



**[Fence]:**

**fe]**

# An Innovative Solution for Railway Cybersecurity Risks

5th ENISA-ERA Conference on Cybersecurity in Railways

---

**AIRBUS** PROTECT

**ALSTOM**

# >>> 7 years of collaboration for Cybersecurity



**ALSTOM**

**Serge Benoliel**

Cybersecurity Governance  
& Expertise Director

*[serge.benoliel@alstomgroup.com](mailto:serge.benoliel@alstomgroup.com)*



**AIRBUS**

PROTECT

**Samuel Schmidlin**

Fence Product Owner  
& Business Analyst

*[samuel.schmidlin@airbus.com](mailto:samuel.schmidlin@airbus.com)*

5th ENISA-ERA Conference on Cybersecurity in Railways

**AIRBUS** PROTECT

**ALSTOM**

# Airbus Protect

An Airbus subsidiary created in July 2022 to protect both internal and external assets

 **+1,700**

professionals based in **France, Germany, the UK, Spain and Belgium**

 **€238m**

2024 **turnover** and continuous growth in all our business sectors with a strategy aligned with our customers

 **4**

**business units:** Safety, Cybersecurity Consulting, Managed Services and Sustainability

 **+300**

**clients:** aerospace and aviation, transport, energy, nuclear, public institutions...



5th ENISA-ERA Conference on Cybersecurity in Railways

AIRBUS PROTECT

ALSTOM

AIRBUS

# Alstom Risk Assessment needs

Why create a risk assessment methodology within a tool?

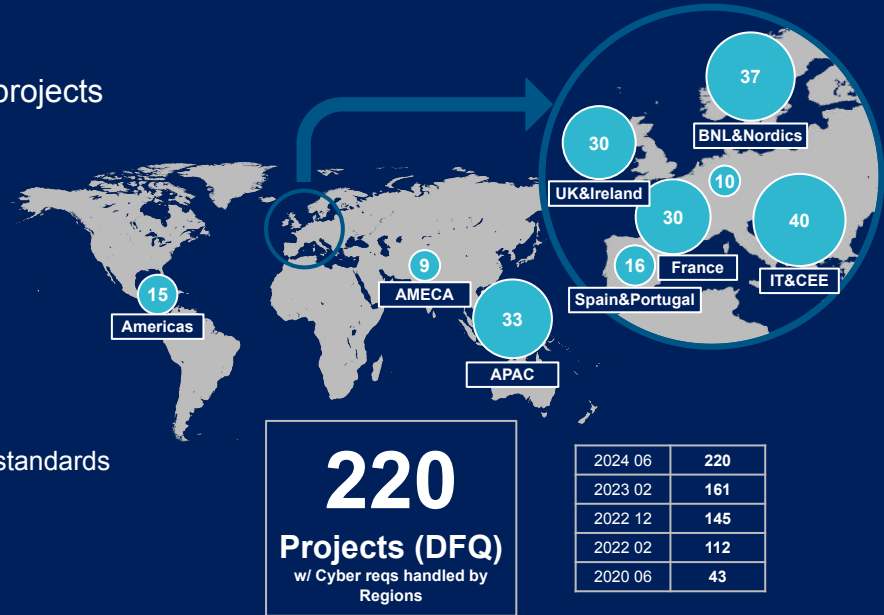
> Initial context of fragmentation of approaches across projects  
(EBIOS RM, EBIOS 2010, various flavor of 62443, TS 50701, ..)

> Need of a consistent and unified approach, to:

- ☒ Conducting reproducible risk assessments
- ☒ Reusing risk assessments across different contexts
- ☒ Simplifying competency management
- ☒ Promoting capitalisation
- ☒ Automating a single methodology

> Key requirements

- ☐ Full compliance with EBIOS RM and 62443 / TS 50701 standards
- ☒ Combining the benefits of these two approaches
- ☒ Support for architectural choices
- ☒ Simple to use once automated with a database



5th ENISA-ERA Conference on Cybersecurity in Railways

# The evolving challenges of Cyber Risk Analysis in Rail Systems

**Mandatory Compliance with  
Interlinked Standards**

**Integrating IT/OT  
Convergence Risks**

**Manual, Time-Consuming  
Analysis**

**Inconsistent and Subjective  
Assessments**

**The Velocity of Change  
(Evolving Threats)**

---

5th ENISA-ERA Conference on Cybersecurity in Railways

**AIRBUS** PROTECT

**ALSTOM**

# ARAMIS: A Risk Assessment Methodology for Industrial Security

A new methodology combining strengths of EBIOS RM & (62443 + TS 50701)

## EBIOS Risk Manager

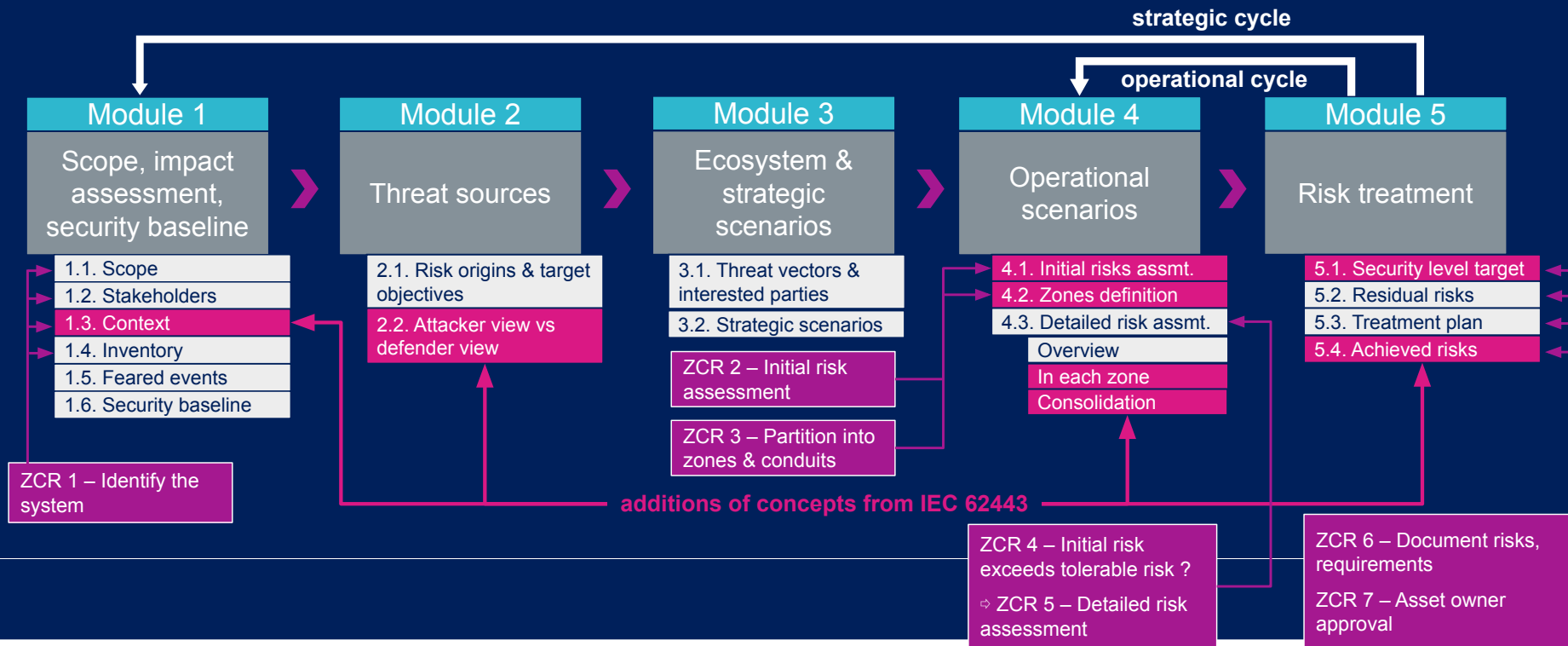
- + A practical, ready-to-use methodology
- + A neat and elegant way to draw attack scenarios
- Focused on risk-related topics
- Complex systems lead to complex scenarios, and difficulty to comprehend the global picture

## ISA/IEC 62443 & CLC/TS 50701

- Limited information on practical application on detail risk assessment
- No representation of attack path scenarios
- + A complete corpus for industrial Cybersecurity Security, defining Security Levels & Foundational Reqs.
- + Concept of Zones & conduits refining a whole system in smaller parts, ideal for handling complexity

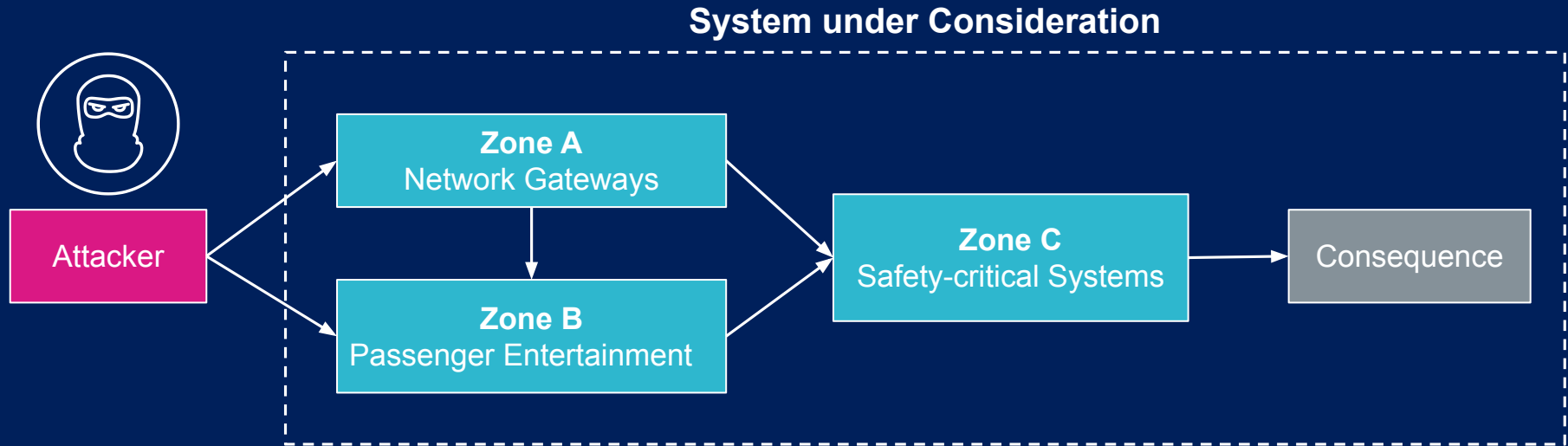
5th ENISA-ERA Conference on Cybersecurity in Railways

# The pragmatic structure of EBIOS RM with additions from ISA/IEC 62443



# Multiple abstraction Level

Detailed Risk Assessment >>> Overview



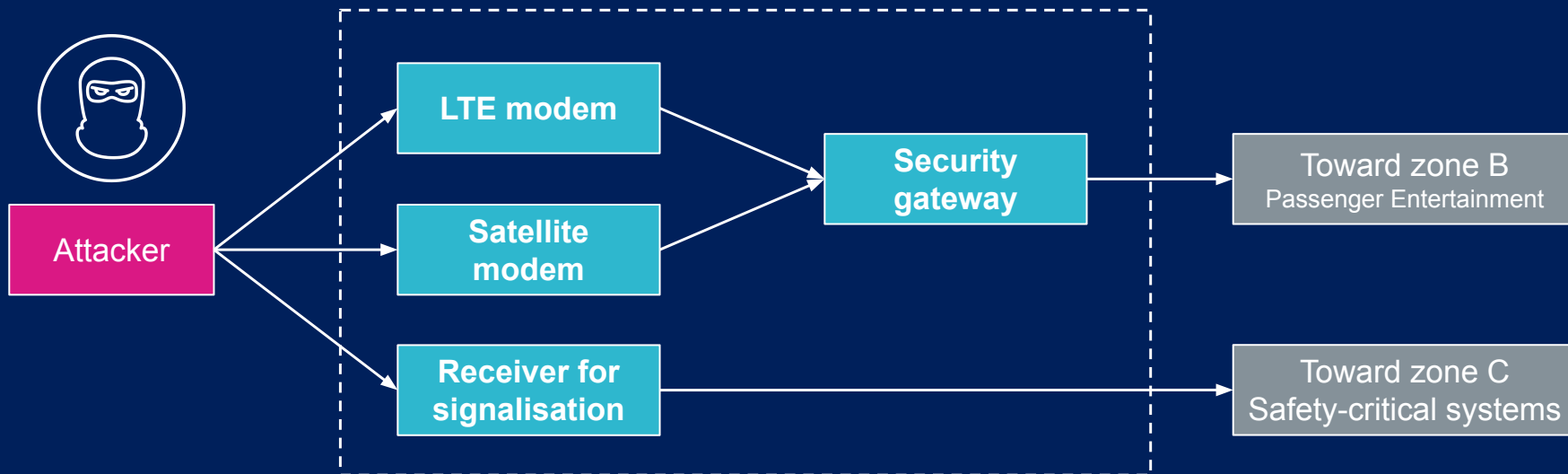
5th ENISA-ERA Conference on Cybersecurity in Railways



# Multiple abstraction Level

Detailed Risk Assessment >>> Focus on Zone

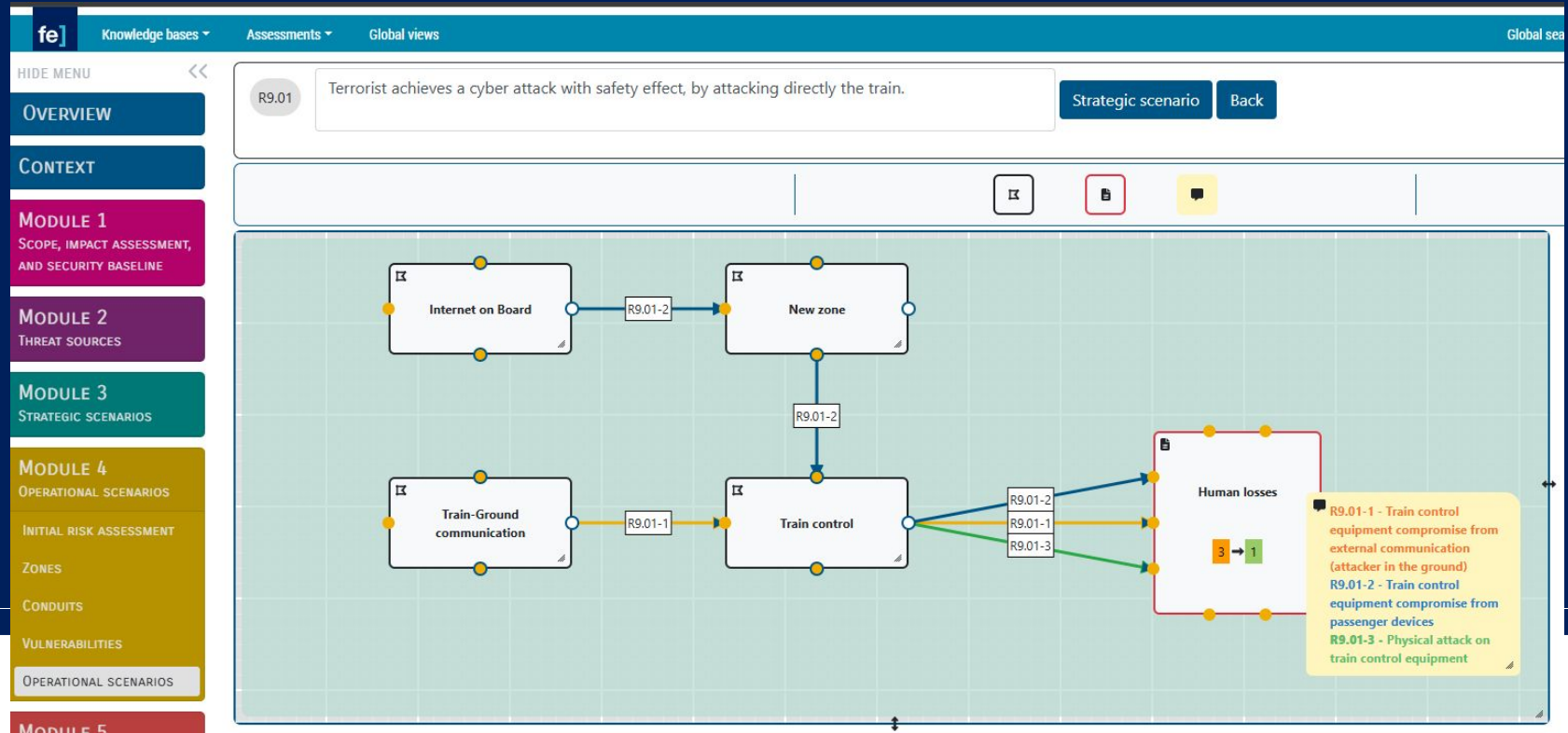
## Zone A - Network Gateways



5th ENISA-ERA Conference on Cybersecurity in Railways

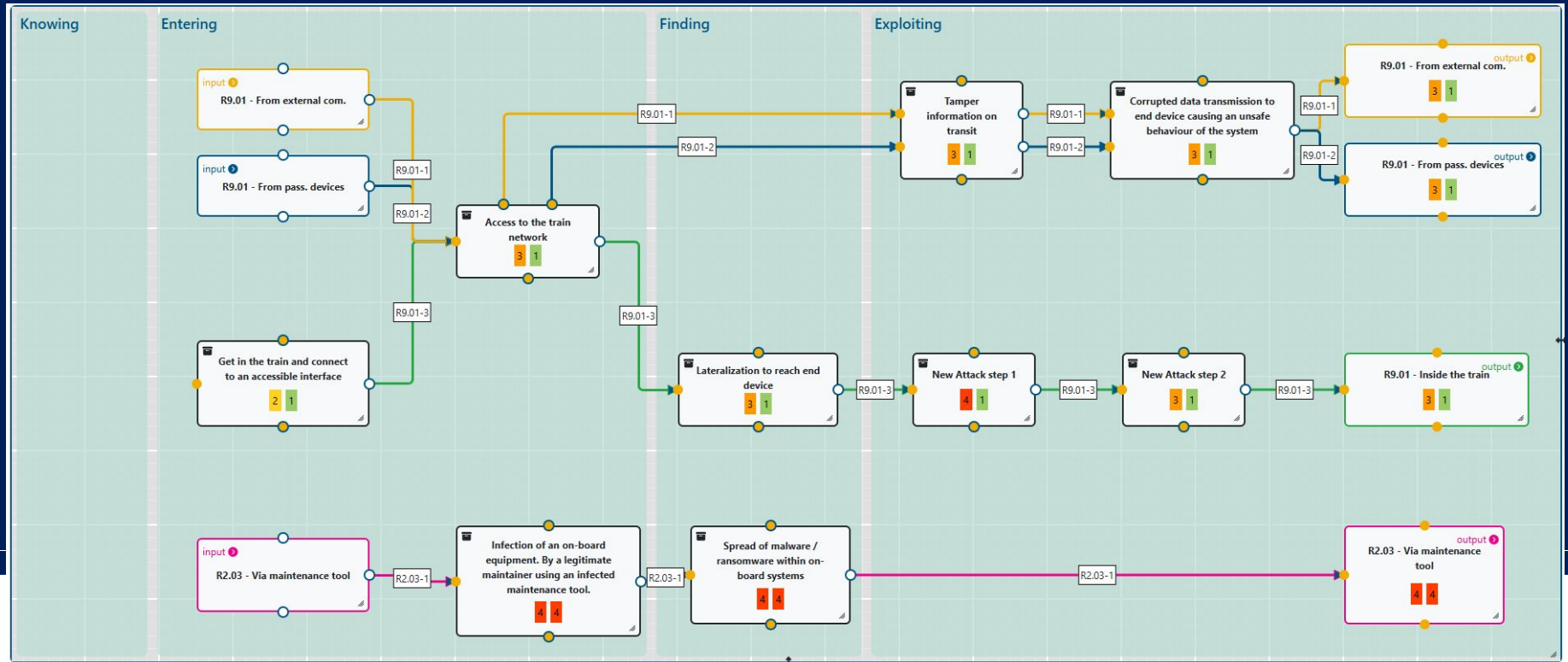
# Operational scenarios

## Detail Risk Assessment >>> Overview

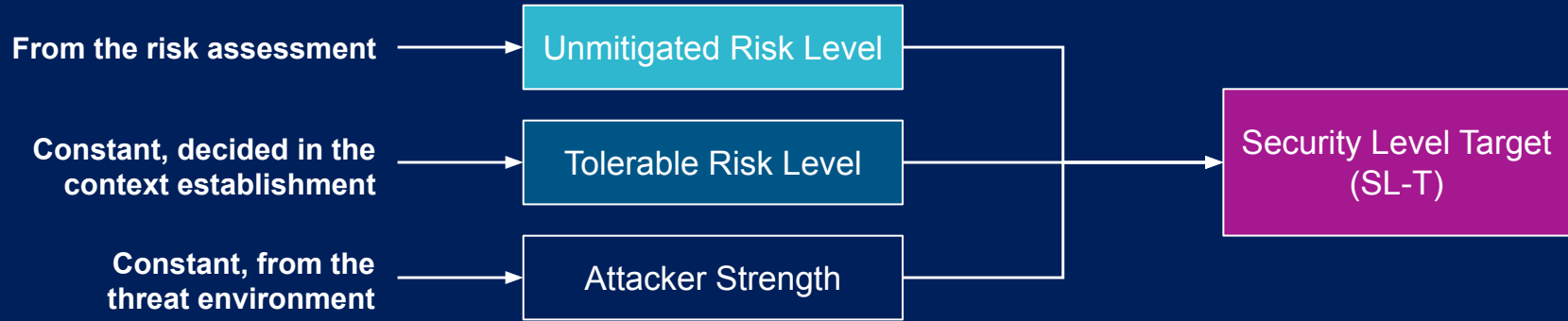


# Operational scenarios

Detailed Risk Assessment >>> Focus on Zone



# Automated Security Level Target (SL-T)



**Security Level** allocated at **Zone** level and on each **Asset**,  
based on **7 Foundational Requirements**.

5th ENISA-ERA Conference on Cybersecurity in Railways

# Automated Security Level Target (SL-T)

## 7 Foundational Requirements

ISA/IEC 62443 Foundational Requirements	
FR 1	Identification and authentication control (IAC)
FR 2	Use control (UC)
FR 3	System integrity (SI)
FR 4	Data confidentiality (DC)
FR 5	Restricted data flow (RDF)
FR 6	Timely response to events (TRE)
FR 7	Resource availability (RA)

**SL-T** are based on

Predefined sets of  
Security Requirements  
from ISA/IEC 62443

⇒ Resulting in a **vector of SLs**

IAC	UC	SI	DC	RDF	TRE	RA
2	2	3		2	3	2

5th ENISA-ERA Conference on Cybersecurity in Railways

# Automated Security Level Target (SL-T)

> Applicable FR Vector calculated automatically in Attack Step

The attacker performs: **T07 Authentication abuse or bypass**, **T08 Privilege abuse or escalation**, **T19 Infrastructure manipulation**

Applicable Foundational Requirements

IAC	UC	SI	DC	RDF	TRE	RA
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Scenario  
SL-T

ID	Scenario name	Method of attack	Unmitigated impact	Unmitigated Likelihood	Unmitigated Risk	Tolerable Likelihood	SL min	AST	AST offset	Scenario SL-T (value)
R9.01	Terrorist achieves a cyber attack with safety effect, by attacking directly the train.	Inside the train	4	3	Very High	1	1	3	0	3

Asset  
SL-T

ID	Supporting asset	IAC	UC	SI	DC	RDF	TRE	RA
	<input type="text" value="Filter ID"/>	<input type="text" value="Filter IAC"/>	<input type="text" value="Filter UC"/>	<input type="text" value="Filter SI"/>	<input type="text" value="Filter DC"/>	<input type="text" value="Filter RDF"/>	<input type="text" value="Filter TRE"/>	<input type="text" value="Filter RA"/>
SA02	Gigabit Ethernet Switches	3	3	3		3	3	3

Zone  
SL-T

ID	Zone name	IAC	UC	SI	DC	RDF	TRE	RA
	<input type="text" value="Filter Zone name"/>	<input type="text" value="Filter IAC"/>	<input type="text" value="Filter UC"/>	<input type="text" value="Filter SI"/>	<input type="text" value="Filter DC"/>	<input type="text" value="Filter RDF"/>	<input type="text" value="Filter TRE"/>	<input type="text" value="Filter RA"/>
Z02	Train control	3	3	3		3	3	3

5th ENISA-ERA Conference on Cybersecurity in Railways

# Looking Forward



: The methodology was validated using use cases and pilot analyses from Alstom. Full deployment is currently underway.

*History: Project start date: 2021. Launch approved after pilot cases: 2024*

: Europe's Rail Joint Undertaking (ERJU) has started using and evaluating the ARAMIS methodology in Fence.

: Statement of Conformity against the following standards:

IEC 62443-3-2:2020  
CLC/TS 50701:2023  
EBIOS RM  
ISO/IEC 27005:2022

5th ENISA-ERA Conference on Cybersecurity in Railways

AIRBUS PROTECT

ALSTOM

# Thank to the Contributors

*Non exhaustive list*

**ALSTOM**

Serge BENOLIEL  
Baptiste MARTINOT-LAGARDE  
Jean-Francois GILLOT  
Loïc BAUDAIS  
Fabrice RAFART  
Dimitrios SISIARIDIS  
Moatazbella MOHAMED  
El-Houssine LOUKILI  
Carlos ARNILLAS GALAN

**AIRBUS**

PROTECT

Sylvain TANGUY  
Florence FOU DRAIN  
Jérémy ROGER  
Cyril SOULA  
Emmanuel PRAT

---

5th ENISA-ERA Conference on Cybersecurity in Railways

**AIRBUS** PROTECT

**ALSTOM**



# Thank you !



**AIRBUS**

PROTECT

**Samuel Schmidlin**

Fence Product Owner  
& Business Analyst

*[samuel.schmidlin@airbus.com](mailto:samuel.schmidlin@airbus.com)*

5th ENISA-ERA Conference on Cybersecurity in Railways

**AIRBUS** PROTECT

**ALSTOM**

# Q&A

# Back-up

5th ENISA-ERA Conference on Cybersecurity in Railways

---

**AIRBUS** PROTECT

**ALSTOM**

# Attack Step

## >>> Determine Unmitigated Likelihood (ZCR 5.4)

Access to the train network

HLA02-IAS01

Access to the train network

The attacker gains access to the train's internal network

The attacker performs: **T07 Authentication abuse or bypass** , **T08 Privilege abuse or escalation** , **T19 Infrastructure manipulation**

Applicable Foundational Requirements						
IAC	UC	SI	DC	RDF	TRE	RA
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

On: **Gigabit Ethernet Switches** , **Security Gateway**

Click to select vulnerabilities...

Unmitigated likelihood 3 SL-T (Allocation) Residual Likelihood 3

Existing mitigations

ID	Title	Effects in this context	Implementation Status
No records.			

EXP

WOO

EQ

Unmitigated likelihood

3

Justification for the unmitigated likelihood

Applicable FRs based on attacker **Techniques** - **Tactics**

**Unmitigated Likelihood** is calculated based on

- > Expertise
- > Window Of Opportunity
- > Equipment


# Automated Security Level Target (SL-T) for Scenarios

Scenarios SL-T (value)										
<a href="#">Clear filters</a>		Show <input type="text" value="25"/> entries.		Showing 1 to 3 of 3 entries (filtered from 8 total entries)					<a href="#">first</a> <a href="#">previous</a> <b>1</b> <a href="#">next</a> <a href="#">last</a>	
ID	Scenario name	Method of attack	Unmitigated impact	Unmitigated Likelihood	Unmitigated Risk	Tolerable Likelihood	SL min	AST	AST offset	Scenario SL-T (value)
R9.01	Terrorist achieves a cyber attack with safety effect, by attacking directly the train.	From external com.	4	3	Very High	1	1	3	0	2
R9.01	Terrorist achieves a cyber attack with safety effect, by attacking directly the train.	From pass. devices	4	3	Very High	1	1	3	0	2
R9.01	Terrorist achieves a cyber attack with safety effect, by attacking directly the train.	Inside the train	4	3	Very High	1	1	3	0	3
										Justification for scenario SL-T overwriting.

Allocation of Zone SL-T					
<a href="#">Clear filters</a>		Show <input type="text" value="25"/> entries.		Showing 1	
ID	Scenario name	Method of attack	Scenario SL-T (value)	Operational scenario	Target zones for the scenario
R9.01	Terrorist achieves a cyber attack with safety effect, by attacking directly the train.	From external com.	2		<ul style="list-style-type: none"><li>• Z01 Train-Ground communication</li><li>• Z02 Train control</li></ul>
R9.01	Terrorist achieves a cyber attack with safety effect, by attacking directly the train.	From pass. devices	2		<ul style="list-style-type: none"><li>• Z02 Train control</li></ul>
R9.01	Terrorist achieves a cyber attack with safety effect, by attacking directly the train.	Inside the train	3		<ul style="list-style-type: none"><li>• Z02 Train control</li></ul>

Method of attack “inside the train” targeting “Z02 train control” requires a higher SL-T value

# Automated Security Level Target (SL-T) for Assets

Asset SL-T vectors									
<div> <b>Clear filters</b> Show <input type="text" value="25"/> entries. Showing 1 to 1 of 1 entries (filtered from 8 total entries) <span>first previous <b>1</b> next last</span></div>									
ID	Supporting asset	IAC	UC	SI	DC	RDF	TRE	RA	Comment
<input type="text" value="Filter ID"/>	<input type="text" value="Gigabit"/>	<input type="text" value="Filter IAC"/>	<input type="text" value="Filter UC"/>	<input type="text" value="Filter SI"/>	<input type="text" value="Filter DC"/>	<input type="text" value="Filter RDF"/>	<input type="text" value="Filter TRE"/>	<input type="text" value="Filter RA"/>	<input type="text" value="Filter Comment"/>
SA02	Gigabit Ethernet Switches	3	3	3		3	3	3	

Asset SL-T =  $\max \{(\text{Attack Step SL-T})_i\}$   
that carry out attacks on this supporting asset.

## LINKED ZONES > GIGABIT ETHERNET SWITCHES

List of the zones that contain this supporting asset and the linked attack steps.

Search

Show

25

entries.

Showing 1 to 11 of 11 entries

first

previous

1

next

last

Zone	Attack Step	IAC	UC	SI	DC	RDF	TRE	RA
		Filter IAC	Filter UC	Filter SI	Filter DC	Filter RDF	Filter TRE	Filter RA
Z02 - Train control	HLA02-IAS01 - Access to the train network	3	3	3		3	3	
Z02 - Train control	HLA02-IAS02 - Get in the train and connect to an accessible interface	3	3				3	
Z02 - Train control	HLA02-IAS03 - Lateralization to reach end device	3	3			3	3	

# Automated Security Level Target (SL-T) for Zones

Zone SL-T vectors (summary)

Download Clear filters Show 25 entries. Showing 1 to 1 of 1 entries (filtered from 8 total entries) first previous 1 next last

ID	Zone name	IAC	UC	SI	DC	RDF	TRE	RA	Comment
Z02	Train control	3	3	3		3	3	3	

Zone SL-T =  $\max \{(\text{Asset SL-T})_i\}$   
of Assets in the Zone

## Z02 - TRAIN CONTROL

List of the supporting assets (and their SL-T) in the zone

Search Show 25 entries. Showing 1 to 4 of 4 entries first previous 1 next last

Supporting asset	IAC	UC	SI	DC	RDF	TRE	RA	Comment
SA01 - Main Processor Unit	3	3	3		2	3	3	
SA02 - Gigabit Ethernet Switches	3	3	3		3	3	3	
SA05 - Brake Control Unit	3	3	3		2	3		
SA06 - Security Gateway	3	3	3		3	3		