CYLUS
Cybersecurity on Track

Solution Brief

CylusOne for Smart Zone and Conduit Partitioning

in the railway environment IEC-62443 and TS-50701

The recent wave of attacks on critical infrastructure have made yearly risk and vulnerability assessments compulsory to railway operations, if they are to remain cyber compliant. Based on these risk assessments, the thousands of railway assets must be assigned to security zones, connected by conduits. Furthermore, the new TS-50701 railway standard requires that each one of these assets be integrated within a security zone or conduit, ensuring that all data flow meets the same cyber-security requirements.

Without the capacity to automatically integrate, assign, and regroup assets within zones and conduits, according a Target Security Level and the possibility to easily manually enter the ranked Achieved Security Level it is impossible to justify the Capability Security Level score, resulting from the implemented countermeasures.

In other words, without a continuous monitoring system providing smart zone and conduit partitioning, supported by configuration tools enabling the assets' dataflow segregation according to security levels, no Railway and Public Transport Operator can become TS-50701 compliant.

Solution Highlights

1. Automated assets regrouping in zones and conduits based on Best practices
2. Full visibility of live asset dataflow
3. Smart partitioning into Zones & Conduits according to multiple criteria selection
4. Partitioning at all levels of the OSI stack, including application layers
5. Easy configuration of authorized dataflow
6. Complying with IEC 62334, TS-50701 & NIS-D

Your Benefits

- Address cybersecurity and compliance needs with a single, efficient, and automated security suite
- Ensure maximum safety, availability and cyber resilience, with early detection of threats and operational incidents
- Involve your managers in the cybersecurity of the assets they are responsible for and simplify their management.

Automatic Smart Partitioning

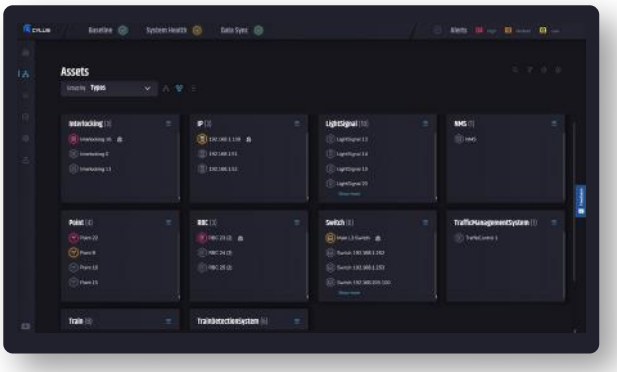
Cylus understands the importance of standards for Public Transport and Railway operators. That is why our solution was developed to be fully compatible with the IEC 62443 and TS-50701 standards. Partitioning, which is one of its main requirements, has been embedded within the overall CylusOne architecture and is one of its core features.

Here's how CylusOne's automatic 3-step approach to partitioning eases the day-to-day life of the cybersecurity teams.

Step 1

Auto-discovery

Once CylusOne is connected to a network through a mirror port, our award winning patented machine learning technology automatically recognizes the assets functionalities and captures the communication dynamic between the network and all their assets.



- Real-time discovery of all assets, including non IP and "hidden" on-board devices
- Entity enrichment of device OS, function, physical & logical location and much more..
- Automatic partitioning into Zones and Conduits according to IEC-62443-3-2 (ZCR3) and TS-50701

Step 2

Automatic Partitioning into Zones and Conduits

In railways a System under Consideration (SuC), either refers to a complete network comprising many subsystems with different security levels, or to any one of these sub-systems with their own assets. To account for this diversity of network complexity, standards have introduced the concepts of zones and conduits. CylusOne automatically designs the security zones and conduits based on railway best practices and standards. Furthermore, CylusOne automatically classifies, regroups, and visualizes assets in these security zone and conduits in matters of seconds, instead of weeks if done manually.

Definition

A zone is the logical or physical grouping of railway assets (i.e., physical assets, applications, or information) sharing identical security requirements. Each zone has a unique set of characteristics and security requirements with various attributes (e.g., security policies and levels; asset inventory; access requirements and control; threats and vulnerabilities, etc.).

A conduit can be considered a specific type of zone, which regroups the communication devices (e.g., switches, routers, firewalls, communications gateways, etc.), enabling the dataflow between zones. On top of a zone's attributes, it also possesses a set of characteristics and security requirements linked to the interconnected zones and communications protocols.

Step 3

Security Level Assignment

The IEC 62443 standard defines security levels as a qualitative method, serving to compare and manage security for different zones of an organization. Through a risk assessment, Professional Service experts will assess three types of security.

Target Security Level	Achieved Security Level	Capability Security Level

Definition

The Target Security Level is the right security level to operate correctly a railway system.

The Achieved Security Level is the measure and rank given by Service Professionals once a system design is established or is already implemented.

The Capability Security Level is the ability of an asset or a sub-system to reach natively the Target Security Level, when configured correctly, without any additional countermeasure.

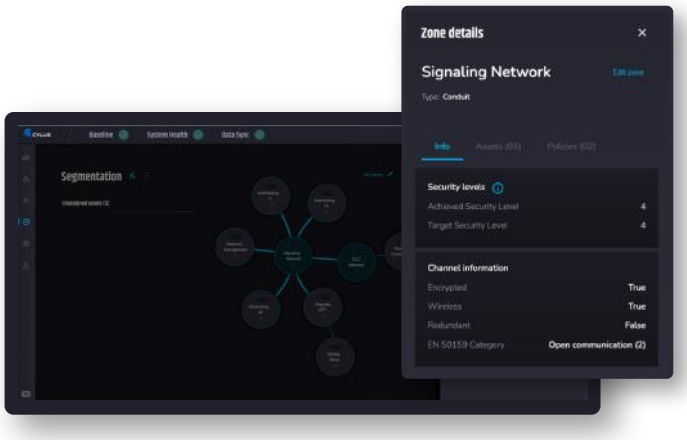
Service Professionals, within their risk and vulnerability assessment, will consider these three level types and assign one of the 5 following Security Levels to any given zone and conduit:

SL	Likely threat actors	Means	Skills	Motivation	Example of attacks
0	Employee	Infected component	None	None	USB stick on non connected printer
1	Individual	Casual or coincidental	No specific hacking skill	By mistake / Extortions attacks	Common cyberthreats on windows workstations e.g: phishing, infected email etc.
2	Cyber Criminals, Hacktivists	Known tools	Generic IT skills	Financial gains Propaganda (taking down public facing system	IT attacks, such as website, servers, ticketing, back-office, CCTV
3	Cyber Criminals Cyber Terrorists Nation state (APT groups)	Sophisticated or coordinated Attacks	OT skills Railway Specific Skills	High financial gains or sabotage - shutting down the network and creating accidents	Attacks on SCADA System, Critical safety systems, Signaling, Train Management Control System, rolling stock
4	Nation state (APT groups)	Sophisticated Targeted attacks (Campaign)	State Sponsored with OT and Railway specific skills	High: Taking over the railway network to paralyse the infrastructure	Attacks on Critical safety systems, Signaling, Train Management Control System, rolling stock infrastructure

Table 1: Security Levels (SL) and examples of attack motivation

In other words, each asset in the same zone and all conduit dataflows will receive the same Security Level from 0 to 4, established in function of similar cybersecurity requirements, for all three security types.

Within CylusOne, the various security levels are easily integrated manually. The interfacing screen allows for an easy update, enabling to take into account any change in the risk profile of the operator.



View of zones with Target-Security-Level and Achieved Security-Level

Addressing Segmentation with CylusOne

Railways have an inherent complexity and diversity of IT and OT systems, which opens the doors to various network attack vectors. Hence, the best protection is provided by a monitoring system that can observe and identify abnormal communication between assets, zones, and conduits. The future railway standard TS-50701 goes further than the IEC Standard 62443 in defining what are abnormal communications. By recommending segmentation criteria, it not only specifies what are acceptable connections but also what type of message content must be filtered. Hence, only railway specific Continuous Monitoring Systems can understand their specific protocols and apply the filters. Industrial security gateways cannot be TS-50701 compliant in OT environments..

CylusOne Automatic Actions

01

Physical location

CylusOne aggregates assets that are located within the vicinity of the same track region.

Benefit

It simplifies the search of attacks as security officers can be sent to the affected region.

02

Safety levels

CylusOne structures the zones and conduits according to the SIL levels, from SIL0 to SIL 4.

Benefit

Compliance with TS-50701, which forbids any communication between assets of different SIL levels.

03

Operational functions

CylusOne understand the assets' property and consolidate them according to their functionality (e.g., braking, door, or maintenance systems).

Benefit

Quick and easy differentiation between attacks and malfunctions of the sub-system

04

Wireless vs Wired connections

CylusOne regroups communicating assets according to their type of technologies and establishes the interfacing connections with all the assets

Benefit

Apply specific rules that protect a unique set of vulnerabilities to each specific wireless technology

05

Assets' Logical connection

CylusOne may apply a virtual segmentation based on the railway's architectural framework

Benefit

Apply the network logic, enabling the cyber security team to identify quickly which asset has been compromised and how vulnerable the system has become.

06

Access restriction

CylusOne can identify quickly access from unauthorized assets at all the level of the OSI layer and interface with other technologies to block the access

Benefit

Flagg out or block any abnormal connection before it starts harming the network

07

Organizational responsibility

CylusOne allows for the designation of an asset's responsibility based on user/department profile

Benefit

Empowerment of asset owners by direct and efficient cyber management tools

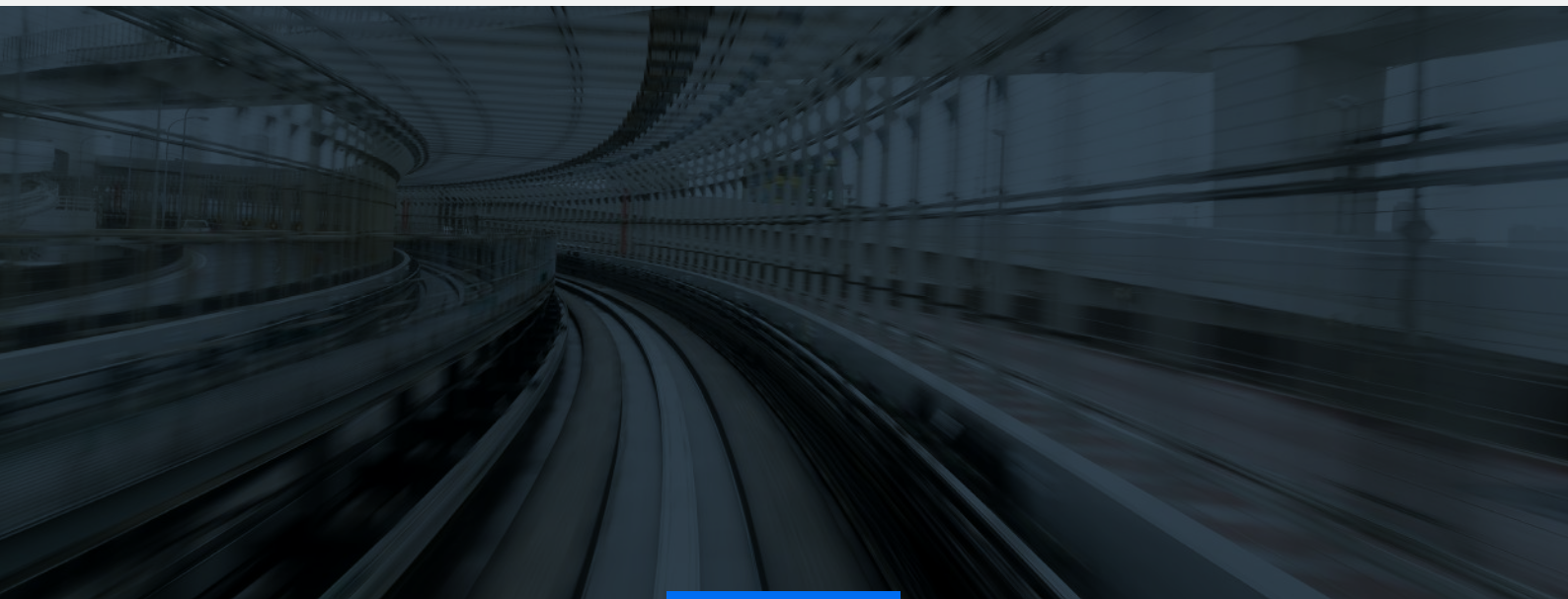
08

Obsolescence management

CylusOne allows for the identification of obsolete hardware and software, building a virtual fence around it.

Benefit

railways must live with obsolete products during many systems' entire life-cycle and can maintain compliance with TS-50701, even with obsolete solutions.



Advanced Policy Management

Identifying and applying manually the rules that can segment the railway systems according to the standard TS-50701 is a daunting task. It is why CylusOne automatically brings a configuration that pre-establishes the main links through the described three first steps. However, cyber compliance according to the TS-50701 standard requires content filtering to meet the segmentation criteria. CylusOne provides a configuration interface that simplifies the application of these filters.

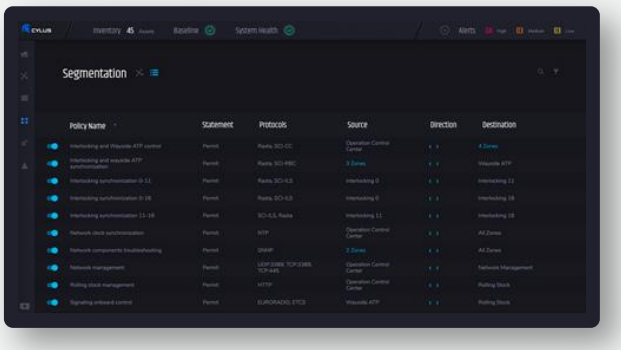
Real time alerts and policy enforcement

The segmentation interface automatically transposes the partitioning rules into text. These rules are working on the principle of white listing, that is, showing only what is permitting, all the other connections being prohibited.

Management of rules for virtual segmentation

In other words, each asset in the same zone and all conduit dataflows will receive the same Security Level from 0 to 4, established in function of similar cybersecurity requirements, for all three security types.

Within CylusOne, the various security levels are easily integrated manually. The interfacing screen allows for an easy update, enabling to take into account any change in the risk profile of the operator.



Segmentation at all level of the OSI stack

Orchestrating with 3rd party security controls

CylusOne conducts continuous risk and vulnerability assessments and maps out the different zones and conduits in your networks. This enables us to identify the associated risk and their impact on your operational environment by matching the corresponding security levels, existing vulnerabilities and the gaps between existing and adequate risk levels. CylusOne then provides vulnerability mitigation recommendations and actions required to reduce the risk to its target level.

Reach us at Info@cylus.com or visit our website www.cylus.com

About Cylus

Cylus is a global leader in rail cybersecurity. We address the full spectrum of cybersecurity needs of rail signaling and rolling stock systems, ensuring safety, service availability and facilitating compliance, for mainline and urban railway companies. Cylus rail cybersecurity solutions are trusted by top-tier railway companies globally and promotes cybersecurity of the rail ecosystem as a whole