Standardisation and security in multi-modal

Jörg Nachbaur

Committee Manager
Austrian Standards International
Vienna / Austria

CitySCAPE Introduction

- CitySCAPE is a project funded by the EU's Horizon 2020 research and innovation program, which consists of 15 partners from 6 European countries, united in their vision to cover the cybersecurity needs of the multimodal transportation.

- The traditional security controls and security assurance arguments are becoming increasingly inefficient in supporting the emerging needs and applications of the interconnecting transport systems, allowing threats and security incidents to disturb all dimensions of transportation.

What‘s the challenge

- Smart and sustainable cities rely on sustainable mobility and transportation providing several benefits to public transport operators and to the citizens. This implies also that the connected system of transportation is safe and secure against cyberattacks and protects personal data of those who take advantage of the transport services.

- To make the ecosystem of an intelligent multimodal transport system resistant against such threads a holistic and proactive approach is needed, covering collaborative analysis of security/privacy persistent threats, forecasts cyber-security incidents, counteracts, assessing the impact in both technical and financial terms. Standardization promotes and supports this approach both in terms of efficiency, effectiveness, continuous improvement and in the uptake by ITS communities.

Standardization Gaps and Needs SURVEY

Is the identification of cybersecurity threats in the transport ecosystem addressed comprehensively?

- Privacy-related threats
- Specific treatment for cybersecurity threats
- Mobile device threats detection and response, security awareness training and threat intelligence
- New cybersecurity issues related to new technologies (e.g. electronic ticketing, mobile services)
- Collaboration among all the involved stakeholders to improve information and knowledge sharing
- Lack of specific security standards for transport ecosystem to support the management of specific threats
- Lack of awareness of the technologies and security measures to be adopted to mitigate the risk associated with cyber threats
- Lack of transparency between stakeholders
- Strong conservativism of transport ecosystem

Standardization Gaps and Needs SURVEY

What are the major shortcomings of the architecture of existing city transport ecosystem?

- Several actors are involved (customers, industry) with no specific requirements
- No specific processes are set up to address cybersecurity; audit is only done when issues are raising
- Lack of consideration of the 'security by design' paradigm
- Lack of integration, stratifications of different technology "eras"
- Security is neither included in the initial specification nor in the acceptance tests
- Inadequate communication among moving transport and central systems
- Minor emphasis on the collaboration and communication with all the involved actors.
- Limited adoption of new interoperability approaches and protocols
- Inadequate integration of Legacy System and Open Data
- Lack of an appropriate data management system (no widely adopted language to model the system of systems)
- Superficial evaluation that leads to underestimation of certain threats and improper security measures
- Lack of proper planning and organization of the security measures that lose their effectiveness over time
- No real consideration of cyber risk
- Lack of a holistic view due to the presence of several independent monitoring systems

Overview of Standards used in Cityscape

- EN 12896, Public transport - Reference data model (all parts)
- CEN/TS 16614, Public transport - Network and Timetable Exchange (NeTEx) (all parts)
- CEN/TS 16157, Intelligent transport systems - DATEX II data exchange specifications for traffic management and information (all parts)
- EN 15531-1, Public transport - Service interface for real-time information relating to public transport operations –Part 1 : Context and Framework
- CEN/TS 15531, Public transport - Service interface for real-time information relating to public transport operations (all parts)
- ISO/IEC 15408, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security (all parts)
- ISO/IEC 18045, Information technology — Security techniques — Methodology for IT security evaluation
- ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 27003, Information technology — Security techniques — Information security management systems — Guidance
- ISO/IEC 27005, Information technology — Security techniques — Information security risk management
- ISO/IEC TS 27008, Information technology — Security techniques — Guidelines for the assessment of information security controls
- ISO/IEC 27009, Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements
- ISO/IEC 27031, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27035, Information technology — Information security incident management (all parts)
- ISO/IEC 27039, Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

Cityscape work in progress

The most important focus points for future standardization activities can be identified as follows:

- Data management
- Handling of all passengers-related data
- Management of real-time operational data between vehicles and vehicles/infrastructure
- Common language for cyber risk modelling and management
- Integration of cybersecurity processes into system architecture to ensure its alignment with business-critical processes

- Development of a specific overarching cybersecurity standard for multi-modal transport that integrates/refers to already existing standards


Smart and
Sustainable
Mobility
for all.
its
EUROPEAN
CONGRESS
TOULOUSE
30 May - 1 June 2022

Thank you!

Detection/Response solution for railway systems

Fabien Pornet

Technical Manager
Airbus Cybersecurity

Airbus CyberSecurity

Airbus Defence and Space

Connected Intelligence

Airbus CyberSecurity

Detection for railway system: the challenges

1

Continuous monitoring during system operational time

- Intervention level definition
- Incident response strategy
- Need for handover after a fix period

2

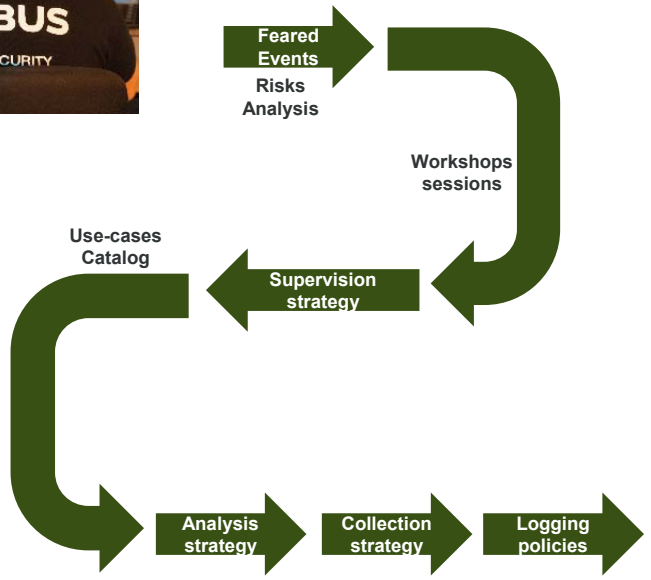
Railway systems not natively in Airbus Portfolio

- Partner identification for Design and Build
- Incremental Integration in sub-systems then global system
- Validation and test

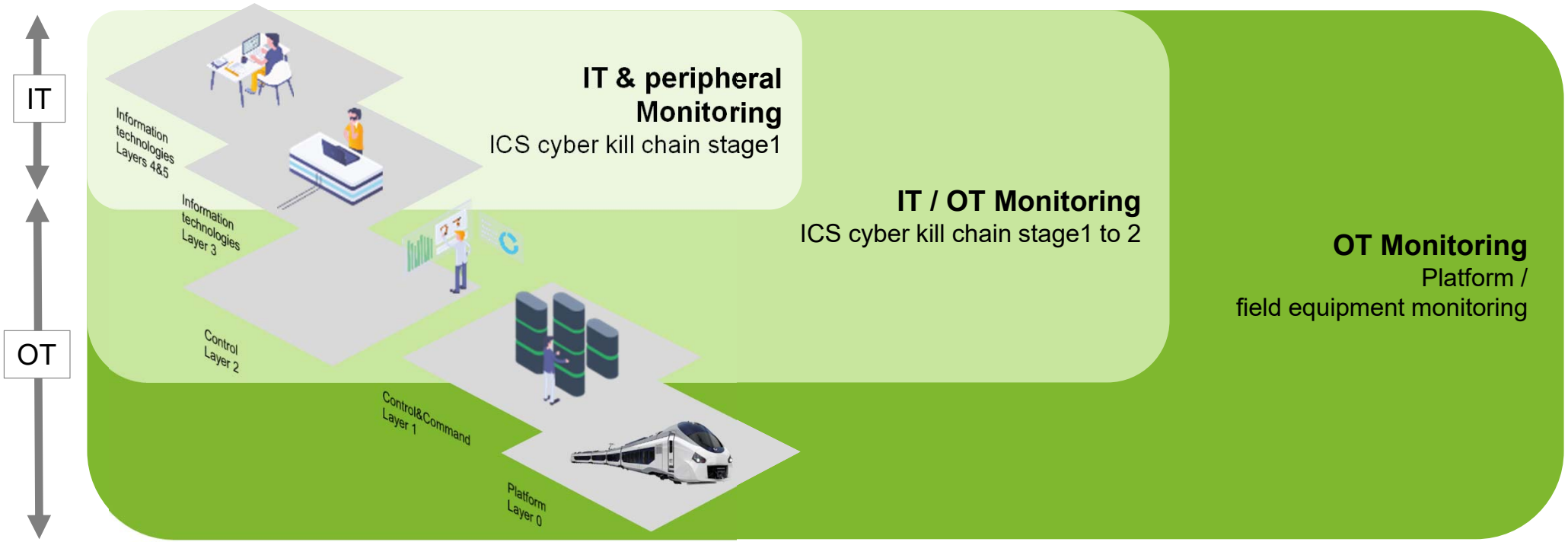
3

Heterogeneity of equipment and logging capabilities

- Identify key assets
- Build relevant use cases



Several supervision strategies



Key feedbacks

1

Foster a step-by-step approach

To master specific railway projects
(very long V-Cycle, risk analysis, vocabulary, sub-system split)

2

Include cybersecurity early in conception

Collection Strategy
Definition of Auditing Policy (Logs)

3

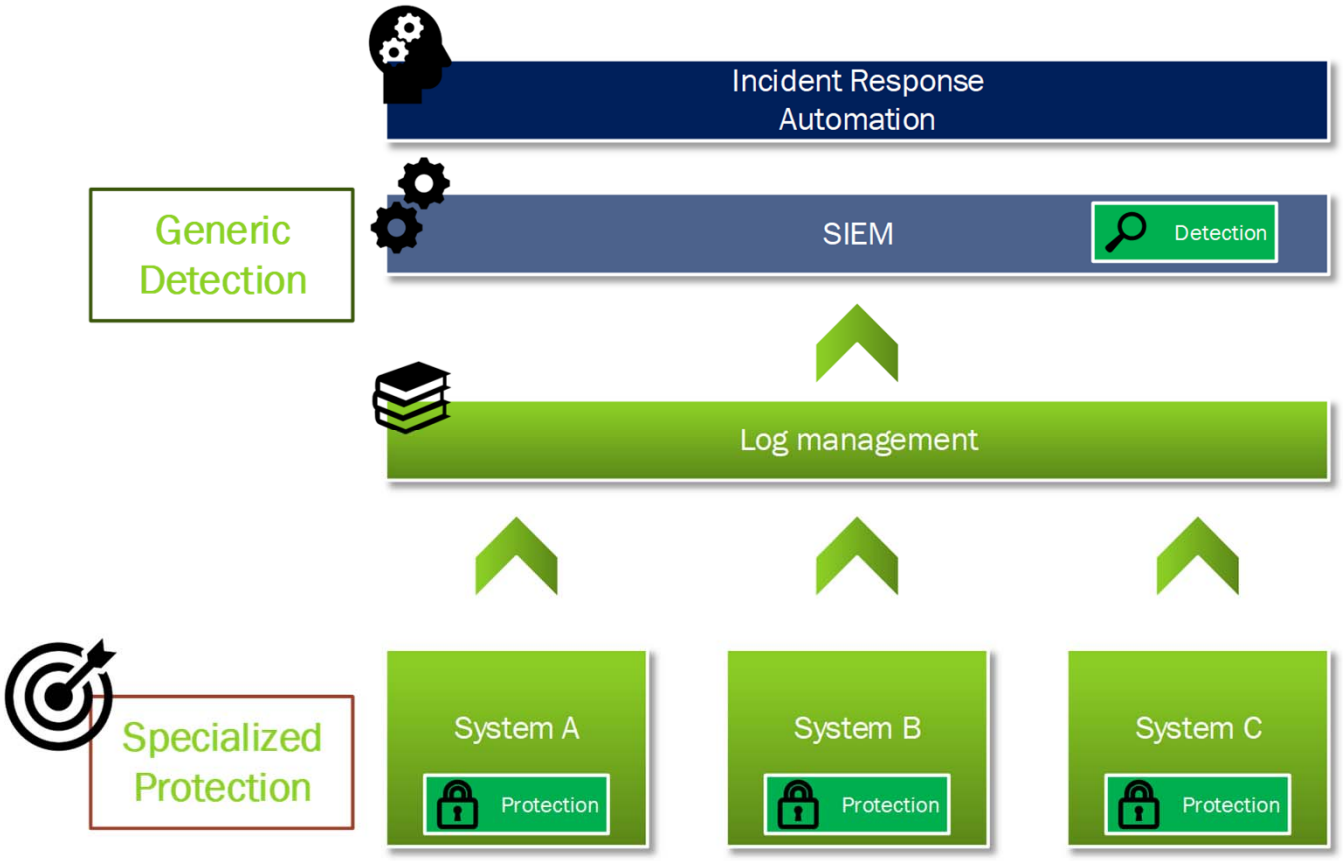
Elaborate a realistic detection strategy

Detailed attack scenarii identification & likelihood
Priorization of asset to secure according to criticity
Extension of Risks scope over time

Current technical detection solution

All SIEM Architecture

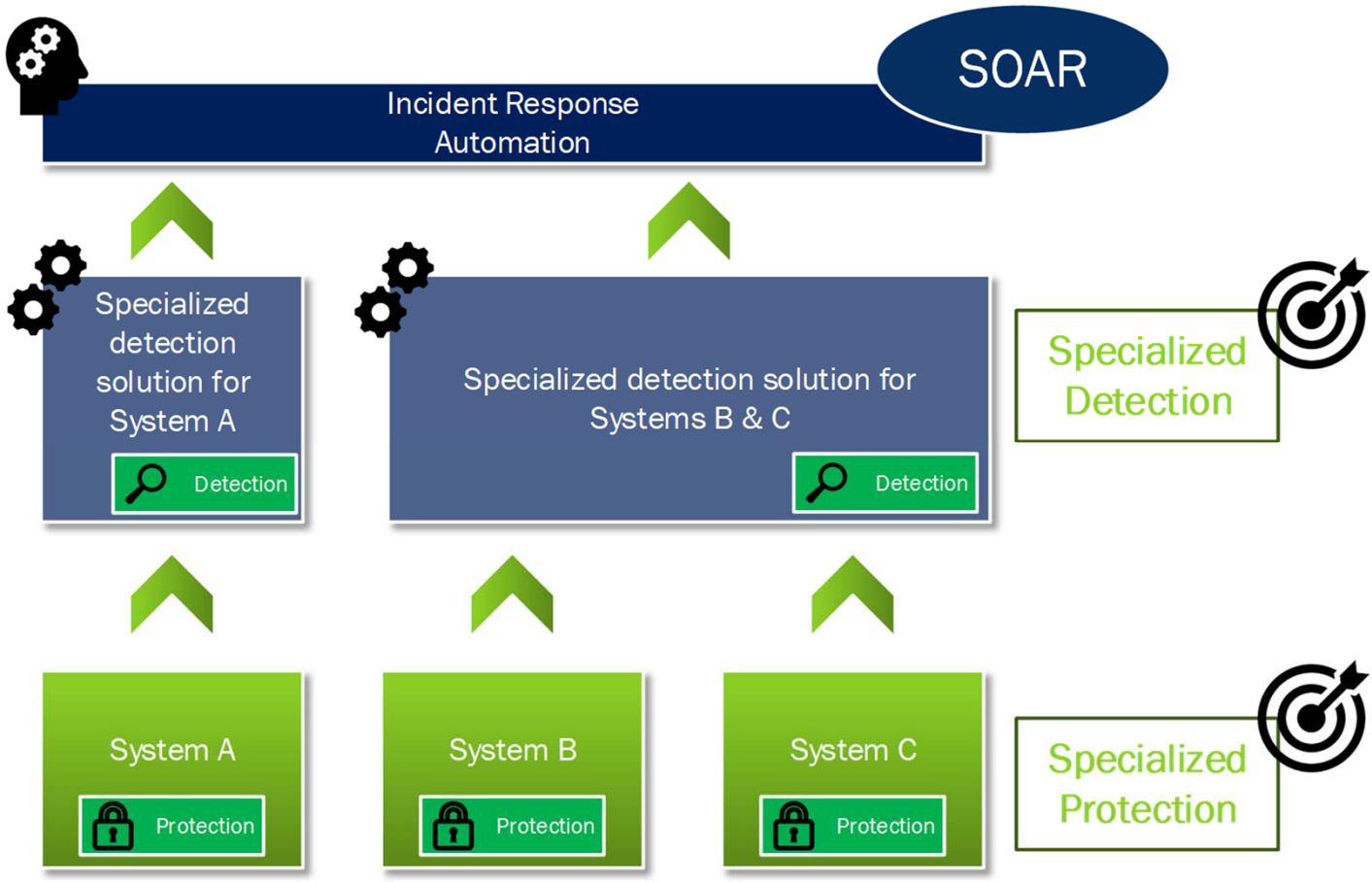
- SIEM agglomerates all logs
- **One tool fit all** systems…
- … so one security team has to master every system
- Usually limited to some systems because of **cost**
  - ➢ Attacks are becoming faster
  - ➢ We need a view on all attack surface…
  - ➢ … at every step of the attack



A new technical paradigm for Detection & Response

SOAR Architecture

- **Specialized** detection
  - Relying on editors' operational knowledge
- SOAR is a **360° Security** view on all IS
- Easier integration of **Remediation** tools
- Increase **Analysts' insight**
- SIEM still a solution along with :
  - EDR
  - NDR
  - DLP
  - Vulnerability management
  - Cloud solutions
  - …




Smart and
Sustainable
Mobility
for all.
its
EUROPEAN
CONGRESS
TOULOUSE
30 May - 1 June 2022

Thank you!