SafeRiver
SAFETY & SECURITY FORGE

HOW TO COPE WITH INTERFACES BETWEEN SAFETY AND SECURITY FOR RAILWAY APPLICATIONS ?

Recent evolution of french regulation applicable to Urban Guided Transportation Systems requires to manage interfaces between Cyber analysis and Safety Cases.
Our approach is based on our return of experience, and state of the art as identified by standards. In particular we examine proposal of IEC 63452 which has listed 7 coordination principles in annex D (informative).

PRINCIPLE 1 | SAFETY AND SECURITY ARE DIFFERENT AND SHOULD BE TREATED AS SUCH

Safety Critical systems are challenged by Cyber Security Considerations. Safety implementations have been developed outside cyber security concerns and can introduce weaknesses or expose vulnerabilities to cyber attacks.
Principle 1 shall be understood as need for coordination between both processes thanks to interfaces and complementary workproducts.

PRINCIPLE 2 | THE SECURITY ENVIRONMENT SHOULD PROTECT ESSENTIAL FUNCTIONS, INCLUDING SAFETY.

Indeed some key assumptions for Safety Analysis and Safety Risk Reduction are questioned or even invalidated considering cyber attacks. In particular safety principles and architectural principles rely on the fact that failures are random events. If attacks are able to create hazards, due to creation of deceptive situations in environment or malevolent manipulations of safety mechanisms, it is clear that safety cannot be guaranteed. Probabilistic assumptions that are sublying to Risk reduction for Safety do not hold when malevolent actions are considered.
Therefore, Security Controls are needed to protect Safety Target against attacks considered as relevant in terms of attackers motivations, attack modes and attractivity of the target system.

PRINCIPLE 3 | CYBERSECURITY THREAT AND RISK ANALYSIS IS THE MAIN INTERFACE WITH SAFETY ANALYSIS.

Threat sources identification, Risk Assessment shall be performed so that Cyber Goals are identified and Target Security Level is allocated to each Cyber Goal. Target Security Level shall take into account Safety Integrity level of Feature that must be protected and attack potential metric.

- Analyze and Identify Security needs with respect to Safety Functions integrity and effectiveness requirements;
- EnsureProtection of Safety Functions thanks to Cyber Security Measures so that attack paths complexity can be continuously monitored depending on state of the art, attack potential and vulnerabilities discovery. The idea is to keep Safety Kernel properties thanks to its internal robustness and perimetric measures so that Safety Kernel cannot be tampered.
- Specify Security Assurance Requirements applicable to Cyber Security architecture and mechanisms.

PRINCIPLE 4 | SEPARATE SECURITY AND SAFETY AS FAR AS POSSIBLE BUT COORDINATE THEM EFFECTIVELY.

Our proposal is to identify a second interface between the processes in order to make sure of the twofold :

- Safety Measures are kept independent of Cyber Security Controls in terms of Safety Concept (architecture and mechanisms).
- Safety Kernel weaknesses do not invalidate the Cyber Protection.

Cross-assumptions formalize conditions that are necessary to ensure mutual coherency and cohesion of Cyber Goals and Safety Goals. The mutual contract obligations may be stated as follows:

- Cyber Goals are covered by Cyber Objectives and Assumptions applicable to Safety Kernel
  - O.Security : Keep Safety Functions free from malevolent interactions caused by attacks with appropriate strength and non bypassability
  - A. Security : Safety Functions are assumed to be coded according to secure coding rules.
- Safety Goals are covered by Safety Objectives and Assumptions applicable to Security Controls
  - O.Safety : Ensure Safety Functions effectiveness with respect to failures and errors
  - A. Safety : Security controls are assumed to be adequate and sufficient to ensure integrity and unbypassibility of safety functions execution with respect to potential attacks.

PRINCIPLE 5 | SECURITY SHOULD BE EVALUATED ON THE BASIS OF INTERNATIONAL STANDARDS E.G. 62443

Safety Case shall identify Assumptions to be verified in Cyber case, to make sure Safety functions do execute in expected conditions. Symmetric assumptions in Cyber case is that some Secure Design Patterns and Security Coding Rules are actually implemented by the Safety kernel and are part of Safety Case evidencies.

In order to coordinate Security and Safety Processes with respect to applicable standards for each domain, the strategy combines

- Threat Analysis and Risk Assessment methodologies recommended in Security standard (HLRA, DRA in 62443-3-2).
- Cyber Concept identifies Partitioning and Security Controls that protect and ensure Safety Kernel is actually executing in appropriate operating environment and is always able to perform safety controls (Foundational Requirements and System Requirements framework in 62443-3-3).
- Secure Design and Coding Rules apply to both Security mechanisms and Safety related Functions. (62443-4-1, EN50716).
- Vulnerability Analysis and Risk Assessment shall be performed to confirm that residual risk is acceptable (62443-3-2).
- Freedom From interference analysis shall be performed in order to make sure Safety Kernel remains independent (EN 50716).

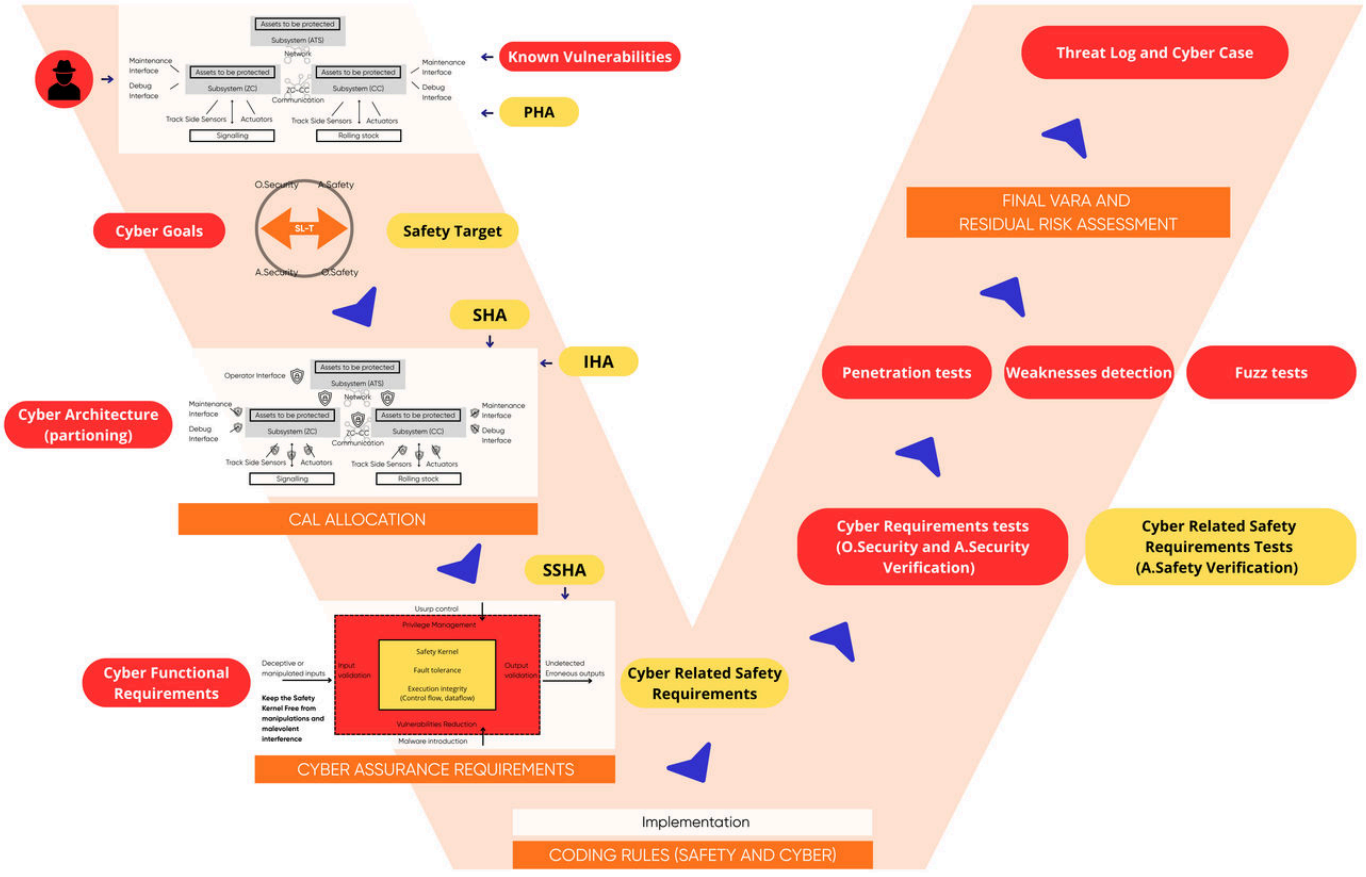
PRINCIPLE 6 | IT IS INFEASIBLE TO EVALUATE THE SECURITY RISK PROBABILISTICALLY

An attack process is not stochastic and cannot be modelled nor evaluated thanks to usual predictive models based on event occurrence distribution models. Cyber Risk evaluation must be linked with attack potential andattack difficulty (Tables E3 and E4 in IEC 63452).

Attack potential metrics are useful for Security Assurance Requirements specification, as recommended in EN 18037 standard.

PRINCIPLE 7 | SAFETY AND SECURITY TARGET MEASURES SHOULD NOT BE COUPLED

Our proposal for principles application considers Security and Safety Processes separately. Interfaces between Cyber Concept and Safety Related Functions are monitored in terms of cross-assumptions and in terms of Freedom From Interference for both Security Functions and Safety Kernel implementations (design and code level).



Authors : Véronique Delebarre | Safety and Cyber Security Specialist | veronique.delebarre@glarros-tech.com
Co Authors : Jean Caire | Cyber and Safety Expert at RATP | jean.caire@ratp.fr | RATP
SafeRiver - A SERMA Safety and Security Company – www.serma-safety-security.com