29 November 2017

Railway Systems:
How to deal with cyber threats

Lovan Pushparatnam
Director, Tramway Systems and Telecoms Department
SYSTRA

SYSTRA

SYSTRA: International Transport Engineering Consultancy

SYSTRA operates at every stage of the project lifecycle:

Transport Planning • Urban Planning and Development • Socio-economic Studies • Sustainability and Environmental Studies • Urban and Architectural Design • Alignment and Track • Bridge Design • Underground Structures • Civil Engineering • Systems Integration • Signalling • Traction Power and Catenary • Communications and Ticketing • Rolling Stock and Maintenance Facilities • Project Management • Project Communication • Construction Management • Testing & Commissioning • Maintenance Programme Management

€612m

revenue
in 2016

6,100

employees
around the world

80

countries

60%

turnover
achieved internationally

Overview

1
- Introduction

2
- Recommended cybersecurity approach for new projects

3
- Summary

Introduction

Why is cyber security an issue for railways?

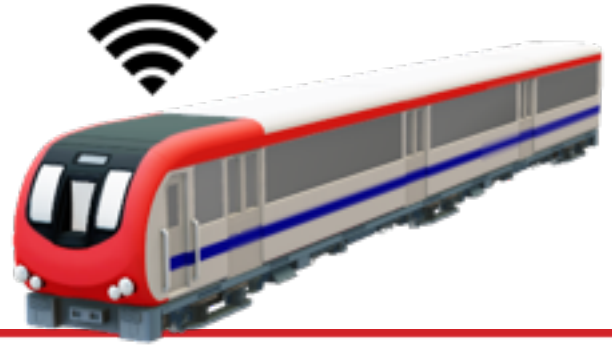
Transport networks (railways, metros etc.) are increasingly relying on complex electronic equipment and information systems

Control networks such as SCADA for traction power control have reached a high level of sophistication and complexity

Previously separated systems (signalling, telecoms, control systems) are more and more interconnected and often passing over a single data transmission bearer

This results in increased performance but also subjects these systems to new threats

Photo: Tripwire



SYSTRA

Putting cyber security into perspective

100% security does not exist

80:20 rule applies to incidents

Majority of incidents are usually unintentional:

- Not respecting procedures
  - Human error (e.g. during testing or maintenance)
  - Virus propagated by unauthorised media (e.g. USB stick).
- Equipment failure

Only a minority of incidents are intentional:

- Hackers
- Terrorists
- Employees

Photo: L. Pushparatnam

Cyber security

The best results are achieved when cyber security is treated as part of an overall security policy that addresses:

- Technical aspects (equipment specifications, system architecture)
- Operating procedures (management of incidents, recovery)
- Continuous assessment and measurement

Cyber security is not about protection it is about preparation

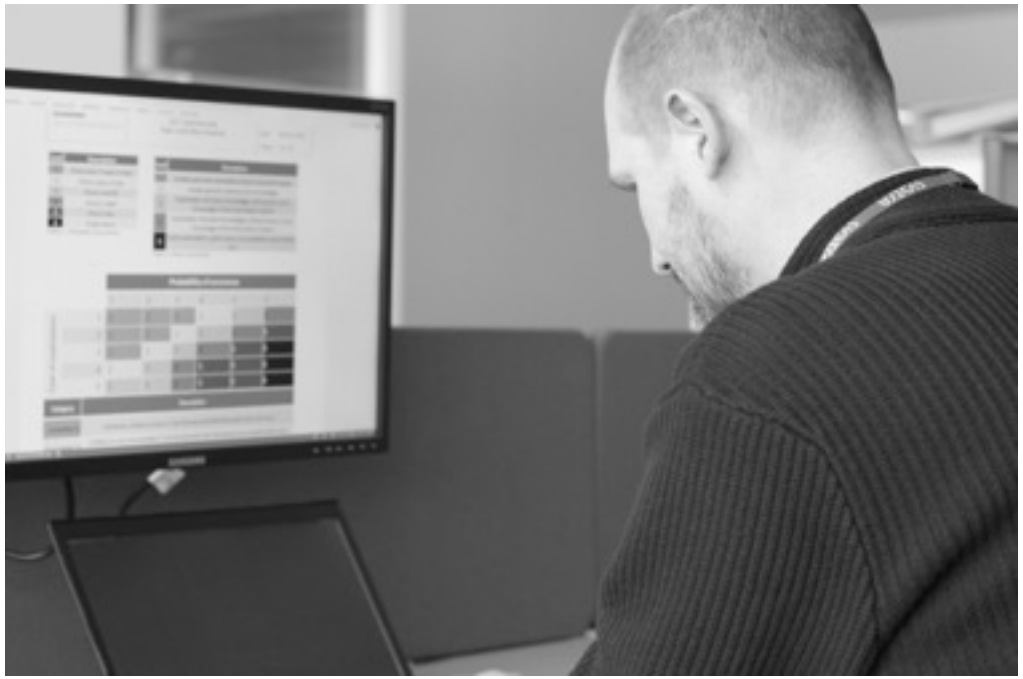


Photo: L. Pushparatnam

Recommended cybersecurity approach

For new projects

Recommendations

Recommendation 1

Information systems security must be integrated at the beginning of each project

Recommendation 1: cybersecurity from day one

Stakeholders' high-level security requirements

E.g. "The maintainer needs access to log files"

Technical Requirements

E.g. "Access for maintainers is limited to backup log files but not to the live system"

Recommendations

Recommendation 2

Technical audit

Recommendation 2: Technical audit

Technical audit

Penetration test

Penetration test

Examples:

- Intrusion to take control of the system
- Stress test by flooding the network to obtain a denial of service

Vulnerabilities that are found need to be corrected

Some may persist and these will be noted in the Final Security Case

Recommendations

Recommendation 3

Identify residual risks

Recommendation 3: Identify residual risks

Residual risks

Residual risks

Examples:

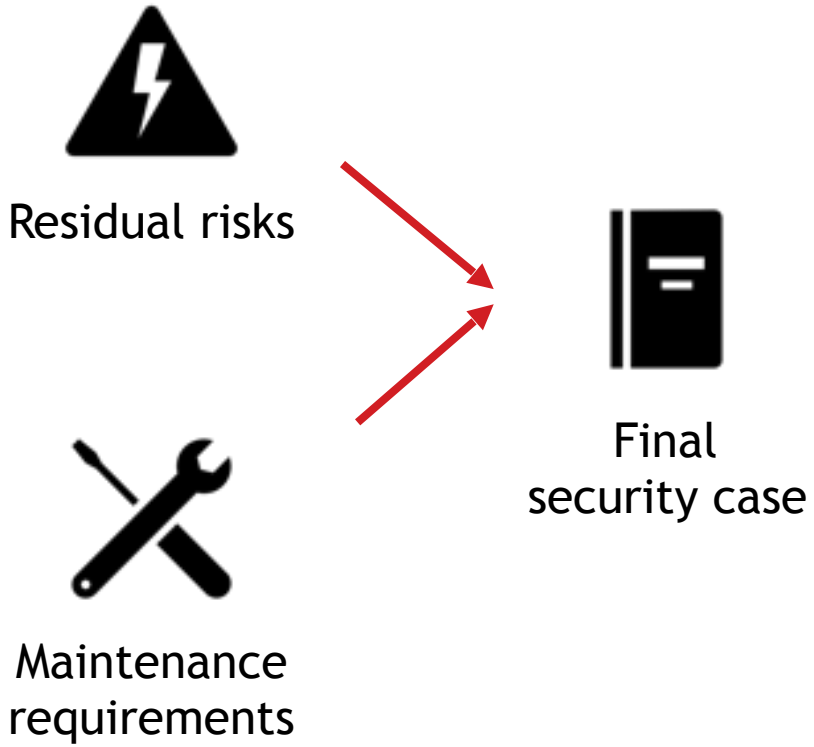
- Use of an operating system that is vulnerable to future virus attack
- Maintainers want to have a single password for all systems
- Maintainers do not want to apply security patches on system during life of system

Recommendations

Recommendation 4

Final Security Case

Recommendation 4: Final safety case



Final Security Case

Along with the residual risks, the requirements on the maintainer will feed into the Final Security Case

Examples of requirements on the maintainer:

- 6-monthly technical audits
- Periodic verifications that there are no infections
- Encryption of maintenance disk drives on laptops

Summary

Summary

Railway systems are more and more interconnected with increased complexity and interfaces

The trend is to mix or interface critical and non-critical systems with varying security requirements

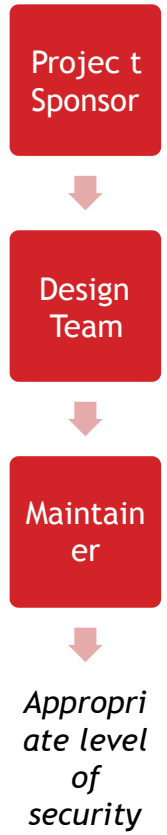
Railway systems are subjected to security incidents some of which are the result of deliberate attack

Security has a cost (investment and operational) but by treating it at the beginning of a project its impact may not be significant since it depends on:

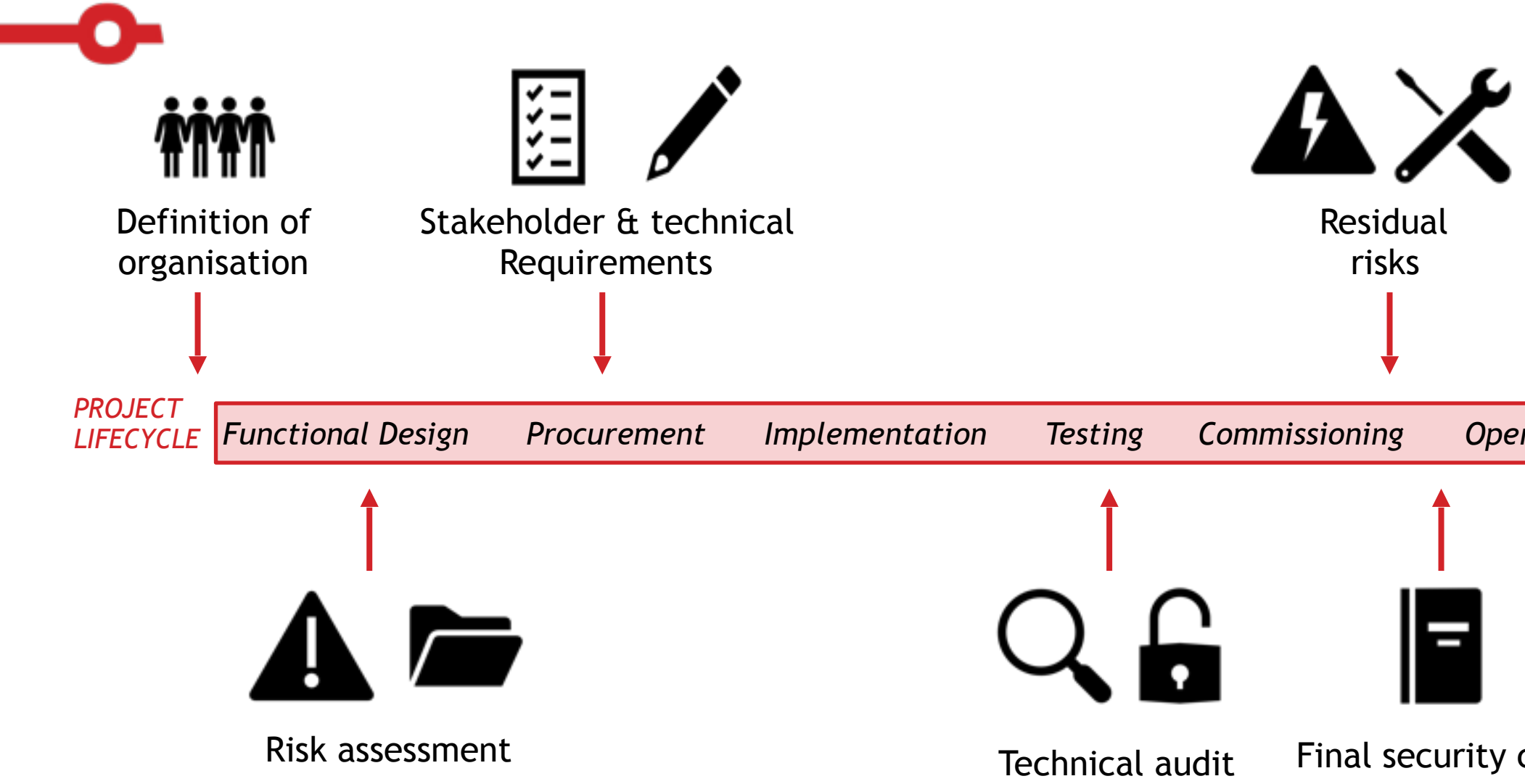
- How and what you specify
- the types of risk and threat
- what level of risk you are willing to accept

Different systems may be maintained by different organisations each with their own security culture

Cyber security is not just for the IT department



Summary of recommendations



Additional points to note

Awareness and training is essential for all stakeholders at all levels (from maintenance technician to project director)

Level of security will decrease over the life of the system either through modification/upgrades or new vulnerabilities that appear

In addition to regular audits a continuous programme of monitoring is necessary so that immediate action may be taken for new threats (e.g. patches)

CONFIDENCE MOVES THE WORLD

SYSTRA