Ansaldo STS

A Hitachi Group Company

13th Florence Rail Forum: Cyber Security in Railways Systems

Immacolata Lamberti
Andrea Pepato

November 25, 2016

Cyber Security context and Cyber Attacks trend

Critical Infrastructures (CIs) are both physical and virtual assets, systems and networks, whose aim is to ensure the life in a country. Transportation systems and telecommunications are CIs: damage or destruction by natural disasters, terrorism and criminal activity may have negative consequences for the security of the entire community.

The Cyber Security activities are aimed to protect the transportation system information, minimizing risks related to data Confidentiality, Integrity and Availability, defined as:

- **Confidentiality**: property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity**: property of accuracy and completeness.
- **Availability**: property of being accessible and usable upon demand by an authorized entity.

Known attacks to Critical Infrastructure are growing. Notwithstanding they are the 3% of the whole attacks, in 2015 this aspect has grown of 154% with respect to 2014. (CLUSIT2016 - Associazione Italiana per la Sicurezza Informatica)

Railways System

Railway systems are becoming vulnerable to cyber attack due to the move away from stand-alone systems to open-platforms, standardized equipment built using Commercial Off The Shelf (COTS) components, and increasing use of networked control and automation systems that can be accessed remotely via public and private networks.

Coexistence between Safety Critical Subsystems and Non Safety Critical ones.

Operating Environment:

- Distributed infrastructure spread over long distances, and unattended systems.
- External systems connected to signaling infrastructure.
- Human factor (operators, maintainers and … passengers).

The Cyber Security Process offers to our Customer (Bidding and Projects) a Security Integrated System aimed to protect the Railways System against: Physical Access Attacks, Dialog Attacks, Penetration Attacks (Software), Hardware Attacks, Social Engineering.

Typical Requirements, Standard and Norms

- “Good Practice Catalogue” issued by the Centre for the Protection of National Infrastructure (CPNI).
- The International Society for Automation IEC 62443 suite of documents (‘Security for Industrial Automation and Control Systems’).
- The National Institute of Standards and Technology NIST SP800-82 ‘Guide to Industrial Control Systems (ICS) Security’.
- EN 50159: Railway applications - Communication, signaling and processing systems - safety-related communication in transmission systems.
- ISO/IEC 27000 family of documents.

Ansaldo STS ISMS Process

The Internal Company Procedures establish an Information Security Management System (ISMS) Process, Separation of Duties Principle based on, according to ISO/IEC 27001:2013.

Governance: to provide procedures and policies to implement the information security framework.
Design: to develop the functional requirements concerning the design of Project Security Protection.
Execution: implementation of countermeasures into the security infrastructures.
Control: to verify that all the previous phases are correctly implemented.

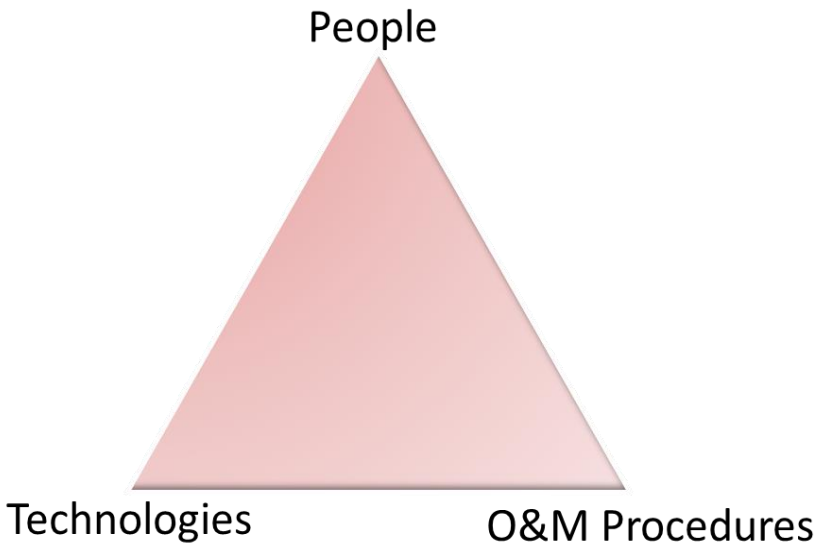
Prevention: aimed at identifying security risks and defining mitigation measures before threats occur.
Detection: aimed at identifying when security incidents occur in order to ensure the activation of the reaction phase.
Reaction: aimed at managing security incidents after occurrence in order to ensure the mitigation of their impacts.

Security and Operational Requirements

- The technological implementation is not sufficient to cover all the Security threats.
- Accurate O&M measures and procedures have to be defined.

The crucial aspect to be considered is people.

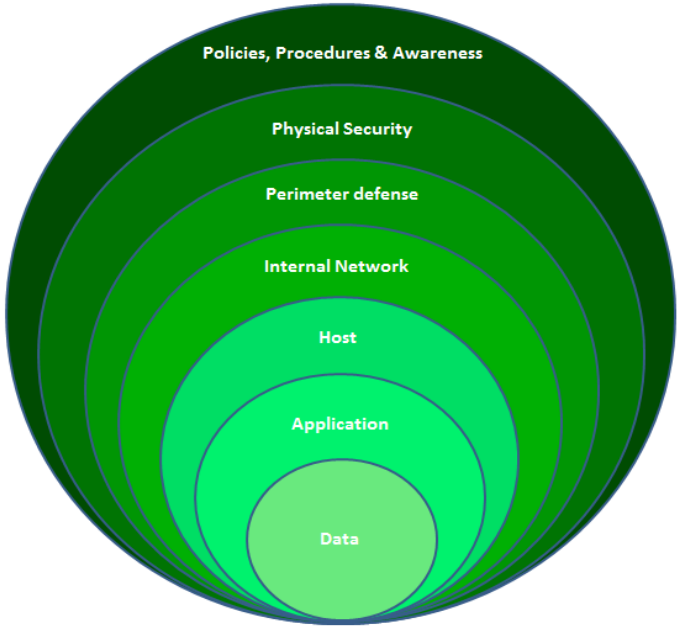
Technologies, O&M procedures and people have to be combined and managed in order to reach a suitable level of protection.



Defence in Depth

The concentric domains protection:

- ***Policies and Procedures.***
- ***Physical Security.***
- ***Perimeter Network Defence.***
- ***Internal Network Defence***.
- ***Host Security***.
- ***Application Security***
- ***Data Security***.



Cyber Security Activities

Objective: comprehensive Security Study aimed to demonstrate appropriate security measures and mitigations (encompassing: people, process, physical and technological aspects) are taken into account.

Related activities:

1. Governance: Policy, Requirements and Procedures Definitions
2. Design:
   - Communication and interface network study, O/S Typologies, Existing Data Flow and Services identification
   - Risk Management and Vulnerability Exposure: Threat analysis and countermeasures identification (Critical Asset Identification, Security Threat Identification, Vulnerability and Consequence Analysis, Security Risk Assessment and Mitigation).
   - Operational Security aspects.
3. Execution:
   - Countermeasures implementation and configuration into the Project Design based on previous requirements (System hardening, Access control mechanisms, Network Perimeter Defense, Network Internal Defense, etc…)
   - Security Policies and Procedures application
   - Incident Management
4. Control: Audit, Vulnerability Assessement and Penetration Test activities

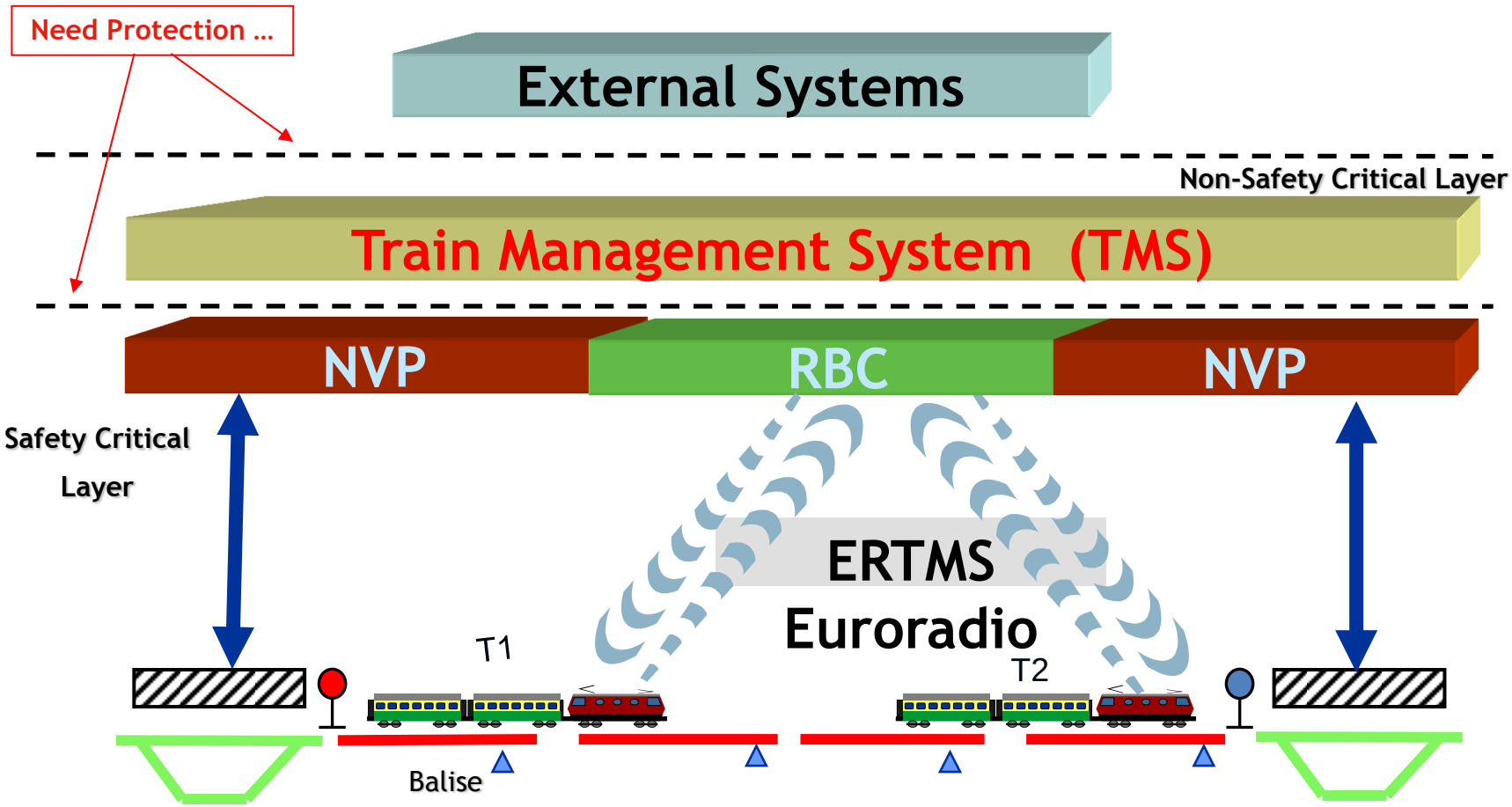
ERTMS/ETCS High Speed System: main threats

ENVIRONMENT	THREAT CLASSIFICATION	CYBER THREATS
Central Site/ Peripheral Sites	Integrity	-Asset theft or alteration -Tampering/Destroy Data -Unauthorized access -Misconfiguration
	Confidentiality	-Intrusion (Hacking, Malware)
	Availability	-Resource Misuse -Service Interruption
WAN & Wireless Infrastructure	Integrity	-Spoofing -Misconfiguration
	Confidentiality	-Loss of confidential data -Unauthorized access
	Availability	-Service Interruption

ERTMS/ETCS High Speed System: main threats

ENVIRONMENT	THREAT CLASSIFICATION	CYBER THREATS
Vital-Non Vital (SILx – No SIL) connections	Availability	-Service Interruption
SCADA Systems	Integrity	-Cyber Warfare -Misconfiguration
	Availability	-Service Interruption
External Connections	Integrity	-Intrusion (Hacking, Malware) -Unauthorized access -Privilege abuse
	Confidentiality	-Remote spy -Loss of confidential data
	Availability	-Service Interruption
Mobile Devices and BYOD	Integrity	-Asset theft or alteration -Unauthorized devices -Malware imports -Unauthorized access
	Confidentiality	-Loss of confidential data

ERTMS/ETCS High Speed System



NVP: Peripheral Kernel - Interlocking

RBC: Radio-Block Center

Conclusions

Cyber Space is today a global domain without border within which governments, institutions and industries are players interested in preventing and debilitating cyber crime.
Transportation Systems are Critical Infrastructures and the potential risks are:

- Insiders
  - ✓Mistakes
  - ✓Sabotage
- Terrorists or Activists
- Hackers or Cyber Criminals

Regulations and International standards
Continuous security technological improvement
Collaboration among Vendors, Industries, Institutions and Governments

THANK YOU FOR YOUR ATTENTION