Integrated Development of Safety and Security

C. Ebert and E. Metzker, Vector
M. Brasse, Hella

Agenda

Welcome
Motivation: Safety Meets Security
Practical Guidance
Hella Case Study
Conclusions and Outlook
Welcome

Vector: Comprehensive Portfolio for Security and Safety

Vector Cyber Security and Safety Solutions

- Security and Safety Consulting
- AUTOSAR Basic Software
- HW based Security
- Tools (PLM, Architecture, Test, Diagnosis etc.)

Engineering Services for Safety and Security
Welcome

Vector Consulting Services

▸ ...supports clients worldwide

▸ ...improving product development, IT and providing interim management

▸ ...offers with the Vector Group a portfolio of tools, software components and services

▸ ...is as Vector Group globally present with 1500 employees and well over 300 Mio. € sales

▸ ...continuously hiring

▸ www.vector.com/consulting
Welcome

Hella Group, Overview

- Partner of the automotive industry and the aftermarket for over 100 years
- Global family-owned company with more than 100 locations in over 35 countries
- Sales of € 5.8 billion FY 2014/2015
- Approx. 32,000 employees worldwide, thereof over 6,000 in Research & Development
- One of the top 40 automotive suppliers in the world and one of the 100 largest German industrial companies

<table>
<thead>
<tr>
<th>Business Segments</th>
<th>Automotive</th>
<th>Aftermarket</th>
<th>Special Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lighting</td>
<td>Headlamps</td>
<td>Parts</td>
<td>Special Original Equipment</td>
</tr>
<tr>
<td></td>
<td>Rear Lamps</td>
<td>- Wear Parts</td>
<td>- Vehicle Diagnostic &amp; Vehicle Data</td>
</tr>
<tr>
<td></td>
<td>Small Lamps</td>
<td>- Spare Parts</td>
<td>- Air Conditioning Service</td>
</tr>
<tr>
<td></td>
<td>Interior Lighting</td>
<td>- Accessories</td>
<td>- Lighting Service</td>
</tr>
<tr>
<td></td>
<td>Lighting Electronics</td>
<td>- Tools</td>
<td>- Battery Service</td>
</tr>
<tr>
<td></td>
<td>Electronics</td>
<td>- Workshop Concepts</td>
<td>- Tools</td>
</tr>
<tr>
<td></td>
<td>Body Electronics</td>
<td>- Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Energy Management</td>
<td>- Technical Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Driver Assistance Systems</td>
<td>- Sales Support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sensors</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Actuators</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Electric Power Steering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Industries</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Street Lighting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Interior Lighting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Industry Lighting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Independent Aftermarket</th>
<th>Wholesale</th>
<th>Workshop Equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Full Range</td>
<td></td>
<td>Vehicle Diagnostic &amp; Vehicle Data</td>
</tr>
<tr>
<td></td>
<td>Parts</td>
<td></td>
<td>Air Conditioning Service</td>
</tr>
<tr>
<td></td>
<td>- Parts</td>
<td></td>
<td>Lighting Service</td>
</tr>
<tr>
<td></td>
<td>- Tools</td>
<td></td>
<td>Battery Service</td>
</tr>
<tr>
<td></td>
<td>- Workshop Concepts</td>
<td></td>
<td>Tools</td>
</tr>
<tr>
<td></td>
<td>- Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Local Branch Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Logistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Sales Support</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7/36 © 2016. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.0 | 2016-09-27
Welcome

Hella Group, Product Portfolio

Light Electronics

Energy Management

Driver Assistance Systems

Body Electronics

Sensors

Actuators

Electrical Power Steering
Agenda

Welcome

- **Motivation: Safety Meets Security**
  - Practical Guidance
  - Hella Case Study
  - Conclusions and Outlook
Motivation: Safety Meets Security

Vector Client Survey on Industry Trends

Safety and security are evolving as a major challenge.

Mid-term challenges:
- Safety and Security
- Efficiency and Cost
- Big Data
- Connectivity
- Innovative Products
- Complexity
- Distributed Development
- Governance
- Others

Current challenges:
- Mid-term challenges
- Safety and Security
- Efficiency and Cost
- Big Data
- Connectivity
- Innovative Products
- Complexity
- Distributed Development
- Governance
- Others

Vector Client Survey 2016. Details: www.vector.com/trends. Sum > 100% because 3 answers per question were allowed. Results from all industries overlap and are thus compiled in this report. Validity big with >4% response rate of 1700 recipients.
Motivation: Safety Meets Security

Different Threats Demand Holistic Systems Engineering

**Functional Safety**
- Goal: Protect health (i.e., inside and outside)
- Risk: Accident
- Governance: ISO 26262, liability, etc.
- Methods:
  - HARA, FTA, FMEA, ...
  - Fail operational, ...
  - Redundancy, ...

**Cyber Security**
- Goal: Protect assets (e.g., safety impact)
- Risk: Attack, exploits
- Governance: ISO 27001, policies, etc.
- Methods:
  - TARA, ...
  - Cryptography, IDIP, ...
  - Key management, ...

**Privacy**
- Goal: Protect personal data
- Risk: Data breach
- Governance: Privacy laws, culture impacts
- Methods:
  - TARA, ...
  - Cryptography, ...
  - Explicit consent, ...

Liability ➔ Risk management ➔ Holistic systems engineering
Motivation: Safety Meets Security

Connectivity + Complexity ➔ Cyber Attacks ➔ Safety Risks

OEM ➔ Suppliers

Eavesdropping, Data leakage

Command injection, data corruption, back doors

OB D

Man in the middle attacks

Password attacks

Physical attacks, Sensor confusion

Rogue clients, malware

Public Clouds

4G LTE

Application vulnerabilities

Public Clouds

Service Provider

ITS Operator

© 2016. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.0 | 2016-09-27
Security and Safety Standards Evolve in Parallel

Motivation: Safety Meets Security

Functional Safety (IEC 61508, ISO 26262)

- Hazard and risk analysis
- Functions and risk mitigation
- Safety engineering

ISO 26262 ed.2 CD will not comprehensively address security, but will refer to and include shared methods, such as TARA

+ Security (ISO 27001, ISO 15408, ISO TC22 new standard; SAE J3061)

- Threat and risk analysis
- Abuse, misuse, confuse cases
- Security engineering

Security and Safety are interacting and demand holistic systems engineering

For fast start security engineering should be connected to safety framework
Motivation: Safety Meets Security

Safety and Security must be addressed in parallel

Innovative functionality...
- Autonomous driving and energy efficiency
- Distributed systems
- External interfaces (V2X; vehicle as IP node)
- Complex feature interaction

... Drives new challenges
- New 3-tier automotive architecture
- Functional development
- Fail-safe and fail-operational behaviors
- Safety-critical functions must be secured against external and internal attacks
- Cost-effective development, evolution and support over the entire life-cycle

Need to efficiently and effectively implement quality requirements
Welcome
Motivation: Safety Meets Security

- **Practical Guidance**
  Hella Case Study
  Conclusions and Outlook
Integrated Safety and Security Engineering

Safety and Security must be an integrated part of the life-cycle
Analysis for Safety and Security Risks ➔ HARA + TARA

Needs and Constraints
- Platform, Needs
- (Refined) Functions

Requirements
- Safety/Security Goals
- Safety/Security Requirements
- Safety/Security Mechanisms

Work products
- HARA and TARA
- Architecture and Functional Model
- Technical Safety/Security Concept
## Safety/Security Requirements Engineering

<table>
<thead>
<tr>
<th>Activity</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply mature requirements engineering process for quality requirements</td>
<td>▶ Hazard/threat analysis, misuse/abuse/confuse cases, goals and related requirements are part of “normal” requirements engineering</td>
</tr>
<tr>
<td>Elicit and manage safety and security requirements</td>
<td>▶ Assets to be protected and critical functions (“nominal behavior”) are clearly specified</td>
</tr>
<tr>
<td></td>
<td>▶ Traceability is maintained to ensure consistency over the life-cycle</td>
</tr>
<tr>
<td></td>
<td>▶ Test oriented requirements engineering (TORE) facilitates coverage and regressions</td>
</tr>
<tr>
<td>Consider and cover the entire life-cycle</td>
<td>▶ Requirements engineering is a life-cycle activity, not just specs, but covering e.g. regression and service</td>
</tr>
<tr>
<td></td>
<td>▶ Use incident management to enhance requirements</td>
</tr>
<tr>
<td></td>
<td>▶ Ensure each upgrade is in a secured release</td>
</tr>
<tr>
<td></td>
<td>▶ Tool support to increase confidence and reduce effort</td>
</tr>
</tbody>
</table>

Requirements Engineering matters! Many safety/security problems result from incomplete and incorrect specifications
Safety and Security by Design: Separate Concerns
Goal
- Avoid design and code errors which can lead to security exploits

Approach
- Use a hardened OS with secure partitioning
  Avoid embedded Linux due to its complexity and rapid change and thus many security gaps, (e.g. NULL function pointer dereferences, which allow hackers to inject executable code).
- Deploy secure boot strategy
  Starting with first-stage ROM loader with a pre-burned cryptographic key, the next levels are verified before executing to ensure authenticity of each component of the boot
- Apply rigorous static code analysis
  Tools like Coverity, Klocwork or Bauhaus allow security checks, such as NULL pointer dereferences, memory access beyond allocated area, reads of uninitialized objects, buffer and array underflows, resource leaks etc.
- Use modified condition/decision coverage (MC/DC)
  Detect backdoors
Safety and Security by Design: MICROSAR 4.3ff and FBL

Key management, crypto handling

Secure On-Board Communication

Firewall, Intrusion Detection

ASIL A-D hardened

Hardware Trust Anchor (HTA)
Practical Guidance

Verification and Validation

- **V&V Methods and Tools**
  - Static / dynamic code analyzer
  - Encryption cracker
  - Vulnerability scanner
  - Network traffic analyzer / stress tester
  - Hardware debugger
  - Interface scanner
  - Exploit tester
  - Layered fuzzing tester

- **Life Hacking**
  - Penetration testing
  - Attack schemes
  - Governance and social engineering attacks

Test for the known – and for the unknown.
Ensure automatic regression tests are running with each delivery.
Ensure that each deployment satisfies safety case and security requirements

- **Safety**: Safety case is updated, documented and validated
- **Data encryption**: Protection of intellectual property by encryption
- **Authorization**: Protection against unauthorized ECU access
- **Validation**: Safeguarding of data integrity in the flash memory
- **Authentication**: Verification of authenticity through signature methods
Welcome
Motivation: Safety Meets Security
Practical Guidance

- Hella Case Study

Conclusions and Outlook
Hella Case Study

Advanced Driver Assistance System – Overview

ADAS Basic Functions (Use cases)
- Warns driver when vehicle is getting too close to preceding vehicle
- Warns driver if vehicle is leaving the driving lane
- Performs action such as counter-steering or braking if required
Step 1: Define the assets of the system which shall be protected

- A1: Messages received (e.g. steering angle, lane information) or send by the LKA-System (warning message, counter steering request)
- A2: Software of the LKA-System
- A3: Security keys
ADAS – Step 2: Hazard and Threat Analysis

- Identification of attacks should be performed without taking into account potential security mechanisms
  - Assess attack potential (e.g. STRIDE, etc.):
    > Expertise required to perform an attack
    > Available knowledge about the system to perform an attack
    > Window of opportunity required to perform an attack
    > Equipment required to perform an attack
  - Use expert judgment, based on available rating scales

**Attacks:**
- A1-AT1: Messages for braking send are manipulated
- A1-AT2: Messages are replayed

**Threats:**
- A1-AT1-T1: Manipulation of braking message can lead to the vehicle suddenly braking with different damages
- A1-AT2-T1: Replay of warning messages at critical situations can lead to erroneous behavior and massive driver distraction
ADAS – Step 3: Safety-Related Security Goals

Security goals are high level security requirements.

- A1-AT1-T1-SG1: The system shall prevent manipulation of the messages send by the driver assistance system.
- The communication between driver assistance and sensors shall prevent manipulations of messages.
- The MAC shall be calculated by a SHE-compliant hardware trust anchor using the algorithm RSA2048.
- The MAC shall be truncated after x byte.
# Hella Case Study

## ADAS – Step 3: Safety-Related Security Goals

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Platform (TBC)</td>
<td>Ast 2</td>
<td>Braking to prevent collision</td>
<td>A</td>
<td>Tht-1</td>
<td>Driver crashes into preceding car. Passengers in both cars are severely wounded or killed.</td>
<td>Expert</td>
<td>Medium</td>
<td>Sensitive</td>
<td>Bespokes</td>
<td>Low</td>
<td>Life-threatening or fatal injuries</td>
<td>Low</td>
<td>High</td>
<td>No impact</td>
<td>Critical</td>
<td>Medium</td>
<td>SG1</td>
<td>If requested the brakes shall be activated</td>
</tr>
<tr>
<td>2</td>
<td>Platform (TBC)</td>
<td>Ast 2</td>
<td>Braking to prevent collision</td>
<td>I</td>
<td>Tht-2</td>
<td>Braking although not authorized, e.g. &gt; 10 km/h</td>
<td>Expert</td>
<td>Medium</td>
<td>Sensitive</td>
<td>Bespokes</td>
<td>Low</td>
<td>Severe and life threatening injuries</td>
<td>High</td>
<td>High</td>
<td>No impact</td>
<td>Critical</td>
<td>High</td>
<td>SG2</td>
<td>Unauthorized braking shall be avoided.</td>
</tr>
<tr>
<td>3</td>
<td>Platform (TBC)</td>
<td>Ast 1</td>
<td>IPR of functions</td>
<td>C</td>
<td>Tht-3</td>
<td>RCTA function becomes public knowledge</td>
<td>Expert</td>
<td>High</td>
<td>Public</td>
<td>Bespokes</td>
<td>Medium</td>
<td>No injuries</td>
<td>High</td>
<td>No impact</td>
<td>No impact</td>
<td>Critical</td>
<td>High</td>
<td>SG3</td>
<td>RCTA function shall remain secret.</td>
</tr>
</tbody>
</table>
Hella Case Study

ADAS – Step 4: Safety/Security Concept (1/3)

- Braking while driving with speed > 10 km/h
  - OR
    - Deliberate Manipulation
    - Systematic / Random HW Fault
      - Plausibility Checks, e.g. Vehicle Speed, Engine_Status
        - AND
          - Write message to CAN
          - Create correct message on CAN

- Manipulation of Radar Object on CAN Bus
  - OR
    - Overtake Brake ECU
    - Deliberate Manipulation
      - Systematic / Random HW Fault
        - Plausibility Checks, e.g. Vehicle Speed, Engine_Status
          - AND
            - Write message to CAN
            - Create correct message on CAN
**Hella Case Study**

**ADAS – Step 4: Safety/Security Concept (2/3)**

- **Secure Communication**
- **Secure Download**
- **Write message to CAN**
- **Create correct message on CAN**
- **Overtake ECU on same CAN Bus**
- **Create authenticated CAN message**
- **Connection to ECU**
- **Know-How CAN message**
- **Access to Flash**
- **Know-How Firmware**
- **Enter programming Session (0x27)**
- **Flash Firmware on ECU**
- **Secure Diagnostics**
- **AND**
Hella Case Study

ADAS – Step 4: Safety/Security Concept (3/3)

Secure Diagnostics
- No Keys on Diagnostic Tool
- Secure Access with organizational access management and guidelines

Secure Internal Communication
- Efficient encryption and message authentication (e.g., H-MAC)
- Rationality Checks (e.g., Vehicle speed < 10 km/h)

Secure Download
- PKI with RSA-2048
- Closing Programming Interface

Secure Implementation
(e.g. Protected Architecture, Design Rules, Coding Guidelines, Governance, etc)

Reduce likelihood of attack
Agenda

Welcome
Motivation: Safety Meets Security
Practical Guidance
Hella Case Study

Conclusions and Outlook
Conclusions and Outlook

Safety and Security Must Cover the Entire Life-Cycle

Safety / Security by design

Development

- Systems and service engineering methods for embedded and IT
- Scalable techniques for design, upgrades, regressions, services
- Multiple modes of operation (normal, attack, emergency, etc.)

Secure provisioning and governance

Services

Monitoring and upgrades

Operations

Needs for safety and security along the life-cycle:
- Systems and service engineering methods for embedded and IT
- Scalable techniques for design, upgrades, regressions, services
- Multiple modes of operation (normal, attack, emergency, etc.)
Safety and security requirements pose similar challenges

- Failures can create accidents with severe consequences
- Technical solutions matter – but it is primarily about culture
- Joint approach along the supply chain from components to the final product and service is necessary

... but Security is a bit special:

- Complex and expensive to cover the whole system and its lifecycle
- Probabilities don’t matter, attack potential is always 100%
- Necessary competences and methods not yet mature in product development

It needs the ability to think like a Criminal and preemptively act as an Engineer
Thank you for your attention. For more information please contact us.


Vector Consulting Services

Phone +49 711 80670-0
Fax +49 711 80670-444
www.vector.com/consulting
consulting-info@vector.com