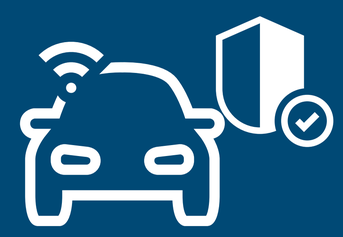
Analyzing security feature design leading to safety related failures



A method for identifying inconsistencies between functional safety and cybersecurity of autonomous vehicles

Priyadarshini, Simon Greiner, Maike Massierer, Oum-El-Kheir Aktouf

1. Background and context

No industry standard on safety and security co-engineering

Independent development with limited interaction

Undetected interdependencies between safety and security

Issues on joint safety-security integration

Architectural design phase

- Functional safety feature design can introduce system vulnerabilities
- Cybersecurity feature design can lead to hazards

Research objective

Identify if cybersecurity features lead to safety related failures

2. Methodology

Inputs	**System Failure Modes & Effects Analysis (SFMEA)**	• Structure analysis • Function analysis • Failure analysis
	Model based system architectural design **→ Behavioral & structural diagrams of security features**	• Internal block diagram • Activity diagram

Methodology

1. **Finding connection between safety analysis and security feature design**

   by

   - selection of a structural element, e.g. communication interface
   - identification of security features designed to protect this element

2. **Detection of potential inconsistencies**

   by

   - behavioral analysis of security features
   - analyze if it leads to safety related failures

3. **Impact analysis of identified inconsistency**

   by

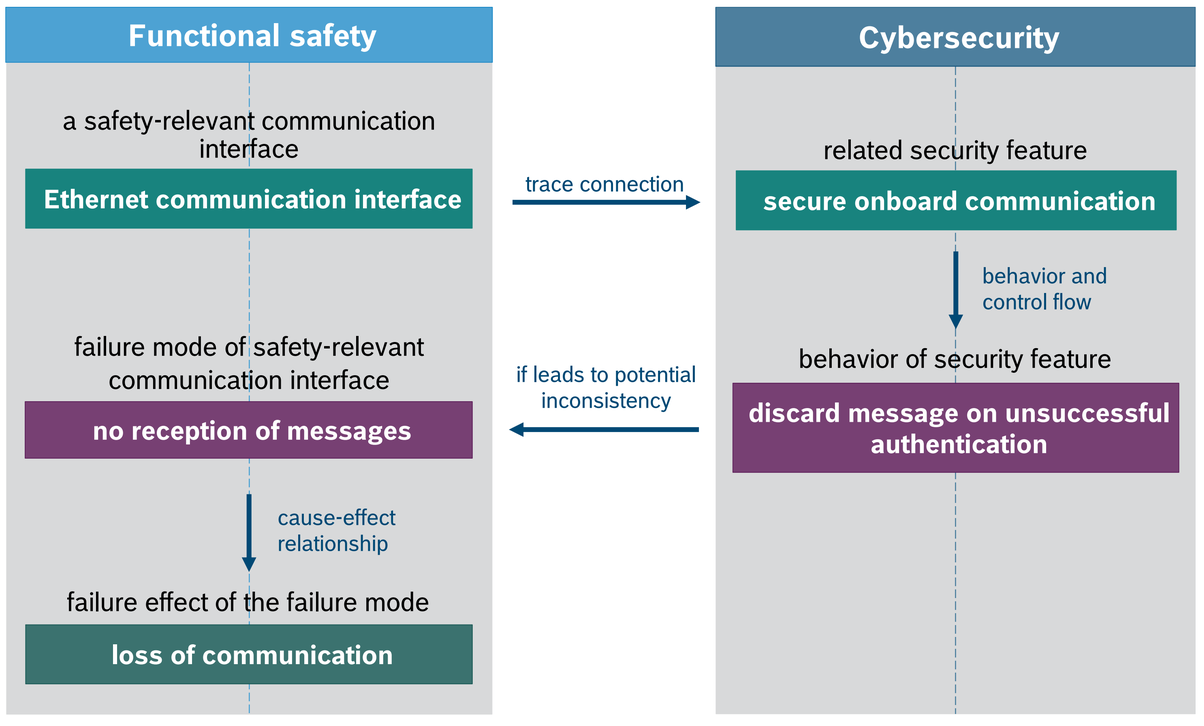
   - determination of failure effects at component and system levels

Outputs

For each structural element
- Security features
- Safety relevant failures
- Failure effects at component and system levels

3. Results

Manual application on a driver assistance system



Main findings

- The security feature ‘secure onboard communication’ discards messages when freshness and authentication verification is unsuccessful.
- This could lead to the failure ‘no reception of messages’, i.e. unavailability of safety-critical messages.

4. Summary and future work

Advantages

- Optimal utilization of resources
- Early detection and resolution of inconsistencies through co-design and co-development

Future work

- Implementation of the method and automation to minimize manual analysis in complex projects
- Investigation of additional diagram types to support our analysis

Contact us

priyadarshini.priyadarshini@de.bosch.com
simon.greiner@de.bosch.com
maike.massierer@de.bosch.com
oum-el-kheir.aktouf@lcis.grenoble-inp.fr

Take a photo and download the complete paper

UGA Université Grenoble Alpes — LCIS Laboratoire de Conception et d'Intégration des Systèmes — BOSCH