Automotive Cybersecurity Webinar

@VectorVCS
Agenda

- Welcome
  - Challenge Cybersecurity
  - Standards for Safety and Security
  - Risk-Oriented Security
  - Systematic Security Engineering
  - Conclusions and Outlook
Welcome

Why Vector Consulting Services?

- **Vector Group** is a global market leader in automotive software, services and engineering tools with over 3,000 employees.

- **Vector Consulting Services** is supporting clients worldwide.
  - **Transformation**
    - Agile Transformation, Efficiency
    - Automotive SPICE
  - **Trust**
    - Safety and Cybersecurity
    - Test Methods, PenTest, Supplier Audits
  - **Technology**
    - E/E Design, AUTOSAR services
    - ALM/PLM, PREEvision introduction
  - **Training**
    - Training, Coaching, Certification
    - Corporate Competence Programs

[www.vector.com/consulting](http://www.vector.com/consulting)
Agenda

Welcome 3

- **Challenge Cybersecurity** 5
  - Standards for Safety and Security 8
  - Risk-Oriented Security 18
  - Systematic Security Engineering 28
  - Conclusions and Outlook 35
Outlook 2020: Risk of Vicious Circle

Vicious circle:
- cost pressure
- lack of competences
- less innovation and quality

Vector provides tailored consulting solutions to keep OEM and suppliers competitive:

Competitiveness – Quality – Innovation
Challenge Cybersecurity

ACES (Autonomy, Connectivity, e-Mobility, Services) ➤ Cyberattacks ➤ Hazards

Cybersecurity will be the major liability risk in the future. Average security gap is detected in 70% of cases by a third party – and will be exploited.
Agenda

Welcome 3
Challenge Cybersecurity 5

- Standards for Safety and Security 8
  Risk-Oriented Security 18
  Systematic Security Engineering 28
  Conclusions and Outlook 35
Cyber Security vs. Functional Safety

- **Functional Safety** is an intrinsic property of a system that performs in a way that does not present an unreasonable risk of injury to humans.

- **Cyber Security** is an intrinsic property of a system that protects itself against intended abuse by an attacker.

- Functional Safety is about random and systematic fault or accidental misuse by the operator.

- Cyber Security is about protection against activities by malicious intent.
Increasing demand for auditable cybersecurity along life-cycle.

**Functional Safety**
- **Goal:** Protect health
- **Risk:** Internal hazards, driven by failures and defects
- **Governance:** ISO 26262 etc.
- **Methods:**
  - HARA, FTA, FMEA, ...
  - Fail operational, ...
  - Redundancy, ...

**Cybersecurity**
- **Goal:** Protect assets
- **Risk:** External threats, driven by humans
- **Governance:** ISO 21434 etc.
- **Methods:**
  - TARA, Def. Coding...
  - Cryptography, ID/IP, ...
  - Key management, ...

**Homologation**
- **Goal:** Protect life and planet
- **Risk:** manipulation, ad-hoc SW changes, inconsistencies
- **Governance:** UNECE etc.
- **Methods:**
  - SUMS, CSMS, ...
  - Impact analysis, ...
  - Traceability, audits, ...
Legal Situation: Product Liability Demands Using Standards

**Functional Safety**
- Generic E/E systems development: IEC 61508
- Automotive functional safety ISO 26262
- Coexistence of quality standards: ISO 26262 refers to shared methods across standards, e.g. TARA
- SOTIF: ISO 21448

**Cybersecurity**
- Product development: ISO 21434 / SAE 3061, (Cybersecurity process and lifecycle activities)
- Enterprise IT Security: ISO 27001 (Security mgmt), TISAX (Trusted Information Security Assessment Exchange)

**Homologation**
- Vehicle cybersecurity and data protection: UNECE WP.29
- Software update management: UNECE WP.29

**Process Maturity:** ISO 330xx
Application of methodological Frameworks Automotive SPICE or CMMI

**Product Development Process:** ISO 9001, ISO/TS 16949

**Product Liability:**
A product, that is put in service, must provide the level of safety which can be expected by general public.
Standards for Safety and Security

Standard ISO 21434: Automotive Cybersecurity

Similar to ISO 26262 strong focus on combining culture, organization and project – but no prescribed methods.
Scope of UNECE comprises all type approval related mandatory regulations

Type approval parameters include: Environment, Theft, Safety, Connectivity, Information Sharing.

- **Environment**: Control units which influence the emission ions, i.e. at least engine control unit.
- **Theft**: Vehicle service protection, e.g. engine control, doors, etc.
- **Safety**: Achievement of safety goals according to the assigned ASIL
- **Availability**: Maintaining availability of vehicle and vehicle functions, in particular during updates
- **Connectivity**: Direct and indirect interfaces to the outside world, e.g. Bluetooth, mobile telephony, OBD, charging etc.
- **Information Sharing**: Control units for internal vehicle communication, e.g. gateways, communication network

Example: ECE R48 Headlight control is an approval parameter. Traceability mandates to show all SW which impacts headlight control.
Standards for Safety and Security

UNECE: Legal Requirements for OEM Cybersecurity and SW Updates

Source: ECE/TRANS/WP.29/GRVA/2019/2
Practice: Establish Efficient Single Master Process

Standards for Safety and Security

There is no Functional Safety without Cybersecurity.

Overlap demands orchestrated process for efficiency and consistency.
Synchronized Safety and Security Demand Holistic Systems Engineering

Process view

Project start

Cybersecurity

Development

Safety

SOP

Product view

Product maturity review gate 1

Product maturity review gate 2

ECU Schematics
ECU Architecture
ECU Layout
ECU FTA
ECU DFMEA
Random hardware failure metric

Product maturity review gate n

Liability ➔ Risk management ➔ Holistic systems engineering
Practical Legal Aspects for Sustainable Safety and Cybersecurity

OEM

- Establish a system-wide safety and security responsibility
- Connect safety and security requirements in their system impact
- Align IT and E/E organizations because both contribute, e.g. key management
- Communicate security strategy and assumptions to your suppliers.
- Ask suppliers to sign a statement "The contractor will observe all relevant standards, laws and legal provisions..."

Supplier

- Demand context information. Security of a subsystem cannot be sustainably secured "out of context".
- Establish OEM-supplier Development-Interface Agreement (DIA) at project start. OEM: overall risk assessment, safety/security concept, interfaces, etc. Supplier: derived safety/security concept, assumptions to OEM, life-cycle deliverables.
- Perform periodic workshops on assumptions that you make to harden your subsystem.

Product liability holds for all products along the supply chain: OEM and supplier.
Agenda

Welcome 3
Challenge Cybersecurity 5
Standards for Safety and Security 8

» **Risk-Oriented Security** 18
 Systematic Security Engineering 28
 Conclusions and Outlook 35
Most security attacks are process and implementation related. They rarely lie within the cryptographic protocols and algorithms.
Secure by Design AND Secure by Life-Cycle

Security by Design
- Promoted by Safety-driven development
- Critical systems should be „secure by design“
- Frontloading with requirements, bottom-up protection and security engineering

„Would you buy a car which will be secured solely by pulled software updates?“

Security by Life-Cycle
- Promoted by experiences in IT and SW-intensive Systems
- Add-on to traditional „security-by-design“ approach
- Counters dynamic changes and evolution of threats and security mechanisms

„Would you buy a car with a weak design that has already been hacked?“

Combine thoughtful and risk-oriented “Security by Design” with fast agile “Security by Life-Cycle”. 
Establish solid traceability from assets to threats to security goals and requirements. Don’t get in paralysis by analysis, as so many companies. Mitigate risks.

= Figure 2 - Requirement generation for cybersecurity relevant items or components, Excerpt from ISO SAE 21434 (Draft DIS)

TARA = Risk Assessment Methodologies in Chapter 8 of ISO SAE 21434 (Draft DIS)
Risk-Oriented Security

First and Pivotal: Determine Assets to be Protected

Consider specific automotive assets derived from Vector extended CIAAG (Confidentiality, Integrity, Availability, Authenticity Governance) scheme.
### Security Properties: CIA/CIAAG

**Security policies**, must be enforced throughout the life-cycle and all operational scenarios.

The **origin** of information (e.g. message, data) or a component (e.g. ECU, firmware) must be verifiable.

Only **authorized access** to protected resources must be possible.

Only **authorized modifications** of information or components must be possible and unauthorized modifications must be **detectable**.

Authorized entities (e.g. hardware modules, software processes, users) must have **proper and timely access** to their data and services.

**CIA properties are mentioned in ISO SAE 21434 (Draft), chapter 3.1.17**
### Determine Necessary Security Level with TARA Results

<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>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ast01</td>
<td>Safety-Mechanisms</td>
<td></td>
<td>Availability</td>
<td>Attacker disables engine control during an overtaking maneuver if system can impact safety-critical functions.</td>
<td>Tha-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Layman</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Not further considered on advice of client because the HU is rated QM with respect to ISO 26262.

### Security Level (SL) vs. Impact Level (IL)

<table>
<thead>
<tr>
<th>Threat Level (TL)</th>
<th>Security Level (SL)</th>
<th>Impact Level (IL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td>1</td>
<td>QM</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>QM</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>QM</td>
<td>Medium</td>
</tr>
<tr>
<td>4</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

- **0** QM Low
- **1** QM Low
- **2** QM Medium
- **3** QM Medium
- **4** Low Medium

**Impact Levels:**
- Low
- Medium
- High
- Critical
## Case Study Powertrain: Threats and Hazards

### Function: Adjust Speed
- **Hazard:** Speed is unintentionally increased during normal operation in cruise control while driving in a city.
- **S/E/C:** S3/E3/C1
- **ASIL:** C

### Function: Change Gears
- **Hazard:** During driving on high speed (Highway) the gear is changing to a higher gear thus reducing acceleration when it is needed during overtaking.
- **S/E/C:** S3/E4/C3
- **ASIL:** C

---

### Relate identified security threats to safety hazard analysis

---

© 2020. Vector Korea IT Inc. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V2.3 | 2020-05-26
## Risk-Oriented Security

**Case Study Powertrain:** From TARA to Safety/Security Concept

### Elements of functional architecture

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Level</td>
<td>Security Goal</td>
</tr>
<tr>
<td>SG05</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>FSR 1</td>
<td>The authenticity and integrity of the user_command signal during reading and transmission shall be assured.</td>
<td>x</td>
</tr>
<tr>
<td>FSR 2</td>
<td>The authenticity and integrity of the authenticity signal during reading and transmission shall be assured.</td>
<td>x</td>
</tr>
<tr>
<td>FSR 3</td>
<td>The authenticity and integrity of the sw_update during reading and transmission shall be assured.</td>
<td>x</td>
</tr>
<tr>
<td>FSR 4</td>
<td>It shall be assured that the signal allow_update generated from the input signals is calculated correctly.</td>
<td>x</td>
</tr>
<tr>
<td>FSR 5</td>
<td>The authenticity and integrity of the allow_update signal during transmission shall be assured.</td>
<td>x</td>
</tr>
<tr>
<td>FSR 6</td>
<td>If an error with regards to authenticity and integrity during reading, transmission or calculation of signals or the actuator status occurs, the system will not install the sw update.</td>
<td>x</td>
</tr>
</tbody>
</table>

**Transform technical security concept to security requirements. Handle security requirements exactly like functional requirements.**
Vector SecurityCheck with COMPASS for TARA and Continuous Documentation

- Use a professional tool for systematic risk assessment, to ensure traceability
- Ensure governance with auditable risk and measure list
- Use heuristic checklists with continuously updated threats and mitigation

COMPASS information: www.vector.com/compass
Agenda

Welcome 3
Challenge Cybersecurity 5
Standards for Safety and Security 8
Risk-Oriented Security 18

▫ Systematic Security Engineering 28

Conclusions and Outlook 35
From TARA to Requirements, Design, Test, and Traceability

Requirements
- Assets, TARA, Security Goals
- Functional security requirements
- Technical security requirements

Architecture
- System
- Functional
- SW/HW

Test
- Grey-Box Penetration Test, Robustness Tests, Fuzzing
- Functional Tests, Security Testing
- Unit Test, Static Code Analysis
Layered Security Concept

Legacy: Outside in

- Secure communication to services outside the vehicle
- Intrusion detection mechanisms
- Firewalls
- Key Infrastructure / Vehicle PKI
- Synchronized secure time
- Authenticity of messages
- Integrity and freshness of messages
- Confidentiality of messages
- Key storage
- Secure boot and secure update
- Crypto library
- HW trust anchor (HTA)

New development: Inside out
Vector recommendation:

- Divide subnets towards manageable units
- Separate connectivity (e.g. cluster, TCU, Head Unit, etc.) from safety-critical components
- Connect safety and security operationally for efficiency – and effectiveness
AUTOSAR allows secure communication stack
Apply safety and security by design, i.e. design principles, traceability SG to FSR/TSR
Use hardened base software, preferably with secure boot
Security by Lifecycle: Verification, Validation and Life-Cycle Management

- **SW Updates**
  - Consider increasing regulation such as UNECE
  - PSIRT Collaboration (Product Security Incident Response Team)

- **OTA Updates: Ensure that each deployment satisfies security requirements**
  - Data encryption: Protection of intellectual property by encryption
  - Authorization: Protection against unauthorized ECU access
  - Validation: Safeguarding of data integrity e.g. in the flash memory
  - Authentication: Verification of authenticity through signature methods
  - Governance: Safety/security documentation is continuously updated

- **Pen Testing**
  - Connect with misuse, abuse and confuse cases
  - Vector Grey-Box PenTest based on TARA and risks
  - DoS, Replay, Mutant/Generated Messages

- **Fuzz Testing**
  - Brute-force CAN Fuzzer for fuzzing the Application SW

- **Code Analysis**
  - CQA, Coverage (e.g., VectorCAST)
  - Design, architecture, (opt) defect analysis
Situation

Vector is supporting many OEM, tier1 and tier2 suppliers with PenTesting

Goals

Set up qualification strategy with Vector test tools and mapping to Fuzzing, PenTesting and regression test

Provide grey-box PenTesting concept

Client Quote

Vector Consulting Services supported Panasonic with cybersecurity, demonstrating an outstanding level of expertise.

The goal of a comprehensive TARA integrated into a security concept was achieved.

The support was intense and very successful!
Agenda

- Welcome
- Challenge Cybersecurity
- Standards for Safety and Security
- Risk-Oriented Security
- Systematic Security Engineering
- Conclusions and Outlook
Conclusions and Outlook

Security as well as Safety Must Cover the Entire Life-Cycle

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.)
Conclusions and Outlook

Vector Cyber Security Solution

Services

Embedded Software

Tools
Conclusions and Outlook

Vector Offers the most Complete Portfolio for Security/Safety

<table>
<thead>
<tr>
<th>Vector Cybersecurity Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consulting and services</strong></td>
</tr>
<tr>
<td>• SecurityCheck and SafetyCheck</td>
</tr>
<tr>
<td>• TARA</td>
</tr>
<tr>
<td>• Security concept</td>
</tr>
<tr>
<td>• Code analysis</td>
</tr>
<tr>
<td>• PenTesting</td>
</tr>
<tr>
<td>• Virtual Security Manager</td>
</tr>
<tr>
<td><strong>Tools</strong></td>
</tr>
<tr>
<td>• COMPASS SecurityCheck and TARA</td>
</tr>
<tr>
<td>• VectorCAST for code analysis and coverage</td>
</tr>
<tr>
<td>• Security Manager Extension for Vector Tools und Fuzz Testing</td>
</tr>
<tr>
<td>• PLM with PREEvision</td>
</tr>
<tr>
<td>• Diagnosis</td>
</tr>
<tr>
<td><strong>AUTOSAR Basic Software</strong></td>
</tr>
<tr>
<td><strong>vHSM for HW based Security</strong></td>
</tr>
</tbody>
</table>

Engineering Services for Security

[www.vector.com/security](http://www.vector.com/security)
Conclusions and Outlook

Vector Consulting Solutions

Trainings
- Cyber Security Workshop (1 Day, Seoul office, 한국어)
  vector-academy.com/vk_class_cybersecurity_ko.html
- Functional Safety Workshop (3 Days, Seoul office, 한국어)
  vector-academy.com/vk_class_functional_safety_ko.html
- In-house trainings tailored to your needs available worldwide
  > Requirement Engineering / Systems engineering / Agile Development

Event
- Vector Forum – Achieving Engineering Competitiveness
  > “Virtual Event” at 25th June 2020

Resources
- COMPASS for security, safety and ASPICE: www.vector.com/compass
- Further webinars and recordings:
  www.vector.com/webinar-security
  www.vector.com/webinar-safety
- Free resources, white papers etc.:
  www.vector.com/consulting-articles
  www.vector.com/consulting-mediacenter
Thank you for your attention.
Please contact us for consulting support.


Vector Consulting Services

@VectorVCS
www.vector.com/consulting
consulting-info@vector.com
Phone: +49-711-80670-1520

© 2020. Vector Korea IT Inc. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V2.3 | 2020-05-26