Driver Assistance System Safety & Security Case Study

Bastian Tenbergen

April 2021

Driver Assistance System Safety & Security

Background

Modern automobiles are increasingly often entrusted with safety-critical functionality, sold to the customer as "driver assistance systems." Examples of such systems are adaptive cruise controls, driver attention systems, blind spot warning systems, front- and rear collision warning systems, etc. Moreover, modern automobiles increasingly often include cloud-based connectivity features such as GM's OnStar, Hyundai BlueLink, Mercedes me Connect, or Tesla's Connected Car. The integration of such cloud-based connectivity features with safety-critical systems offers new attack vectors for malicious users.

Disclaimer:
The author neither claims knowledge nor implies the existence of vulnerabilities in the above referenced examples.

Case Study Overview

The aim of this case study is to apply security hardening, risk assessment, and countermeasure development in class in a small-scale development project. This project simulates a common scenario, where a car manufacturer, seeks to develop cloud-based integration of driver assistance systems for their flagship vehicle. The learner will:

- gain an in-depth understanding of the hardware and software properties of the driver assistance systems;
- conduct requirements engineering for one of four driver assistance systems with cloud integration;
- conduct safety analyses to ensure that the likelihood of humans and external systems to suffer injury, damage, or death is sufficiently low;
- conduct risk assessment, preform threat modeling, and develop suitable counter-measures on requirements level.

Student Instructions

Milestone 1

Task 1. Research the Hyundai Santa Fe Quick Reference Guide and Owner's Manual. You may also use a car manual of comparable vehicles that are available to you, as long as they specify one of the following systems:

- the blind-spot detection system with "safe-exit" feature;
- the rear-view camera with cross-traffic detection, rear collision avoidance, and smart trunk hatch;
- the smart cruise control with forward collision avoidance; and
- the lane assist system with driver attention warning.

Note that not all information might be in the same place within the documents. The manual might treat the "safe exit" feature as a driver comfort system and the blind-spot detection feature as a safety system, yet realistically, they are the same system that makes use of the same sensors. So, relevant information might be spread out across the document.

Select one of these systems are your case example.

Task 2. Document adequate requirements for your system. Begin by defining goals and scenarios, as well as functional requirements for the core functionality of the system. Document adequate preliminary safety and security quality requirements.
(Optional: Document your requirements in an IEEE 830-compatible template).

Milestone 2

Task 1. Using the tutorial slides from the references, conduct a functional hazard analysis. Consider every system function and discover as many hazards as possible. Define adequate safety goals and functional requirements to fulfil the safety goals.

Task 2. Extend the functional hazard analysis from Task 1 with proper risk assessment. Identify the initial risk mishap index *before* implementation of safety mitigations and final risk mishap index *after* implementation of the mitigations. Assess their impact on driver security and privacy and model possible attack vectors if the functionality from Milestone 1 are exposed to a cloud-based connectivity system. If these render hazardous operating conditions for the passengers, amend your functional hazard analysis accordingly.

Task 3. Develop risk mitigations and countermeasures for any identified security vulnerability. Include these as functional requirements in the document from Milestone 1. Therein, also include your artifacts from Milestone 2, Task 1 and 2.

Milestone 3

Task 1. Based on the previous artifacts produced in Milestones 1 and 2, develop a system architecture for your case example system. Include the architecture as a UML Class Diagram in the document from Milestone 2, Task 3.

Task 2. Based on the previous artifacts produced in Milestones 1 and 2 as well as the system architecture, develop the detailed design for your case example system. Include suitable UML State Machine Diagrams and/or Activity Diagrams in the document from Task 1.

Task 3. Your specification document should now consist of functional requirements, including hazard analyses and threat models, corresponding hazard mitigations and security countermeasures, a system architecture, and behaviour models. Repeat now your hazard analyses and risk assessments from Milestone 2, Task 2 and 3, but based on the information documented in the system architecture and behaviour models. The aim of this is twofold: Firstly, validate that previously found hazards and vulnerabilities are sufficiently mitigated. Secondly, identify any additional hazards and/or vulnerabilities that may have been introduced. Add your findings to your specification document

Task 4. Develop risk mitigations and countermeasures for any identified security vulnerability as well as safety hazard like you did for Milestone 2, Task 3. Be sure to update your natural language functional requirements from Milestone 1 as well as your system architecture and behaviour models from Tasks 1 and 2 accordingly.

Instructor notes

This case study may be assigned as a semester-long team project for learners in groups of 3-5. Milestones should be spaced out across the whole semester, i.e. roughly three to four weeks between due dates. This will allow plenty of time to introduce the relevant topics, attempt to solve the milestones, present progress in class and receive feedback, before improved solutions can be submitted for grading.

If used in conjunction with weekly, low-stakes homework assignments focusing on correctness of applied techniques, grading of this project case study should focus on consistency and completeness of specification.

The resulting artifact should be one document, ideally IEEE 830-compatible, which grows by the solutions form each task of teach milestone.

Example solution

The main learning outcome of this case study is knowledge discovery and application. Therefore, no example solution is applicable, as the solution is what students make of it.

References

Firesmith, D.: "Common Concepts Underlying Safety, Security, and Survivability Engineering." Technical Report, Software Engineering Institute, 2003. Available at: https://apps.dtic.mil/sti/citations/ADA421683, accessed 1 March 2021.

Hyundai Motor Company: "The Hyundai Santa Fe Owner's Manual." Online resource available at: https://owners.hyundaiusa.com/content/dam/hyundai/us/myhyundai/glovebox-manual/2020/santa-fe/2020%20Santa%20Fe%20Owner's%20Manual.pdf, accessed 1 March 2021.

Hyundai Motor Company: "The Hyundai Santa Fe Quick Reference Guide." Online resource available at: https://owners.hyundaiusa.com/content/dam/hyundai/us/myhyundai/glovebox-manual/2020/santa-fe/2020%20Santa%20Fe%20Quick%20Reference%20Guide.pdf, accessed 1 March 2021.

Squair, M.: "System Safety M7: Functional Hazard Analysis (FHA) v1.2". Tutorial slides, available at https://msquair.files.wordpress.com/2015/12/m7-functional-hazard-analysis-v1-2.pdf, accessed 5 March 2021.

Broy, M.: "Automotive Software Engineering." In Proceedings of the 25th Intl. Conference on Software Engineering, 2003.

Broy, M.: "Challenges in Automotive Software Engineering." In Proceedings of the 28th Intl. Conference on Software Engineering, 2006.

Pretchner, A., Broy, M., Krüger, I., and Stauner, T: "Software Engineering for Automotive Systems: A Roadmap." In Proceedings of Future of Software Engineering, 2007.