INTERNATIONAL UNION
OF RAILWAYS

unity, solidarity, universality

Asset management of computerized signaling systems: how to keep the balance between safety, security and investments?

23th November 2016

Dr. Marc Antoni
FIRSE – AFFI – VDEI
Rail System Director
antoni@uic.org

Sommaire

Asset Management (1)

Reminders to clarify our ideas

What is Asset Management? Different definitions:

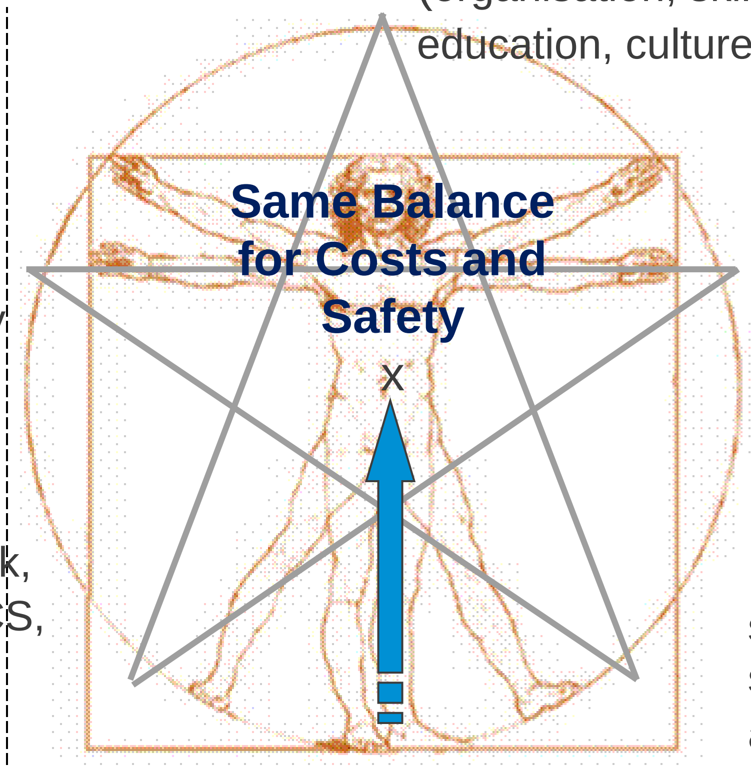
- PAS 55 (UK / for all industries),
- IAM (World / for all industries)
- ISO 55000 (World / for all industries)
  - UIC Guide line approved by IAM (World / Railway industry)

Asset Management (2)

The “railway is a system” an signalling is his heart

Human capital
(organisation, skills, education, culture…)

Environment by sub network
(economical and safety targets, traffic, track ownership policy…)



Operation principles - Rules (operation rules including ETCS, laws, technical directives, track ownership management…)

Infrastructure (track, signalling including ETCS, traffic management, overhead lines, monitoring…)

Rolling stock (signaling systems including ETCS, speed, load, aerodynamics, acceleration, monitoring…)

Asset Management (3)

Asset management in practice

Main goals:

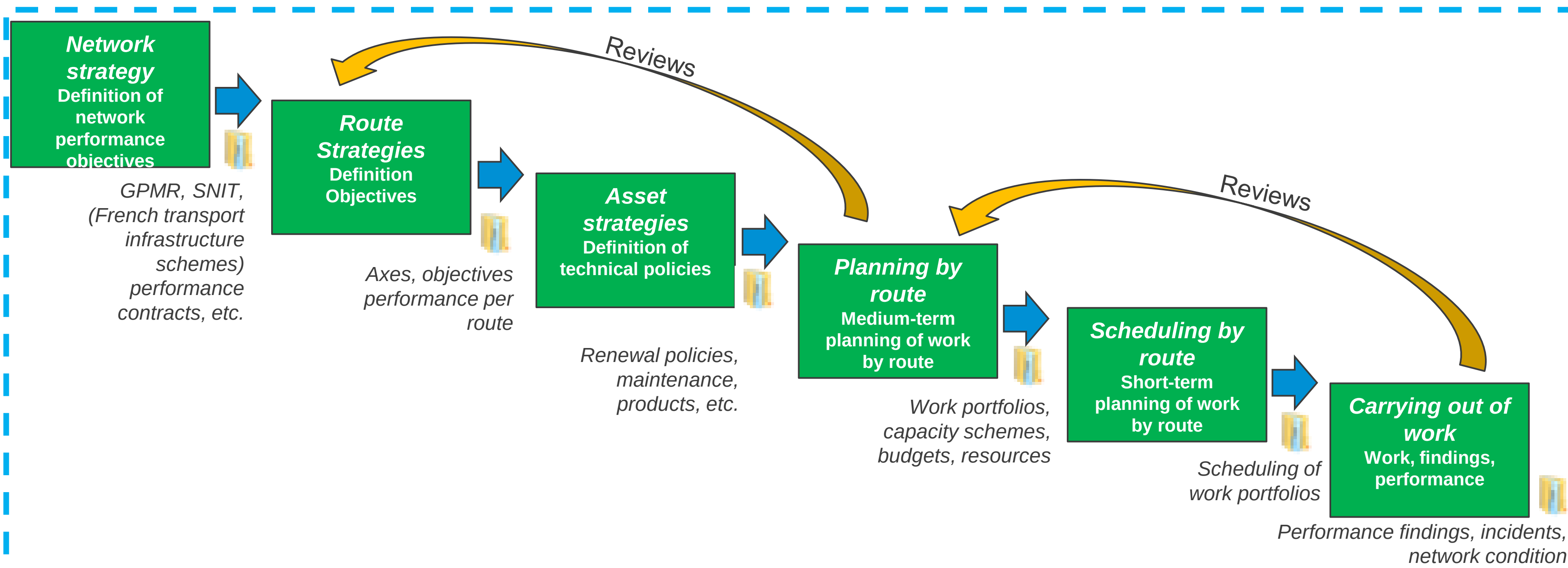
- Develop specific methods and tools for the lowest whole life, whole system cost.
- Develop specification and procurement methods to minimize the future for the lowest whole life, whole system cost
- Asset management is the art of striving for high performance in a context of “shortages” – individual resource managers are not aware of overall shortages

Asset Management (4)

Asset management in practice

TARGET INDUSTRIAL PROCESS => including Costs, Safety, Security

Network Strategy → Asset manager → Production



Asset Management System

Asset Management (5)

Asset management in practice

Governance - necessary conditions but not sufficient for asset managers to operate effectively:

- Establishing strategies ensuring long-term vision, in terms of network performance and renewal trajectories (> 5 years)
- Stabilizing the impact of maintenance and other work, route by route within a 5-year time frame
- Stabilizing production needs (>3 years)
- ... **especially difficult for computerized systems**

Asset Management (6)

Asset management in practice

- **It is a question of making these resources available within a "unique time and space"**
  ➔ to synchronise resources and planning and operation (with inevitable repercussions on capacity)
  ➔ **Miracles do not happen just like that, they need governance!**

- **Control over technical choices** make it possible to define the impact on capacity, life cycle costs and to integrate them in these processes
  ➔ **Technical choices must de directed towards bringing greater flexibility to future operations, safety and security demonstrations**

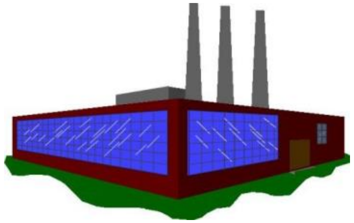
What about AM of signaling systems? (1)

<u>Railway is an “always living system”, signalling is the heart</u>

> We can only renew or maintain the “always living railway system” that we have given thought to in advance

> If we haven’t given it any thought in advance we would have to pay much more to do the same… if possible in a safe way

➔ Railway and signalling system in particular is not a factory

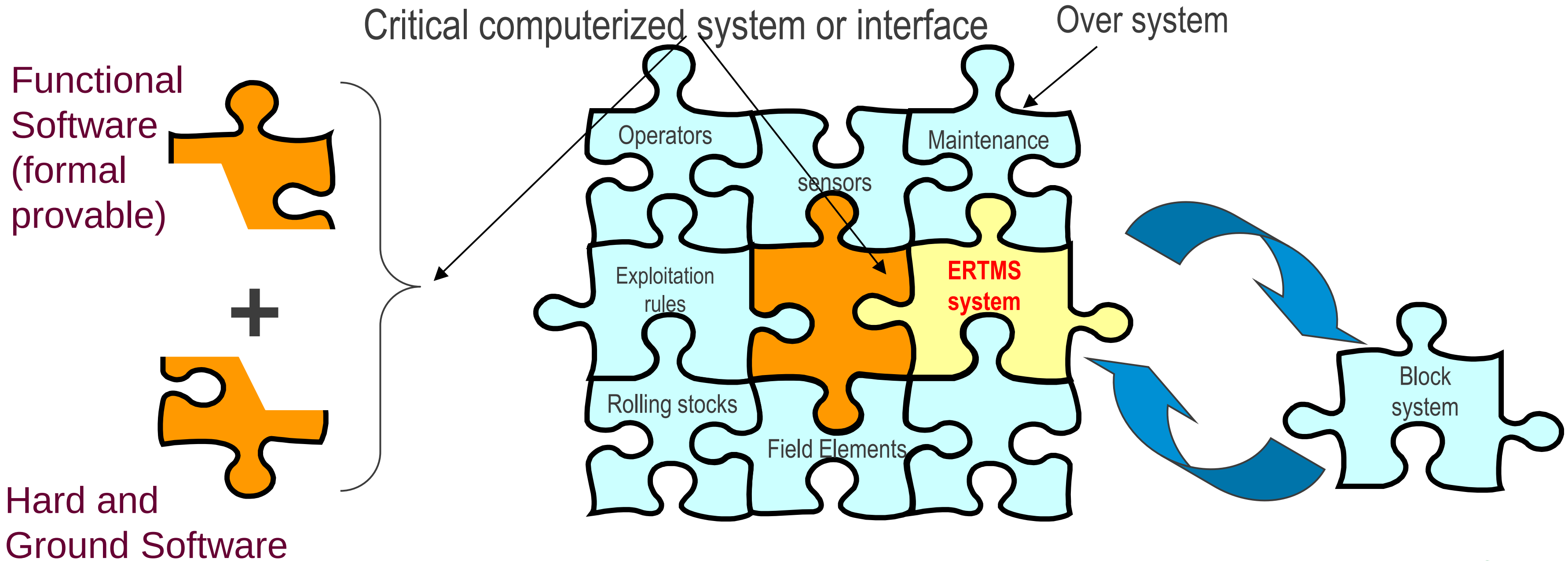


The battle of Asset Management is won in the design phase - The impact of new design and renewal is huge

What about AM of signaling systems? (2)

Railway is an "always living system", signalling is the heart

ATO, ETCS (or any other signalling module) has to be interfaced with the whole railway system, especially the legacy signalling system that must remain → **Design choices are key**



What about AM of signaling systems? (3)

Examples of design choices impacts

- Formal versus natural language for computerized signalling systems requirements?
  - what is the best for the life cycle cost of the computerized signalling systems? For their safety and security demonstration? For their future evolutions?...

Complex system → (never provable never for safety, never for security)

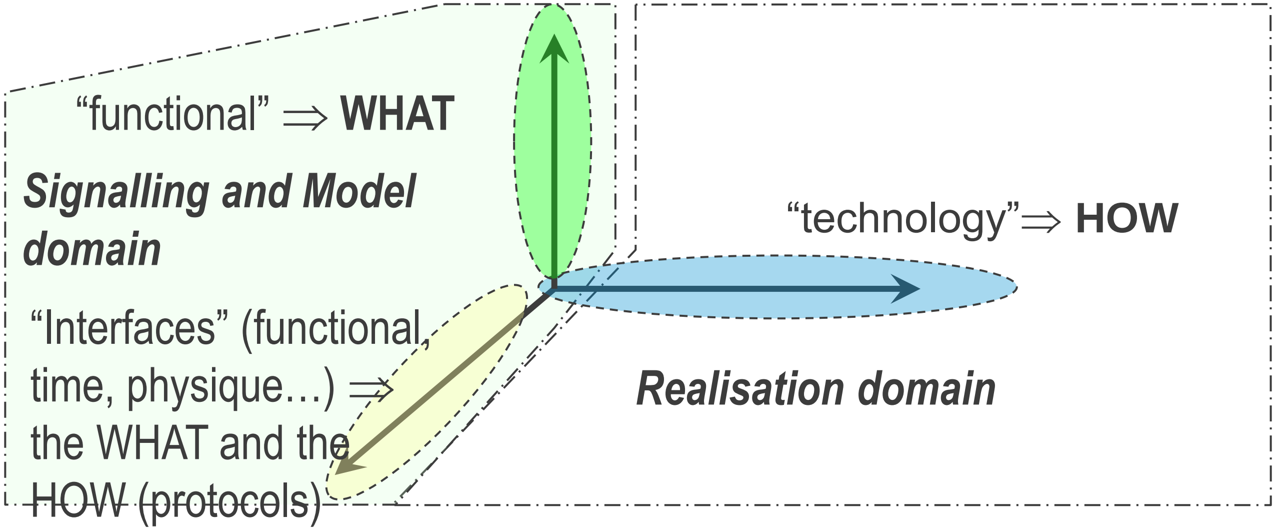
← Complicated system (can be proved for both)

Not asset manageable!

What about AM of signaling systems? (4)

Examples of design choices impacts

- Formal versus natural language for computerized signalling systems requirements?
  - how to master the complexity of the system, modularity...



What about Safety of signaling systems? (1)

Interconnected computerized systems ➔ a new paradigm regarding the safety assessment and the validation

The classical methods have notable disadvantages:

1. Classical m ses:

2. Criticality c could be not affordable e the boundaries of all system proof formally that the system aries)

➔ **"formal me ce of "black swans"** - impossible with "test cases" applied on the integrated system**.**

What about Safety of signaling systems? (2)

To separate hardware from functional software

Hardware of computerised systems

Software of computerised systems

Random HW failures

External stress Random aspects

Systematic failures of functional SW

Probability studies

N/P architecture

Quality assurance

Application of standards EN50128, DO178B, CEI61508

Formal Methods !

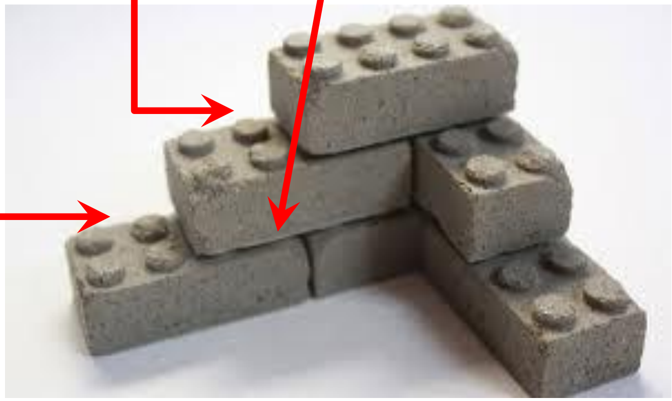
What about Safety of signaling systems? (3)

System integration in the railway system

The signalling system uses different levels. Each has its own life time et renewal criteria:

Formal functional Interfaces defined by the IM

- ✓ **Remote control centre**: without safety function, “sequential”, central
- ✓ **ETCS** : block and speed control system (European) → ATO
- ✓ **IXL** : Interlocking, national (operation and shunting rules, track layout…), “sequential”, nodal
- ✓ **Field resources**: national, “combinatorial”, punctual



What about Safety of signaling systems? (4)

System integration in the railway system

The specifications shall apply information (formal) at functional level

Beyond of technology detailed aspects

To enable the de-coupling of functional software from the implementable hardware

-**Benefit: Foster the migration, maintenance, avoidance of obsolescence (Avoidance of “vendor lock-in”)**

➔ **Formal functional specifications are necessary for safety**

What about Security of signaling systems? (1)

Cyber security in the railways

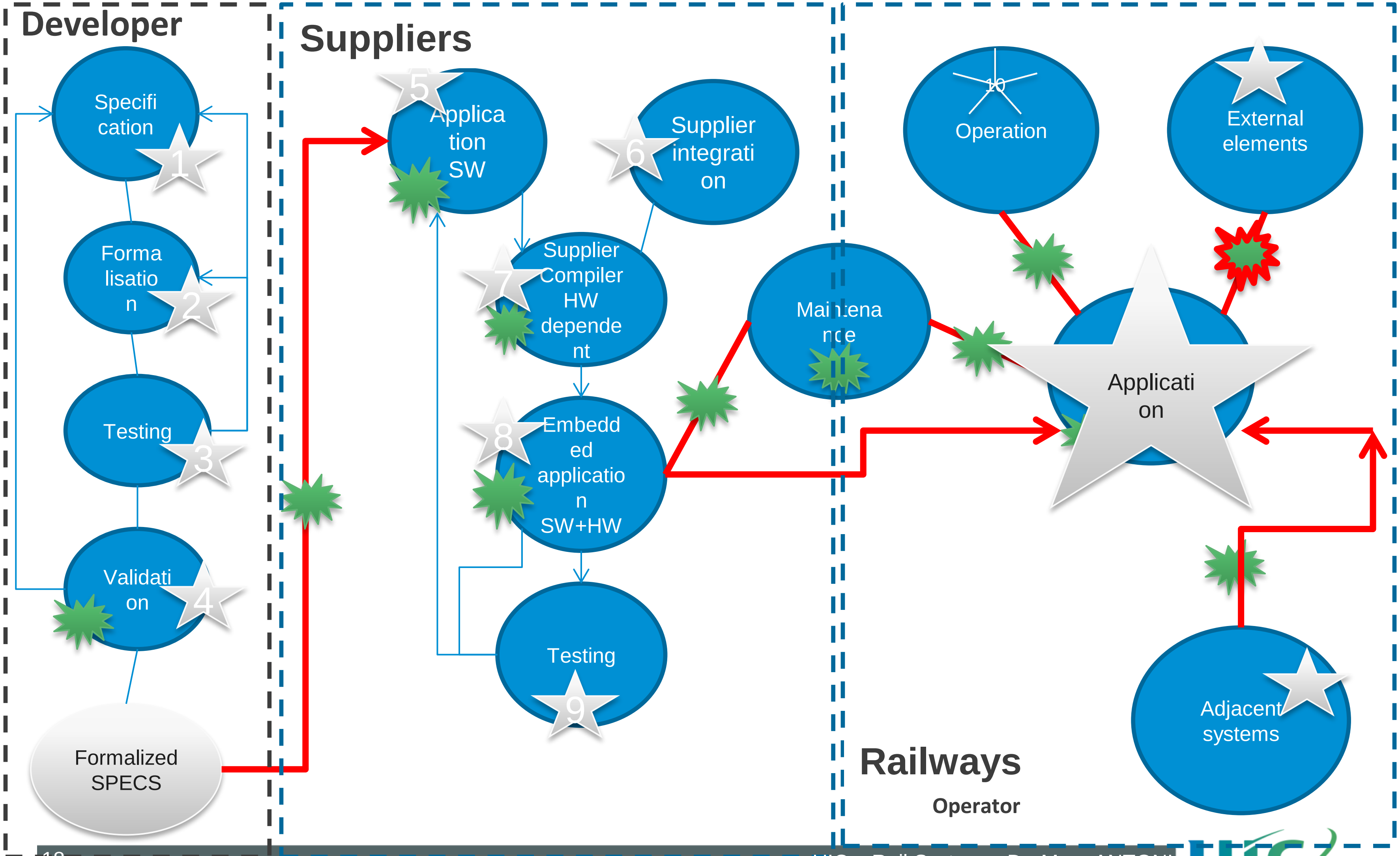
→ **System concerned**: Interlocking systems, speed control (ATP), traffic management (ATS), automatic driving (ATO), SCADA, ventilation, remote monitoring and supervision, management system of the railway, communication for infrastructure...
➔ **all the network have to be considered as "open network"**

→ Characteristic of the data's:

- Confidentiality ➔ **masquerade lead to un-safety**
- Integrity
- Availability ➔ **unavailability lead to un-safety**

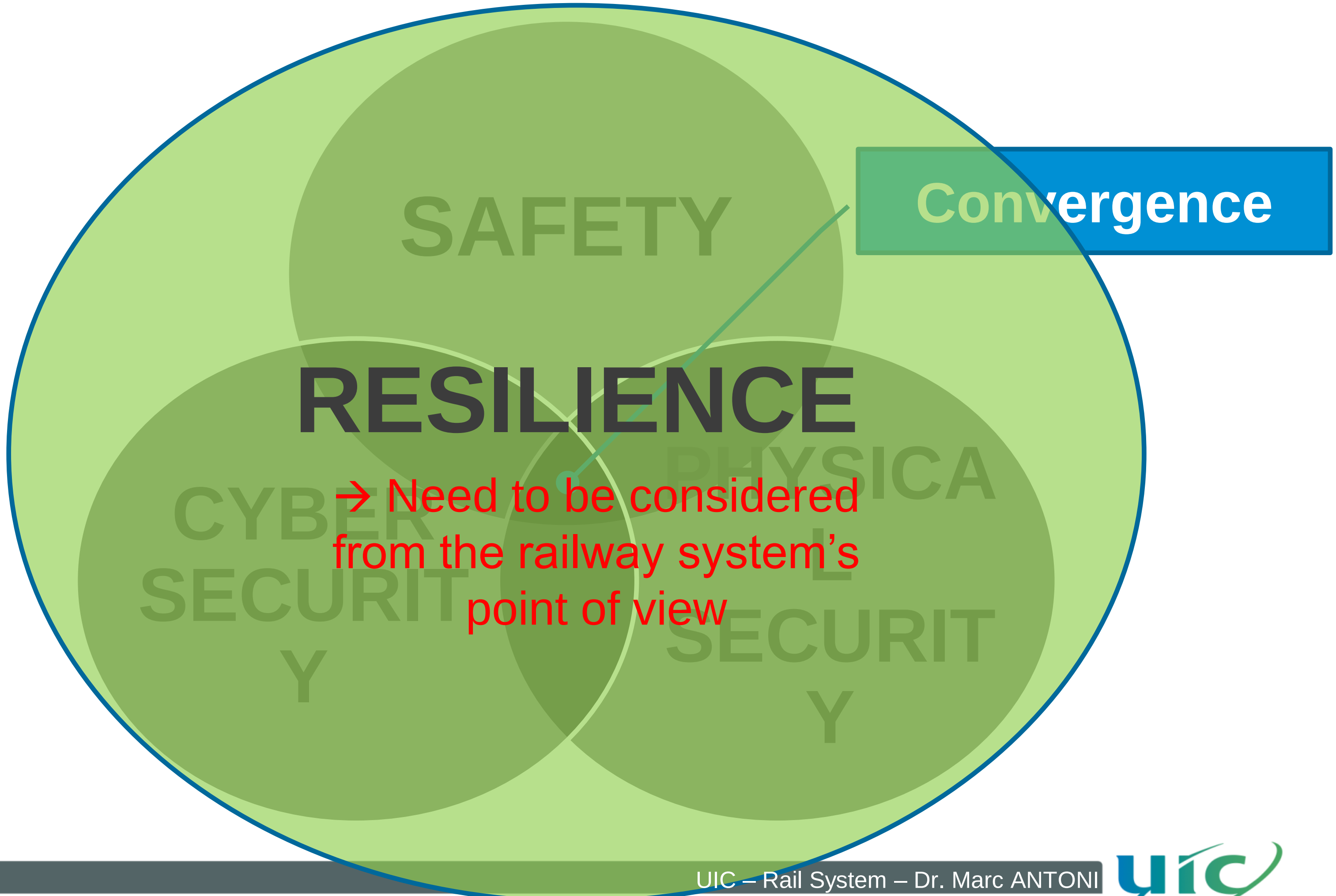
→ Where in the development process? From the birth to the end of the life cycle

What about Security of signaling systems? (2)



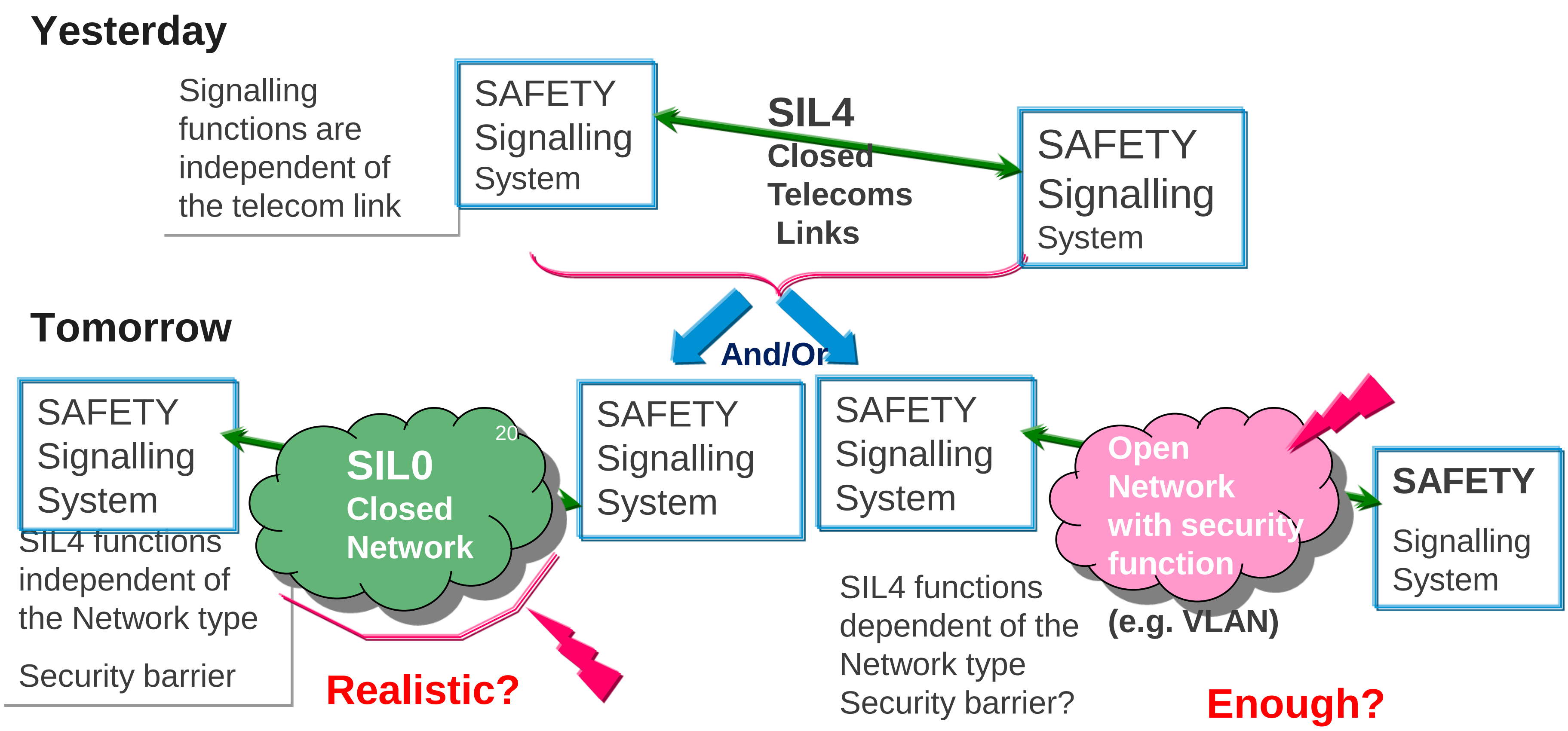
What about Security of signaling systems? (3)

“’Security-is-Safety & Safety-is-Security”



What about Security of signaling systems? (4)

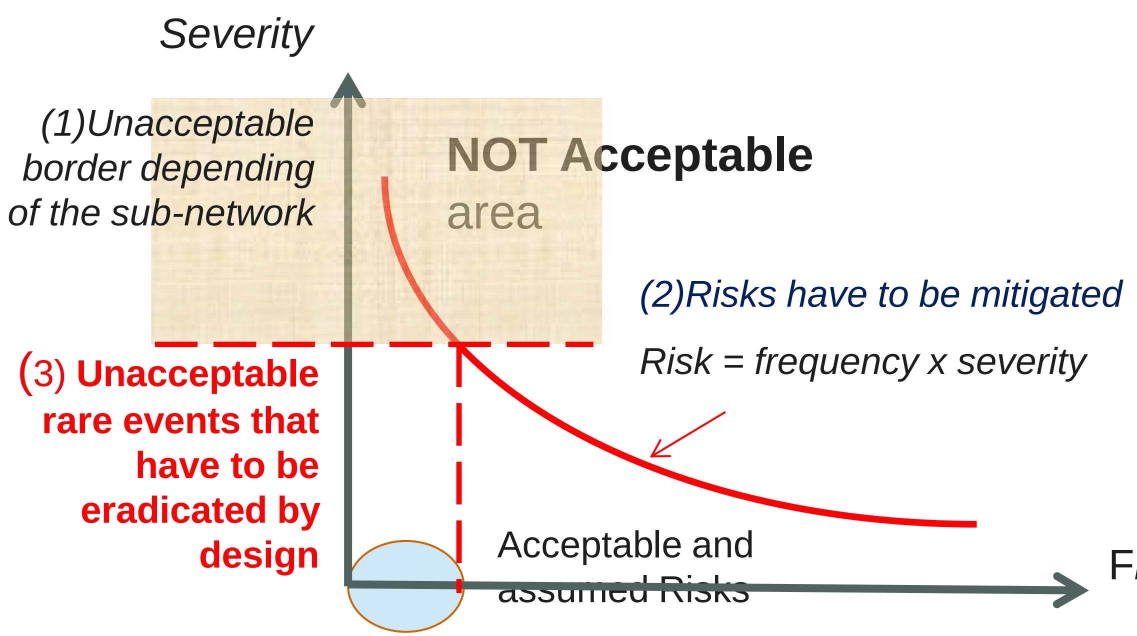
Identification of the threats



What about Security of signaling systems? (5)

Identification of the acceptable and not acceptable threats

The "**acceptable**" and "**unacceptable**" consequences have to be considered differently: **The unacceptable consequences have to be eradicated by design vs. the acceptable one can be mitigated**

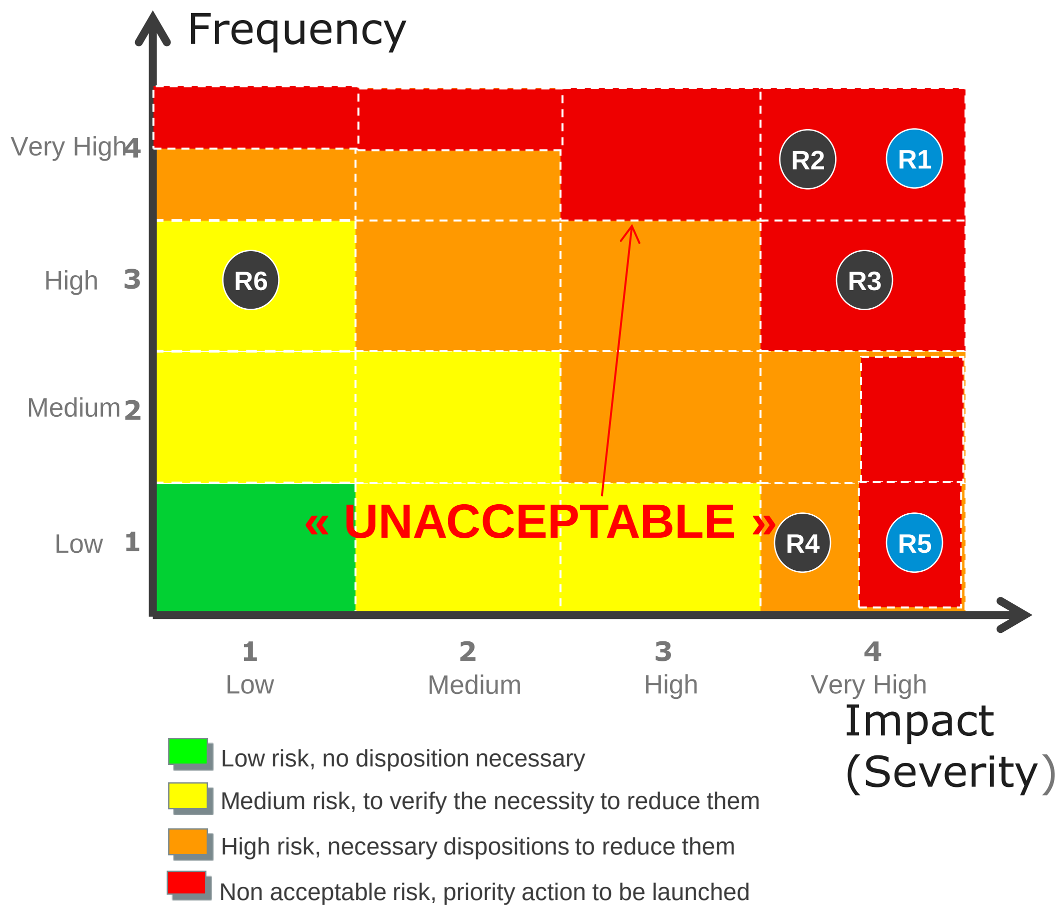


- → Where is the border ?
- → The "Risk = Frequency x Severity" approach is not always acceptable for railways
- → How to estimate the "Frequency" ? An attack can be too much!

Frequency (exposition to cyber attacks)

What about Security of signaling systems? (6)

Risks cartography (Ex of a IP signalling network)



For each identified category of systems, networks, sub-networks, functions (security level 1 to 4)

→ Leads to different packages of coherent solutions on different axles on the Supplier and railway sides

→ The battle of the safety is won or lost in the first stage of design

What about Security of signaling systems? (7)

Security & Safety have to be considered together

→ **The design of a critical signalling system has to consider from the first design stage the security challenges:**
- to include the right “axioms” to be able to prove the security
- to consider the operations rules and the management of the degraded mode...

→ **Railway safety and security are dependant**: one can only be demonstrated considering the other. Security has to be considered as one of the key elements needed to deliver the railway Digitalisation programs

→ **Railway safety and security have to be considered at the “system level”** with the “operation and asset management” choices

What about Security of signaling systems? (8)

Four pillars for a coherent security system vision

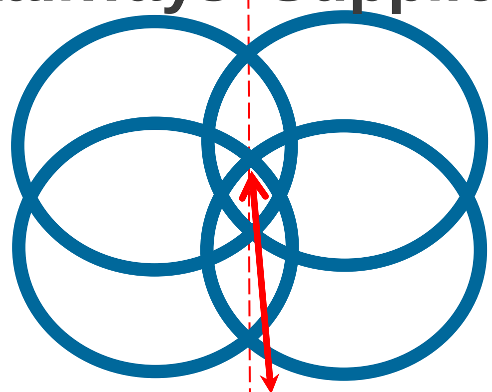
Functional level

(coherence between the context and the input data… formal proof, detection system (IDS), functional automatic detection and commutation…)

IP level Mitigation measures

(firewall; Privacy of data collected; Integrity of data collected; VPN; Events monitoring; Intrusion detection system (IDS); DMZ, network segmentation)

Railways **Suppliers**



Organisation and architecture system

(Security and safety management system, skill, education, confinement of the accesses, authorizations…)

IT level

(Safe operating system vs. specific real time operating system not known, distinction between HW + basic SW and Functional SW...)

CONVERGENCE: Reduce the possibility to go through

What about Security of signaling systems? (9)

Example of Generic design choices or mitigation measures

→ Independent layers requiring different types of competence: telecoms + real time signalling modules + real-time signalling functional white boxes + human organisational

→ Generic design and build of signalling and networks in a common multi-technical team: Operation, Telecom, Signalling, Safety...

→ Implementing measures & solutions for "business continuity“: to ensure resilience

→ Preserving or renewing Class1 relay interlocking as much as possible: link to RBC or other TCC with a formal proven ILU

What about Security of signaling systems? (10)

Example of Generic design choices or mitigation measures

→ “Functional monitoring and control activities on the networks" beyond operational control

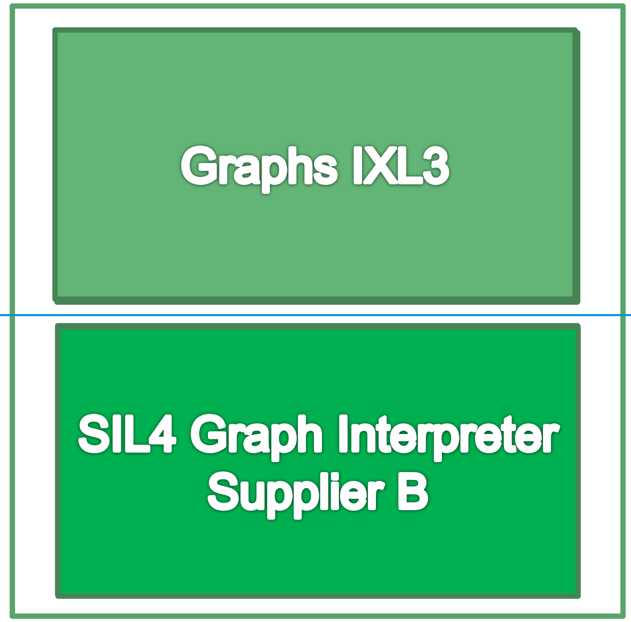
→ Physical independence between signalling close network and other intranet or internet operation & services networks

→ Distinction between “signalling sub-network level” and “real signalling local level” networks: interlocking unit realize a barrier between the two levels of networks = confinement: Distinction (independence) between Telecom and Signalling links – Automatic intrusion detection of the sub-network networks

→ Etc.

What about Security of signaling systems? (11)

Example of Generic mitigation measures for critical module



Signalling interpretable functional requirements - "formal proven"

How to write?

How to interpret?

UIC "tools" and IRS

Hardware and basis Software - SIL4

Computerized signalling unit (UIC open HW and SW)

What about Security of signaling systems? (12)

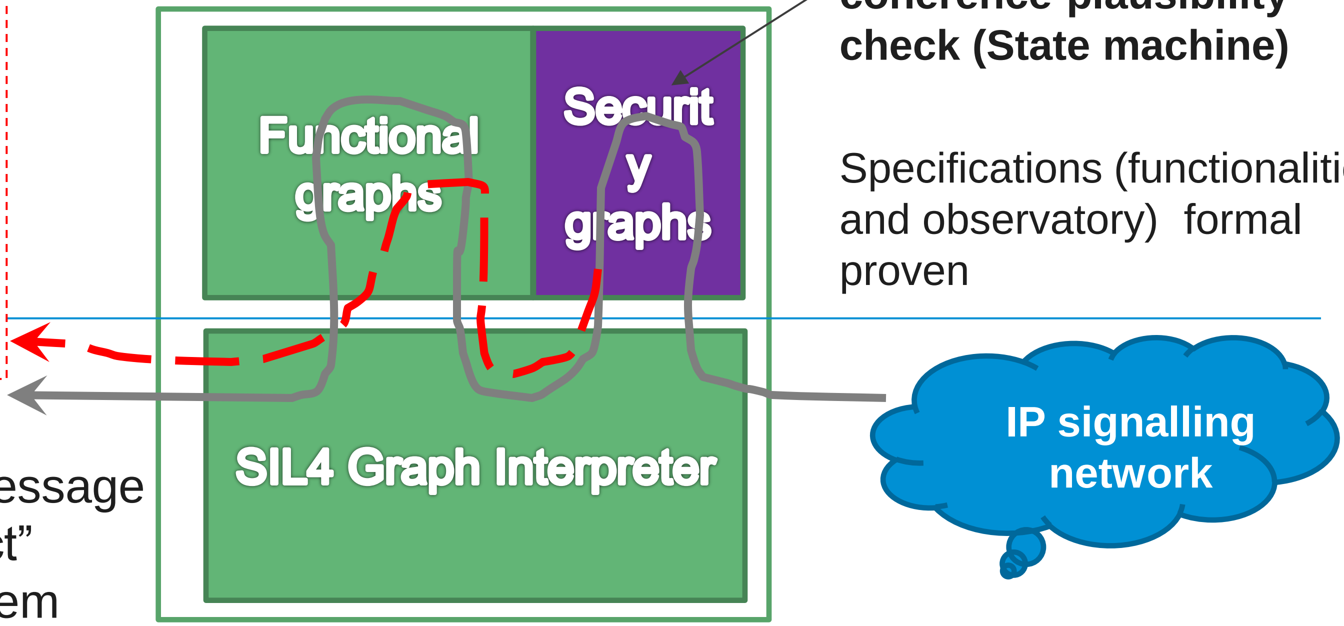
Example of Generic mitigation measures for critical module

If not :

Adapted reaction is the module is attacked
→ safe reaction regarding the system

Railway specific functional coherence-plausibility check (State machine)

Specifications (functionalities and observatory) formal proven

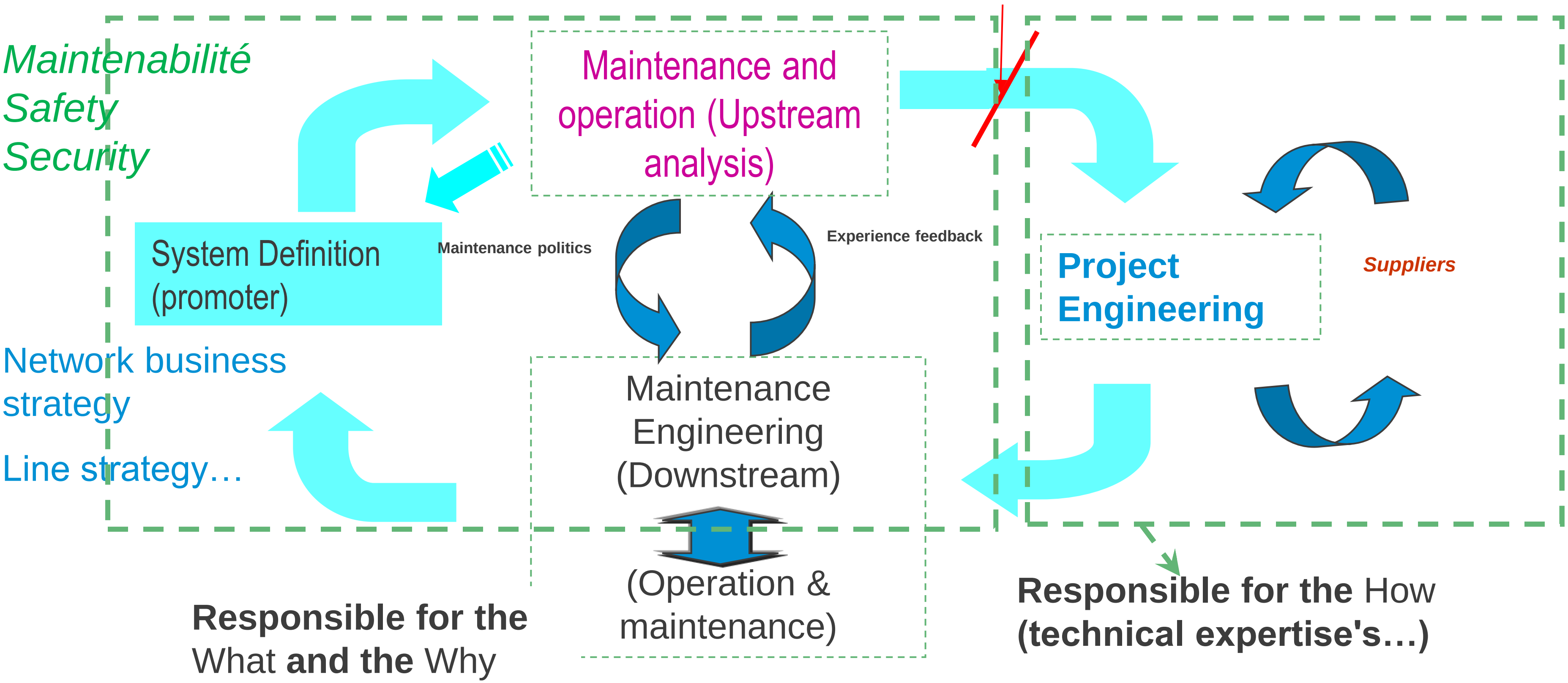


If the functional message received is “correct” regarding the system state of the IXL, its topology...

Computerized signalling unit

Key principles for a better future (1)

In a general governace and system point of view



Key principles for a better future (2)

Modularity and interfaces challenges:

- The asset manager has to control the modularity of the railway system. It’s the only way to be responsible for performance, safety-security, maintenance...
- This gives the possibility to estimate the right failure-degradation laws, to identify the wearing of pieces and facilitate their replacement, the integration of the whole railway system on long term

➔ *Power is the control of the incertitude's of the other...*

Key principles for a better future (3)

<u>Formalisation of the sub-system requirements:</u>

- To become "simulable" and/or "formally provable" before the launch of new sub-systems, to facilitate their integration and safety-security demonstration... Regarding the real condition of use

➔ *A miracle is never coming alone, its needs to be facilitated*

➔ *If we don't think of the future, we will pay for it!*

Key principles for a better future (4)

<u>**Formal specification language**</u>

→ **Define a railway formal specification language**
- to be able to formalize the functional requirements of new assets connected to existing signalling systems
- to be able to prove formally the safety & security properties and the signalling functional properties

→ **Define a real-time interpretable functional formal language** (by SIL4 target machines)
- must be useable without transposing the signalling functionalities defined by the railways' "white box units"
- to facilitate future asset management (inc. developments)

→ **A generic computerized module architecture familiar to the IM's** → functional white box vs. suppliers' black boxes

Key principles for a better future (5/N)

The Asset manager needs simulations to:

> Describe and justify each possible scenario regarding the different packages of constraints

> Project itself in the different possible future scenarios

> Prioritize the possible actions to be launched... regarding the possible impacts of different technical strategies

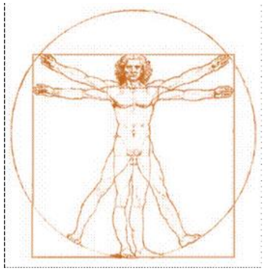
→ *enlighten the strategist of the middle and long term consequences of his choices – especially in signalling systems with shorter and shorter life times, more and more risks regarding safety and security*

Conclusion

- The asset manager needs a clear asset strategy support because the battle for asset management is won or lost at the system definition & design stage
- It is essential to consider the industrial balance of the trio made up of “Maintenance costs – Network Performances – Quality-Security-Safety”
- The asset manager needs a clear asset strategy support by a complete reflexion of all the points seen before: ability to integrate the new components, maintain and operate the system, in safety and security and efficiency

→ UIC is working to define a « guide line » for railways: asking itself the right questions, in the right order, regarding each specific context...

Thanks for your kind attention



Dr. Marc Antoni

FIRSE – AFFI – VDEI
Rail System Director
antoni@uic.org