Avoiding Safety and Cybersecurity Risks in Autonomous Systems



Dhanabal Arunachalam discusses a proposed safety analysis technique that allows synergy between safety and cybersecurity during the development of partial, conditional, high and full driving automation vehicles. He provides an overview of the technique and the analysis concepts where safety measures are identified and cybersecurity conflicts are resolved. He also identifies and addresses the challenges confronted when conducting the analysis during development of hardware, software and the overall system.

Safety and cybersecurity engineering are fundamental areas upon which autonomous vehicle design should be focused on risks (both safety and cybersecurity) related to driving. Both disciplines are widely used at various stages of vehicle development – to assist in design, verification, and interfacing with other software of vehicle electrical/electronic systems.

Safety and cybersecurity analysis should go together during the product development lifecycle. For example, in a connected car, a safety analyst provides proper safety measures to deploy an airbag during a crash. However, the cybersecurity analyst provides cybersecurity measures for denial of airbag deployment if an external attacker has taken controllability of the airbag system, thus leading to potential conflicts. Hence, to address this problem, it is necessary to have synergy between the disciplines, especially during safety and cybersecurity risk analysis.

The following image illustrates that when safety and cybersecurity analysis are executed independently, we see that the different discipline mindsets don't help in reaching the overall goals of achieving a sufficiently safe and secure autonomous vehicle.





Different mindsets can emerge as safety is concerned with inadvertent unintended behaviour, whereas security deals with goal-seeking opponents.

To ensure safety and cybersecurity are synergised as shown in the figure, the following proposed technique allows safety and cybersecurity team to work together to achieve autonomous safety and cybersecurity intended objectives.



Safety and Cybersecurity – scope

The goal of this article is therefore to provide a concept overview and process workflow for a proposed safety analysis technique for developing harmonised safety and cybersecurity vehicle functions.

The starting point for this is the extraction of concepts from the automotive safety standard "ISO 26262" [1] and cybersecurity standard "ISO 21434" [2]. These standards are the foundation of this article, as they reflect current best practice in managing safety and cybersecurity risks for the automotive industry.

Safety and cybersecurity measures should go hand-in-hand to achieve state-of-the-art solutions in an autonomous vehicle.

Safety and Cybersecurity – ISO standard overview

Relevant extracts from ISO 26262 about cybersecurity in the concept phase are as follows:

- cybersecurity threats to be analyzed as a hazard from a functional safety perspective in order to support the completeness of the hazard analyses and risk assessment and the safety goals
- functional safety can provide information such as hazards and associated risks to support the cybersecurity identification of threats

Note that ISO 26262 does not address cybersecurity threats, however, it provides guidance on potential interaction of functional safety with cybersecurity.

Relevant extracts from ISO 21434 about functional safety cover the interdisciplinary exchange of the following activities:

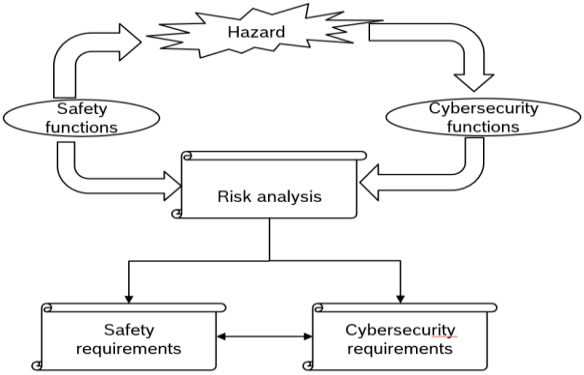
- threat scenarios and hazard (ISO 26262-1:2018 [1]) information
- cybersecurity goals and safety goals (ISO 26262-1:2018 [1])
- cybersecurity requirements conflicting or competing with functional safety requirements (ISO 26262-1:2018 [1])

Functional safety should therefore consider cybersecurity threats with safety impacts, identified through security analysis, and make corresponding additions to the safety analysis. Cybersecurity should look at the safety related hazards identified through safety analyses and if it is possible for an external attacker, to trigger the safety faults in the system through external manipulation.

Safety and cybersecurity engineering are fundamental areas upon which autonomous vehicle design should be focused on risks related to driving.

Risk analysis process overview

Safety and cybersecurity functions play a crucial role in determining hazards that occur due to violation of safety and/or cybersecurity goals, as shown by the processes in the top section of the figure.

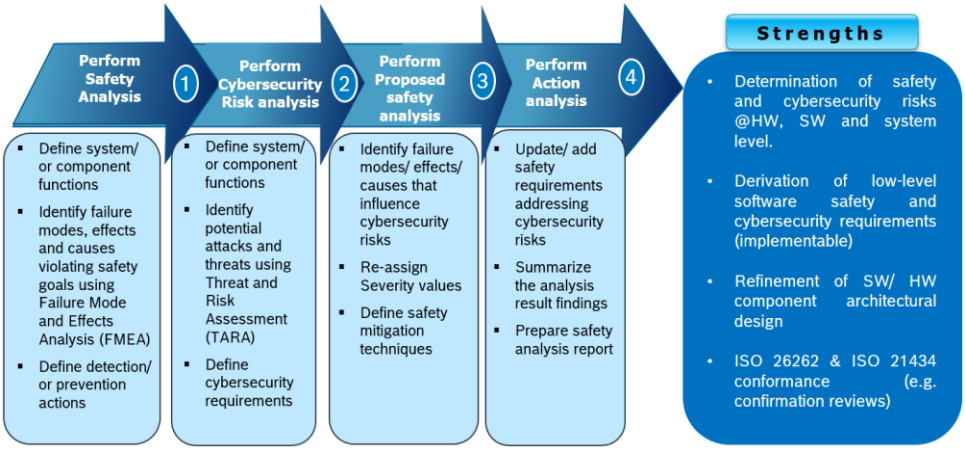


These functions are then further assessed (lower part of the figure) through risk analysis management, which defines safety and cybersecurity requirements, and it is evaluated via risk analysis (ie. The proposed safety analysis technique), to identify critical safety, cybersecurity, and liability risks.

For example, in connected car camera/radar systems, an attacker can either activate automatic emergency braking (AEB) when not needed, or make the brakes fail when needed. The proposed analysis will help derive safety & cybersecurity requirements on intended activation of AEB.

Proposed safety analysis - workflow

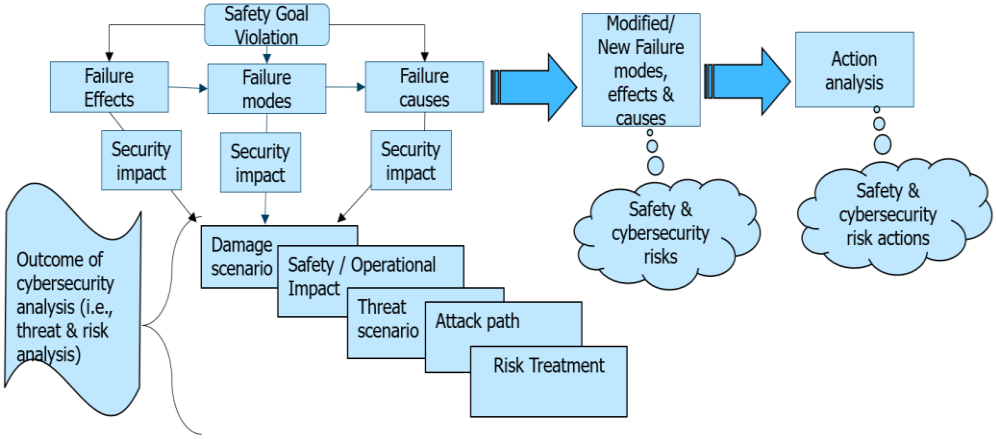
The proposed safety analysis performs safety and cybersecurity risk management in a harmonized manner as depicted in the following diagram.



Steps 1 and 2 of the diagram defines safety and cybersecurity risk management processes that safety and cybersecurity teams execute independently. From Step 3 onwards, core attributes associated with cybersecurity failures are mutually aligned with the safety team and safety mitigation strategies are defined to address those cybersecurity risks. As part of the safety mitigation strategy, measures like degradation states, fail safe and fail operational concepts are refined based on the cybsersecurity risk mitigation strategy.

Detailed workflow diagram of proposed safety analysis

The detailed activities of Step 3 from the above proposed process are illustrated in the following diagram.

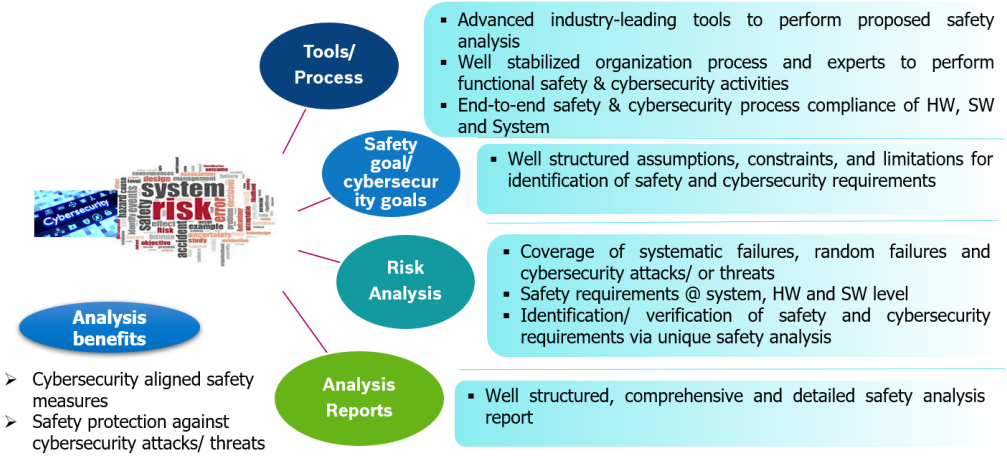


This process starts by considering safety risks from potential attacks and vulnerabilities, which are obtained via damage scenario and threat scenarios.

Initially, failure modes impacting safety goals are determined via typical Failure Mode & Effects Analysis (FMEA). On the security side, damage scenarios and threat scenarios are identified via Threat Analysis and Risk Assessment (TARA). Next, Failure modes are checked against each of the damage scenarios, threats, and attack paths. As part of this check, critical points like violation of safety goal by damage scenarios, threats, and attack paths are taken into consideration. This verification activity is repeated for each of the failure effects and failure causes. As an outcome, it is possible that new hazards and safety goals will be identified. As a post verification activity, action analysis is executed upon which all occurrence and prevention measures are re-analysed. Also, the severity level of safety effects is revised, and risk priority numbers are modified accordingly. As an outcome of this analysis, the safety mitigation strategy is refined in a way that cybersecurity risk strategies are integrated.

Proposed safety analysis - benefits

The proposed safety analysis offers a wide variety of merits e.g., well-trusted and effective processes, customized use of standardised safety analysis tools and methods to ensure end-to-end adherence with functional safety and cybersecurity standards, compliance against product safety/ or cybersecurity process with an established functional safety and cybersecurity intent, assumptions/ limitation during execution of proposed safety analysis, conform to cohesive safety/ cybersecurity culture and traceable documentation, etc.



Proposed safety analysis - summary

The proposed safety analysis technique allows safety and cybersecurity problems to be addressed during various stages of the safety development lifecycle and it provides a state-of-the-art solution for the major issues faced during autonomous vehicle development. A unique failure mode analysis along with guidelines and processes are followed during execution of the proposed safety analysis for system, hardware, and software development. This ensures that both safety and cybersecurity issues along with vehicle scenarios are analysed and corresponding cybersecurity aligned safety measures are identified.

References

[1] ISO 26262: 2018	Road vehicles – Functional safety, Part [1], [3], [4], [9]
[2] ISO 21434	Road vehicles – Cybersecurity engineering, Chapter [8], [9], [10]

Dhanabal Arunachalam, Functional Safety Expert, Robert Bosch LLC, USA

Dhanabal has spent over 16+ years working on functional safety engineering for automotive and railway systems. His functional safety expertise includes hazard analysis and risk assessment, FMEA/FMEDA, FTA, DFA, tool qualification, software component certification support, SOTIF analysis, safety case & safety manual preparation and safety-cybersecurity interaction analysis. He has a rich experience in harmonized process & guideline derivation for functional safety and cyber security activities and has been involved in a number of safety related projects for achieving compliance of EN50126, EN50128, ISO 26262, ISO 21448 & ISO 21434 standards.