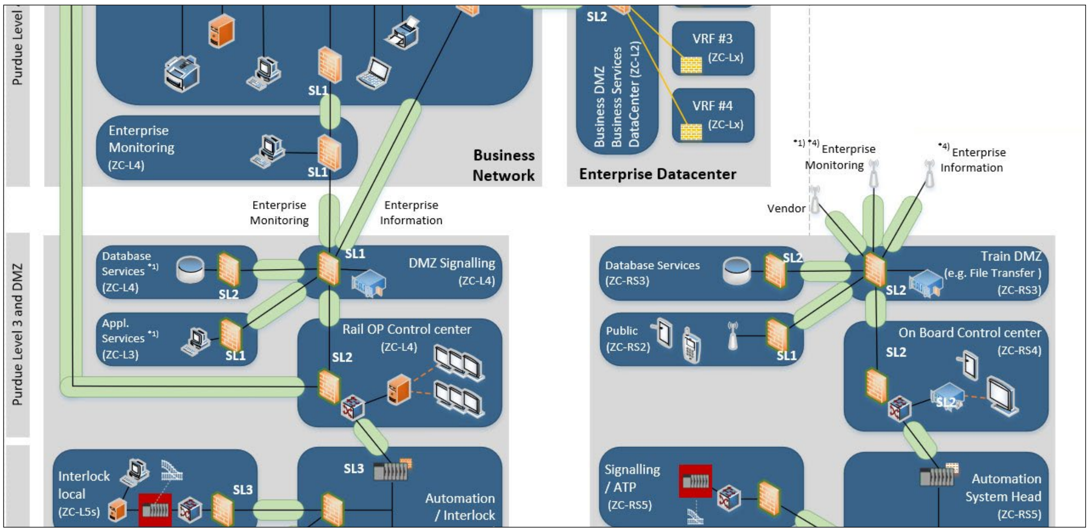
Scenario	Group Name	Group Type	Risk	Likelihood	Impact
Loss of Safety	DIST_1 (DAE)	BP	81%	8	5
Loss of Safety	DIST_2 (D2D)	BP	78%	8	5
Loss of Safety	STATION_B (S6S)	BP	78%	8	5
Denial of Control	POWER_GEN_2 (PLW)	BP	77%	8	5
Loss of Availability	POWER_GEN_2 (PLW)	BP	77%	8	5
Loss of Control	POWER_GEN_2 (PLW)	BP	77%	8	5
Loss of Safety	POWER_GEN_2 (PLW)	BP	77%	8	5
Manipulation of Control	POWER_GEN_2 (PLW)	BP	77%	8	5
Denial of Control	SUBSTATION_Backup (S...	BP	77%	8	5
Loss of Availability	SUBSTATION_Backup (S...	BP	77%	8	5

Radiflow's CIARA OT Risk Assessment & Management Platform analyzing thousands of data points for network and asset properties, threat intelligence and impact calculation, toward providing various KPIs and full reports for the network's risk state.

All asset, network, threat and SuC owner-provided data points are used to run numerous breach and attack simulations (Radiflow's BAS simulations are non-destructive (as they don't involve any operations on the OT network itself).

The simulations determine the most impactful threats to the network and subsequently the most effective mitigation controls that deliver the most risk reduction per dollar spent.

The results of Radiflow's risk assessment are provided in the form of various high-level and detailed reports used for budgeting, auditing and follow up, as well as a detailed mitigation plan listing the most effective (high-ROI) mitigation measures, accounting for the user's budget and risk management preferences.


Purdue Level
SL1
Enterprise Monitoring (ZC-L4)
SL1
Business Network
SL2
Business DMZ
Business Services
DataCenter (ZC-L2)
VRF #3 (ZC-Lx)
VRF #4 (ZC-Lx)
Enterprise Datacenter
*1) *4) Enterprise Monitoring
*4) Enterprise Information
Vendor
Enterprise Monitoring
Enterprise Information
Purdue Level 3 and DMZ
Database Services *1) (ZC-L4)
SL2
SL1
DMZ Signalling (ZC-L4)
Appl. Services *1) (ZC-L3)
SL1
Rail OP Control center (ZC-L4)
SL2
Database Services (ZC-RS3)
SL2
Train DMZ (e.g. File Transfer) (ZC-RS3)
SL2
Public (ZC-RS2)
SL1
On Board Control center (ZC-RS4)
SL2
SL2
Interlock local (ZC-L5s)
SL3
SL3
Automation / Interlock
Signalling / ATP (ZC-RS5)
Automation System Head (ZC-RS5)

Example for defining Security Levels for Zones, from ENISA's Zoning and Conduits Guidelines for Railway operators. Radiflow risk assessment process strictly follows these principles.

5. Conclusion

While the awareness of the need to bring railways' OT network security up to par has (finally) reached maturity, there still exists a huge need for expertise and guidance, especially when it comes to vulnerability analysis, risk management and the intricacies of mandatory OT security regulations and compliance certification.

Radiflow's OT security experts closely accompany users from initial vulnerability and security analysis and implementing a central alerting and monitoring SOC to risk assessment and OT security optimization, using the most advanced, tried-and-true OT security tools.