Cybersecurity challenges at Volvo Group

Autosec FFI conference 2019-10-10

Daniel Karlsson

Vehicle sophistication

Attack benefits

EE architecture complexity

Attack surfaces

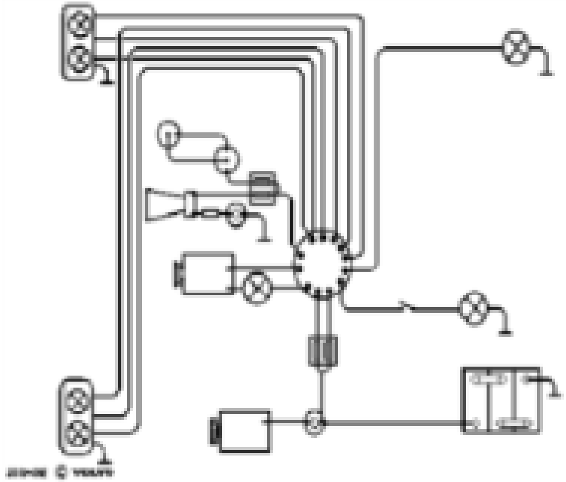
Vehicle sophistication

Mechanics

Attack benefits

Insignificant

EE architecture complexity



Battery, cables, switches, light bulbs, radio

Attack surfaces

Cable cut
Tampered radio signal

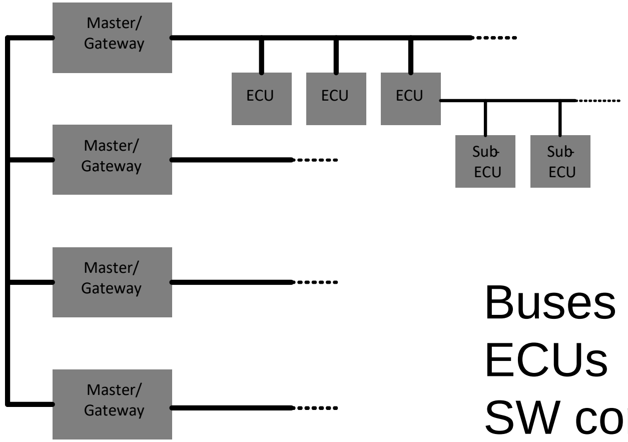
Vehicle sophistication

Electronics

Attack benefits

Subsystem/subnet manipulation and control
Access to confidential subsystem data

EE architecture complexity



Buses
ECUs
SW controlled sensing and actuation

Attack surfaces

Cable cut
Tampered radio signal
CAN buses
OBD port
Data on wireless interfaces

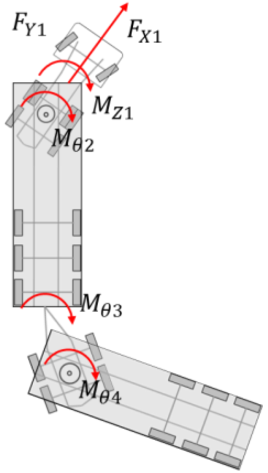
Vehicle sophistication

Data centric

Automation

Connectivity

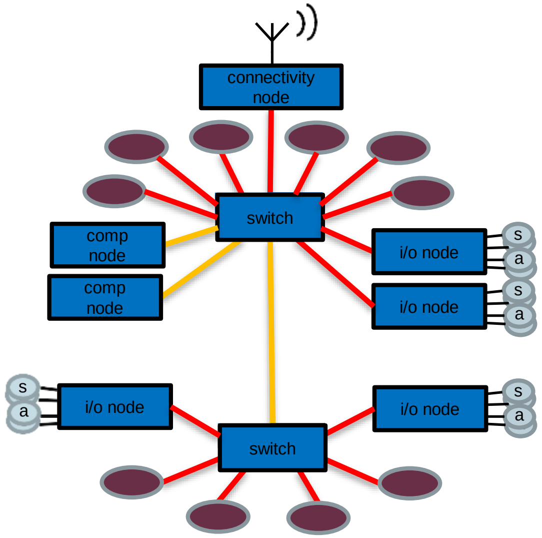
Attack benefits



Vehicle manipulation and control

Access to confidential vehicle data

EE architecture complexity



Networks

Centralised computation

Attack surfaces

Cable cut

Tampered radio signal

CAN buses

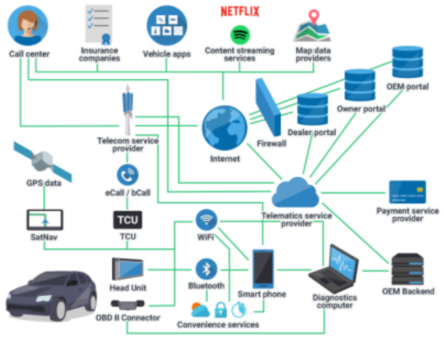
OBD port

Data on wireless interfaces

Ethernet networks,

Vehicle control on wireless interfaces

Vehicle sophistication

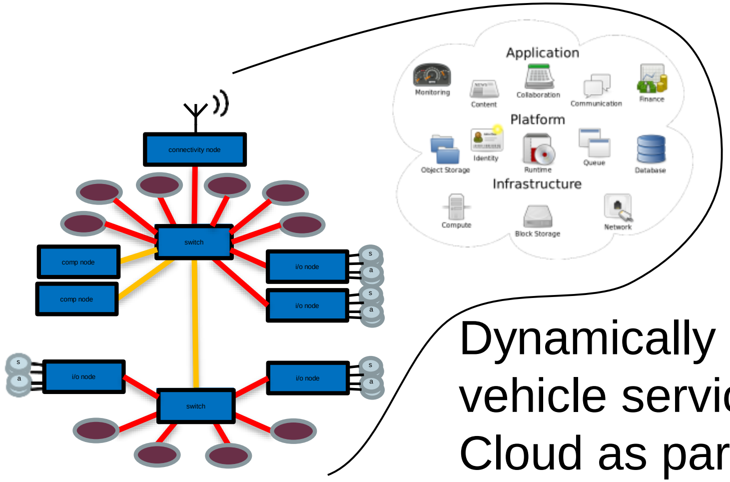


Service centric

Attack benefits

Fleet manipulation and control
Access to confidential fleet data

EE architecture complexity



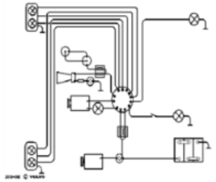
Dynamically deployable vehicle services
Cloud as part of the vehicle

Attack surfaces

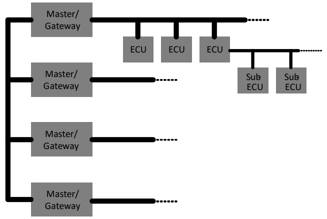
Cable cut
Tampered radio signal
CAN buses
OBD port
Data on wireless interfaces
Ethernet networks,
Vehicle control on wireless interfaces
Cloud infrastructure

VOLVO
VOLVO GROUP

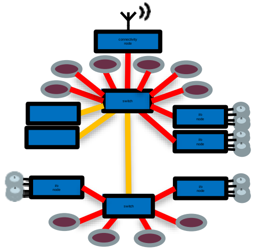
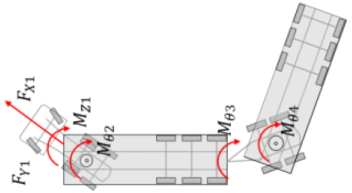
Phase 1: Mechanics

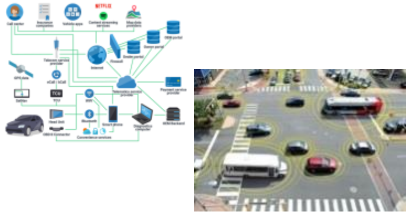
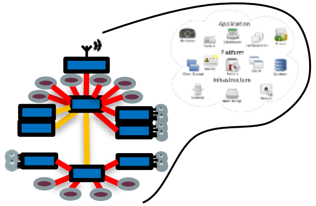
Phase 2: Electronics


Phase 3: Data


Phase 4: Services

UNECE cyber security principles, effective ~2021-2022, requires the industry to deal with cyberresilience **puts requirements on cybersecurity for type approval**

Puts requirements on cybersecurity for type approval

6.5.5. The evidence required for vehicle approval shall include:

1. How the vehicle manufacturer has implemented the cyber security principles identified in this paper;
2. How the vehicle manufacturer has considered threats and vulnerabilities, including those detailed in annex A, within their risk assessments;
3. What mitigations the vehicle manufacturer has implemented to minimise the risks to a level acceptable to the authority through describing:
   - i. The vehicle architectures and systems;
   - ii. The significant components of those architectures and systems that are relevant to cyber security;
   - iii. The interactions of those architectures and systems with other vehicle architectures, systems and external interfaces;
   - iv. The risks posed to those architectures and systems that have been identified in the risk assessment;
   - v. The mitigations that have been implemented on the systems listed and how they ...ess the stated ri...

UNECE Cyber security principles

3.3.6. The security of software should be managed throughout its lifetime;

3.3.7. The storage and transmission of data should be secure and should be controlled;

3.3.8. The vehicle manufacturer should assess security functions with testing procedures;

3.3.9. The vehicle should be designed to be resilient to cyber attacks;

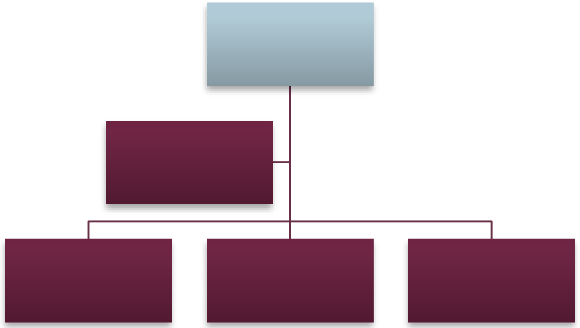
3.3.10. The vehicle should be designed with the capability to detect cyber-attacks and respond appropriately.

VOLVO
VOLVO GROUP

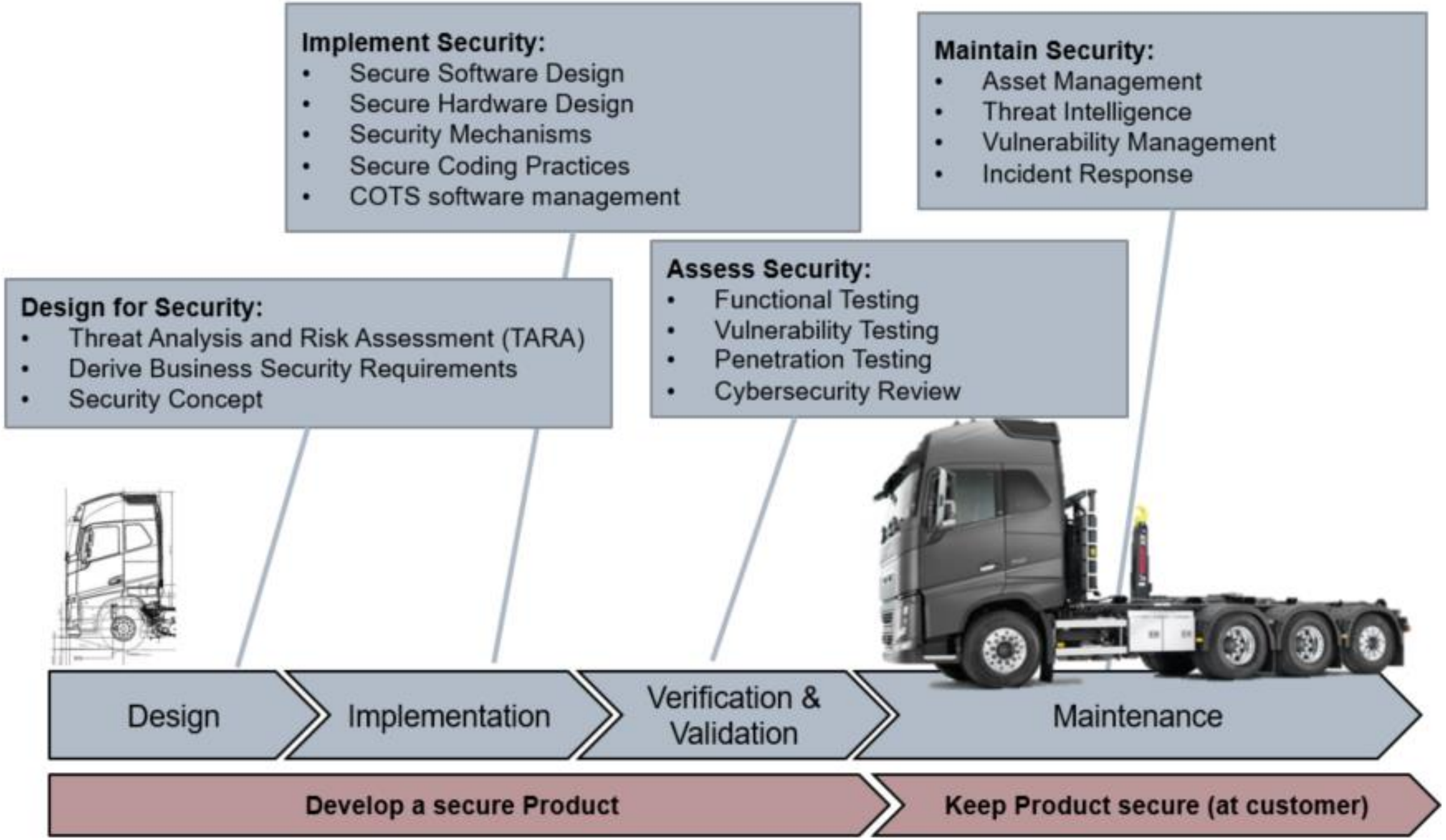
Challenges ahead!

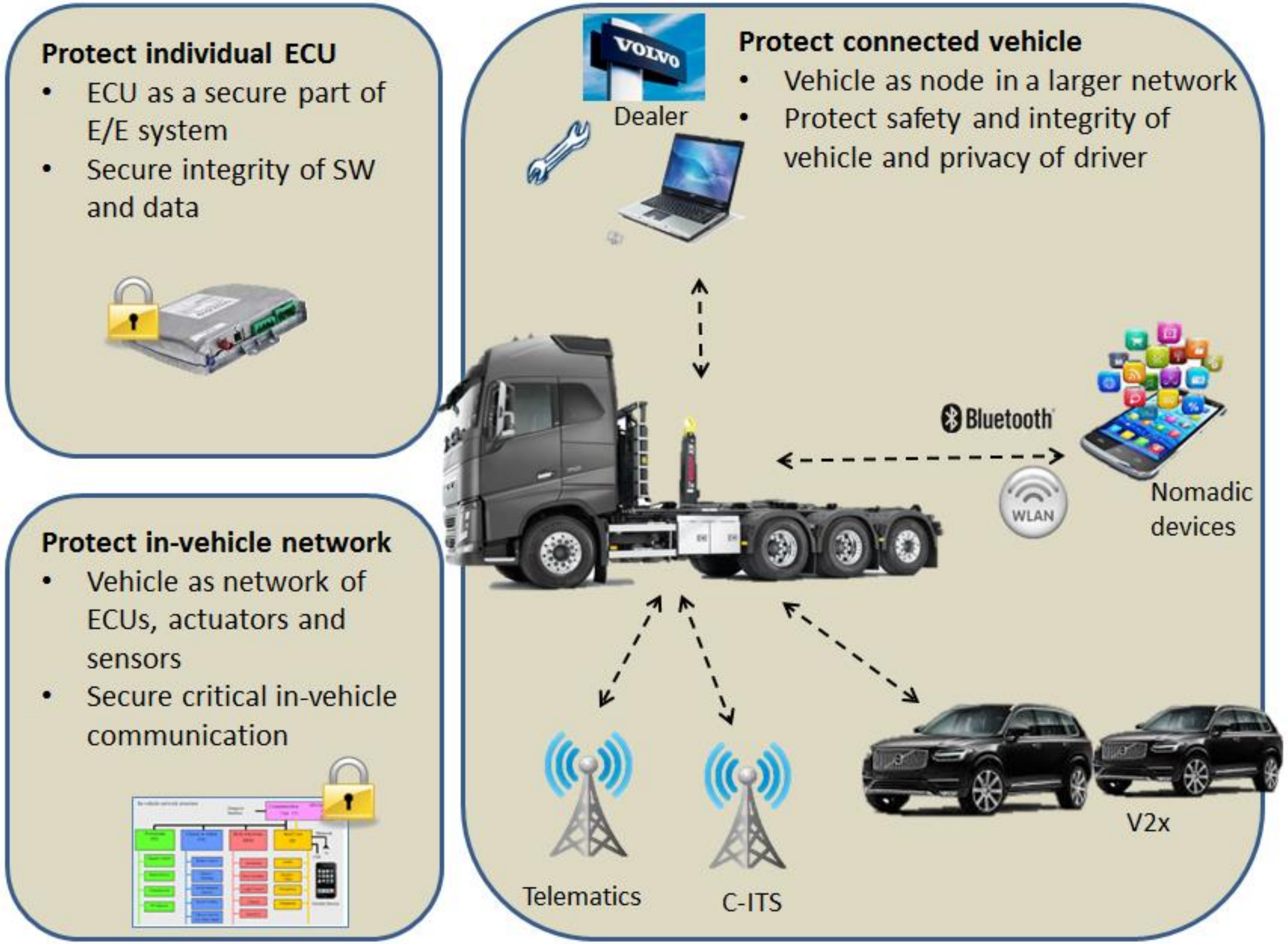
Lifecycle

Technology



Organisation


Implement Security:
Secure Software Design
Secure Hardware Design
Security Mechanisms
Secure Coding Practices
COTS software management
Maintain Security:
Asset Management
Threat Intelligence
Vulnerability Management
Incident Response
Design for Security:
Threat Analysis and Risk Assessment (TARA)
Derive Business Security Requirements
Security Concept
Assess Security:
Functional Testing
Vulnerability Testing
Penetration Testing
Cybersecurity Review
Design
Implementation
Verification & Validation
Maintenance
Develop a secure Product
Keep Product secure (at customer)


Protect individual ECU
• ECU as a secure part of E/E system
• Secure integrity of SW and data
Protect in-vehicle network
• Vehicle as network of ECUs, actuators and sensors
• Secure critical in-vehicle communication
VOLVO
Dealer
Protect connected vehicle
• Vehicle as node in a larger network
• Protect safety and integrity of vehicle and privacy of driver
Bluetooth
WLAN
Nomadic devices
Telematics
C-ITS
V2x

Process, methods and tools

- How can we work with and manage cybersecurity more efficiently, especially in the context of connectivity and automation?
- How can we apply ISO21434 more efficiently and better integrate it in the existing development process based on agile and CI/CD?
- How can we comply with the type approval recommendations from UNECE?

Impact on functional safety

- How do we find the right design trade-offs between security and safety?
- How can we still maintain safety in the presence of an attack?

Protection mechanisms

Intrusion detection

- How can we build inherent support for protection and detection in the EE architecture?
- How can we efficiently detect attacks?

Recovery mechanisms

- How can we recover from an attack, maximising uptime?

Post-event analysis

- How can we provide faster security updates to large fleets?
- How can we better and faster learn from attacks, and feedback the insights into the development of future products?

Secure cloud functionality

- How do we ensure a secure (and safe) operation as dependency on the cloud increases?

- How do we keep up with the competence?

→ Competence development

- How can we find competent people?

→ Recruitment

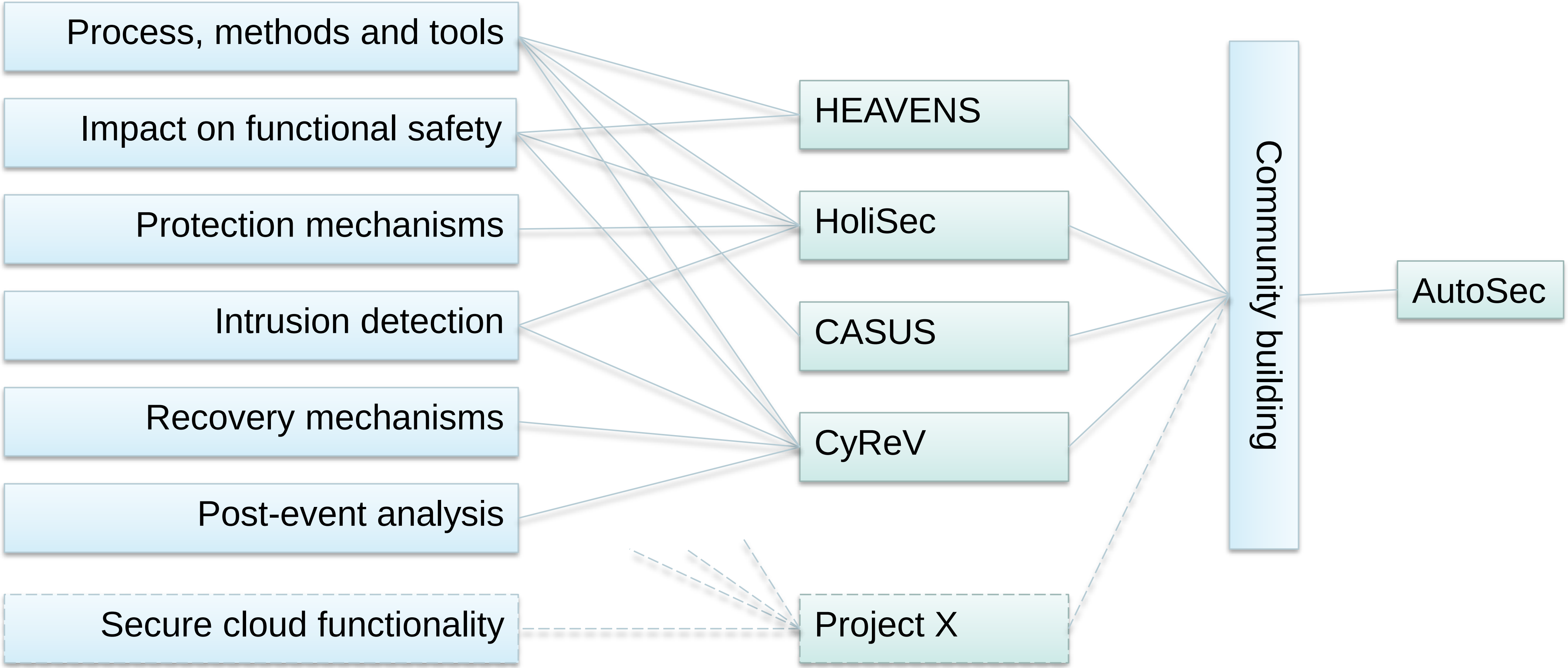
- How do we spread cybersecurity knowledge in the organisation?
- How do we increase awareness of cybersecurity to developers?

→ Communication

- How do we manage cybersecurity in the organisation in the best way?
- How do we build efficient incident management?

→ Organisation


Challenges ahead!
Let's embrace them together.


Process, methods and tools
Impact on functional safety
Protection mechanisms
Intrusion detection
Recovery mechanisms
Post-event analysis
Secure cloud functionality
HEAVENS
HoliSec
CASUS
CyReV
Project X
Community building
AutoSec

Process, methods and tools

Impact on functional safety

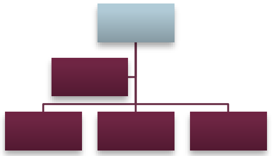
Protection mechanisms

Intrusion detection

Recovery mechanisms

Post-event analysis

Secure cloud functionality



Competence development

Recruitment

Communication

Organisation