6th SmartRaCon Scientific Seminar, 23-24/10-2024

Cybersecurity Risk Assessment of Virtually Coupled Train Sets

Aria Mirzai, Ramana Reddy Avula, Marvin Damschen
Dependable Transport Systems, RISE Research Institutes of Sweden

Cybersecurity Risk → Safety Risk

- "ICT in railway has improved the reliability, maintainability, operational efficiency, capacity as well as the comfort of passengers. This adoption **introduces new vulnerabilities** and entry points for hackers to launch attacks"[1]

- Over 20 trains sabotaged in Poland via a simple **"radio-stop" command that anyone could broadcast** using $30 equipment (2023)[2]

[1] *Kour, R., Thaduri, A. and Karim, R., 2020. Predictive model for multistage cyber-attack simulation. International Journal of System Assurance Engineering and Management, 11, pp.600-613*

[2] *https://www.wired.com/story/poland-train-radio-stop-attack/*

EU Regulations & Directives

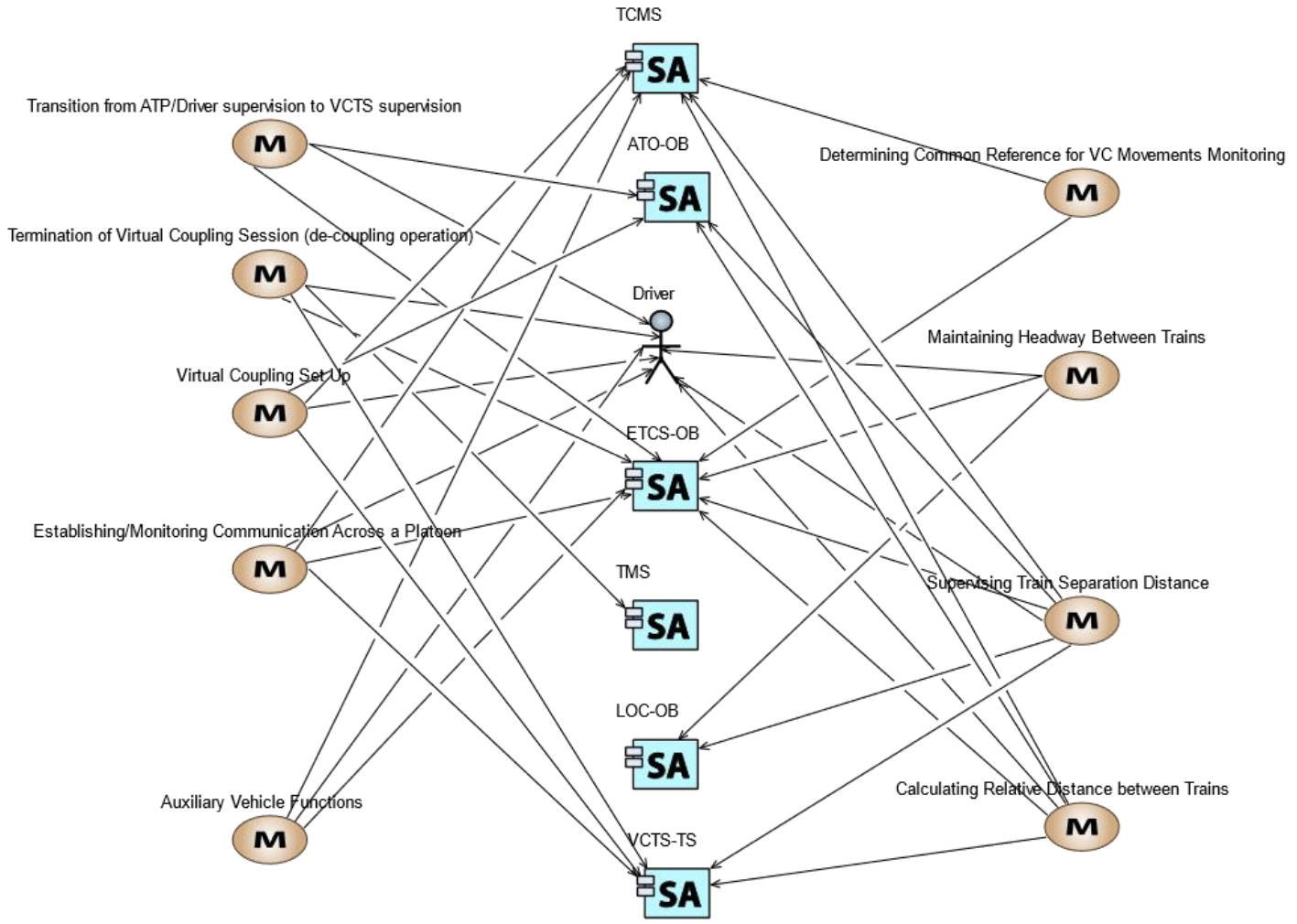
Risk Assessment of Virtually Coupled Train Sets (VCTS)

- Methodology (X2Rail-5 D11.1) based on:
  - **IEC 62443 series (part 3-2 “Security Risk Assessment and System Design”)**
  - **CLC/TS 50701: Railway applications – Cybersecurity**
  - ISO 27000 series for conducting risk assessment
  - NIST special publications for IACS
- Application of publicly available Risk Assessment Excel tool (X2Rail-5 D14.3)
- Outcome: **Identify target security level** for the assessed system

System Description

- Primary asset: Core function performed by the System under Consideration (SuC)[3]

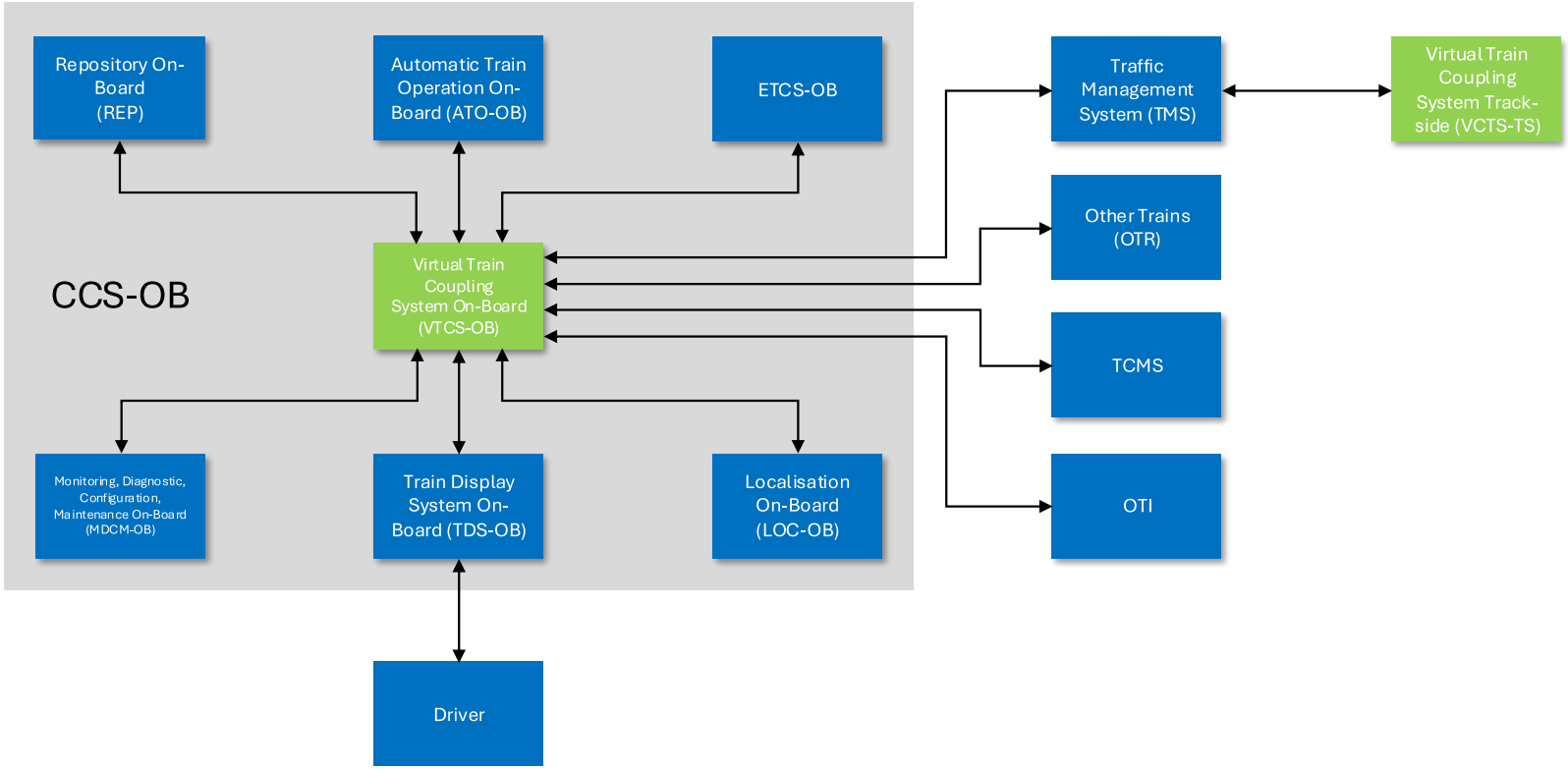
- **VCTS missions defined in X2Rail-3 identified as essential functions**
  → Primary assets in this assessment



[3] *CLC/TS 50701: Railway applications – Cybersecurity*

System Description

- **Supporting assets (SA)**: Components the primary assets depend on, categorised into:
  - Embedded device
  - Network device
  - Host device
  - Software application



SZ Name	SA-ID	SA Type	Security Zone
VCTS-Onboard	VCTS-OB	Software Application	OB-Z
VCTS-Trackside	VCTS-TS	Software Application	TS-Z

Initial Risk Assessment

Feared Event	Primary Asset	Safety	Performance	Reputation	Compliance	Overall Impact	Rationale
Loss of Confidentiality	Virtual Coupling Set Up	1	1	2	3	**2**	➢ Safety: No loss of life, no injuries. ➢ Performance: Train might need to be replaced after the trip. ➢ Reputation: Adverse local/regional media reports. ➢ Compliance: Major non-compliance with contract and regulation.
Loss of Integrity	Virtual Coupling Set Up	3	4	3	3	**4**	➢ Safety: Major loss of life. ➢ Performance: Major area blocked, or main infrastructure blocked during >1 week. ➢ Reputation: Extensive national media reports. ➢ Compliance: Extensive non-compliance with contract.
Loss of Availability	Virtual Coupling Set Up	4	3	2	3	**4**	➢ Safety: Major loss of life. ➢ Performance: Major area blocked, or main infrastructure blocked during >1 week. ➢ Reputation: Extensive national media reports. ➢ Compliance: Extensive non-compliance with contract.

Initial Risk Assessment

Feared Event	Primary Asset	Safety	Performance	Reputation	Compliance	Overall Impact	Rationale
Loss of Confidentiality	Virtual Coupling Set Up	1	1	2	3	**2**	➢ Safety: No loss of life, no injuries. ➢ Performance: Train might need to be replaced after the trip. ➢ Reputation: Adverse local/regional media reports. ➢ Compliance: Major non-compliance with contract and regulation.
Loss of Integrity	Virtual Coupling Set Up	3	4	3	3	**4**	➢ Safety: Major loss of life. ➢ Performance: Major area blocked, or main infrastructure blocked during >1 week. ➢ Reputation: Extensive national media reports. ➢ Compliance: Extensive non-compliance with contract.
Loss of Availability	Virtual Coupling Set Up	4	3	2	3	**4**	➢ Safety: Major loss of life. ➢ Performance: Major area blocked, or main infrastructure blocked during >1 week. ➢ Reputation: Extensive national media reports. ➢ Compliance: Extensive non-compliance with contract.

Initial Risk Assessment

Feared Event	Primary Asset	Safety	Performance	Reputation	Compliance	Overall Impact	Rationale
Loss of Confidentiality	Virtual Coupling Set Up	1	1	2	3	**2**	➢ Safety: No loss of life, no injuries. ➢ Performance: Train might need to be replaced after the trip. ➢ Reputation: Adverse local/regional media reports. ➢ Compliance: Major non-compliance with contract and regulation.
Loss of Integrity	Virtual Coupling Set Up	3	4	3	3	**4**	➢ Safety: Major loss of life. ➢ Performance: Major area blocked, or main infrastructure blocked during >1 week. ➢ Reputation: Extensive national media reports. ➢ Compliance: Extensive non-compliance with contract.
Loss of Availability	Virtual Coupling Set Up	4	3	2	3	**4**	➢ Safety: Major loss of life. ➢ Performance: Major area blocked, or main infrastructure blocked during >1 week. ➢ Reputation: Extensive national media reports. ➢ Compliance: Extensive non-compliance with contract.

Initial Risk Assessment

Feared Event	Primary Asset	Safety	Performance	Reputation	Compliance	Overall Impact	Rationale
Loss of Confidentiality	Virtual Coupling Set Up	1	1	2	3	**2**	➢ Safety: No loss of life, no injuries. ➢ Performance: Train might need to be replaced after the trip. ➢ Reputation: Adverse local/regional media reports. ➢ Compliance: Major non-compliance with contract and regulation.
Loss of Integrity	Virtual Coupling Set Up	3	4	3	3	**4**	➢ Safety: Major loss of life. ➢ Performance: Major area blocked, or main infrastructure blocked during >1 week. ➢ Reputation: Extensive national media reports. ➢ Compliance: Extensive non-compliance with contract.
Loss of Availability	Virtual Coupling Set Up	4	3	2	3	**4**	➢ Safety: Major loss of life. ➢ Performance: Major area blocked, or main infrastructure blocked during >1 week. ➢ Reputation: Extensive national media reports. ➢ Compliance: Extensive non-compliance with contract.

Unmitigated Risk Analysis

- VCTS Event Initiation Likelihood (EIL):

Weights/Multiplicative factor			Consideration factor of threat actor (if an actor is not relevant, please use "0" for that specific threat actor)									
CAP	INT	TARG	1	1	1	1	1	1	1	1	1	1
1	2	3	Event Initiation Likelihood (EIL)									
			Hacker/ Cracker	Terrorist	Competitor	Government Organisation	Hacktivist	Criminal Organisation	Script Kiddy	Layman	Insider	Max EIL
			EIL	EIL	EIL	EIL	EIL	EIL	EIL	EIL	EIL	
			3	3,83	2,67	3,17	3	4	2	1,5	3,67	**4**
Delta value (δ)	1	Pessimistic EIL	3,00									
		Balanced EIL	2,98									
		Optimistic EIL	2									

Unmitigated Risk Analysis

- VCTS Event Initiation Likelihood (EIL):

Weights/Multiplicative factor			Consideration factor of threat actor (if an actor is not relevant, please use "0" for that specific threat actor)									
CAP	INT	TARG	1	1	1	1	1	1	1	1	1	1
1	2	3	Event Initiation Likelihood (EIL)									
			Hacker/ Cracker	Terrorist	Competitor	Government Organisation	Hacktivist	Criminal Organisation	Script Kiddy	Layman	Insider	Max EIL
			EIL	EIL	EIL	EIL	EIL	EIL	EIL	EIL	EIL	
			3	3,83	2,67	3,17	3	4	2	1,5	3,67	4
Delta value (δ)	1	Pessimistic EIL	3,00									
		Balanced EIL	2,98									
		Optimistic EIL	2									

Unmitigated Risk Analysis

- VCTS Overall Unmitigated Likelihood (excerpt):

SA-ID	STRIDE Threat Category	Vulnerability Rationale	CVSS Score	EIL	Overall Unmitigated Likelihood
VCTS-OB	Spoofing Identity	Attacker can access VCTS-OB and spoof identity via ETCS or TCMS network + remote access interface (e.g. SSH)	8.9	3	**2**
VCTS-OB	Tampering with data	Attacker can access VCTS-OB and tamper the data via ETCS or TCMS network + remote access interface (e.g. SSH)	8.9	3	**2**
VCTS-OB	Repudiation	Attacker can access VCTS-OB and delete or modify security log or monitoring service via ETCS or TCMS network + remote access interface (e.g. SSH)	7.3	3	**2**
VCTS-OB	Information disclosure	Attacker can access VCTS-OB and steal or collect information via ETCS or TCMS network + remote access interface (e.g. SSH)	3.5	3	**1**
VCTS-OB	Denial of Service	Attacker can access VCTS-OB and steal or collect information via ETCS or TCMS network + remote access interface (e.g. SSH)	6.5	3	**1**
VCTS-OB	Elevation of Privilege	Attacker can access the VCTS-OB via ETCS or TCMS network and gain more privileges	7.9	3	**2**

Unmitigated Risk Analysis

- VCTS Overall Unmitigated Likelihood (excerpt):

SA-ID	STRIDE Threat Category	Vulnerability Rationale	CVSS Score	EIL	Overall Unmitigated Likelihood
VCTS-OB	Spoofing Identity	Attacker can access VCTS-OB and spoof identity via ETCS or TCMS network + remote access interface (e.g. SSH)	8.9	3	**2**
VCTS-OB	Tampering with data	Attacker can access VCTS-OB and tamper the data via ETCS or TCMS network + remote access interface (e.g. SSH)	8.9	3	**2**
VCTS-OB	Repudiation	Attacker can access VCTS-OB and delete or modify security log or monitoring service via ETCS or TCMS network + remote access interface (e.g. SSH)	7.3	3	**2**
VCTS-OB	Information disclosure	Attacker can access VCTS-OB and steal or collect information via ETCS or TCMS network + remote access interface (e.g. SSH)	3.5	3	**1**
VCTS-OB	Denial of Service	Attacker can access VCTS-OB and steal or collect information via ETCS or TCMS network + remote access interface (e.g. SSH)	6.5	3	**1**
VCTS-OB	Elevation of Privilege	Attacker can access the VCTS-OB via ETCS or TCMS network and gain more privileges	7.9	3	**2**

Unmitigated Risk Analysis

- VCTS Overall Unmitigated Likelihood (excerpt):

SA-ID	STRIDE Threat Category	Vulnerability Rationale	CVSS Score	EIL	Overall Unmitigated Likelihood
VCTS-OB	Spoofing Identity	Attacker can access VCTS-OB and spoof identity via ETCS or TCMS network + remote access interface (e.g. SSH)	8.9	3	2
VCTS-OB	Tampering with data	Attacker can access VCTS-OB and tamper the data via ETCS or TCMS network + remote access interface (e.g. SSH)	8.9	3	2
VCTS-OB	Repudiation	Attacker can access VCTS-OB and delete or modify security log or monitoring service via ETCS or TCMS network + remote access interface (e.g. SSH)	7.3	3	2
VCTS-OB	Information disclosure	Attacker can access VCTS-OB and steal or collect information via ETCS or TCMS network + remote access interface (e.g. SSH)	3.5	3	1
VCTS-OB	Denial of Service	Attacker can access VCTS-OB and steal or collect information via ETCS or TCMS network + remote access interface (e.g. SSH)	6.5	3	1
VCTS-OB	Elevation of Privilege	Attacker can access the VCTS-OB via ETCS or TCMS network and gain more privileges	7.9	3	2

Results

- (Unmitigated) risk levels mapped to each STRIDE domain and security zone:

Max Risk Per Zone	S	T	R	I	D	E
OB-Z	8	8	8	4	4	8
TS-Z	8	8	8	4	4	8

- Risk levels mapped to the 7 foundational requirements of IEC 63442 and their corresponding target security level (SL-T):

	IAC	UC	SI	DC	RDF	TRE	RA
OB-Z	2	2	2	2	2	2	1
TS-Z	2	2	2	2	2	2	1

- Using the SL-T, requirements from IEC 62443-3-3 (zone/system level) and IEC 62443-4-2 (component/SA level) can be identified and allocated

Conclusions & Future Directions

- Key findings highlight the importance of continuous improvement of risk assessment methodologies

- Future enhancements could include:

  - More **detailed guidelines and examples for generating system-specific vulnerability vectors**, possibly leveraging attack trees or other techniques

  - **Broader asset types**, including information assets and processes to cover IM needs

  - Aligning with **ENISA's Transport Threat Landscape for the European Union** would increase legitimacy

Thank you!

Contact: **Aria Mirzai** | aria.mirzai@ri.se

https://www.ri.se/en/what-we-do/projects/europes-rail-r2dato

Funded by the European Union

Europe's Rail

This work is funded by the European Union (grant agreement nº 101102001) and Trafikverket (TRV 2022/46318). It is supported by the Europe's Rail Joint Undertaking and its members. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union of Europe's Rail Joint Undertaking. Neither the European Union nor the granting authority can be held responsible for them.

TRAFIKVERKET
SWEDISH TRANSPORT ADMINISTRATION

RI. SE

Methodology Flowchart

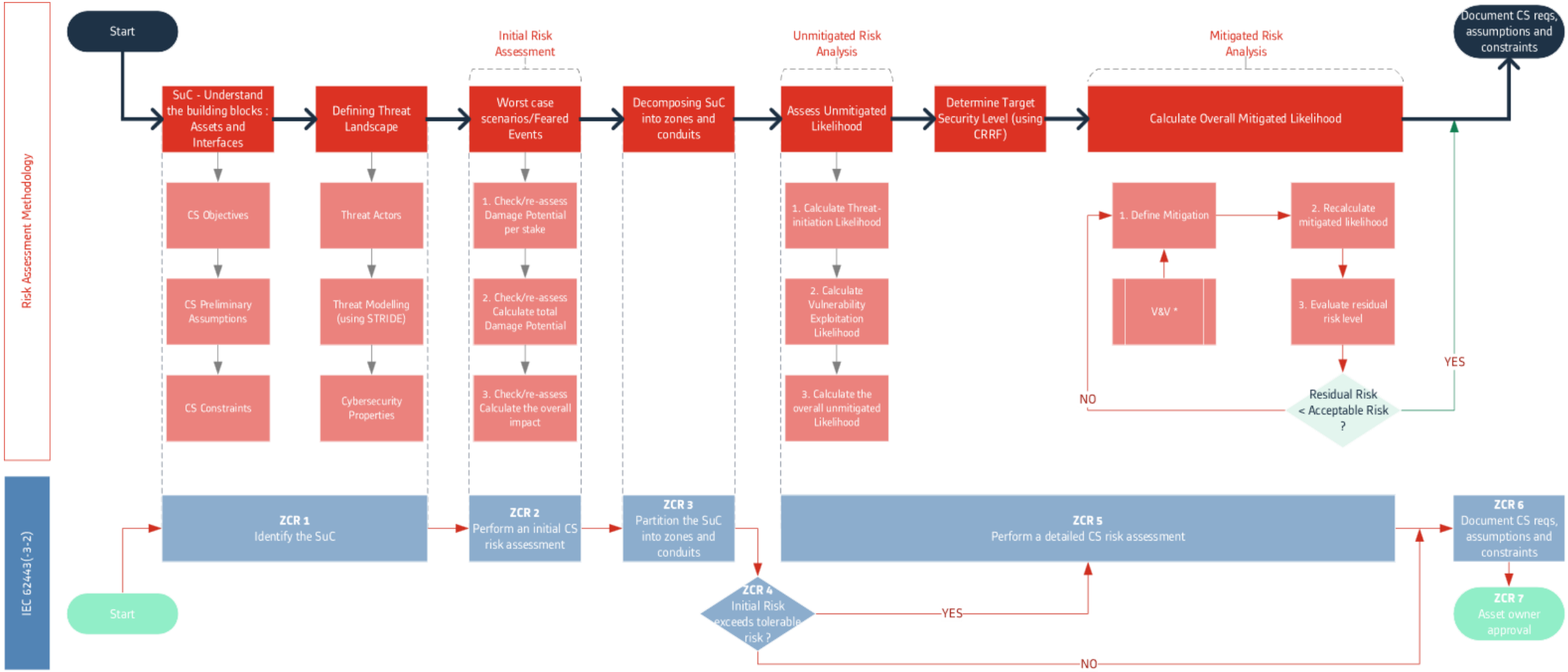


Image source: X2Rail-5 D11.1

Partition the SuC into Zones and Conduits

- Zone: Logical grouping of the supporting assets (logical or physical) that share common security needs **based on the conducted impact study on the signalling subsystem functions.**

- Conduits: The inter-zone communication channels, a representation of any data going from a zone to another. A conduit may aggregate several communication channels.

- Identified zones and conduits are later allocated requirements from IEC 62443-3-3 and IEC 62443-4-2.

Event Initiation Likelihood (EIL)

- **EIL** for each threat actor can be calculated as:

$$Max\ EIL = \left\lceil \frac{\sum_{i}^{k} \delta_i EIL}{\sum_{i=1}^{k} \delta_i} \right\rceil$$

where

$$EIL = \frac{w_i * CAP * w_i * INT * w_i * TARG}{\sum_{i=1}^{n} w_i}$$

Wi: Weights assigned to adversarial threat actor's capability, intent and targeting.

δi: Weight associated to each threat attacker type (δi = 1 in this assessment).

k: Number of actors.

⌈⌉: Represents rounding up to next nearest integer.

The EIL value can range from 1 to 4.

Threat Landscape

- Vulnerability Severity (VS): **Probability of a threat event successfully exploiting** a given vulnerability in the targeted environment, causing an adverse impact.

- VS will be based on the **Common Vulnerability Scoring System (CVSS 3.1)**, which both describes the characteristics of a software vulnerability and measures its severity.

Common Vulnerability Scoring System (CVSS)

- **CVSS** is an open framework for communicating the characteristics and severity of software vulnerabilities.
- The Base metrics produce a **score ranging from 0 to 10**. A CVSS score is also represented as a **vector string**, a compressed textual representation of the values used to derive the score.

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	Adjacent Network (AV:A)	Local (AV:L)	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	Low (PR:L)	High (PR:H)

User Interaction (UI)*

None (UI:N)	Required (UI:R)

Scope (S)*

Unchanged (S:U)	Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Low (C:L)	High (C:H)

Integrity Impact (I)*

None (I:N)	Low (I:L)	High (I:H)

Availability Impact (A)*

None (A:N)	Low (A:L)	High (A:H)

Unmitigated Vulnerability Severity (UVS) using unmitigated CVSS score

UVS	Unmitigated CVSS score
1 (critical)	0 ≤ UCVSS < 4
2 (high)	4 ≤ UCVSS < 7
3 (medium)	7 ≤ UCVSS < 9
4 (low)	9 ≤ UCVSS 10

- **Overall unmitigated likelihood = ⌊(EIL x UVS) / 4⌋**
  (likelihood of a risk event occurring without mitigation measures in place)
- The value is based on the combination of the likelihood of the threat occurring and the vulnerability of the asset being targeted:
  1 = Unlikely , 2 = Possible, 3 = Likely, 4 = Certain.

Threat Actors

	Level 1	Level 2	Level 3	Level 4
CAP (capability)	The attacker has limited resources, expertise, and opportunities to support a successful attack.	The attacker has moderate resources, expertise and opportunities to support multiple successful attacks.	The attacker has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.	The attacker has a very sophisticated level of expertise, is well-resourced and can generate opportunities to support multiple successful, continuous and coordinated attacks.
INT (intent)	The attacker actively seeks: - to obtain critical or sensitive information; - to disrupt the system's cyber resources; The attacker does not concern about attack detection or disclosure.	The attacker seeks: - to obtain or modify specific critical or sensitive information; - to disrupt the system's cyber resources; - to impede system functionalities by establishing a foothold in the organization's ICS. The attacker is concerned about minimizing attack detection/disclosure, particularly whe n carrying out attacks over long time periods.	The attacker seeks: - to undermine or impede critical aspects of a core system function; - to place itself in a position to do so in the future by maintaining a presence in the system. The attacker is very concerned about minimizing attack detection/disclosure, particularly while preparing for future attacks.	The attacker seeks: - to undermine, severely impede, or destroy a core business function or component by exploiting a presence in the system. The attacker is concerned about disclosure only to the extent that it would impede its ability to complete stated goals.
TARG (targeting)	The attacker uses publicly available information to target a class of high-value railway vendors / companies / organizations by seeking: - targets of opportunity of this class.	The attacker analyses publicly available information to target persistently specific high-value railway vendors / companies / organizations by focusing on: - key position employees; - programs; - the system itself; - information used by the system.	The attacker analyses information obtained via reconnaissance to target persistently a specific organization, enterprise, railway system or system function by focusing on: - specific high value or mission critical information; - resources; - supply flows; - system functions or specific employees supporting these functions; - key position employees.	The attacker analyses information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, railway system or system function by focusing on: - specific high value or mission critical information; - resources; - supply flows; - system functions, or specific employees supporting these functions or even supporting infrastructure. - key position employees; - providers / suppliers; - partner organizations

Threat Landscape

Security property	Threat Category	Software Applications	Network Devices	Host Devices	Embedded Devices
Integrity	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	[SPOOFING THROUGH NETWORK DEVICES] Spoofing identities to access and control network device. Techniques: T0819, T0866, T0822, T0883, T0886, T0848, T0862, T0860, T0812, T0866, T0886, T0859, T0830, T0885	[SPOOFING THROUGH HOST DEVICES] Spoofing identities to access and control host device. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0812, T0866, T0867, T0886, T0859, T0885, T0884, T0869, T0856, T0831, T0832	[SPOOFING THROUGH EMBEDDED DEVICES] Most embedded device doesn't have I&A protection, few might have simple password protection, the attack can spoof identities to access with weak/default password or brute force attack. The attacker can also perform MITM attack or Session hijacking to gain access to embedded device. Techniques: T0883, T0847, T0862, T0864, T0860, T0856, T0812, T0859, T0845, T0885, T0869, T0856, T0831
Integrity	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	[NETWORK DEVICES TAMPERING] -Physically, tamper the network device by switching network or signal wires. Hundred kilometers of cables are distributed along the trackside making access very easy. -Or access the network device by using console port, remote access tools, default/weak password. Then tamper the network configuration. (e.g. Firewall configuration, route table, ACL). Final scenario, tampering the information flow from network to change the network behavior/performance. (e.g. DDoS, DNS poisoning, ARP spoofing). -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. Techniques: T0862, T0823, T0834, T0830, T0885, T0878, T0803, T0804, T0805, T0835, T0838, T0857, T0806, T0836, T0839, T0879, T0813, T0826, T0827, T0828, T0837	[HOST DEVICES TAMPERING] -Tamper the host device and targeting on the OS level, by using trojans/viruses/worms, remote access tools. Then attacker can modify software or data in the host. (e.g. change firewall configuration in interlocking, add/change user data). -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0807, T0871, T0823, T0874, T0853, T0863, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0835, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	[EMBEDDED DEVICES TAMPERING] -Tamper the embedded device to change its function against the intended purpose. -Disturbance due to radiation: Attacker causes EMI affecting the network cabling or connected devices of the wireless network interfaces. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with hardware: Attacker injects a fault into a hardware of a TCMS device after gaining physical access to the device. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. Techniques: T0862, T0858, T0807, T0821, T0834, T0889, T0873, T0843, T0845, T0885, T0869, T0800, T0878, T0803, T0804, T0805, T0809, T0835, T0838, T0851, T0857, T0806, T0836, T0839, T0856, T0855, T0879, T0813, T0826, T0828, T0837, T0880, T0831

Image source: X2Rail-5 D11.1

Risk Heat Map

- Risk - Security Level matching:

Tolerable Risk	4		
Risk	**CRRF**	**SL-T**	**SL-T Agreed**
1	0,25	0	0
2	0,50	0	0
3	0,75	0	0
4	1,00	0	0
6	1,50	1	1
8	2,00	2	2
9	2,25	2	2
12	3,00	3	3
16	4,00	4	4

CRRF	Security Level
[0..1]	SL 0: No specific requirements or security protection necessary
]1..2[	SL 1: Protection against casual or coincidental violation
[2..3[	SL 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation
[2..4[	SL 3: Protection against intentional violation using sophisticated means with moderate resources, IASC specific skills and moderate motivation
[4..16]	SL 4: Protection against intentional violation using sophisticated means with extended resources, IASC specific skills and high motivation

Image source: X2Rail-5 D14.3