Application of FprTS 50701

Attilio Ciancabilla, Giulio Magnanini - RFI

Francesco Sperotto - HaslerRail

Davide Amato - SADEL

ENISA-ERA Conference: Cybersecurity in Railways

16 March 2021

Why an example

- An example of application of FprTS 50701 could be useful for several reasons:
  - **to check** our own interpretation, and solve our misunderstandings;
  - **to test the TS**, and find out shortcomings or inconsistencies, if any;
  - **to explain the TS**, and eliminate possible obscure or misleading passages.

Which example

Which Railway Application to choose for the example?

- the criteria
  - Most important criterion: **avoid using well known systems** to help ourselves and our audience to remain focused on the cybersecurity aspects of the system design
  - Second important criterion: find a ***new*** **railway application**, because FprTS 50701 applies mainly to new systems
  - Third criterion: select an application that possibly has **more than one security zone**.
- the choice
  - An **On-Board** electronic application with **Train-To-Ground** communications seemed to be a good choice to see how FprTS 50701 performs in practice
  - Eventually, we decided for a simplified and maybe partially re-invented **Train Integrity System**

A train integrity device

What is a Train Integrity System?

- According to X2Rail WP4 statement definition(*): *The on-board train integrity (OTI) [… has …] the main goal to autonomously verify the completeness of the train, while train is in operation. If the train tail is advancing coherently with the front of the train and the distance between the first and the last pieces of rolling stock remains unchanged it means that all is working correctly. Otherwise, the on-board system will detect the loss of train integrity, will apply the defined actions and will inform the Radio Block Center (RBC).*

- X2Rail WP4 did a great job with "Deliverable D4.1 Train Integrity Concept and Functional Requirements Specifications", but Cybersecurity was out of their scope

- We extended the OTI concept by adding an on-ground part, in order to simplify the head-tail communication problem and to add more security zones

(*) https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-2

RFI
RETE FERROVIARIA ITALIANA

Drivers

How to do secure design according to FprTS 50701?

- the **Quality** of a product cannot be obtained by simply adding on it the ISO 9000 mark after it has been produced

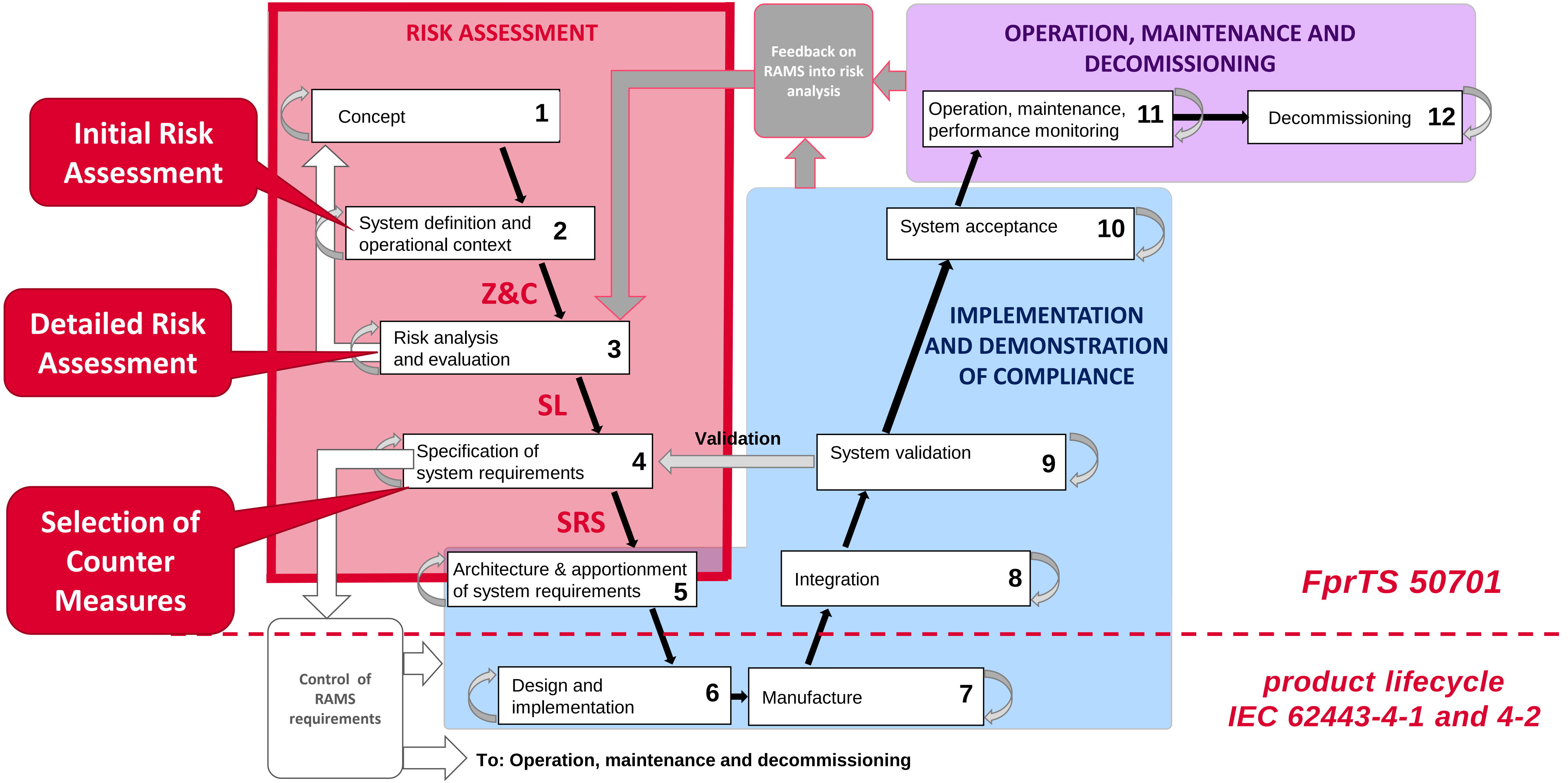
- the **Safety** of a system cannot be proved by simply looking at its requirements specifications, especially if it contains software applications

- the **Security** of a system cannot be added *ex post*

- For **FprTS 50701**, Security of a Railway Application is something that can be obtained only by **interweaving security into the application life cycle**

❑ FprTS 50701 **Table 1** “*Security-related activities within a railway application lifecycle (EN 50126-1)*” was our guide to develop the application example

Current scope of the example

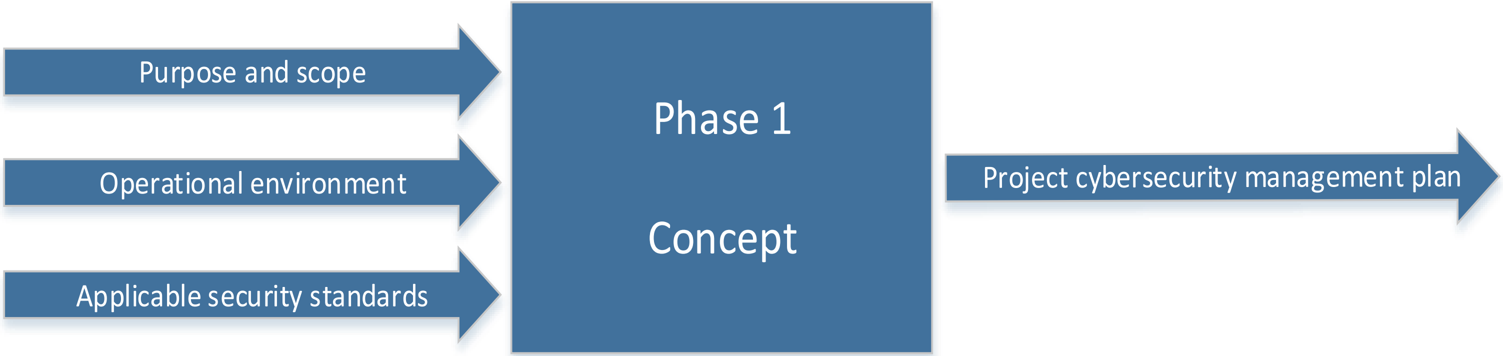


EN 50126-1:2017 - Figure 7 — The V-cycle representation

Phase 1- Concept

In this phase, the System under Consideration (SuC) is identified in terms of its Purpose and Scope, Operational Environment and Applicable Security Standards

- For this phase, FprTS 50701 defines three inputs and one output



- Cybersecurity activities added to this phase by TS 50701 are:

[5.3 Table 1 Phase 1]
- Review of the level of security achieved up to now
- Analysis of the project's security implication and context (incl. generic threats) (see 5.4)
- Alignment with railway operator / asset Owner and stakeholder’s security goals
- Consideration of security lifecycle aspects (patch management, monitoring etc.) (see Clause10)
- Plan cybersecurity-related activities

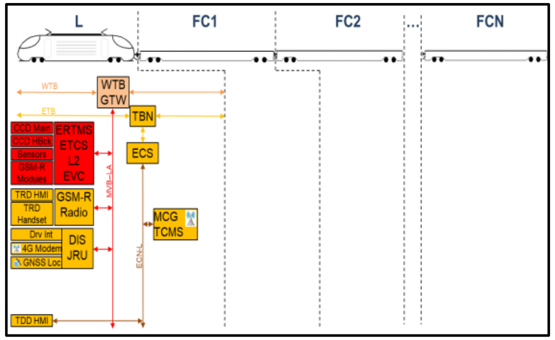
Phase 1 - Input

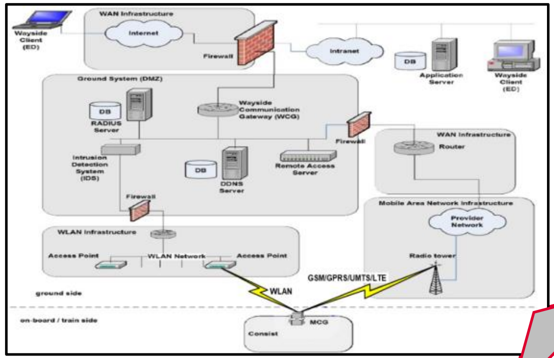
Purpose and scope

The system under consideration (SuC) is composed by an on-ground application, hosted in the cloud, and one or more software applications, hosted in on-board devices for each and all the trains.
The on-board software applications are responsible to get train run data, add the train position and the measured train composition length and send these data to the on-ground application.
The on-ground application use this information to notify an alarm if measured train composition length does not match with train run data.

Operational environment

The operational environment defined by the customer is identified in the two following figures.





Applicable security standards

NIS directive	Critical infrastructure cybersecurity
EN 50126-1,2:2017	Railway application RAMS
EN 50657:2017	Railways Applications. Rolling stock applications. Software on Board Rolling Stock
IEC 61375-1:2012	Electronic railway equipment - Train communication network (TCN) - Part 1: General
IEC 61375-2-1:2012	Electronic railway equipment - Train communication network (TCN) - Part 2-1: Wire Train Bus (WTB)
IEC 61375-2-2:2012	Electronic railway equipment - Train communication network (TCN) - Part 2-2: Wire Train Bus conformance testing
IEC 61375-2-5:2014	Electronic railway equipment - Train communication network (TCN) - Part 2-5: Ethernet train backbone (ETB)
IEC 61375-2-6:2018	Electronic railway equipment - Train communication network (TCN) - Part 2-6: On-board to ground communication
IEC 61375-3-1:2012	Electronic railway equipment - Train communication network (TCN) - Part 3-1: Multifunction Vehicle Bus (MVB)
IEC 61375-3-2:2012	Electronic railway equipment - Train communication network (TCN) - Part 3-2: MVB (Multifunction Vehicle Bus) conformance testing
IEC 61375-3-4:2014	Electronic railway equipment - Train communication network (TCN) - Part 3-4: Ethernet Consist Network (ECN)
TS 50701	Railway application cybersecurity
IEC 62443 series	Industrial automation cybersecurity
ISO/IEC 27001:2013	Information technology -- Security techniques -- Information security management systems – Requirements

Phase 1 - Output

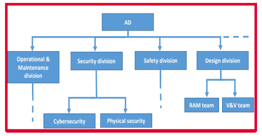
Project Cybersecurity Management Plan

The main goal of this document is to define the strategy and the organization involved in the implementation of the cybersecurity project.

1. Cybersecurity activities management
2. Cybersecurity Context (could be a set of references to other documents)
3. Cybersecurity Risk Management (could be a set of references to other documents)
4. Cybersecurity Design (could be a set of references to other documents)
5. Cybersecurity Assurance and Acceptance (could be a set of references to other documents)
6. Vulnerabilities and Cybersecurity issues Management (could be a set of references to other documents)
7. Third Parties Risk Management (could be a set of references to other documents)

(reference to)

Project Organization Chart



....

Risk Matrix

Risk matrix Example		Likelihood				
		1	2	3	4	5
Threat impact	E	Low	Low	Low	Low	Medium
	D	Low	Low	Low	Medium	Significant
	C	Low	Low	Medium	Significant	High
	B	Low	Medium	Significant	High	High
	A	Medium	Significant	High	High	Very high

(reference to)

(reference to)

CRS

Cybersecurity Requirements Specification

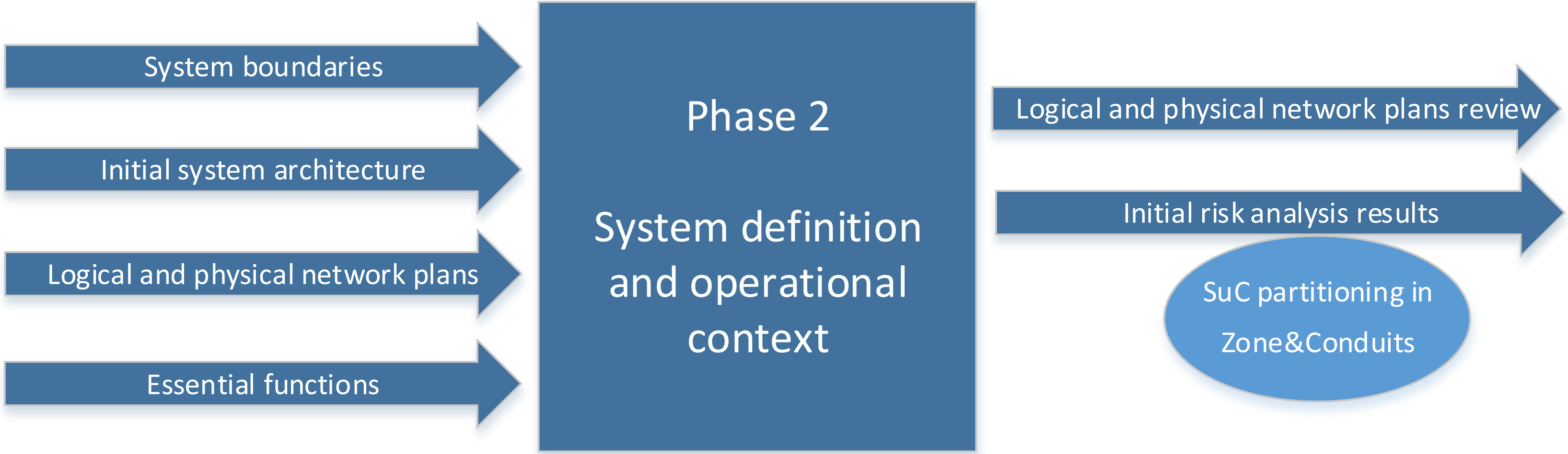
....

Cybersecurity Case

(reference to)

Phase 2 – System definition and operational context

In this phase the SuC is defined in terms of its boundaries, architecture, network plan and essential functions.



- cybersecurity activities foreseen by the FprTS 50701 for this phase are:

[5.3 Table 1 Phase 2]

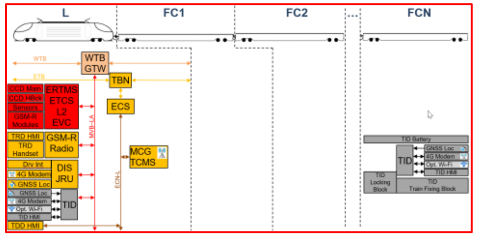
- Review of the logical and physical network plans
- * Initial Risk Assessment for the SuC (see 6.3)
- * Partitioning of the SuC into zones and conduits (see 6.4)
- * Documentation of components, interfaces and characteristics for each zone and conduit (see 6.5)

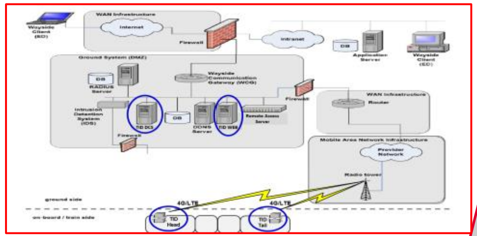
*: This activity and the corresponding synchronization point may also be conducted in phase 3.

Phase 2 - Input

System boundaries
Initial system architecture
Logical and physical network plans

For the scope of our example, the first three inputs of this phase (System boundaries, Initial system architecture, Logical and physical network plans) are represented by figures and associated descriptions.





- **SuC name: STIMS** (Secure Train Integrity Monitoring System)
- **Description:** STIMS is composed by at least two **TID** on-board devices per train and one **TIS** on-ground.
  - **TID** (Train Integrity Device): continuously acquires its position and communicates it to TIS. It shall be installed in head-unit and in tail wagon. The TID has the following main blocks:
    - Localization block based on a **GNSS** (Global Navigation Satellite System) receiver. This receiver could use Galileo, GPS, Glonass or Beidou technology.
    - Wireless communication block based on a single or multiple **Modem** (Gateway). This modem could use 2G, 3G, 4G, 5G or GSM-R/GPRS-R technology.
    - Driver Interface block placed on the driver desk. This **TID HMI** could be a simple set of LED and switches, or a touch-screen monitor.
    - **TID computing block**. This is the elaboration unit based on a microcontroller, microprocessor, FPGA, RAM based memory, Flash based memory and some interfaces.
    - *Optional* **Wi-Fi communication block** able to allow the interaction of the TID with a laptop, tablet or smartphone. This block could be based on Wi-Fi, BlueTooth or other wireless short-range technology.
  - **TIS** (Train Integrity Service): continuously collects TID data, computes train length and notifies alarms in case of anomalies. A TIS has the following main blocks:
    - **TIS DCS** (Train Integrity Service Data Collection Server): provides communications services to collect and process data from on-board TID devices
    - **TIS WEB** (Train Integrity Service Web Application): provides centralized configuration, analysis and management services to STIMS operators

Phase 2 - Input

Essential functions

Essential functions

An essential function is defined as “function or capability that is required to maintain health, safety, the environment and availability for the equipment under control”.
If the essential functions are compromised, this normally means loss of protection, loss of control or loss of view.

If not directly available in system design, essential function can be derived from overall functional description with the simple process (illustrated by the table aside):

1) list all function;
2) if a function is required to maintain at least one of the four properties health, safety, environment and availability, then it is essential.

	REQUIRED TO MAINTAIN				Essential
FUNCTION	HEALTH	SAFETY	ENVIRON.	AVAIL.	
- On board					
○ Get application specific essential train run data from TCMS: EVN, Composition.		X		X	YES
○ Get positions of train head and of train tail		X		X	YES
○ Calculate train length		X		X	YES
○ Send data to ground		X		X	YES
○ Send diagnostics info to TCMS					NO
○ Send alert to driver (HMI)		X		X	YES
- On ground					YES
○ Receive data from on-board applications		X		X	YES
○ Store received data		X		X	YES
○ Validate received data		X		X	YES
○ Check for train length anomalies		X		X	YES
○ Notify position of train to external systems					NO
○ Record excessive delays in order to raise fines					NO
○ Send real-time status to the maintenance system to permit drone recognition over the tracks				X	YES
○ Notify alarms in case anomalies are detected		X		X	YES
○ Web User Interface				X	YES

RFI RETE FERROVIARIA ITALIANA

Phase 2 – Output: Initial Risk Evaluation

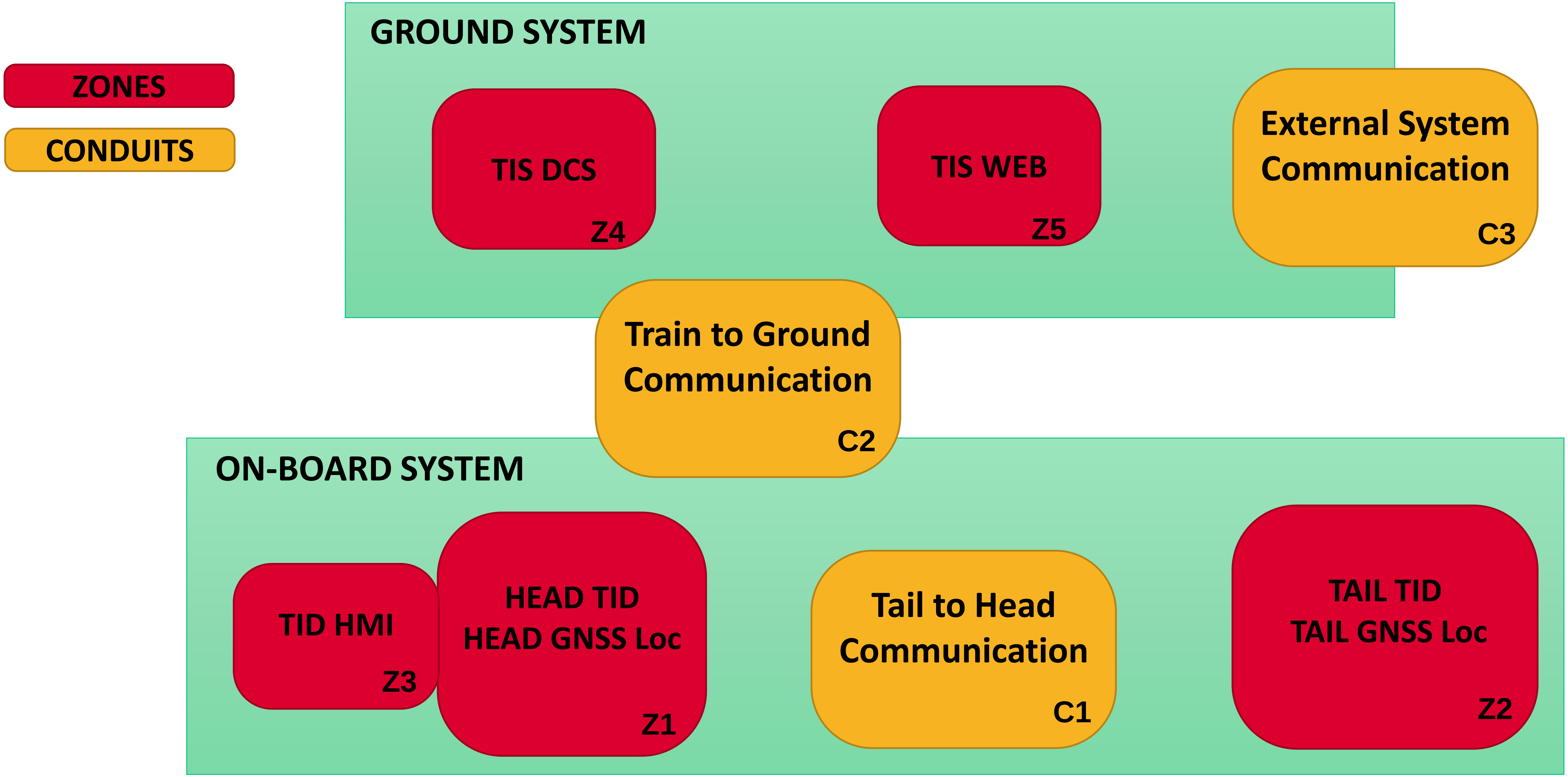
Initial Risk evaluation for assets

Asset	Impact	Likelihood	Risk	Acceptable ?
TID HMI	B	3	Significant	NO
Head TID	B	3	Significant	NO
Head GNSS Loc	C	4	Significant	NO
Tail to Head Communication	B	2	Medium	YES
Tail TID	B	5	High	NO
Tail GNSS Loc	C	5	High	NO
Train to Ground Communication	B	3	Significant	NO
TIS DCS	B	1	Low	YES
TIS WEB	D	4	Medium	YES
External System Communication	C	4	Significant	NO

Classification in Zones and Conduits

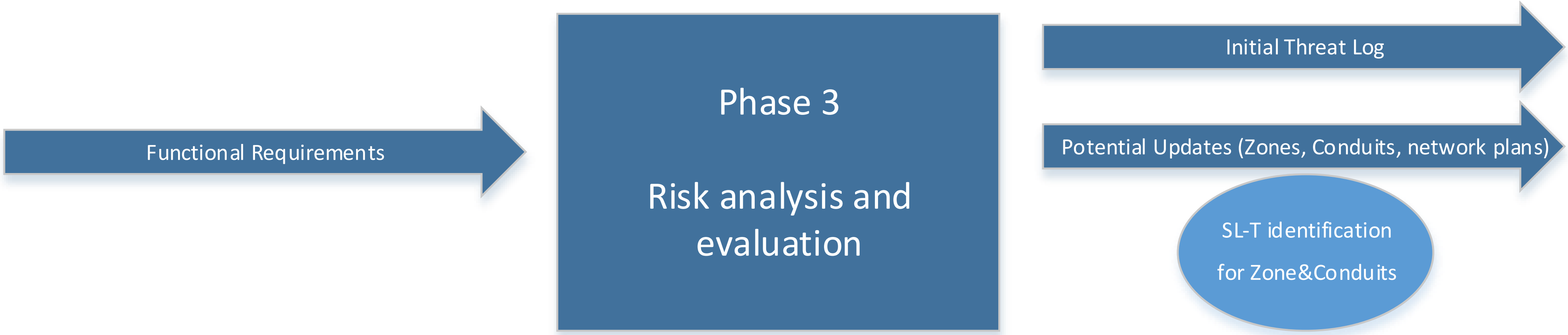
N° zone/conduit	Type	Including	Risk
Z1	Zone	Head TID, Head GNSS Loc	Significant
Z2	Zone	Tail TID, Tail GNSS Loc	High
Z3	Zone	TID HMI	Significant
Z4	Zone	TIS DCS	Low
Z5	Zone	TIS WEB	Medium
C1	Conduit	Tail to Head Comm.	Medium
C2	Conduit	Train to Ground Comm.	Significant
C3	Conduit	External System Comm.	Significant

Phase 2 – Zones and conduits



Phase 3 – Risk analysis and evaluation

In this phase the design of the SuC is submitted to a detailed risk assessment



- cybersecurity activities foreseen by the FprTS 50701 for this phase are:

[5.3 Table 1 Phase 3]

- *Detailed Risk Assessment (DRA) (see Clause 7): derive technical (e.g. SL-T), physical and organizational countermeasures or assumptions for zones and conduits*
- *Consider business continuity aspects (incl. incidence response and recovery) for the SuC*

Phase 3 - Output

Initial Threat Log

For each threat at least, the following information shall be documented in the threat log:

a) the threat sources

b) the capability or skills or motivation of the threat source

c) the possible threat scenarios and actions

d) the potentially affected assets (as identified in the initial risk assessment)

e) the vulnerabilities of the SuC (if known)

Threat name	Threat source	Capability or skills or motivation of threat source	Possible threat scenarios and actions	Potentially affected assets	Vulnerabilities of the SuC (if known)
T.PhysicalAttacks	External	Demonstration, Theft	Intentional damage, theft	Z1, Z2, Z3	Perimeter protection vulnerabilities
T.UnintentionalDamage	Internal	Knowledge of target	Wrong installation	Z1, Z2, Z3	Account Management
T.FailuresAndOutages	Internal External	Hacking	Denial Of Service	Z1, Z2, Z3,C3	Unpatched components
T.EavesdroppingInterceptionHijacking	External	Hacking	Data exfiltration	C2,C3	Clear text comm., Network addressing vulnerabilities
T.MaliciousActivity	External	Cybercrime	Command and Control	Z1, Z2, Z3	Poor auth., Unpatched components
T.Legal	External	-	-	-	-

Phase 3 - Output

The SL-T vector

IAC	UC	SI	DC	RDF	TRE	RA

FORMAT → SL-?([FR,]domain) = { IAC UC SI DC RDF TRE RA }

where

SL-? = (Required) The SL type (see A.2.2). The possible formats are:

- SL-T = Target SL
- SL-A = Achieved SL
- SL-C = Capabilities SL

[FR,] = (Optional) Field indicating the FR that the SL value applies. The FRs are written out in abbreviated form instead of numerical form to aid in readability.

domain = (Required) The applicable domain that the SL applies. Domains can refer to zones, control systems, subsystems or components. Some examples of different domains from Figure A.1 are SIS zone, BPCS zone, BPCS HMI, Plant DMZ domain controller, Plant DMZ to Control Center conduit and SIS to BPCS serial conduit. In this particular document, all requirements refer to a control system, so the domain term is not used as it would be by other documents in the ISA‑62443 series.

EXAMPLE 1 → SL-T(BPCS Zone) = { 2 2 0 1 3 1 3 }

EXAMPLE 2 → SL-C(SIS Engineering Workstation) = { 3 3 2 3 0 0 1 }

EXAMPLE 3 → SL-C(RA, FS-PLC) = 4

7 Foundational Requirements

1) Identification and authentication control
2) Use control
3) System integrity
4) Data confidentiality
5) Restricted data flow
6) Timely response to events
7) Resource availability

IEC 62443-3-3:2019
Annex A.3.3

Phase 3 - Output

SL-T vectors in our example

		IAC	UC	SI	DC	RDF	TRE	RA
Z1	SL-T (Head TID) =	{ 3	3	3	3	2	3	3 }
Z2	SL-T (Tail TID) =	{ 3	3	3	3	2	3	3 }
Z3	SL-T (TID HMI) =	{ 2	2	2	3	2	2	2 }
C2	SL-T (Train to Ground Comm.) =	{ 0	0	0	3	3	0	0 }
C3	SL-T (External System Comm.) =	{ 3	3	3	3	3	3	3 }

Phase 4 – Specification of system requirements

In this phase the deliverable Cybersecurity Requirements Specification is finally produced

Phase 4

Specification of system requirements

→ System Cybersecurity Requirements Specification

- cybersecurity activities foreseen by the FprTS 50701 for this phase are:

[5.3 Table 1 Phase 4]

- ***SuC-specific refinement of normative requirements*** *(see Clause 8)*
- *Definition of organizational and physical requirements*
- *Definition of security-related application conditions (see Clause 7)*

Phase 4 – Output

System Cybersecurity Requirements Specification

1) SUC description
2) Zone and conduit drawings
3) **Zone and conduit characteristics**
4) Operating environment assumptions
5) Threat environment
6) Organizational security policies
7) Tolerable risk
8) Regulatory requirements

IEC-ISA-62443-3-2, D7E2 April 2018

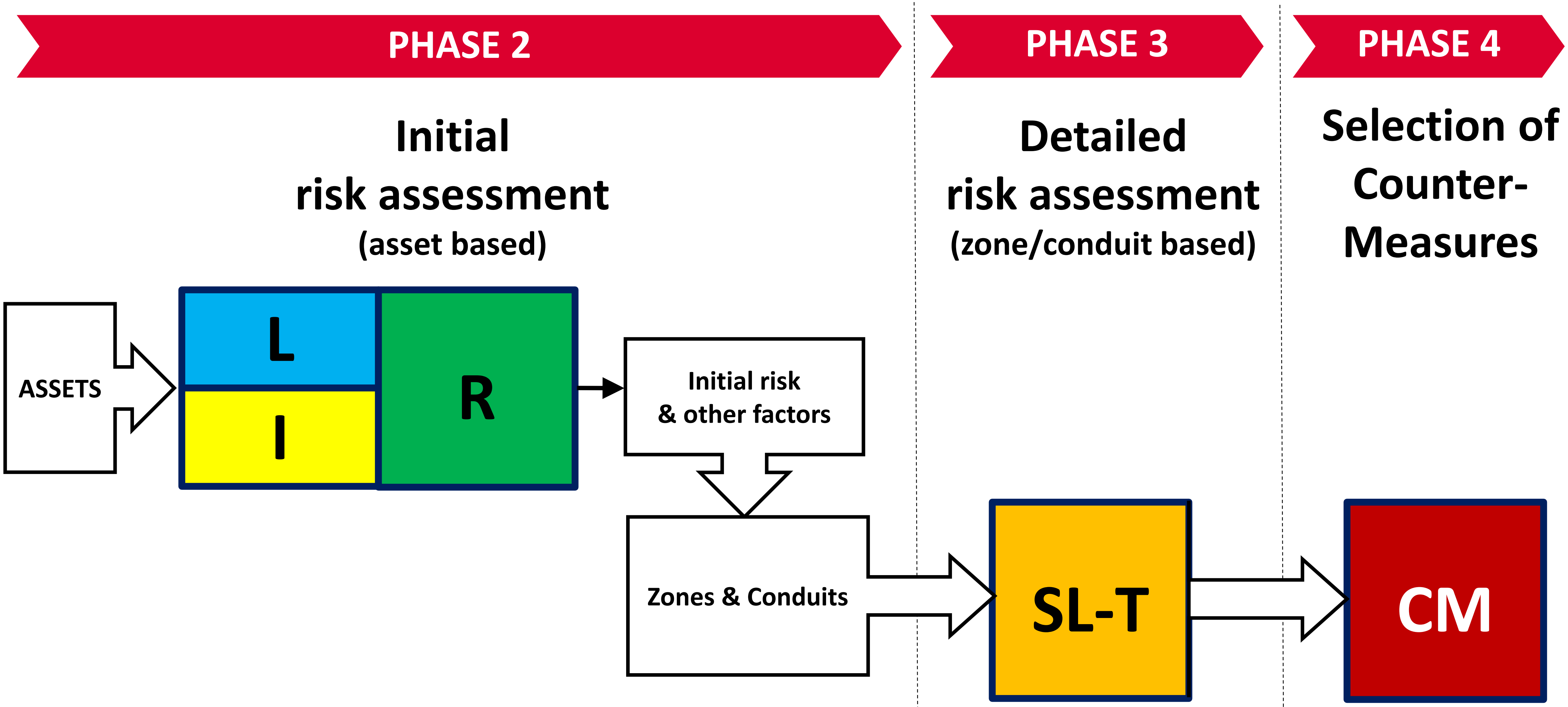
Zone and conduit characteristics

a) Name and/or unique identifier
b) Accountable organization(s)
c) Definition of logical boundary
d) Definition of physical boundary, if applicable
e) Safety designation
f) List of all logical access points
g) List of all physical access points
h) List of data flows associated with each access point
i) Connected zones or conduits;
j) List of assets and their classification, criticality and business value
k) **SL-T**
l) **Applicable security requirements**
m) Applicable security policies
n) **Assumptions and external dependencies**

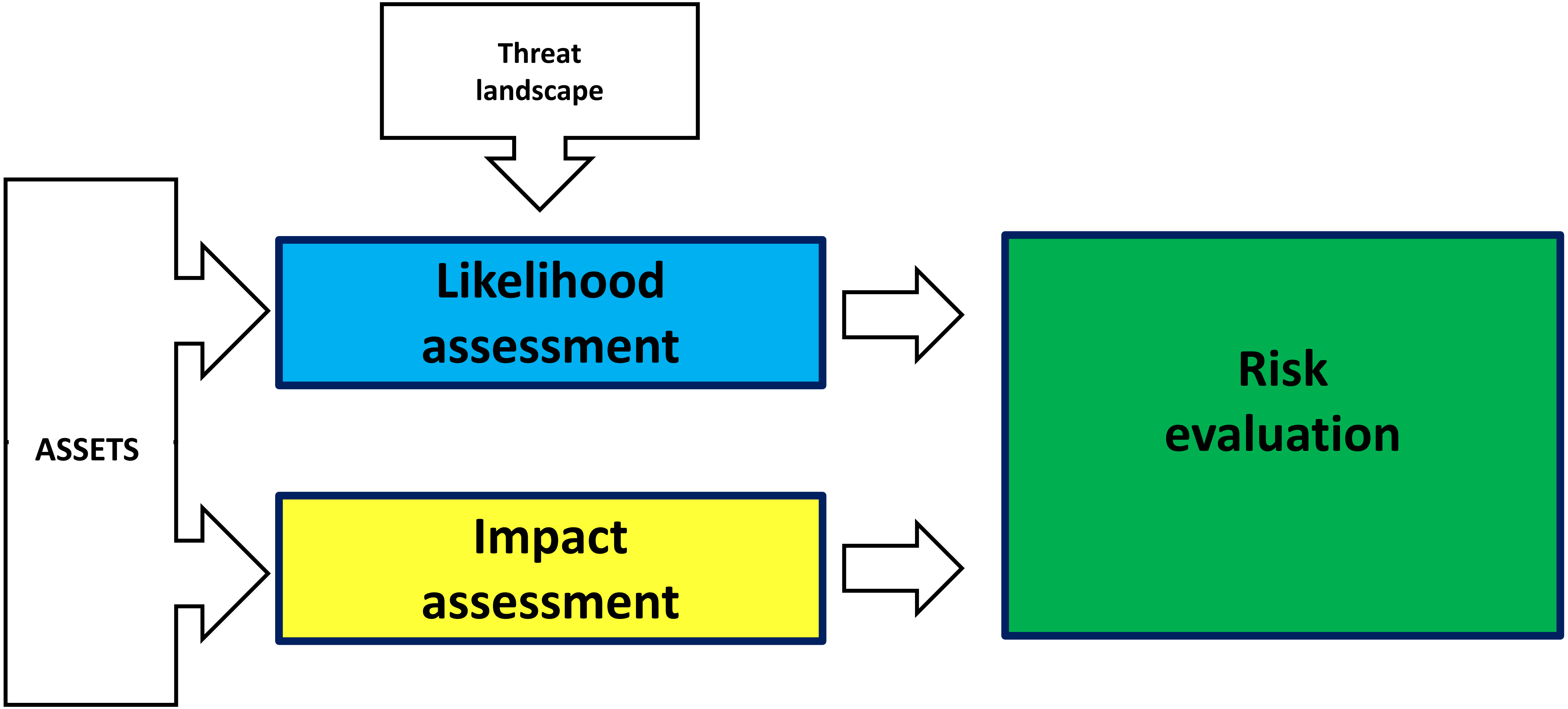
IEC-ISA-62443-3-2, D7E2 April 2018

o) Security Related Application Conditions (SecRAC) added by FprTS 50701

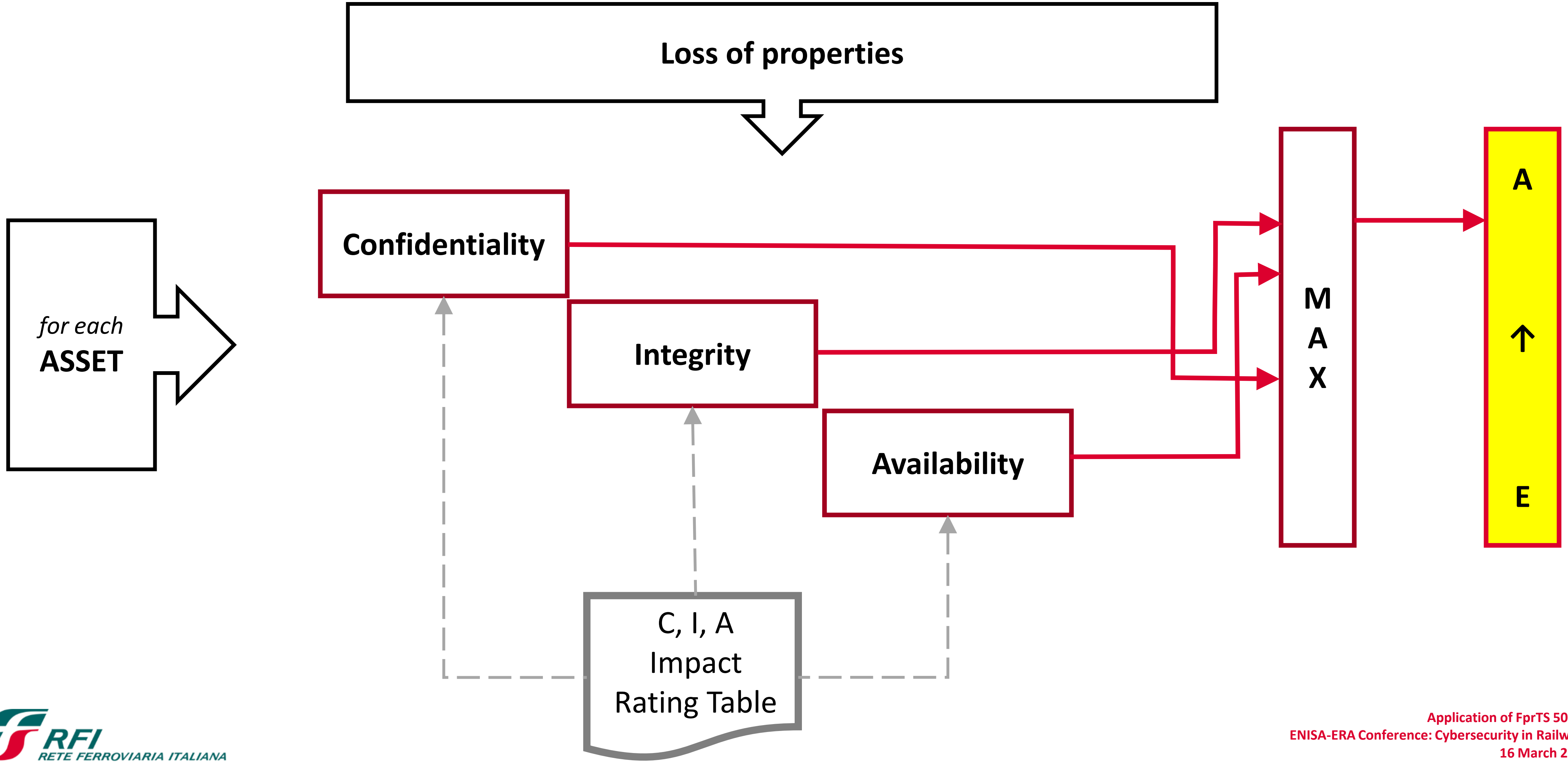
Detailing the process (excerpt for phases 2,3,4)



Phase 2 - Initial Risk Assessment



Phase 2 - Impact Assessment

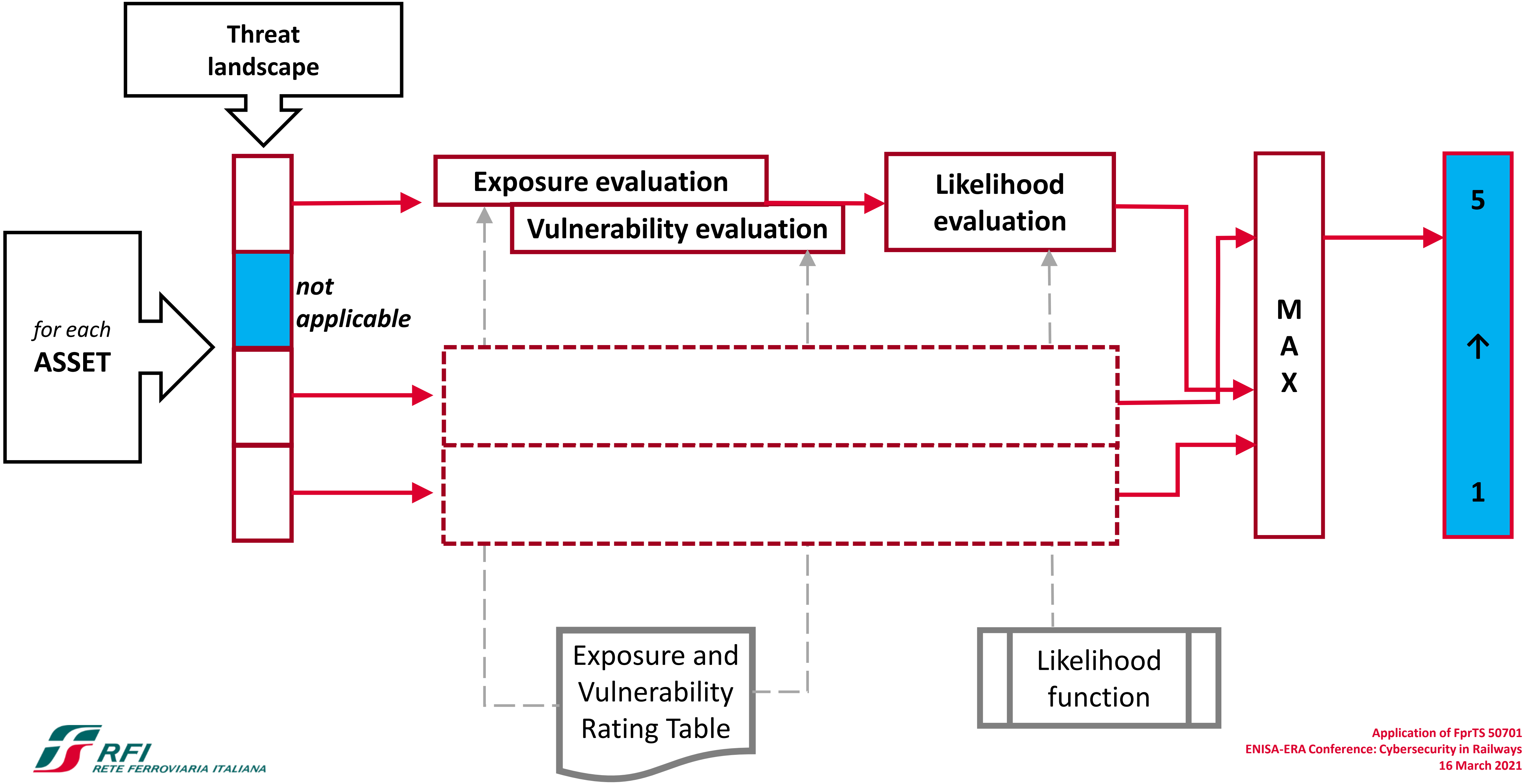


Phase 2 – C, I, A Impact Rating Table

FprTS 50701 - Table E.5: Impact assessment matrix – Example 2

Category	Availability	Integrity (Safety)	Confidentiality	Integrity (Business)
A	Major interruption of operation affecting a network or a fleet or loss of service more than 500.000 people for a long time[1]	Catastrophic accident, typically affecting a large number of people and leading to multiple fatalities	Loss of security related information. e. g. credentials, giving direct access to the system and leading to catastrophic safety, availability or business impacts.	Catastrophic business impact possibly leading to bankruptcy or loss of license of operator
B	Major interruption of operation affecting a network or a fleet or loss of service to more than 500.000 people for a significant time[1] or of a line or station or few vehicles for a long time	Critical accident, typically affecting a small number of people and leading to a single fatality	Loss of security related information, no direct access to the system is possible (physical protection), attacker could perform commands leading to at least critical availability, safety and business impacts.	Critical business impact possibly leading to severe impact in revenue or earnings (>10% on annual basis)
C	Significant interruption of operation affection a network or fleet or more than 500.000 people for a short time[1] OR of a line or station or few vehicles for a significant time	safety implications, typically leading to injuries requiring hospitalization	Loss of security related information, no direct access to the system is possible (physical protection), attacker cannot perform any critical safety-related commands; for example: only read access to diagnostic data is possible; loss of data under data protection law or commercially sensitive data	Significant business impact possibly leading to substantial impact on revenue or earnings (on annual basis)
D	Significant interruption of operation of a line or station or a few vehicles for a significant time	minor safety implications, typically leading to injuries without hospitalization	Loss of non-security relevant data, data are not under data protection; attacker can make commercial use of the data by combing with other information	Marginal business impact
E	typically, no influence	typically, no safety implications	Loss of non-security relevant data, data are not under data protection	Negligible business impact

Phase 2 - Likelihood Assessment



Phase 2 - Exposure and Vulnerability Rating Table

Rating	Exposure (EXP)	Vulnerability (VUL)
1	Highly restricted logical or physical access for attacker, e.g. - highly restricted network and physical access, or - product or components cannot be acquired by attacker or only with high effort	- Successful attack is only possible for a small group of attackers with high hacking skills (high capabilities needed) - Vulnerability is only exploitable with high effort, and if strong technical difficulties can be solved, non-public information about inner workings of system is required - State of the art security measures to counter the threat - High chance for attacker to be traced and prosecuted
2	Restricted logical or physical access for attacker, e.g. - internal network access required, or - restricted physical access, or - product or components can be acquired by attacker with medium effort	- Successful attack is feasible for an attacker with average hacking skills (medium capabilities needed) - Vulnerability is exploitable with medium effort, requiring special technology, domain or tool knowledge - Some security measures to counter the threat - Medium chance for attacker to be traced and prosecuted
3	Easy logical or physical access for attacker, e.g. - Internet access sufficient, or - public physical access, or - attacker has access as part of daily work, operation, or maintenance activities, or - product or components can be acquired by attacker with low effort	- Successful attack is easy to perform, even for an unskilled attacker (little capabilities needed) - Vulnerability can be exploited easily with low effort, since no tools are required, or suitable attack tools freely exist. - No or only weak security measures to counter the attack caused by the threat - Low chance for attacker to be traced and prosecuted

FprTS 50701 - Table 4: Likelihood assessment matrix – Example

L=EXP+VUL-1

FprTS 50701 - 6.3.2
The likelihood function

Phase 2 - Risk evaluation

Risk Matrix

Impact vs **Likelihood**

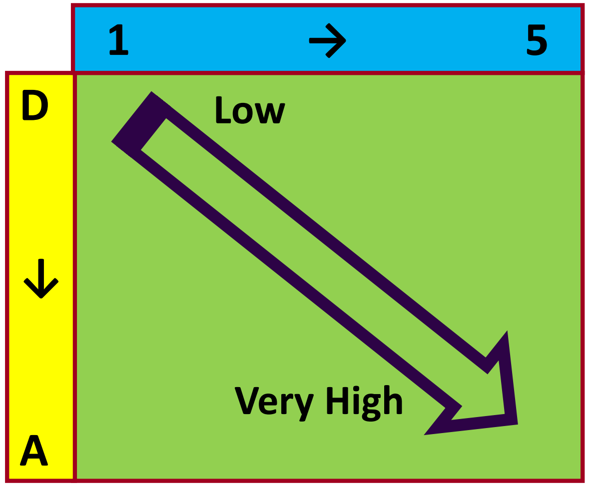


Table 5
[4x5]

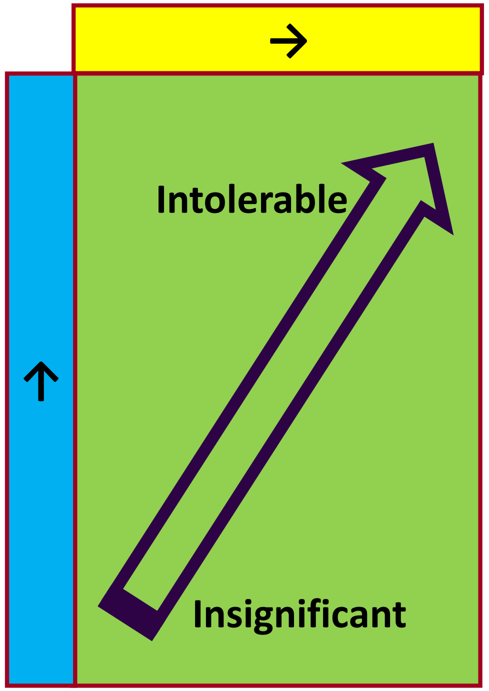


Table E.1
[6x4]

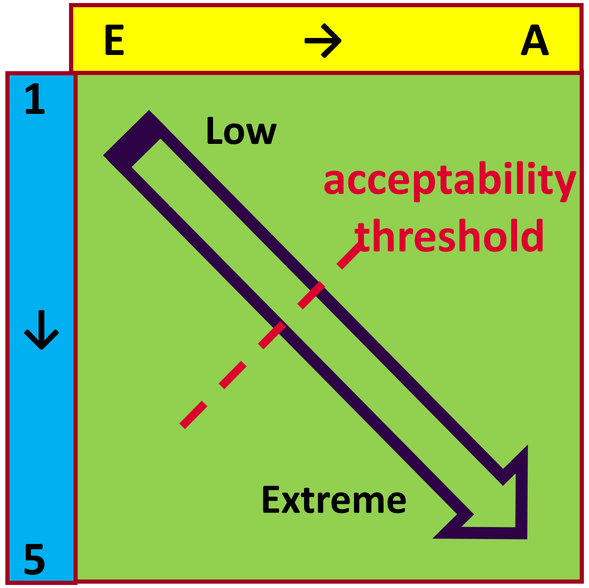


Table E.7
[5x5]

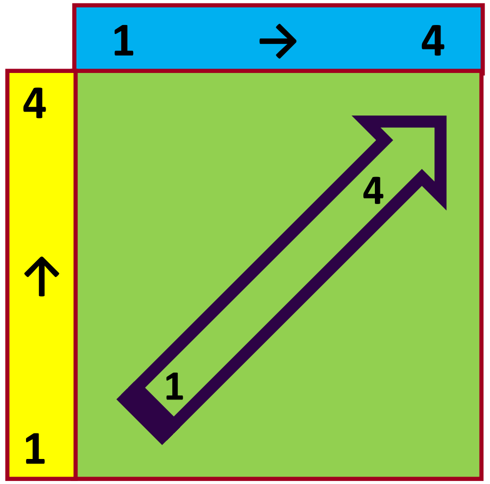


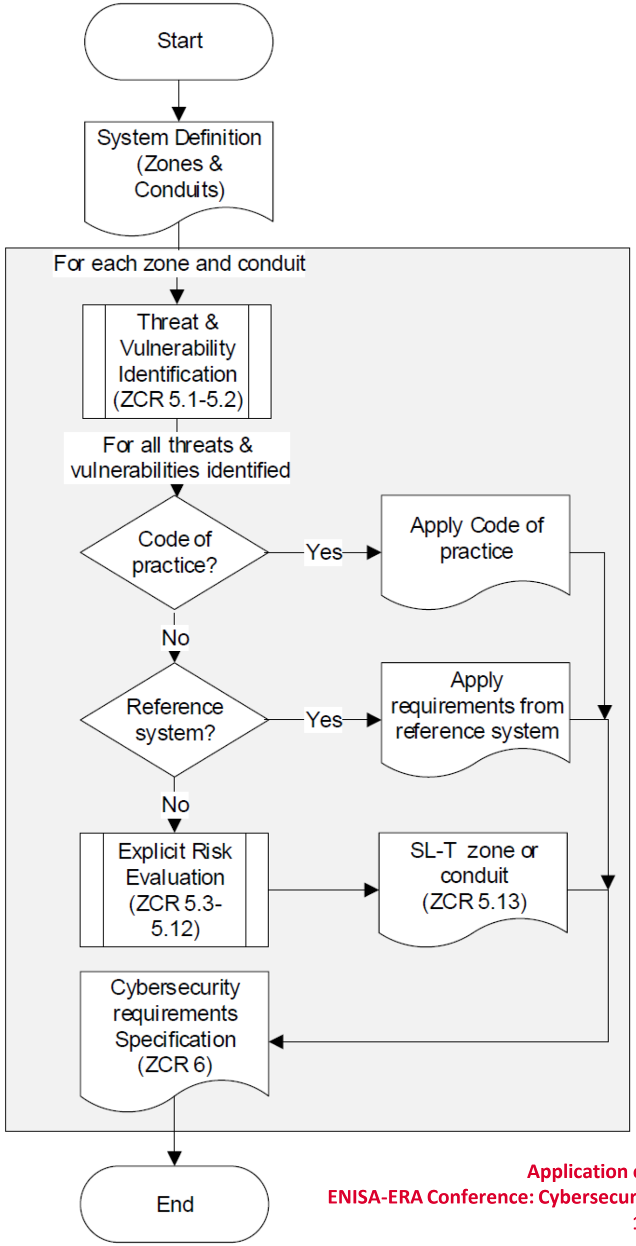
Table E.11
[4x4]

Phase 3 – Detailed risk assessment

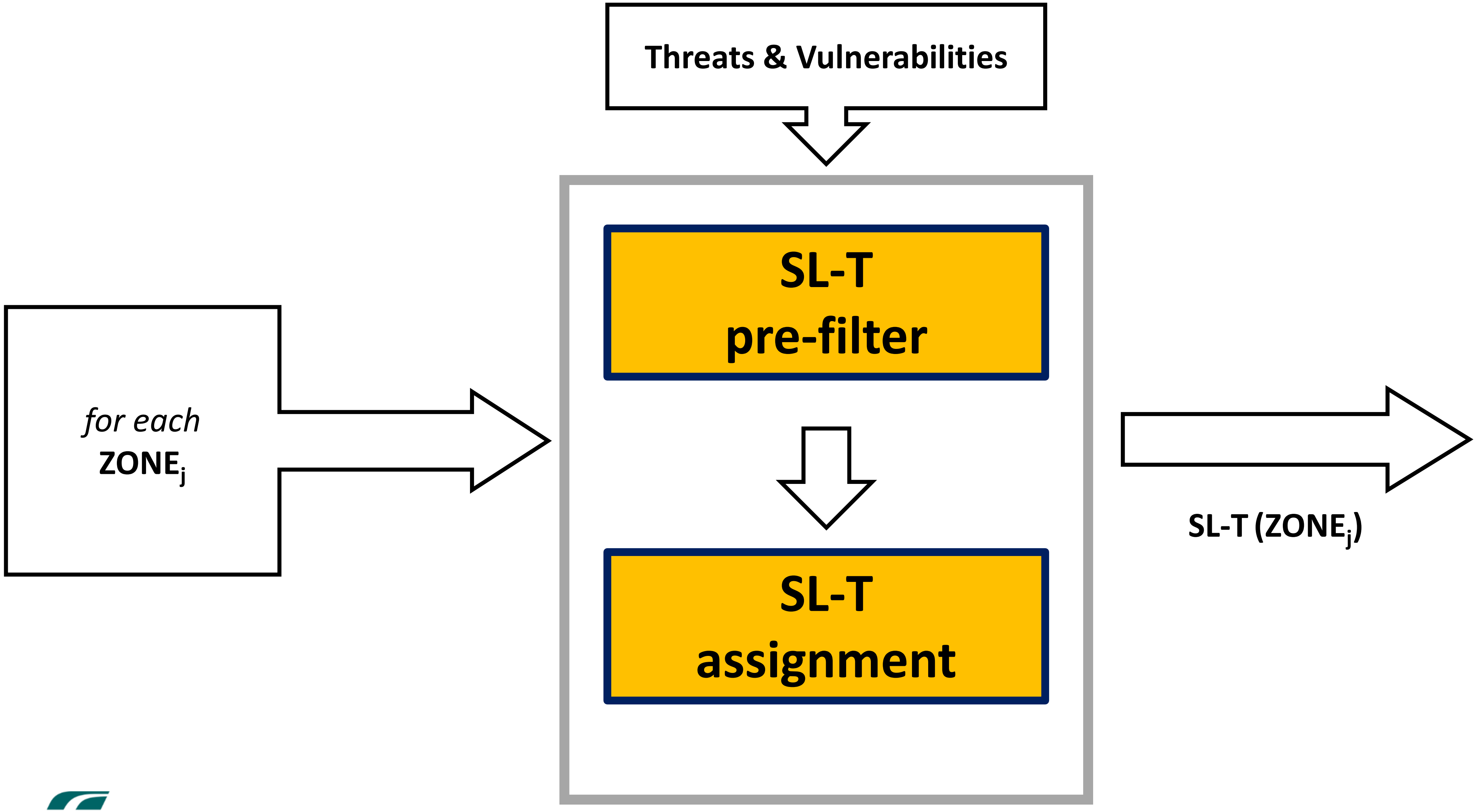
For each zone and conduit

for each threat and vulnerability

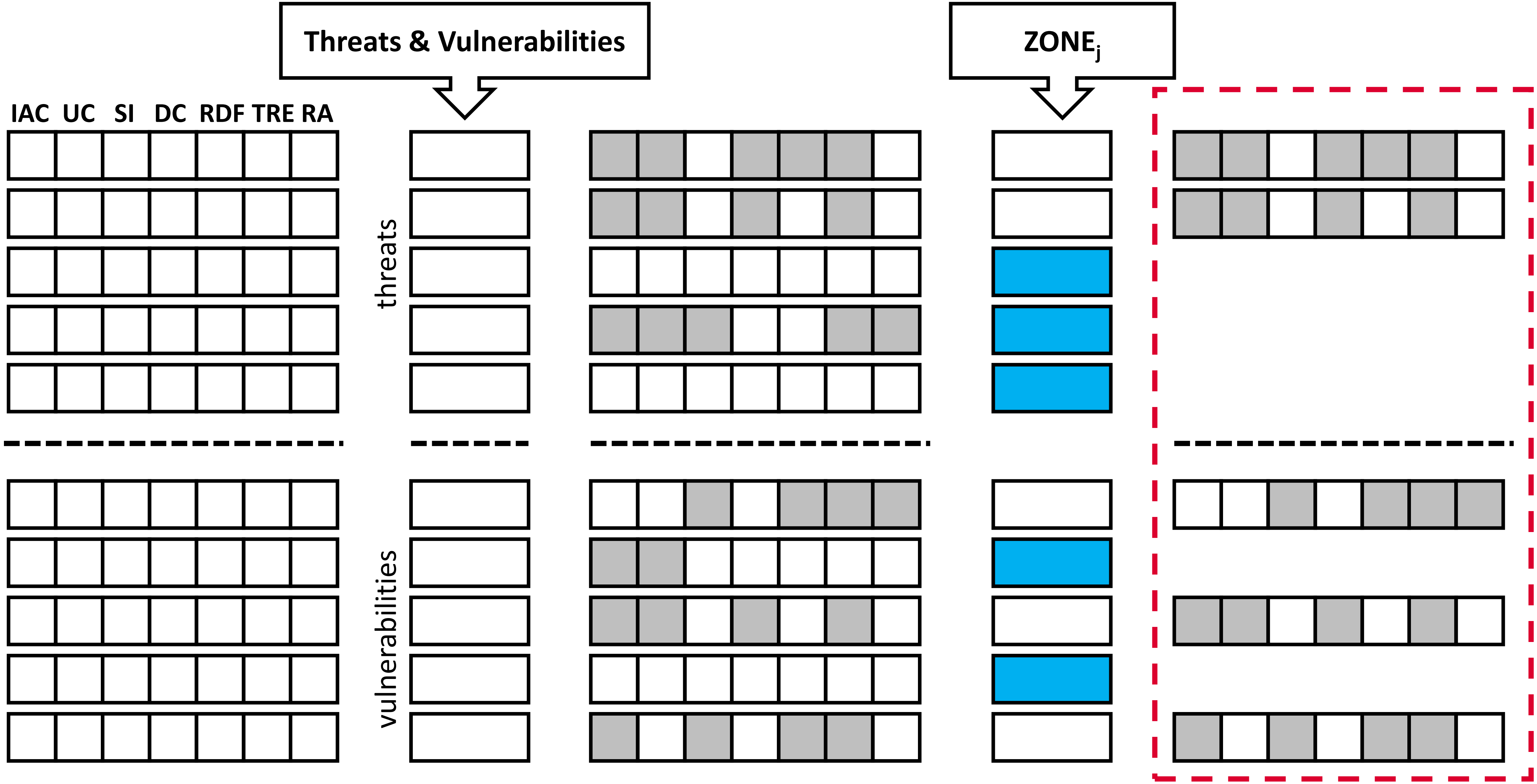
derive the SL-T vector



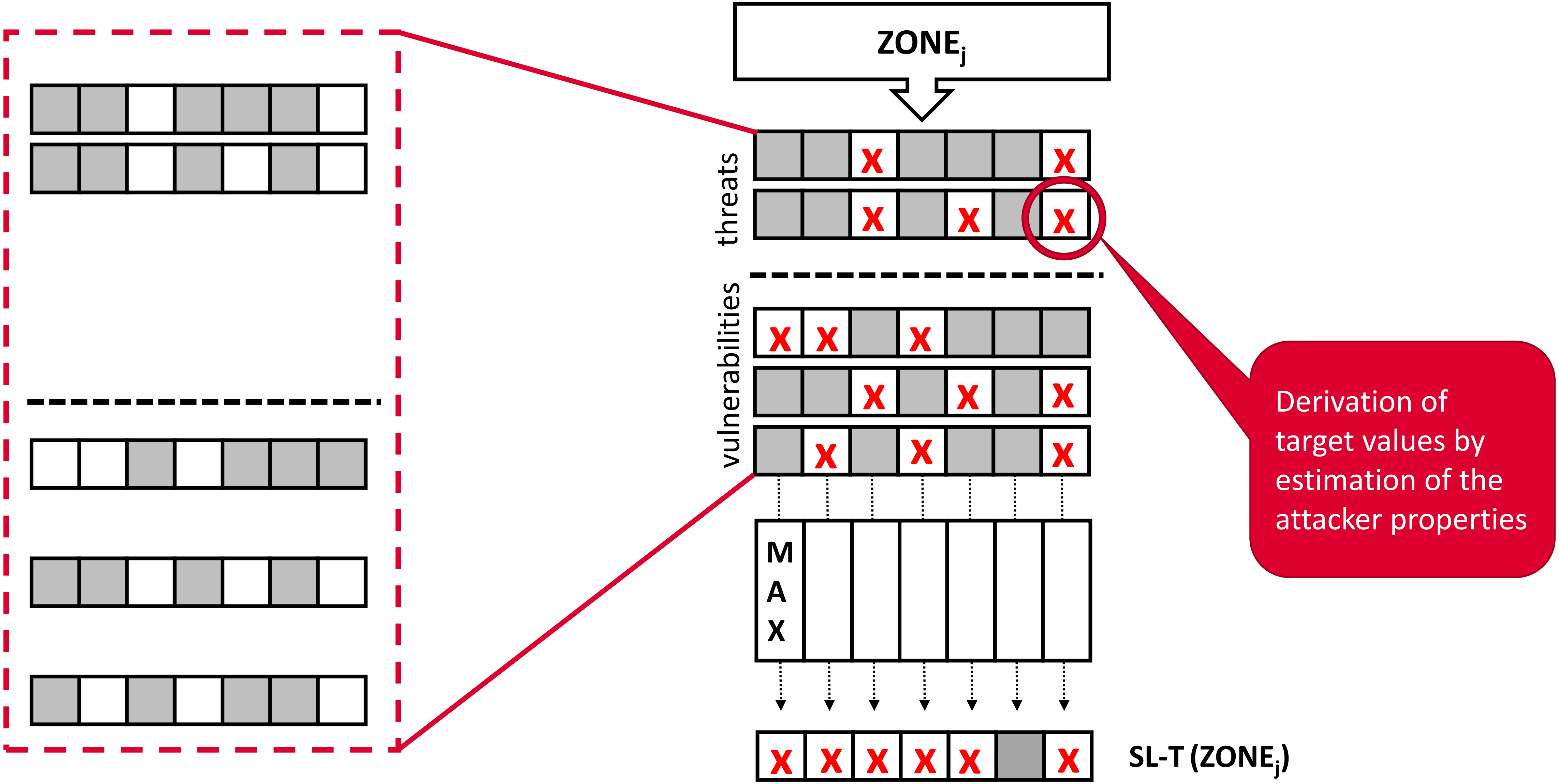
Phase 3 – Detailed risk assessment



Phase 3 – SL-T prefiltering



Phase 3 – SL-T assignment



Phase 3 – derivation of SL-T by estimation of the attacker properties

<table>
<tr><th></th><th>Violation</th><th>Means</th><th>Resources</th><th>Skills</th><th>Motivation</th></tr>
<tr><td>SL 0</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>SL 1</td><td>casual or coincidental</td><td></td><td></td><td></td><td></td></tr>
<tr><td>SL 2</td><td rowspan="3">intentional</td><td>simple</td><td>few</td><td>generic</td><td>low</td></tr>
<tr><td>SL 3</td><td rowspan="2">sophisticated</td><td>moderate</td><td rowspan="2">specific</td><td>moderate</td></tr>
<tr><td>SL 4</td><td>extended</td><td>high</td></tr>
</table>

FprTS 50701 - 7.2.5

More explanations of Security Levels in:
IEC 62443-3-3:2019
Annex A.3.2, level definitions

Phase 4 – Selection of countermeasures

A set of 100 cybersecurity requirements is given in IEC 62443-3-3. They are grouped by FR and classified with their SL value.

The SL vector is a key to enter the table and select a subset of these requirements.

FR>	IAC	UC	SI	DC	RDF	TRE	RA		tot
SL 1	10	8	5	2	4	1	7		37
SL 2	6	4	5	2	2	1	3		23
SL 3	6	9	6	1	4	1	3		30
SL 4	2	3	3	1	1	0	0		10
tot	24	24	19	6	11	3	13		**100**

Number of system requirements *given in IEC 62443-3-3:2019, per FR groups and SL values*

Phase 4 – Selection of countermeasures

A set of 100 cybersecurity requirements is given in IEC 62443-3-3. They are grouped by FR and classified with their SL value.

The SL vector is a key to enter the table and select a subset of these requirements.

FR>	IAC	UC	SI	DC	RDF	TRE	RA		tot
	{ 2,	2,	0,	1,	3,	1,	3 }		
SL 1	10	8	5	2	4	1	7		37
SL 2	6	4	5	2	2	1	3		23
SL 3	6	9	6	1	4	1	3		30
SL 4	2	3	3	1	1	0	0		10
tot	24	24	19	6	11	3	13		**100**

For instance:

SL-T (Zone$_j$) = { 2, 2, 0, 1, 3, 1, 3 }

selects the upper 54 requirements

Number of system requirements
given in IEC 62443-3-3:2019,
per FR groups and SL values

Phase 4 – Selection of countermeasures

FprTS 50701 - Table 5: System Security Requirements and Foundational Classes (derived from IEC 62443-3-3:2019)

Req	SL	Title
FR 1		
SR 1.1	1	Human user identification and authentication
SR 1.1 RE(1)	2	Unique identification and authentication
SR 1.1 RE(2)	3	Multifactor authentication for untrusted networks

FR = Foundational Requirement
SR = System Requirement
RE = Requirement Enhancement

Phase 4 – Selection of countermeasures

FprTS 50701 - Table 5: System Security Requirements and Foundational Classes (derived from IEC 62443-3-3:2019)

Req	SL	Title	Railway notes (informative)	Relevant design principles	Stake-holder	Type
FR 1	**Identification and authentication control (IAC)**					
SR 1.1	**1**	Human user identification and authentication	This includes application interfaces such as web server, file transfer protocol (FTP) server, OPC, and remote desktop interfaces that provide network access to human users and that do not securely convey the authenticated IACS user identity to the application during connection. It is acceptable to implement this requirement in combination with other external authentication solutions including physical security measures in railways.	4 - Grant least privilege 6 - Authenticate requests 7 - Control access	Op Sys Sup	Tech Proc
SR 1.1 RE(1)	**2**	Unique identification and authentication	-	6 - Authenticate requests 13 - Precautionary principle	Sys Sup	Tech
SR 1.1 RE(2)	**3**	Multifactor authentication for untrusted networks	The feasible multifactor authentication solutions outside the IT system in railways are generally external and could comprise a badge or a physical recognition of presence for the human user e.g. by a phone call. This could equally apply to regularly planned maintenance activities.	6 - Authenticate requests 12 - Proportionality principle	Sys Sup	Tech

FR = Foundational Requirement
SR = System Requirement
RE = Requirement Enhancement

RFI
RETE FERROVIARIA ITALIANA

Phase 4 – Selection of countermeasures

SL (IAC) = 3

	Requirements	SL
	SR 1.1	1
	SR 1.1 RE(1)	2
	SR 1.1 RE(2)	3
	SR 1.1 RE(3)	4

RFI
RETE FERROVIARIA ITALIANA

Phase 4 – Selection of countermeasures: an alternative approach

SL (IAC) = 3

	Requirements	SL
	SR 1.1	1
	SR 1.1 RE(1)	2
	SR 1.1 RE(2)	3
	SR 1.1 RE(3)	4

first approach

SL (IAC) = 3

	Requirements	SL
	SR 1.1	1
	SR 1.1 RE(1)	2
	SR 1.1 RE(2)	3
	SR 1.1 RE(3)	4

second approach

Conclusions

Objectives

The scope of the example was to test **how FprTS 50701 behaves in practice.**
FprTS 50701 provided a **qualitative process** to find the **minimum list** of cybersecurity requirements for a given new railway application. This qualitative process is compatible with the **standard railway application lifecycle (EN 50126).**

Results & future directions

So far, we've tested the TS for the first 5 phases, from Concept to Specification of Requirements, and we can say that FprTS 50701 can be a feasible and standard way to implement a **secure by design** system.
With the two tools of **Risk Assessment** and **Security Levels** and the guidance of the TS, a **standard list of cybersecurity requirements** for the Train Integrity Monitoring System has been derived.
The work is proceeding with the remaining phases; a final assessment by WG26 would be desirable.

Main remarks

- **Explicit risk evaluation** might be a long and time-consuming task.
- The correlation between derivation of **Security Levels** and selection of **requirements** could be questionable.
- The suite of **IEC 62443** is still in evolution, and this could undermine the basics of TS 50701.

Thank you for your attention

a.ciancabilla@rfi.it

g.magnanini@rfi.it

francesco.sperotto@haslerrail.com

davide.amato@sadel.it