HoliSec

Holistic Approach to Improve Data Security

HoliSec Final Open Workshop

26 March, 2019

VINNOVA FFI VOLVO VOLVO ARC CORE CHALMERS ASSURED SECURITY CONSULTANTS RI.SE Research Institutes of Sweden

HoliSec

Holistic Approach to Improve Data Security

External Research Collaboration within Cybersecurity in the Volvo Group

Daniel Karlsson

March 26, 2019. Time 09:00 – 09:30

VINNOVA FFI VOLVO VOLVO ARC CORE CHALMERS ASSURED SECURITY CONSULTANTS RI. SE Research Institutes of Sweden

It's A Journey

..full of challenges
..and excitement

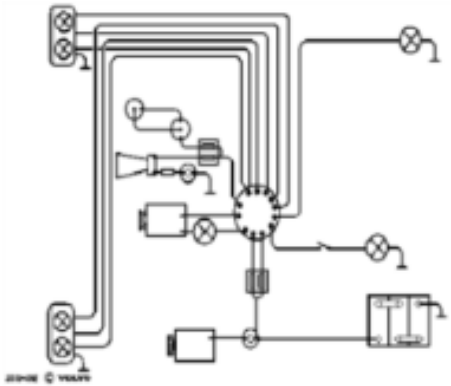
Vehicle sophistication

Mechanics

Attack benefits

Insignificant

EE architecture complexity



Battery, cables, switches, light bulbs, radio

Attack surfaces

Cable cut
Tampered radio signal

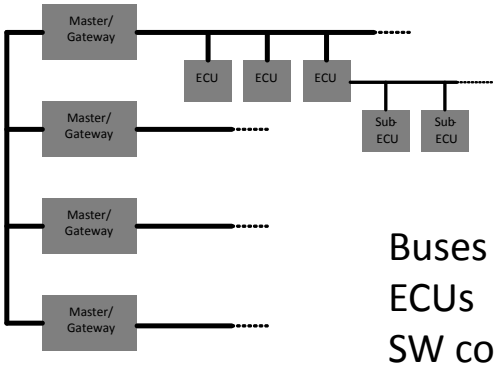
Vehicle sophistication

Electronics

Attack benefits

Subsystem/subnet manipulation and control
Access to confidential subsystem data

EE architecture complexity



Buses
ECUs
SW controlled sensing and actuation

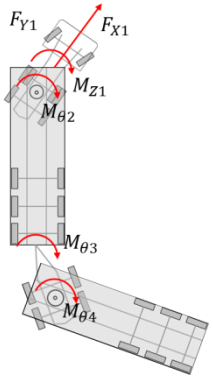
Attack surfaces

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

Vehicle sophistication

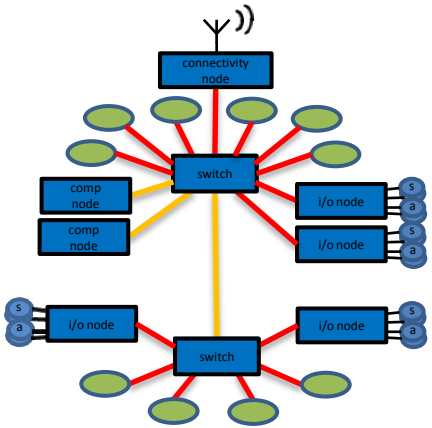
Data centric

Attack benefits



Vehicle manipulation and control
Access to confidential vehicle data

EE architecture complexity



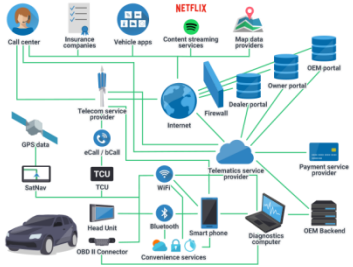
Networks
Centralised computation

Attack surfaces

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

Ethernet networks,
Vehicle control on wireless interfaces

Vehicle sophistication

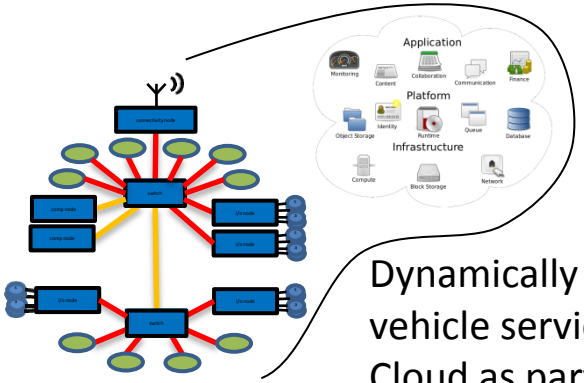


Service centric

Attack benefits

Fleet manipulation and control
Access to confidential fleet data

EE architecture complexity

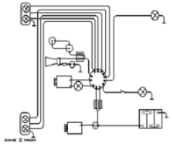
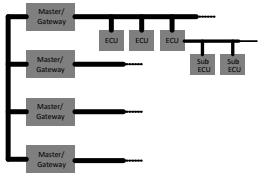
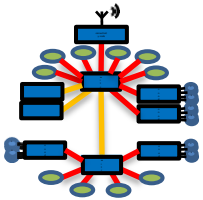
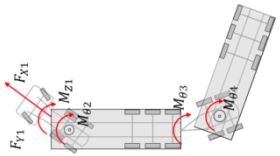
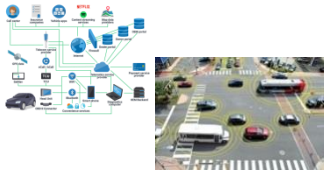
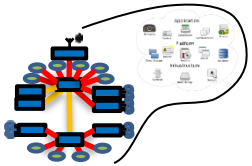


Dynamically deployable vehicle services
Cloud as part of the vehicle

Attack surfaces

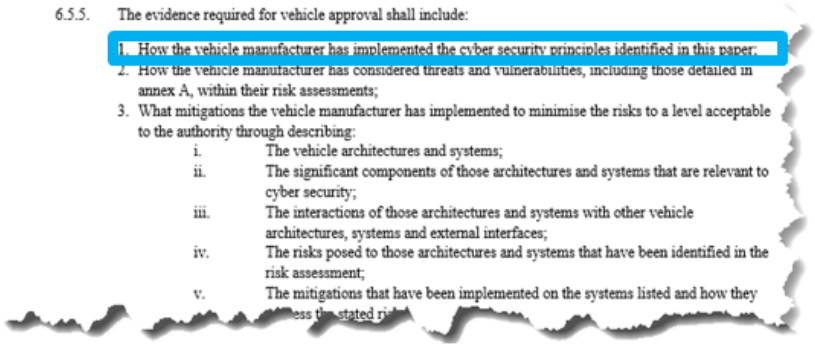
Cable cut
Tampered radio signal
CAN buses
OBD port
Data on wireless interfaces
Ethernet networks,
Vehicle control on wireless interfaces

Cloud infrastructure

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**

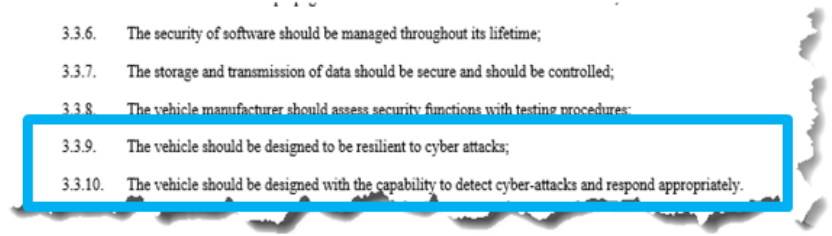
Puts requirements on cybersecurity for type approval



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

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.

Challenges ahead!

Let’s embrace them together.

- Process, methods and tools
- Impact on functional safety
- Protection mechanisms
- Intrusion detection
- Recovery mechanisms
- Post-event analysis

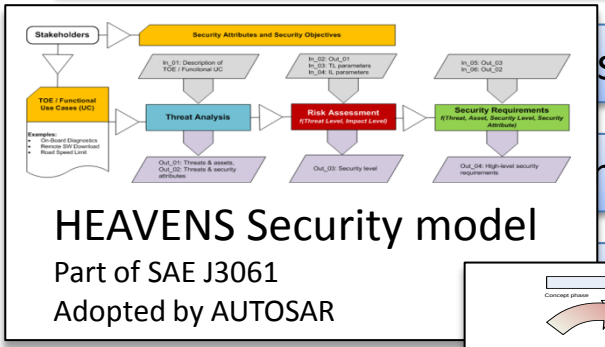
Process, methods and tools

Impact on functional safety

Post-event

HEAVENS

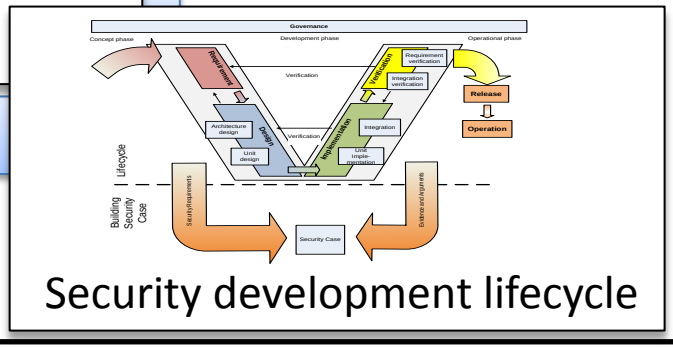
Interplay between functional safety and cybersecurity



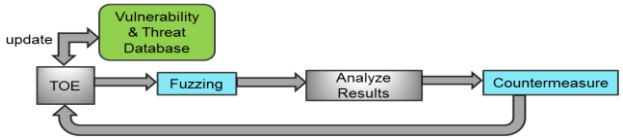
HEAVENS Security model

Part of SAE J3061

Adopted by AUTOSAR



Security development lifecycle



Security testing and evaluation

Attack Surface Analysis & Attack Tree

Static Analysis Tools Evaluation

MISRA C and CERT C Coding Guidelines

Vulnerability Assessment and Fuzzing

Security terminology

Adopted by AUTOSAR

Process, methods and tools

Impact on functional safety

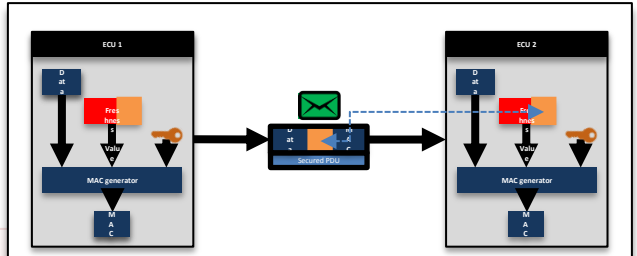
Protection mechanisms

Intrusion detection

Recovery mechanisms

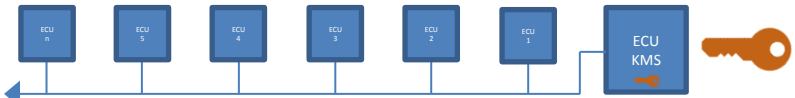
HEAVENS

HoliSec

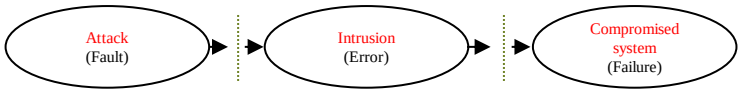


Security mechanisms

Secure vehicle diagnostics
Secure communication
Intrusion detection



Cryptographic support and key management



Interplay between safety, security and privacy

Secure development & governance

Secure software and system design
Secure software verification and validation

Process, methods and tools

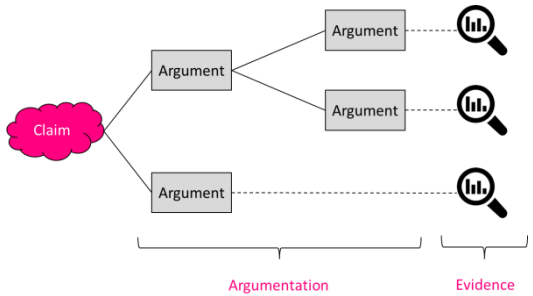
Impact on functional safety

Protection mechanisms

HEAVENS

HoliSec

CASUS

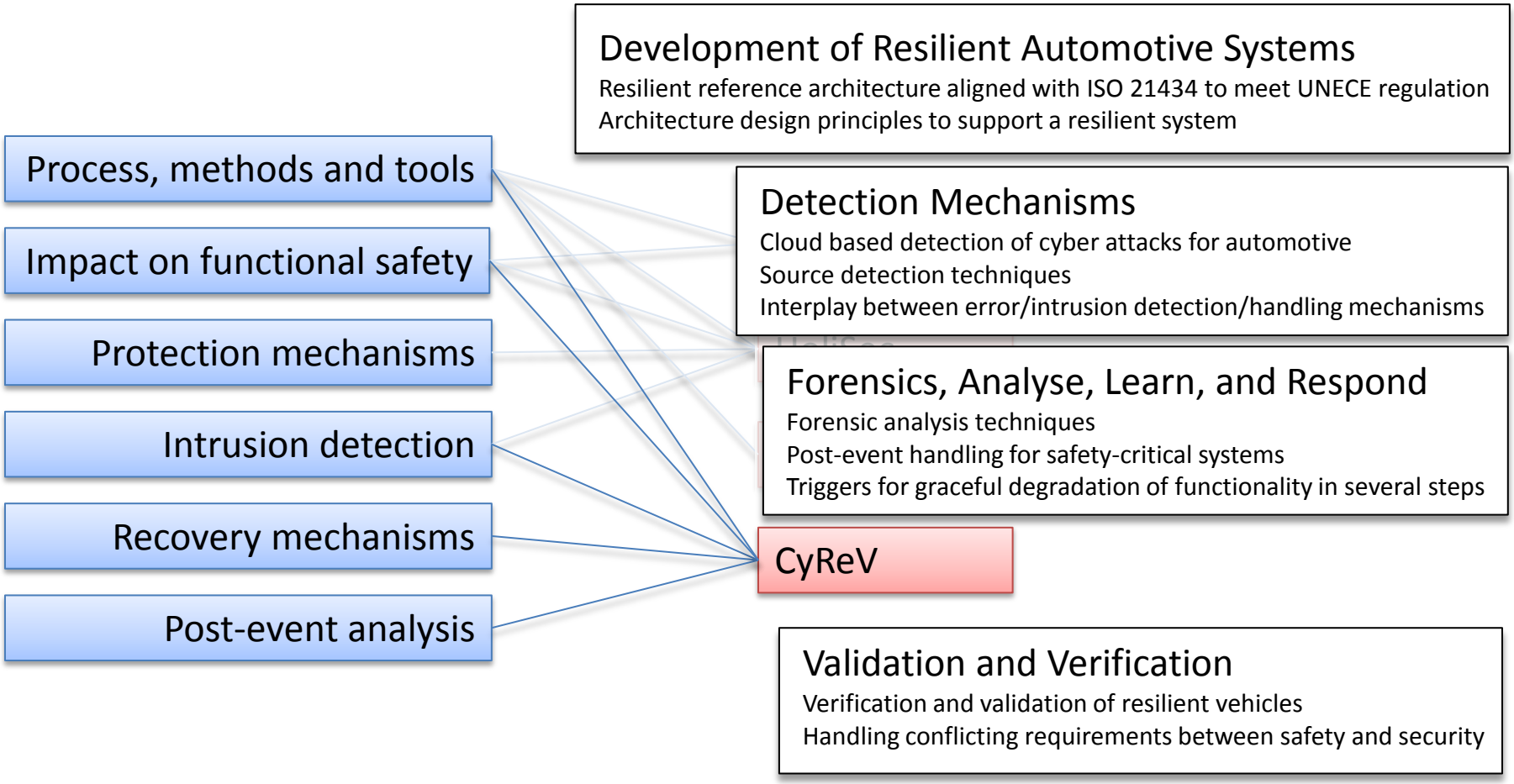


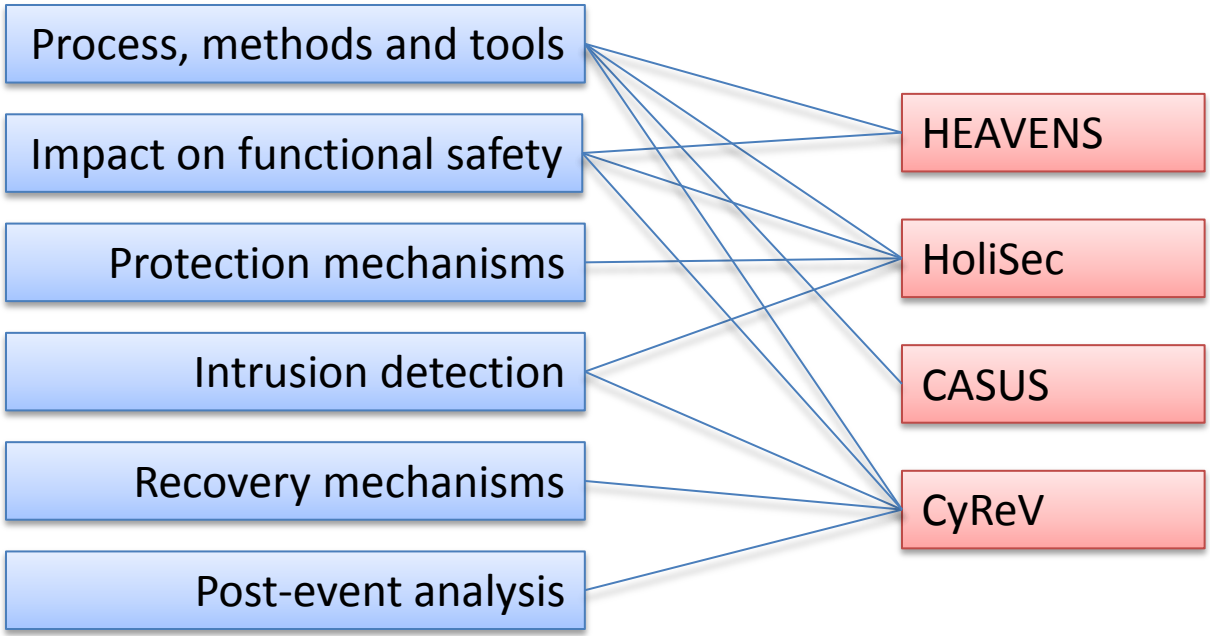
Security assurance cases

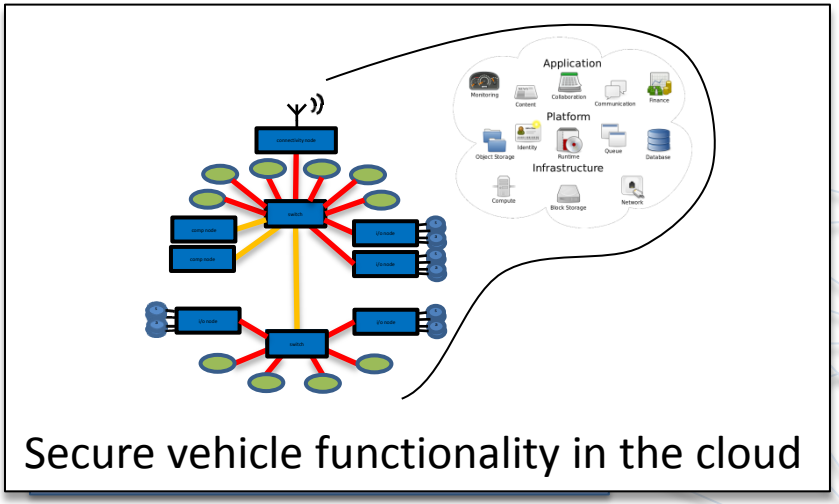
Methodology

Library of patterns, according to security levels

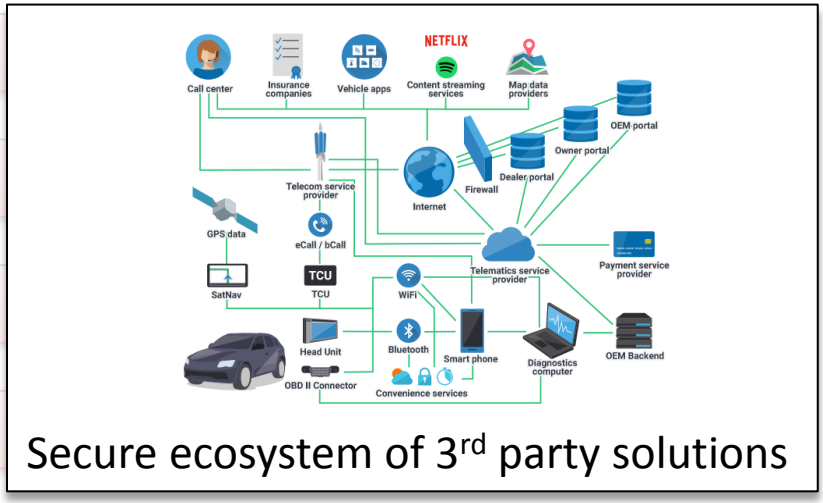
Integrate agile development methods and continuous delivery


Development of Resilient Automotive Systems
Resilient reference architecture aligned with ISO 21434 to meet UNECE regulation
Architecture design principles to support a resilient system
Process, methods and tools
Impact on functional safety
Protection mechanisms
Intrusion detection
Recovery mechanisms
Post-event analysis
Detection Mechanisms
Cloud based detection of cyber attacks for automotive
Source detection techniques
Interplay between error/intrusion detection/handling mechanisms
Forensics, Analyse, Learn, and Respond
Forensic analysis techniques
Post-event handling for safety-critical systems
Triggers for graceful degradation of functionality in several steps
CyReV
Validation and Verification
Verification and validation of resilient vehicles
Handling conflicting requirements between safety and security


Process, methods and tools
Impact on functional safety
Protection mechanisms
Intrusion detection
Recovery mechanisms
Post-event analysis
HEAVENS
HoliSec
CASUS
CyReV



Secure vehicle functionality in the cloud



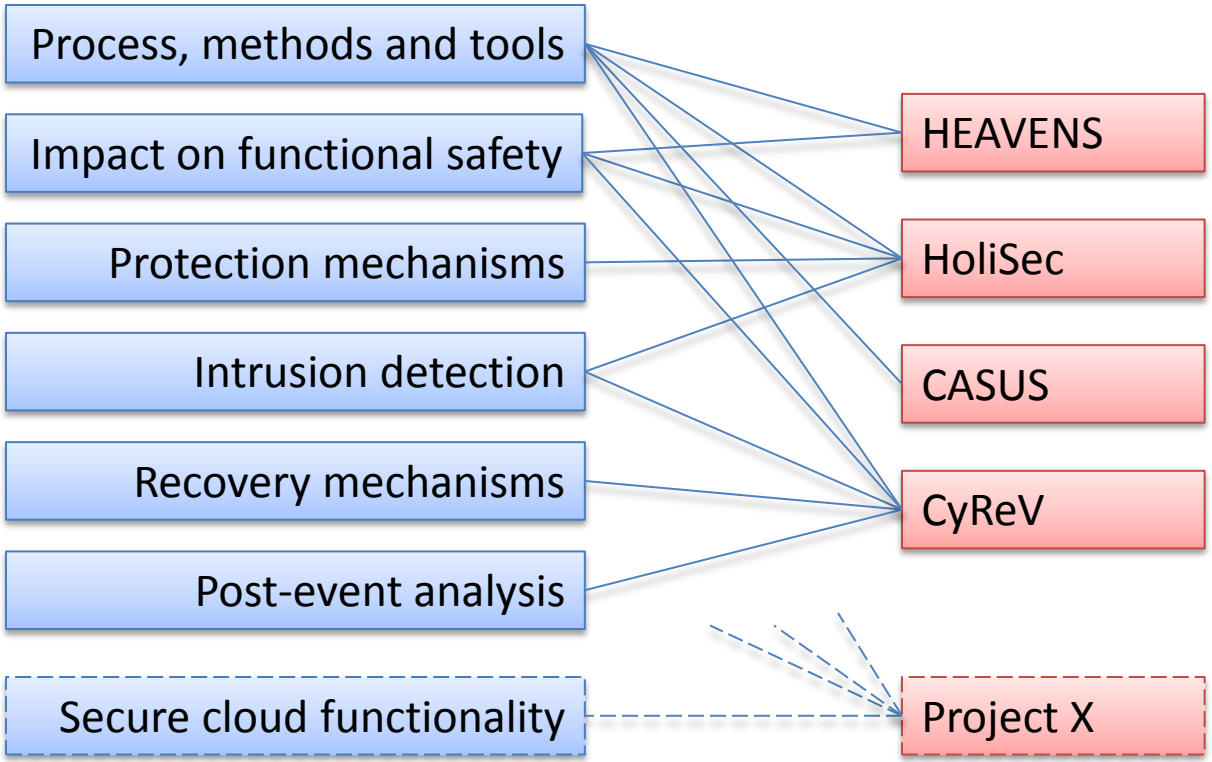
Secure ecosystem of 3rd party solutions

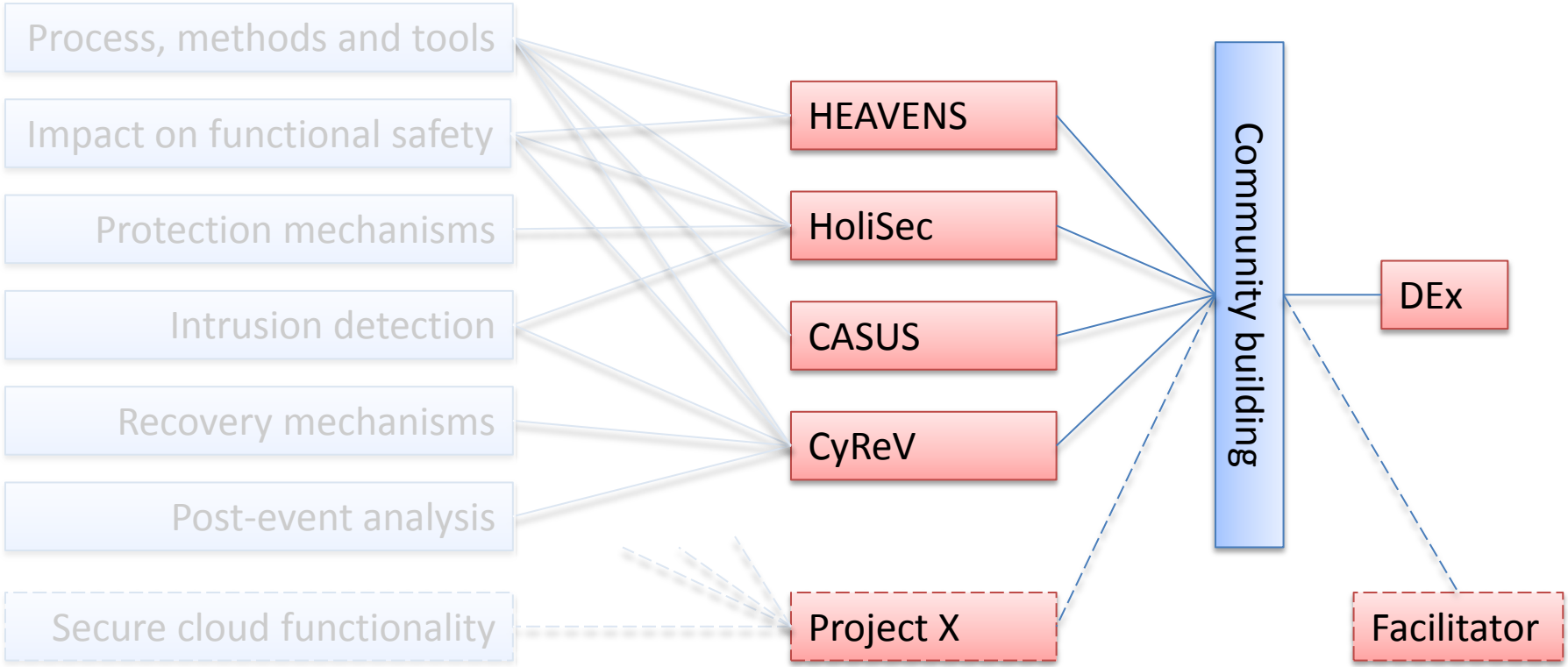
Recovery mechanisms

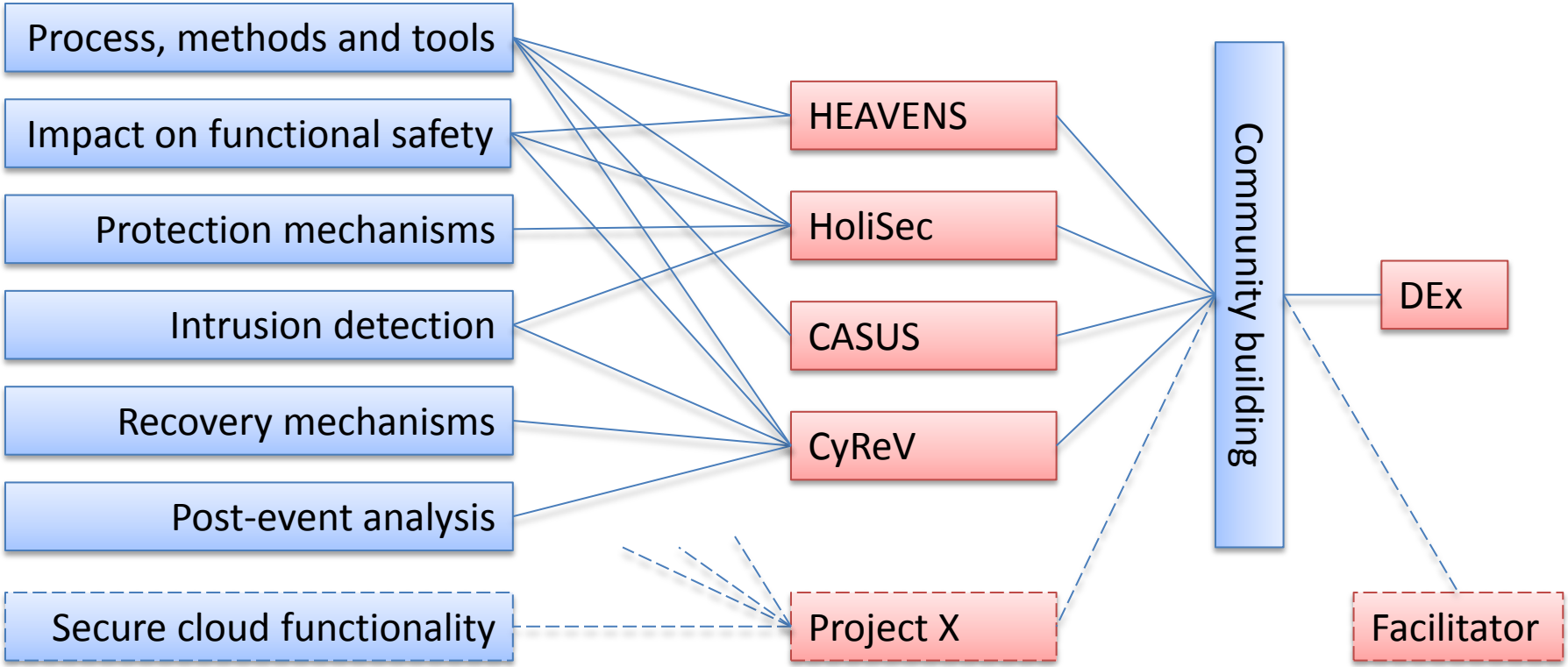
Post-event analysis

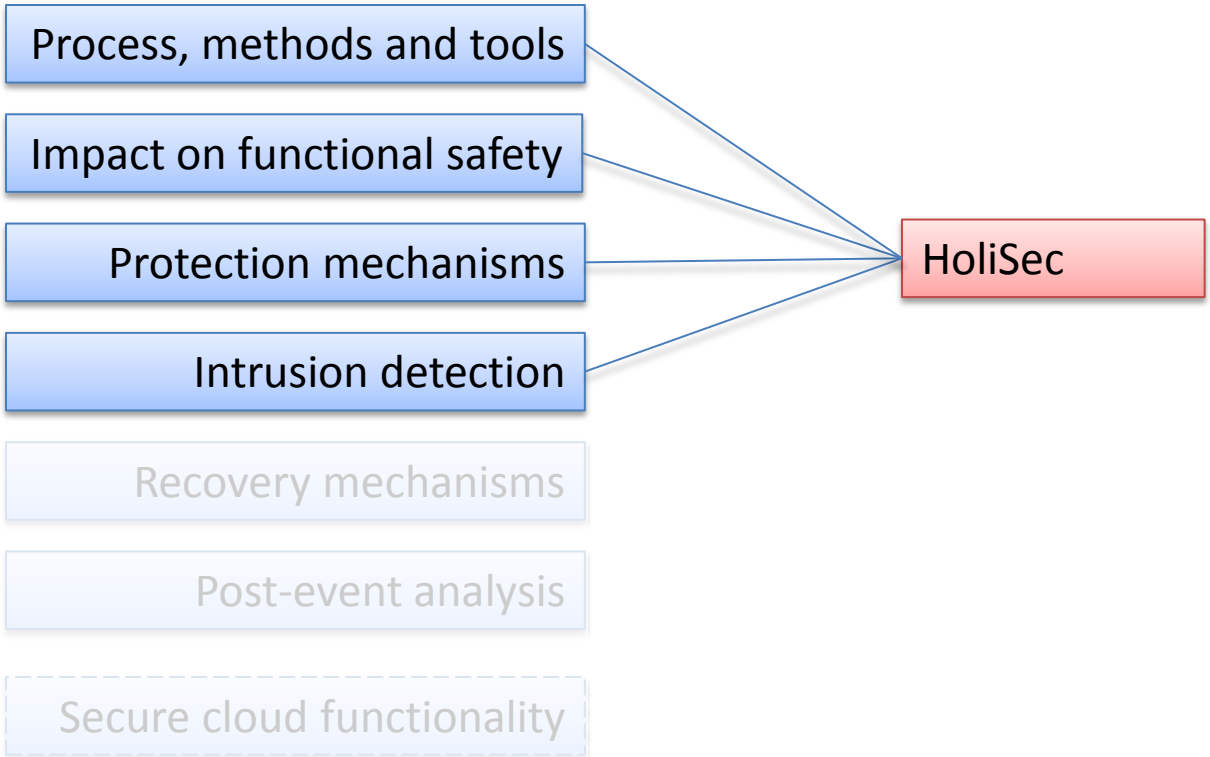
Secure cloud functionality

Project X


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


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
DEx
Facilitator


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
DEx
Facilitator


Process, methods and tools
Impact on functional safety
Protection mechanisms
Intrusion detection
Recovery mechanisms
Post-event analysis
Secure cloud functionality
HoliSec

Process, methods and tools

Impact on functional safety

Protection mechanisms

Intrusion detection

Recovery mechanisms

Post-event analysis

Secure cloud functionality

Time	Title	Presenter
09.00	External Research Collaboration for Cybersecurity Work at Volvo Group – Where Are We Heading?	Daniel Karlsson, Volvo Group
09.30	Intrusion Detection for In-vehicle Networks: Reflection on Practical Challenges and the Road Ahead	Nasser Nowdehi, Volvo Cars David Thiringer, Chalmers Sebastian Kvarnström, Chalmers
10.15	ESCAR 2018 recap	Tomas Olovsson, Chalmers
11.00	AUTOSAR Secured On-Board Communication: Introduction to AUTOSAR'S SecOC Module, and Key Management Techniques Proposal	Bashar Dawood, Arccore
11.15	AUTOSAR Secure Onboard Communication: Goals and Reasoning Behind the Freshness Design	Christian Sandberg, Volvo Group
11.30	AUTOSAR Secured On-Board Communication: Testing SecOC with Various Communication Methodology	Kaushik Naik, Volvo Group Brian Katumba, Volvo Group
11.45	Lunch break and Demos (coffee and sandwiches will be served)	
12.45	State of The Art of Secure Vehicular Communication and Design	Thomas Rosenstatter, Chalmers Alojscha Lautenbach, Chalmers Nasser Nowdehi, Volvo Cars
13.30	Evolving Threat Analysis Techniques to Catch What Matters	Katja Tuma, Gothenburg University Mathias Widman, Volvo Group
14.15	Interplay Between Safety and Security	Peter Folkesson, RISE
15.00	Bug Bounties In the Automotive Domain – The Past and the Road Ahead	Ana Magazinius, RISE Jonas Magazinius, Assured

Process, methods and tools

Impact on functional safety

Protection mechanisms

Intrusion detection

Recovery mechanisms

Post-event analysis

Secure cloud functionality

Time	Title	Presenter
09.00	External Research Collaboration for Cybersecurity Work at Volvo Group – Where Are We Heading?	Daniel Karlsson, Volvo Group
09.30	Intrusion Detection for In-vehicle Networks: Reflection on Practical Challenges and the Road Ahead	Nasser Nowdehi, Volvo Cars David Thiringer, Chalmers Sebastian Kvarnström, Chalmers
10.15	ESCAR 2018 recap	Tomas Olovsson, Chalmers
11.00	AUTOSAR Secured On-Board Communication: Introduction to AUTOSAR'S SecOC Module, and Key Management Techniques Proposal	Bashar Dawood, Arccore
11.15	AUTOSAR Secure Onboard Communication: Goals and Reasoning Behind the Freshness Design	Christian Sandberg, Volvo Group
11.30	AUTOSAR Secured On-Board Communication: Testing SecOC with Various Communication Methodology	Kaushik Naik, Volvo Group Brian Katumba, Volvo Group
11.45	Lunch break and Demos (coffee and sandwiches will be served)	
12.45	State of The Art of Secure Vehicular Communication and Design	Thomas Rosenstatter, Chalmers Alojscha Lautenbach, Chalmers Nasser Nowdehi, Volvo Cars
13.30	Evolving Threat Analysis Techniques to Catch What Matters	Katja Tuma, Gothenburg University Mathias Widman, Volvo Group
14.15	Interplay Between Safety and Security	Peter Folkesson, RISE
15.00	Bug Bounties In the Automotive Domain – The Past and the Road Ahead	Ana Magazinius, RISE Jonas Magazinius, Assured

Process, methods and tools

Impact on functional safety

Protection mechanisms

Intrusion detection

Recovery mechanisms

Post-event analysis

Secure cloud functionality

Time	Title	Presenter
09.00	External Research Collaboration for Cybersecurity Work at Volvo Group – Where Are We Heading?	Daniel Karlsson, Volvo Group
09.30	Intrusion Detection for In-vehicle Networks: Reflection on Practical Challenges and the Road Ahead	Nasser Nowdehi, Volvo Cars David Thiringer, Chalmers Sebastian Kvarnström, Chalmers
10.15	ESCAR 2018 recap	Tomas Olovsson, Chalmers
11.00	AUTOSAR Secured On-Board Communication: Introduction to AUTOSAR'S SecOC Module, and Key Management Techniques Proposal	Bashar Dawood, Arccore
11.15	AUTOSAR Secure Onboard Communication: Goals and Reasoning Behind the Freshness Design	Christian Sandberg, Volvo Group
11.30	AUTOSAR Secured On-Board Communication: Testing SecOC with Various Communication Methodology	Kaushik Naik, Volvo Group Brian Katumba, Volvo Group
11.45	Lunch break and Demos (coffee and sandwiches will be served)	
12.45	State of The Art of Secure Vehicular Communication and Design	Thomas Rosenstatter, Chalmers Alojscha Lautenbach, Chalmers Nasser Nowdehi, Volvo Cars
13.30	Evolving Threat Analysis Techniques to Catch What Matters	Katja Tuma, Gothenburg University Mathias Widman, Volvo Group
14.15	Interplay Between Safety and Security	Peter Folkesson, RISE
15.00	Bug Bounties In the Automotive Domain – The Past and the Road Ahead	Ana Magazinius, RISE Jonas Magazinius, Assured

Process, methods and tools

Impact on functional safety

Protection mechanisms

Intrusion detection

Recovery mechanisms

Post-event analysis

Secure cloud functionality

Time	Title	Presenter
09.00	External Research Collaboration for Cybersecurity Work at Volvo Group – Where Are We Heading?	Daniel Karlsson, Volvo Group
09.30	Intrusion Detection for In-vehicle Networks: Reflection on Practical Challenges and the Road Ahead	Nasser Nowdehi, Volvo Cars David Thiringer, Chalmers Sebastian Kvarnström, Chalmers
10.15	ESCAR 2018 recap	Tomas Olovsson, Chalmers
11.00	AUTOSAR Secured On-Board Communication: Introduction to AUTOSAR'S SecOC Module, and Key Management Techniques Proposal	Bashar Dawood, Arccore
11.15	AUTOSAR Secure Onboard Communication: Goals and Reasoning Behind the Freshness Design	Christian Sandberg, Volvo Group
11.30	AUTOSAR Secured On-Board Communication: Testing SecOC with Various Communication Methodology	Kaushik Naik, Volvo Group Brian Katumba, Volvo Group
11.45	Lunch break and Demos (coffee and sandwiches will be served)	
12.45	State of The Art of Secure Vehicular Communication and Design	Thomas Rosenstatter, Chalmers Alojscha Lautenbach, Chalmers Nasser Nowdehi, Volvo Cars
13.30	Evolving Threat Analysis Techniques to Catch What Matters	Katja Tuma, Gothenburg University Mathias Widman, Volvo Group
14.15	Interplay Between Safety and Security	Peter Folkesson, RISE
15.00	Bug Bounties In the Automotive Domain – The Past and the Road Ahead	Ana Magazinius, RISE Jonas Magazinius, Assured

Process, methods and tools

Impact on functional safety

Protection mechanisms

Intrusion detection

Recovery mechanisms

Post-event analysis

Secure cloud functionality

Time	Title	Presenter
09.00	External Research Collaboration for Cybersecurity Work at Volvo Group – Where Are We Heading?	Daniel Karlsson, Volvo Group
09.30	Intrusion Detection for In-vehicle Networks: Reflection on Practical Challenges and the Road Ahead	Nasser Nowdehi, Volvo Cars David Thiringer, Chalmers Sebastian Kvarnström, Chalmers
10.15	ESCAR 2018 recap	Tomas Olovsson, Chalmers
11.00	AUTOSAR Secured On-Board Communication: Introduction to AUTOSAR'S SecOC Module, and Key Management Techniques Proposal	Bashar Dawood, Arccore
11.15	AUTOSAR Secure Onboard Communication: Goals and Reasoning Behind the Freshness Design	Christian Sandberg, Volvo Group
11.30	AUTOSAR Secured On-Board Communication: Testing SecOC with Various Communication Methodology	Kaushik Naik, Volvo Group Brian Katumba, Volvo Group
11.45	Lunch break and Demos (coffee and sandwiches will be served)	
12.45	State of The Art of Secure Vehicular Communication and Design	Thomas Rosenstatter, Chalmers Alojscha Lautenbach, Chalmers Nasser Nowdehi, Volvo Cars
13.30	Evolving Threat Analysis Techniques to Catch What Matters	Katja Tuma, Gothenburg University Mathias Widman, Volvo Group
14.15	Interplay Between Safety and Security	Peter Folkesson, RISE
15.00	Bug Bounties In the Automotive Domain – The Past and the Road Ahead	Ana Magazinius, RISE Jonas Magazinius, Assured

Process, methods and tools

Impact on functional safety

Protection mechanisms

Intrusion detection

Recovery mechanisms

Post-event analysis

Secure cloud functionality

Time	Title	Presenter
09.00	External Research Collaboration for Cybersecurity Work at Volvo Group – Where Are We Heading?	Daniel Karlsson, Volvo Group
09.30	Intrusion Detection for In-vehicle Networks: Reflection on Practical Challenges and the Road Ahead	Nasser Nowdehi, Volvo Cars David Thiringer, Chalmers Sebastian Kvarnström, Chalmers
10.15	ESCAR 2018 recap	Tomas Olovsson, Chalmers
11.00	AUTOSAR Secured On-Board Communication: Introduction to AUTOSAR'S SecOC Module, and Key Management Techniques Proposal	Bashar Dawood, Arccore
11.15	AUTOSAR Secure Onboard Communication: Goals and Reasoning Behind the Freshness Design	Christian Sandberg, Volvo Group
11.30	AUTOSAR Secured On-Board Communication: Testing SecOC with Various Communication Methodology	Kaushik Naik, Volvo Group Brian Katumba, Volvo Group
11.45	Lunch break and Demos (coffee and sandwiches will be served)	
12.45	State of The Art of Secure Vehicular Communication and Design	Thomas Rosenstatter, Chalmers Alojscha Lautenbach, Chalmers Nasser Nowdehi, Volvo Cars
13.30	Evolving Threat Analysis Techniques to Catch What Matters	Katja Tuma, Gothenburg University Mathias Widman, Volvo Group
14.15	Interplay Between Safety and Security	Peter Folkesson, RISE
15.00	Bug Bounties In the Automotive Domain – The Past and the Road Ahead	Ana Magazinius, RISE Jonas Magazinius, Assured

Process, methods and tools

Impact on functional safety

Protection mechanisms

Intrusion detection

Recovery mechanisms

Post-event analysis

Secure cloud functionality

Time	Title	Presenter
09.00	External Research Collaboration for Cybersecurity Work at Volvo Group – Where Are We Heading?	Daniel Karlsson, Volvo Group
09.30	Intrusion Detection for In-vehicle Networks: Reflection on Practical Challenges and the Road Ahead	Nasser Nowdehi, Volvo Cars David Thiringer, Chalmers Sebastian Kvarnström, Chalmers
10.15	ESCAR 2018 recap	Tomas Olovsson, Chalmers
11.00	AUTOSAR Secured On-Board Communication: Introduction to AUTOSAR'S SecOC Module, and Key Management Techniques Proposal	Bashar Dawood, Arccore
11.15	AUTOSAR Secure Onboard Communication: Goals and Reasoning Behind the Freshness Design	Christian Sandberg, Volvo Group
11.30	AUTOSAR Secured On-Board Communication: Testing SecOC with Various Communication Methodology	Kaushik Naik, Volvo Group Brian Katumba, Volvo Group
11.45	Lunch break and Demos (coffee and sandwiches will be served)	
12.45	State of The Art of Secure Vehicular Communication and Design	Thomas Rosenstatter, Chalmers Alojscha Lautenbach, Chalmers Nasser Nowdehi, Volvo Cars
13.30	Evolving Threat Analysis Techniques to Catch What Matters	Katja Tuma, Gothenburg University Mathias Widman, Volvo Group
14.15	Interplay Between Safety and Security	Peter Folkesson, RISE
15.00	Bug Bounties In the Automotive Domain – The Past and the Road Ahead	Ana Magazinius, RISE Jonas Magazinius, Assured

Process, methods and tools

Impact on functional safety

Protection mechanisms

Intrusion detection

Recovery mechanisms

Post-event analysis

Secure cloud functionality

Time	Title	Presenter
09.00	External Research Collaboration for Cybersecurity Work at Volvo Group – Where Are We Heading?	Daniel Karlsson, Volvo Group
09.30	Intrusion Detection for In-vehicle Networks: Reflection on Practical Challenges and the Road Ahead	Nasser Nowdehi, Volvo Cars David Thiringer, Chalmers Sebastian Kvarnström, Chalmers
10.15	ESCAR 2018 recap	Tomas Olovsson, Chalmers
11.00	AUTOSAR Secured On-Board Communication: Introduction to AUTOSAR'S SecOC Module, and Key Management Techniques Proposal	Bashar Dawood, Arccore
11.15	AUTOSAR Secure Onboard Communication: Goals and Reasoning Behind the Freshness Design	Christian Sandberg, Volvo Group
11.30	AUTOSAR Secured On-Board Communication: Testing SecOC with Various Communication Methodology	Kaushik Naik, Volvo Group Brian Katumba, Volvo Group
11.45	Lunch break and Demos (coffee and sandwiches will be served)	
12.45	State of The Art of Secure Vehicular Communication and Design	Thomas Rosenstatter, Chalmers Alojscha Lautenbach, Chalmers Nasser Nowdehi, Volvo Cars
13.30	Evolving Threat Analysis Techniques to Catch What Matters	Katja Tuma, Gothenburg University Mathias Widman, Volvo Group
14.15	Interplay Between Safety and Security	Peter Folkesson, RISE
15.00	Bug Bounties In the Automotive Domain – The Past and the Road Ahead	Ana Magazinius, RISE Jonas Magazinius, Assured

Process, methods and tools

Impact on functional safety

Protection mechanisms

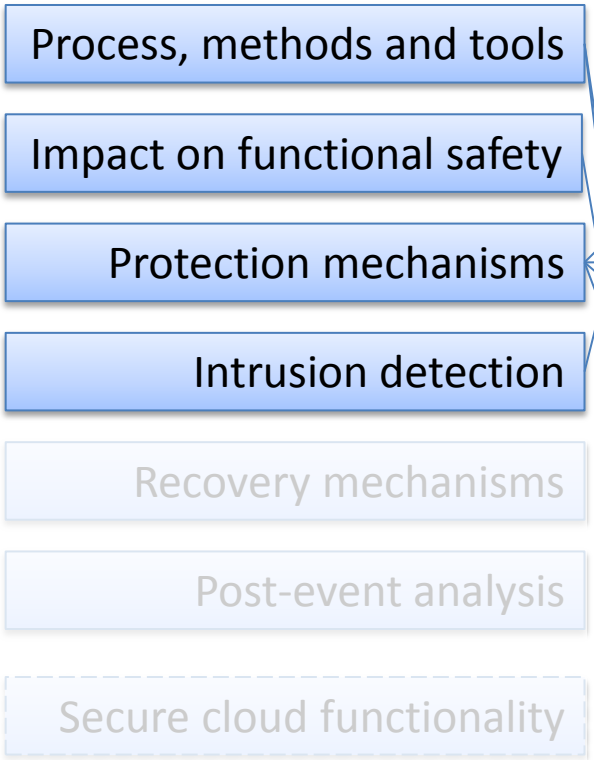
Intrusion detection

Recovery mechanisms

Post-event analysis

Secure cloud functionality

Time	Title	Presenter
09.00	External Research Collaboration for Cybersecurity Work at Volvo Group – Where Are We Heading?	Daniel Karlsson, Volvo Group
09.30	Intrusion Detection for In-vehicle Networks: Reflection on Practical Challenges and the Road Ahead	Nasser Nowdehi, Volvo Cars David Thiringer, Chalmers Sebastian Kvarnström, Chalmers
10.15	ESCAR 2018 recap	Tomas Olovsson, Chalmers
11.00	AUTOSAR Secured On-Board Communication: Introduction to AUTOSAR'S SecOC Module, and Key Management Techniques Proposal	Bashar Dawood, Arccore
11.15	AUTOSAR Secure Onboard Communication: Goals and Reasoning Behind the Freshness Design	Christian Sandberg, Volvo Group
11.30	AUTOSAR Secured On-Board Communication: Testing SecOC with Various Communication Methodology	Kaushik Naik, Volvo Group Brian Katumba, Volvo Group
11.45	Lunch break and Demos (coffee and sandwiches will be served)	
12.45	State of The Art of Secure Vehicular Communication and Design	Thomas Rosenstatter, Chalmers Alojscha Lautenbach, Chalmers Nasser Nowdehi, Volvo Cars
13.30	Evolving Threat Analysis Techniques to Catch What Matters	Katja Tuma, Gothenburg University Mathias Widman, Volvo Group
14.15	Interplay Between Safety and Security	Peter Folkesson, RISE
15.00	Bug Bounties In the Automotive Domain – The Past and the Road Ahead	Ana Magazinius, RISE Jonas Magazinius, Assured



Time	Title	Presenter
09.00	External Research Collaboration for Cybersecurity Work at Volvo Group – Where Are We Heading?	Daniel Karlsson, Volvo Group
09.30	Intrusion Detection for In-vehicle Networks: Reflection on Practical Challenges and the Road Ahead	Nasser Nowdehi, Volvo Cars David Thiringer, Chalmers Sebastian Kvarnström, Chalmers
10.15	ESCAR 2018 recap	Tomas Olovsson, Chalmers
11.00	AUTOSAR Secured On-Board Communication: Introduction to AUTOSAR'S SecOC Module, and Key Management Techniques Proposal	Bashar Dawood, Arccore
11.15	AUTOSAR Secure Onboard Communication: Goals and Reasoning Behind the Freshness Design	Christian Sandberg, Volvo Group
11.30	AUTOSAR Secured On-Board Communication: Testing SecOC with Various Communication Methodology	Kaushik Naik, Volvo Group Brian Katumba, Volvo Group
11.45	Lunch break and Demos (coffee and sandwiches will be served)	
12.45	State of The Art of Secure Vehicular Communication and Design	Thomas Rosenstatter, Chalmers Alojscha Lautenbach, Chalmers Nasser Nowdehi, Volvo Cars
13.30	Evolving Threat Analysis Techniques to Catch What Matters	Katja Tuma, Gothenburg University Mathias Widman, Volvo Group
14.15	Interplay Between Safety and Security	Peter Folkesson, RISE
15.00	Bug Bounties In the Automotive Domain – The Past and the Road Ahead	Ana Magazinius, RISE Jonas Magazinius, Assured

HoliSec

Holistic Approach to Improve Data Security

Thank you for your attention!