INTERNATIONAL UNION
OF RAILWAYS

unity, solidarity, universality

ARGUS

"Security & safety analysis for electric and computerized signalling systems"

Dr.Marc ANTONI
UIC - CCS & Operations
Rail System Department

Summary

1. New challenge: security for electric signaling system
2. The ARGUS project
3. Security standards
4. A project to clarify the vision of new issues
5. Conclusion

New challenge in security of networked critical systems

Appearance of **new risks** related to (malware, attack on control systems and communication interfaces)

Which approach of **risk analysis for real-time system**?

How to consider the **human factors on the life cycle**?

Model of the "**security levels**" function of the strength of attacks?

Which **safety standards** for electric signaling systems for instance?

Specification of security requirements for electric signaling systems?

The ARGUS Project

ARGUS is a hundred-eyed guardian

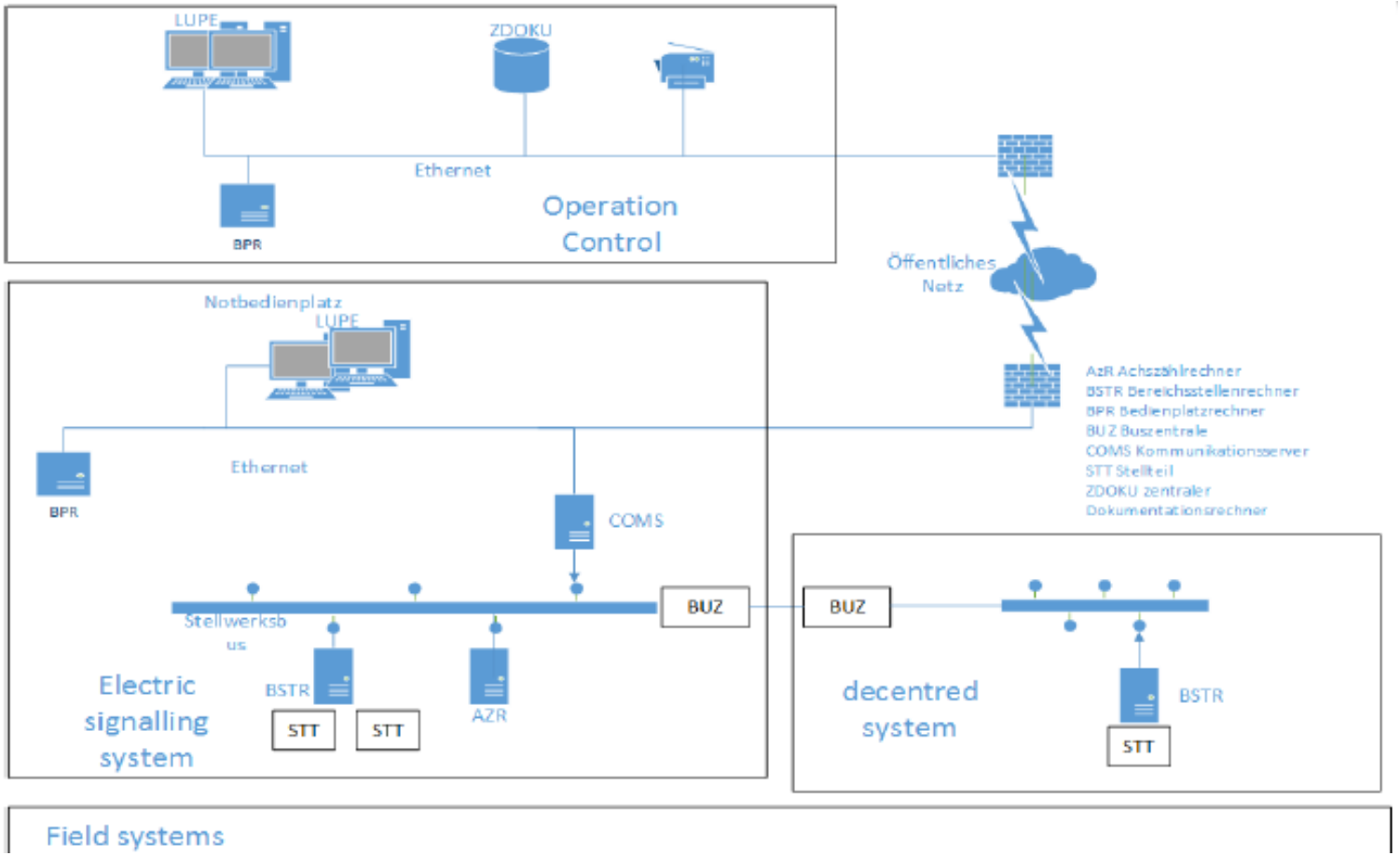
- Having “ARGUS EYES”
  - to be lucid and vigilant (miss nothing)
- The spirit to be shared with the members

ARGUS has been defeated by the magic flute of Mercury
→ he fall asleep

The project aims at designing a security analysis approach, based on risk analysis standard, for railways electric signaling systems, including human factors.

Challenge of safety and security of real-time systems

The current signaling systems



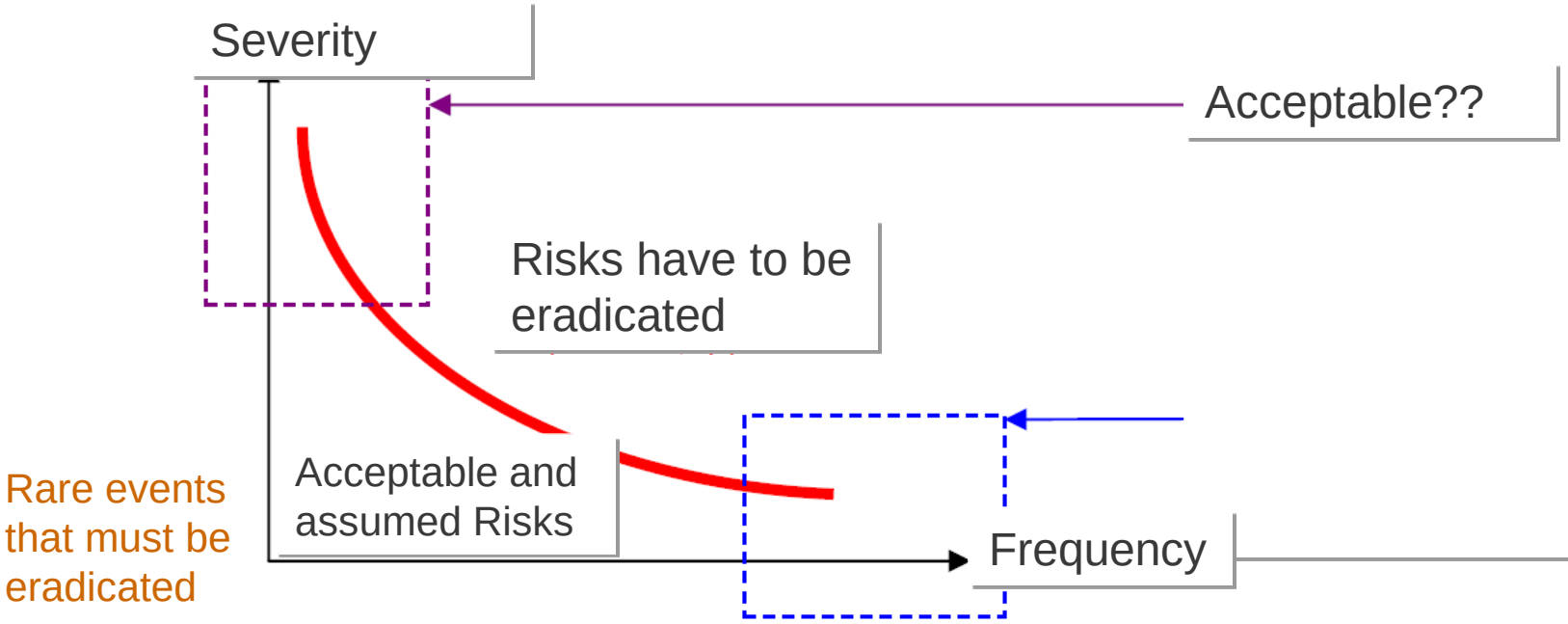
Challenge of safety and security of real-time systems

What is the «assumable» risk level regarding the consequences of the threats ?

→ Safety of the railway system presume the postulate of a closed world

→ Using IP Network leads to open system regarding external threats

→ Is « Risk = Frequency x Severity » acceptable ?



Challenge of safety and security of real-time systems

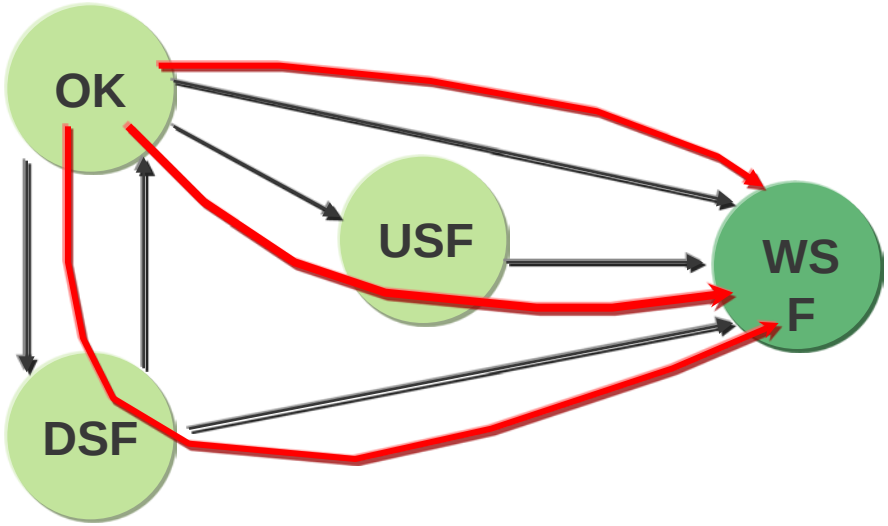
Dangerous situation leading from possible attacks

Three types of threat can lead to unacceptable situations:

1 - OK→WSF (event leading directly to a dangerous wrong side failure)

2 - OK→USF and USF→WSF (normal event following a unknown safe failure)

3 - OK→DSF and DSF→WSF (human error following a detected safe failure)



Occurrence probabilities of threaten attacks: 3 > 2 > 1

The challenge: security for electric signalling system

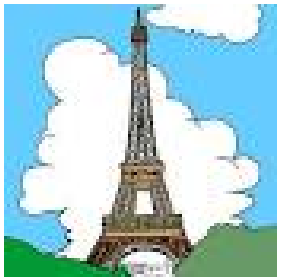
Dangerous situation leading from possible attacks

The railway system has priority for military target !

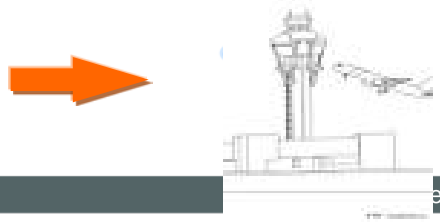
Many armies have now 4 “army”

→ Air force, Navy, Earth army and **Digital army**

Example 1 :



Attack initiated in system components



The challenge: security for electric signalling system

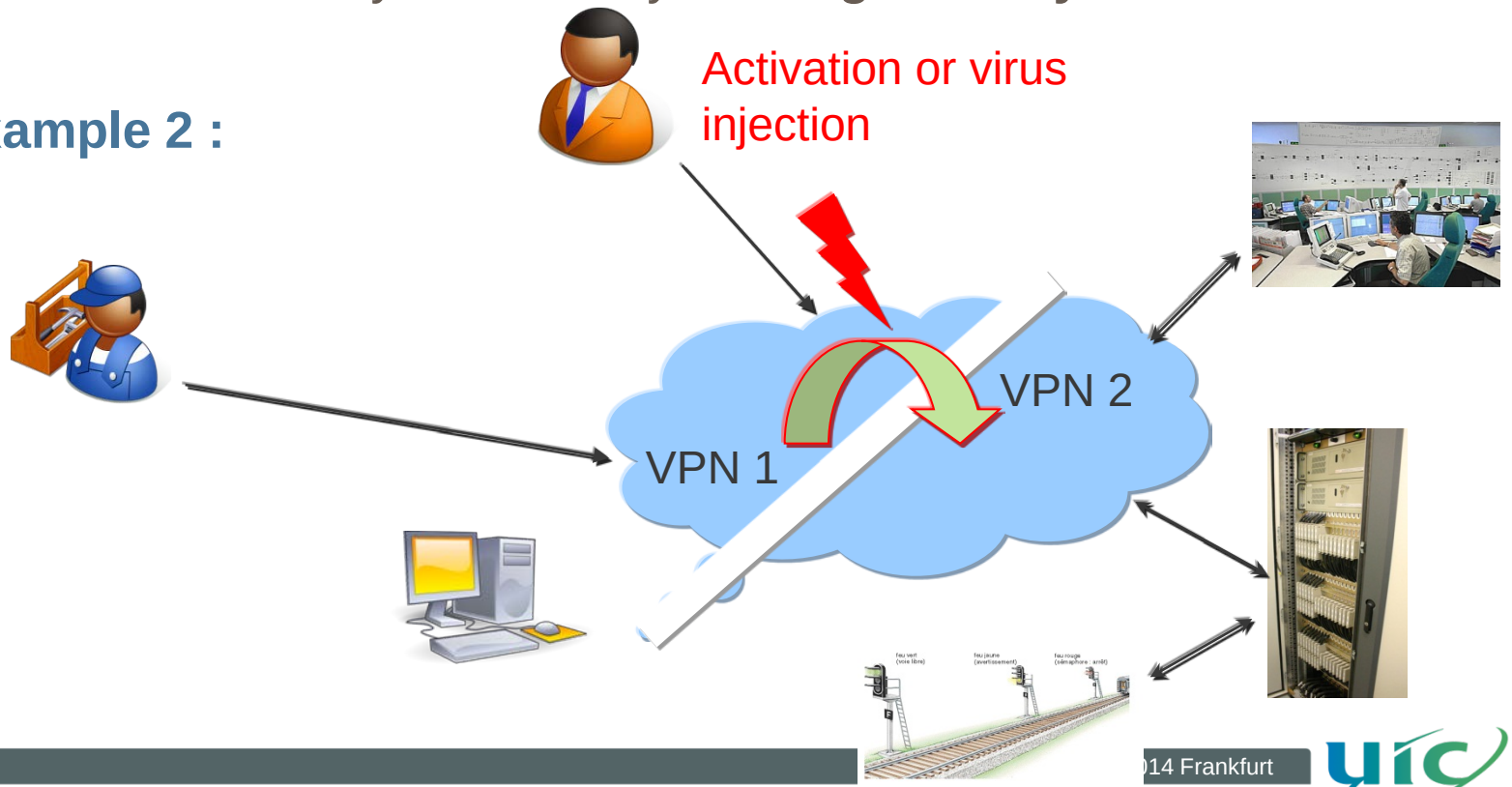
Dangerous situation leading from possible attacks

The railway system has priority for military target !

Many armies have now 4 “army”

→ Air force, Navy, Earth army and **Digital army**

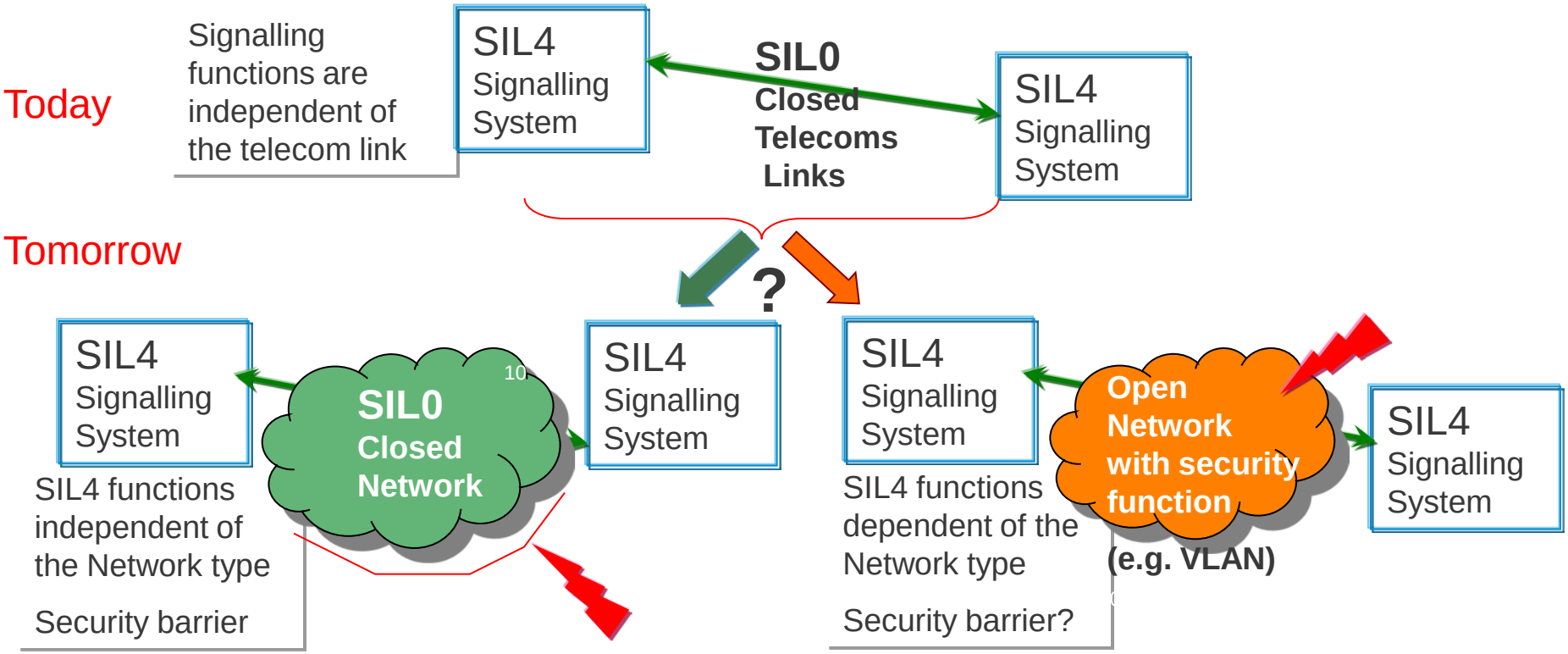
Example 2 :



The challenge: security for electric signalling system

Evolution of the situation → Which strategy in order to:

- save costs (renewal & maintenance)
- control the life span of the real time critical signalling systems, their availability (common mode especially), security and safety?



Component design issue

Architecture choice for a critical networked system

Classical architecture

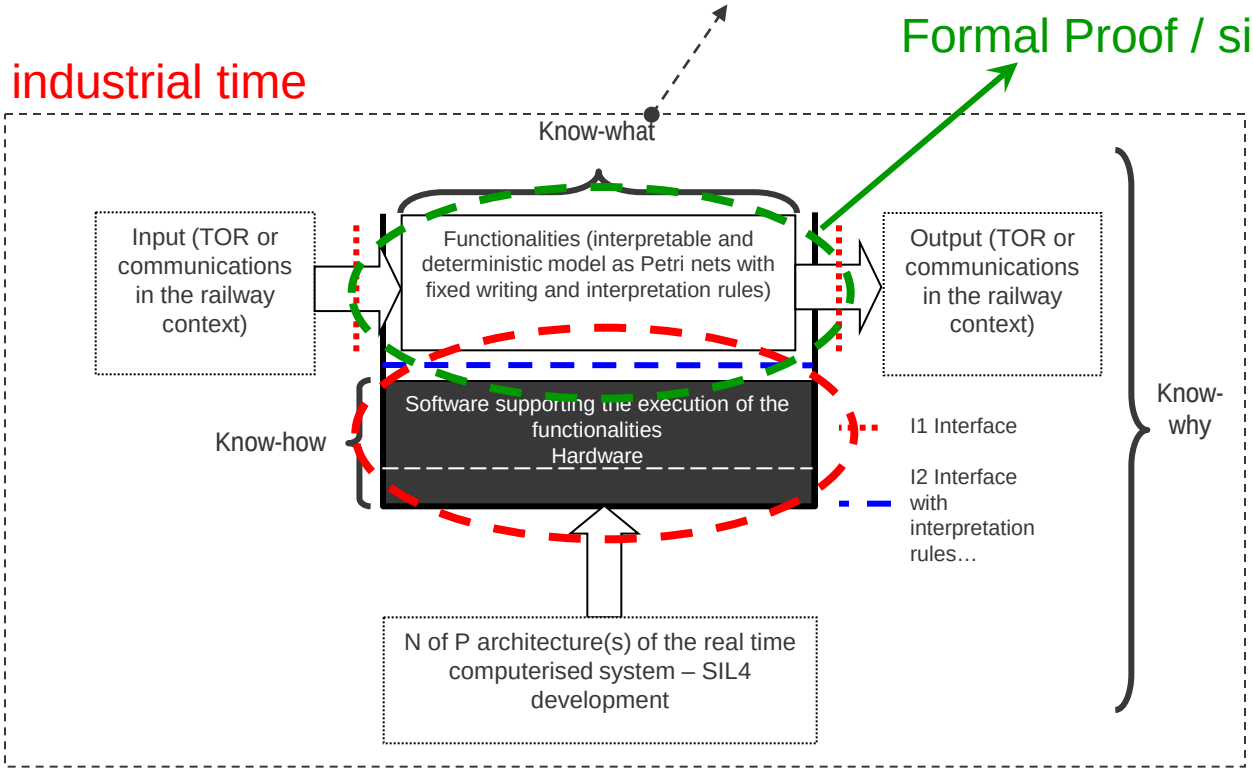
- Without independence between System and Functional SW

Proposed architecture

- With distinction between HW&System SW and the functional SW

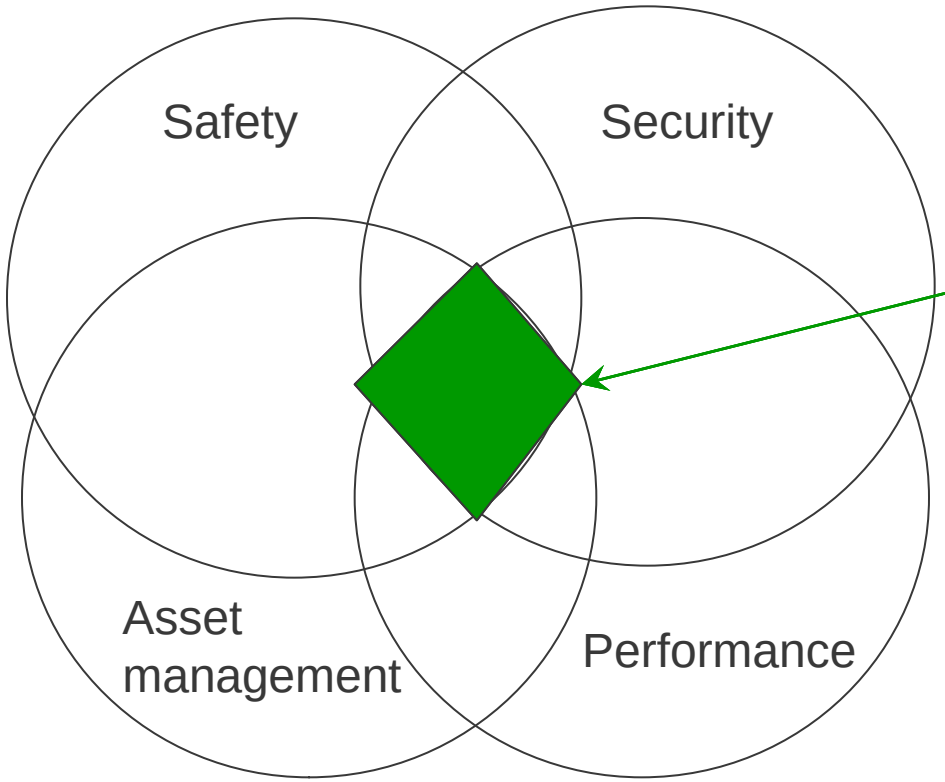
HW&SW / industrial time

Formal Proof / signalling time



System design issues

Formal methods for safety and security is a key for a high speed railway critical networked systems, and can help to improve the system durability and to reduce the maintenance Costs.



The battle of safety and costs is won or lost at the first stage of the system design !!

12

Security standards

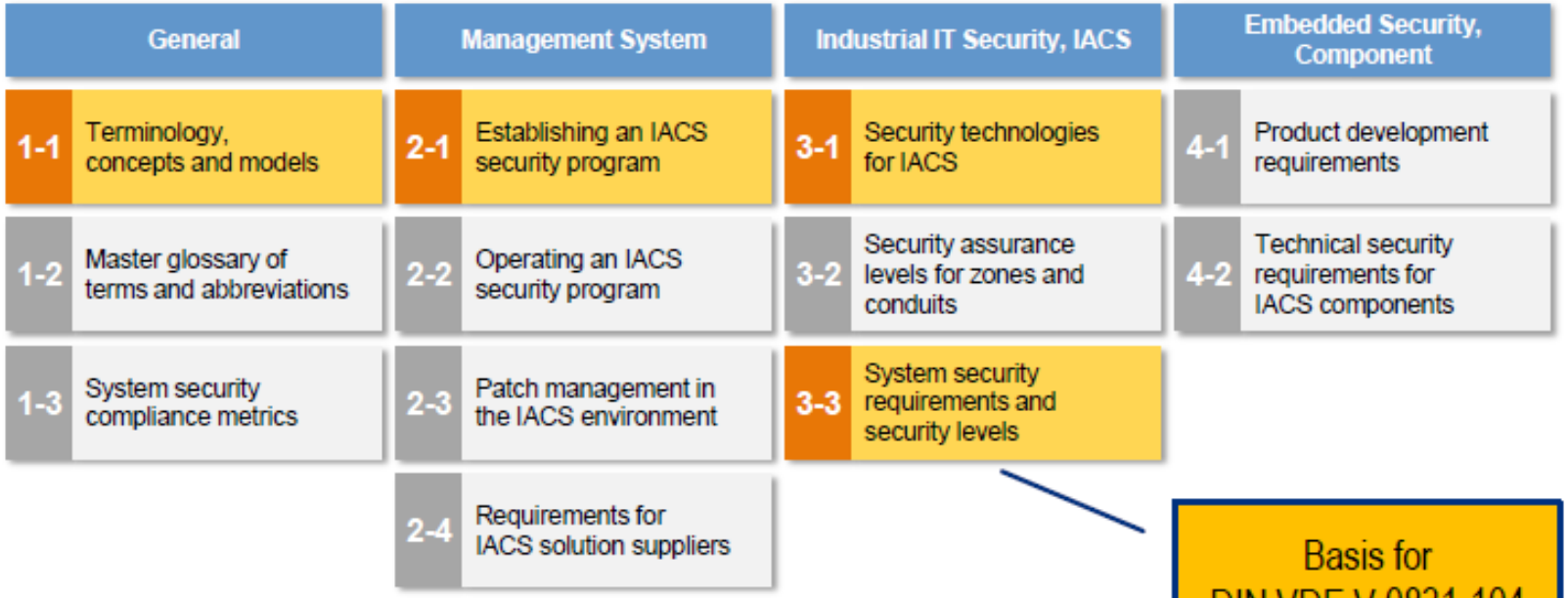
EN 50159, VDE V 0831-102, VDE V 0831-104, IEC 27000…:

- Safety-relevant threats only
- No internal attacker
- No consideration of real-time systems
- EN 50159, VDE V 0831-102 : protection of communication
- VDE V 0831-104 : description of an approach for security analysis, guide line
- IEC 27000…

➔ No consideration of the peculiarities of critical signalling systems!

Security standards

IEC 62443 series…



Risk model:

Risk = damage * probability (Unit: € / year)

➔ What about « non assumable » damage?

Security standards

IEC 62443 series… Classical risk analysis approach

Alternative Approach 1?

- Structure analysis of the target system
- Identification of the relevant threats
- Estimation of damage and probability
- Derivation of security measures to reduce unacceptable risks

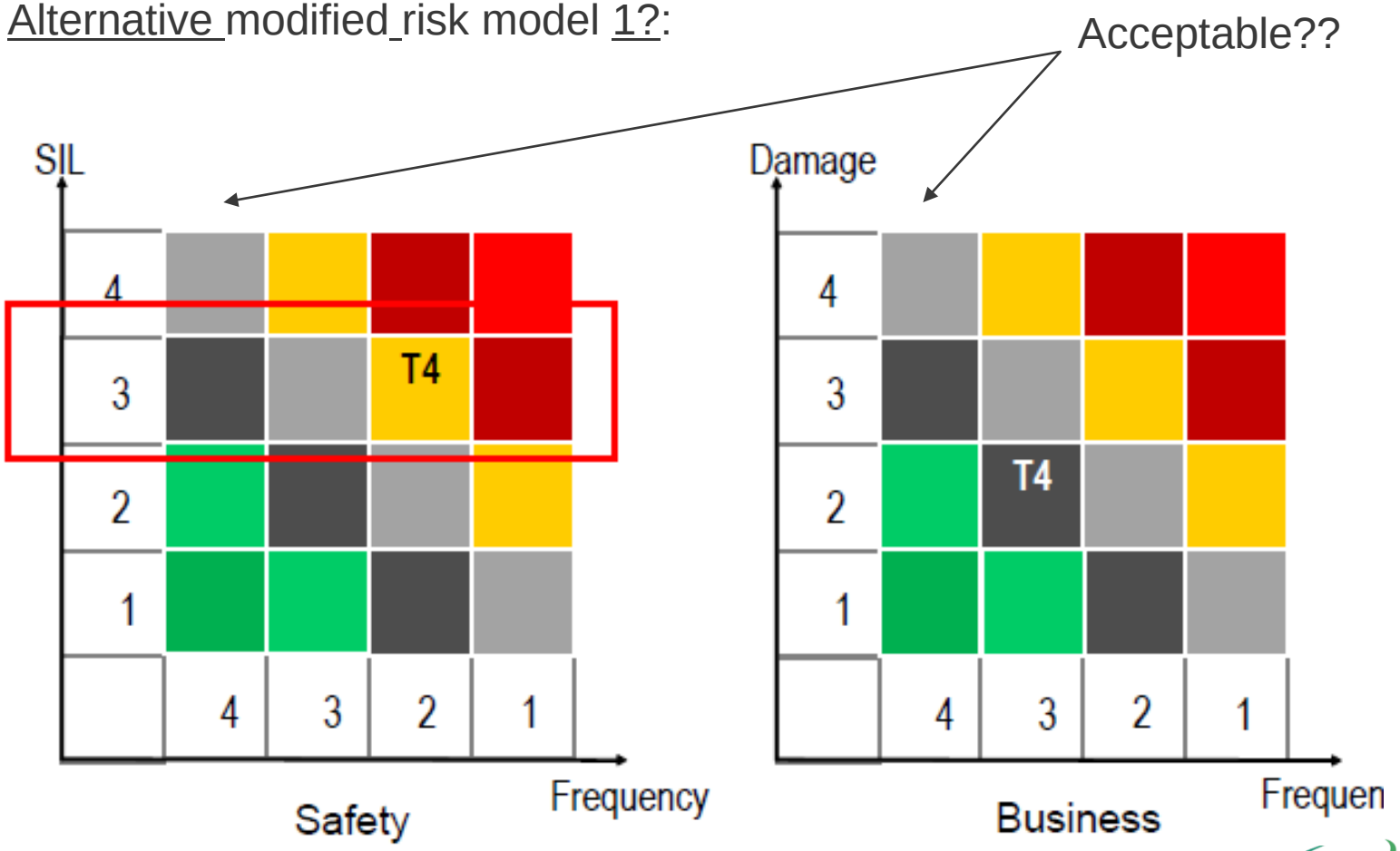
Prerequisites:

- Defined methodology for risk analysis
- Defined classes of damage and probabilities
- Defined threat catalogue

Security standards

IEC 62443 series… Classical risk analysis approach

Alternative modified risk model 1?:



Security standards

IEC 62443 series… Model for strength of attacker

Alternative 2: Strength of attacker defined through some parameters

➔ Security level “measure of confidence that the system is free from vulnerabilities and function in the intended manner”

➔Definition of risk-based security levels (SL)

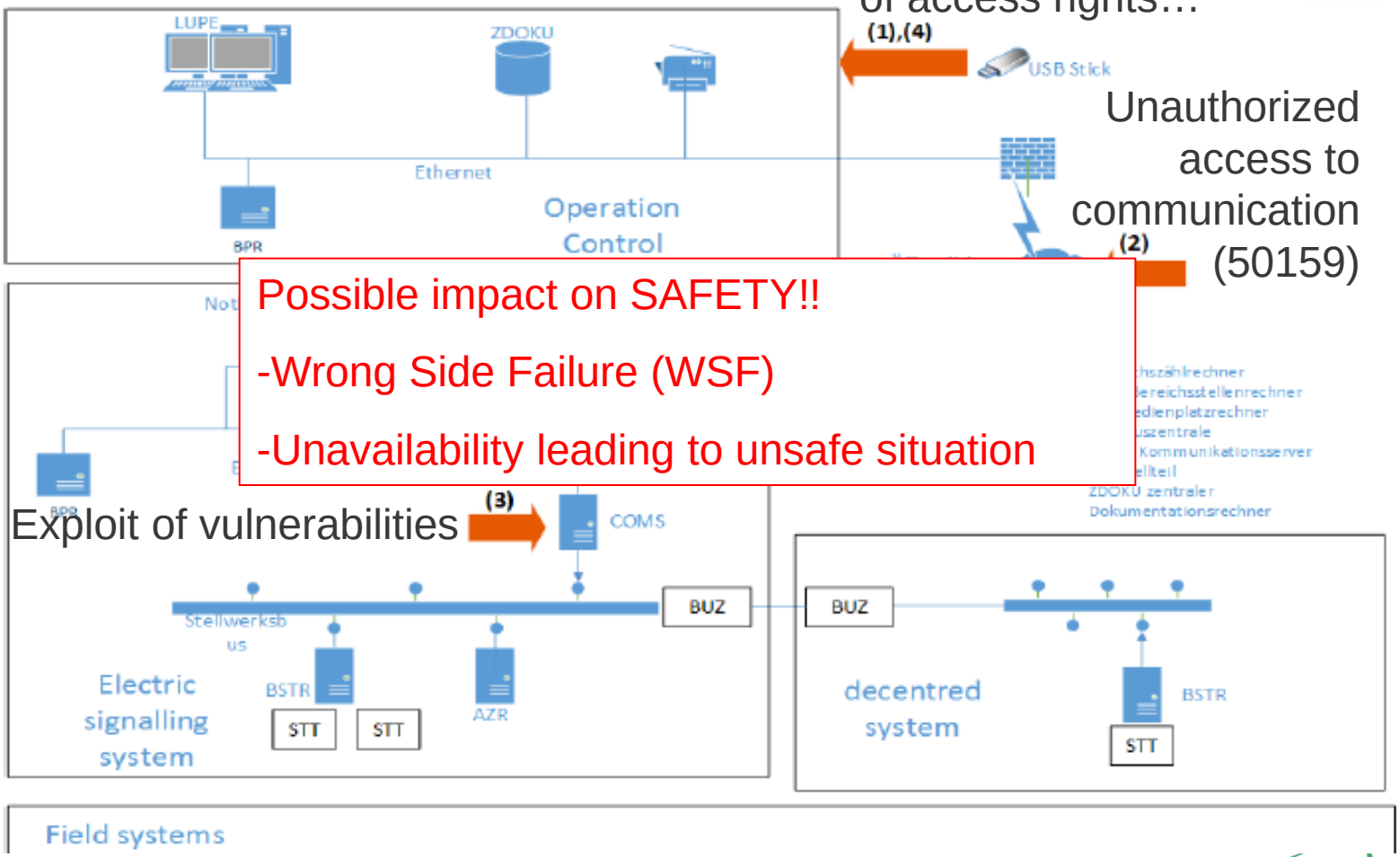
- **SL0**: no protection requirements
- **SL1**: protection against casual or coincidental violation
- **SL2**: protection against intentional violation using simple means with low resources, generic skill and motivation
- **SL3** protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation
- **SL4** protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation

SIL4 Signaling System

Security standards

Threats for signalling systems

Malicious software, Escalation of access rights…



Security standards

Steps for security inspection design ?

Steps for security inspection or certification ?

Are IEC 62443-xxx enougth for signalling systems?

Witch coherence with EN50126, 128, 129 standards?

How to manage the following issues ?

- all life cycle,
- the real-time aspects,
- the human factor,
- the evolution of the technology

A long work has to be done to reach a common approach for all UIC infrastructure signalling system

Conclusion

Strategic aim of ARGUS:

- How to avoid at “railway level” sad consequences coming from threats (cyber attacks, …) on operational signaling networks?
  - **Availability (fall down of the network)**
  - **Security (intrusion) and Safety (malware)**
  - **“Security” management during all the life of the network**
- How to provide alternative structures/architecture to operate until the main structures have been “cleaned”
- To converge as quick as possible, using the existing or in progress works for all domains or kind of systems

20

Thank you for your kind attention

Project leader in France Dr. Marc Antoni

antoni@uic.org
+33 6 29 91 77 43