An Integrated Safety and Cybersecurity Resilience Framework for the Automotive Domain

Pierre Kleberger, Peter Folkesson, Behrooz Sangchoolie

An Integrated Safety and Cybersecurity Resilience Framework for the Automotive Domain

Pierre Kleberger, Peter Folkesson, and Behrooz Sangchoolie
Dependable Transport Systems
RISE Research Institutes of Sweden
Borås, Sweden
{pierre.kleberger, peter.folkesson, behrooz.sangchoolie}@ri.se

***Abstract*—As vehicles become more and more connected with their surroundings and utilize an increasing number of services, they also become more exposed to threats as the attack surface increases. With increasing attack surfaces and challenges faced when eliminating vulnerabilities, vehicles need to be designed to work even under malicious activities, i.e., under attacks. In this paper, we present a resilience framework that integrates analysis of safety and cybersecurity mechanisms. We also integrate resilience for safety and cybersecurity into the *fault – error – failure* chain. The framework is useful for analysing the propagation of faults and attacks in between the three abstraction layers of hardware, software, and system where the mechanisms are implemented on. This facilitates identification of adequate resilience mechanisms at different system layers as well as deriving suitable test cases for verification and validation of system resilience using fault- and attack injection.**

***Index Terms*—automotive, cybersecurity, safety, resilience, framework**

I. Introduction

The transformation of vehicles from being non-connected systems into automated, fully inter-connected digital systems put high requirements on safety and cybersecurity. Vehicle functions, such as brake-by-wire and adaptive cruise control systems, as well as those that are under development for future automated vehicles, must be safe and secure, even in an inter-connected environment. However, since software and hardware components still come with defects and vulnerabilities, they would need to be regularly updated or replaced. Due to the complexity of the automotive development supply chain, it is reasonable to think of situations when vulnerabilities are not easily fixed, and therefore vehicles need also to be able to sustain attacks and continue to function even in such situations. One way to enable such continuation of functions is to develop vehicles with resilience in mind and to implement mechanisms that are able to adapt or be reconfigured to new situations.

In previous work, Sangchoolie et al. [1] analysed 17 security mechanisms with respect to dependability and security attributes. Resilience was however not considered by the authors of the work. Rosenstatter et al. [2] conducted a literature review and presented a framework of resilience techniques for the automotive domain, divided into detection, mitigation, recovery, and endurance. Strandberg et al. [3] surveyed published attacks against vehicles and presented a framework of associated countermeasures from [2] to the identified attacks with the goal of a resilient vehicle design. We do not present different resilience techniques, nor design solutions. In this paper, we present a framework that can be used to identify and analyse mechanisms suitable for achieving resilience to faults and attacks. Moreover, we investigate propagation of faults and attacks in between the three abstraction layers of hardware, software, and system where the mechanisms are implemented on.

The rest of this paper is outlined as follows. In Section II, a definition of resilience is presented, followed by presentation of concepts for a chain mapped to the traditional *fault – error – failure* chain [4] which we call *attack – intrusion – compromised system* chain. In this section, we also categorise the means of achieving resilience. In Section III, the proposed framework is presented. The paper concludes in Section IV with an outlook on future work.

II. Background

A. Defining Resilience

There is yet no single definition of the term *resilience*. The term has been introduced in different domains and a discussion of different meanings and usages can be found in Deliverable D1.1 from the CyReV research project [5]. Therefore, to have a clear definition for our work and discussions, we use the following definition adopted by the CyReV project:

Definition 1 (Resilience)**.** Property of a system with the ability to maintain its intended operation in a dependable and secure way, possibly with degraded functionality, in the presence of faults and attacks. *Note to definition:* Dependable and secure refer to attributes such as safety, confidentiality, integrity, privacy and maintainability.

We conclude from Definition 1 that a resilient vehicle is one that can sustain attacks and continue to function under faults and malicious activities. This definition is close to what is considered survivability in [6].

B. The Attack – Intrusion – Compromised System Chain

Avizienis et al. [4] define an attack as a special type of fault which is human made, deliberate and malicious, affecting

This research was conducted within the CyReV project, which is funded by the VINNOVA FFI program – the Swedish Governmental Agency for Innovation Systems (Diary number: 2018-05013, 2019-03071).

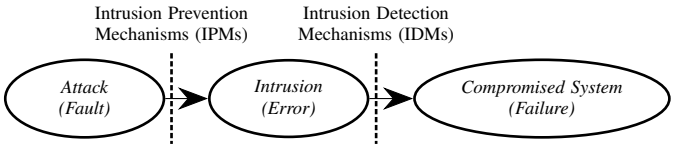

Figure 1. The attack – intrusion – compromised system chain.

hardware or software from external system boundaries and occurring during the operational phase. The mapping between fault and attack could also facilitate the mapping of error and failure to intrusion and a compromised system, respectively, as illustrated in Figure 1 [7]. In other words, an intrusion is made into the target system as a result of an attack, if the intrusion prevention mechanisms (IPMs) fail to prevent the intrusion from occurring. Moreover, the target system could be compromised if the intrusion detection mechanisms (IDMs) fail to identify the intrusions that have occurred in the target system. A compromised system could then consequently go into a failure state depending on the requirements that are violated.

C. Resilience Mechanisms

Before continuing further, let us clarify what we mean by the term *mechanism*. Considering resilience as a system property, a *resilience mechanism* may be considered *a process or means to implement and maintain system resilience*. This distinction between property and mechanism follows the approach presented by Cherdantseva and Hilton [8].

As previously noted, our definition of resilience is closely connected to the term survivability. Survivability is defined by Firesmith [9] as "the degree to which essential services continue to be provided in spite of either *accidental* or *malicious* harm" and is expressed by the three factors *prevention*, *detection*, and *reaction*:

- *Prevention* is defined as "the degree to which hazards and threats are resisted so that essential services continue to be provided both during and after accidents and attacks" [9].
- *Detection* is defined as "the degree to which relevant accidents and attacks (or the harm they cause) are recognized as they occur so that the system can react accordingly to maintain essential services" [9].
- *Reaction* is defined as "the degree to which the system responds (e.g., recovers) after an accident" [9].

Thus, following Definition 1, a resilient system needs to provide all three factors of survivability; prevent intrusions by means of IPMs, detect intrusions by means of IDMs, but also handle intrusions to maintain the system's intended operation in a dependable and secure way.

III. An Integrated Resilience Framework

We present an integrated resilience framework that is an extension of the model in Figure 1. The IPMs–IDMs are extended with intrusion handling mechanisms (IHMs), which all together capture the three factors of survivability listed in Section II-C.

The framework is presented by two different models. First, a layered resilience framework (see Figure 2) is described that captures the propagation of faults and attacks in between mechanisms implemented on different abstraction layers, i.e., hardware, software, and system layers. Then, the *attack – intrusion – compromised system* chain (see Figure 1) is extended with resilience mechanisms and system states (see Figure 3) from the layered resilience framework to enable handling of intrusions.

A. A Layered Resilience Framework

The proposed layered resilience framework, adapted from [10, p. 13], is presented in Figure 2. The framework facilitates analysis of a system under test (SUT) including all its safety and security mechanisms with respect to its resilience to different types of faults. These faults are those that are rooted within SUT components (such as hardware, software, sensor, and communication components) and could cause an error in the system. Note that, security attacks are also considered as a special type of faults that could result in security intrusions.

As presented in Section II-B, an error may lead to a system failure. The failure could be of type *catastrophic* or *benign*. These are often classified in fault- and attack injection experiments as (see [7]):

- *Catastrophic Failure.* The injected fault or attack results in undetected erroneous outputs in the SUT, where the deviation from the nominal value is outside an acceptable range, which is defined according to the requirements of the SUT.
- *Benign Failure.* The injected fault or attack results in undetected erroneous outputs in the SUT, where the deviation from the nominal value is within an acceptable range, which is defined according to the requirements of the SUT.

While *catastrophic failures* contribute to a system's lack of resilience, *benign failures* contribute to the system's resilience. This also follows what Laprie writes: "A system whose failures can only be — or more generally are to an acceptable extent — benign failures is a **fail-safe system**." [11]. In addition to the benign failures, resilience could be obtained by *detecting* and *handling* the errors, as well as by degrading the system functions. Moreover, errors may also be latent [4] or overwritten. Such errors also contribute to the system's resilience. Note that for as long as an error is latent, it is present in the SUT, but not detected nor causing a failure.

According to the layered resilience framework presented in Figure 2, detection and handling of errors are done using mechanisms implemented in the three layers of hardware, software, and system. In this framework, we consider hardware and software mechanisms to be implemented in a single node, while system mechanisms may be implemented and distributed over a set of nodes. The first two lines of defence are conducted using hardware and software-layer detection and handling mechanisms that aim to handle the errors at these

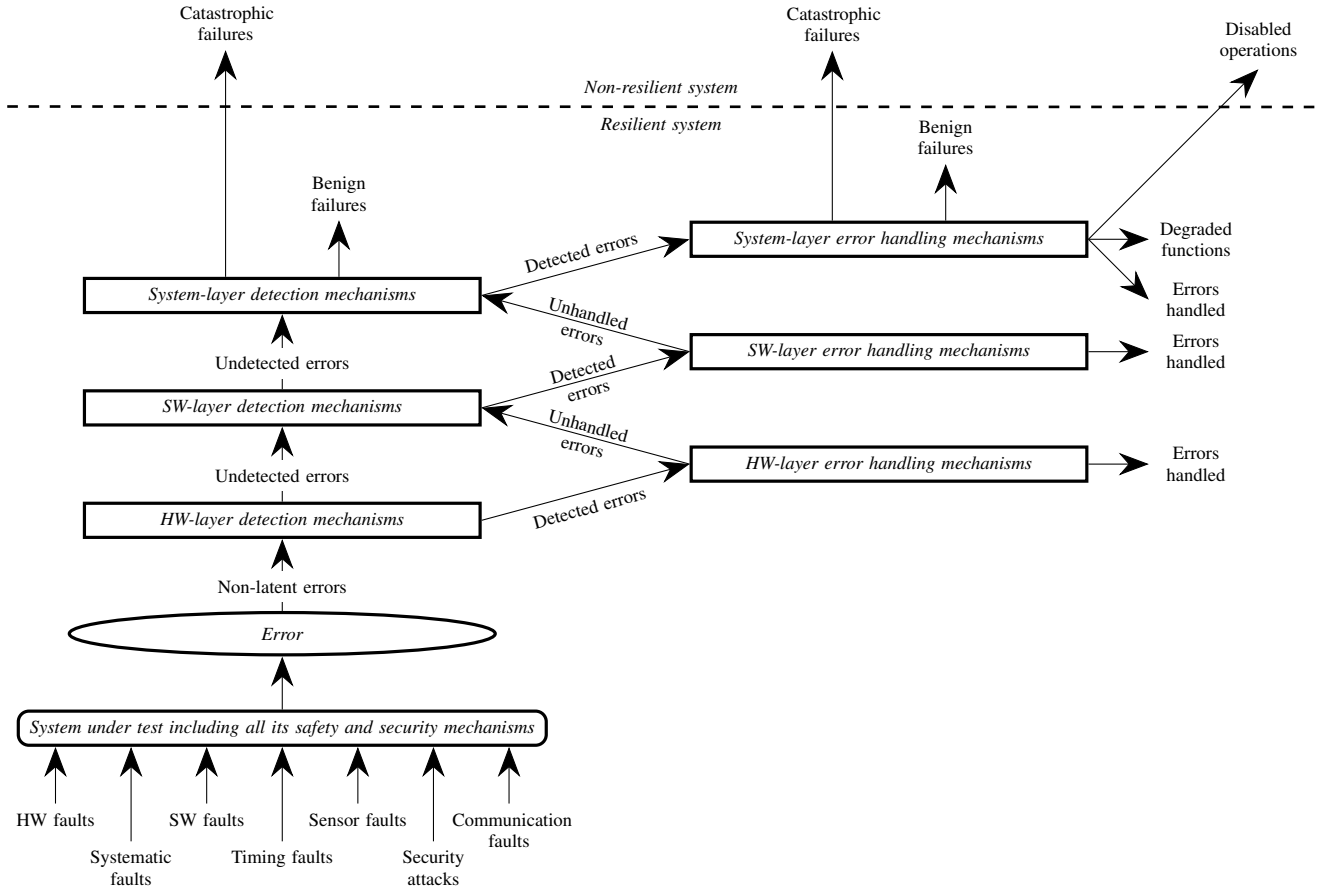

Figure 2. The layered resilience framework. Note that security intrusions are considered as specific types of errors that are the result of security attacks.

layers (in a single node) and signal those that are unhandled to the system-layer (at the top). At the system-layer, the errors may (i) be handled using system-layer handling mechanisms, or (ii) the SUT may continue to function in a degraded mode. Both cases contribute to the system's resilience in a way similar to the benign failures. The errors might also be handled by the system-layer handling mechanism using a safe system shutdown that could also be obtained by disabling the system's operation. However, this type of handling does not contribute to the system's resilience if, according to Definition 1, the system cannot maintain its intended operation after the safe shutdown. Errors that remain undetected or unable to be handled by the system-layer mechanisms may cause catastrophic or benign failures.

B. An Attack – Intrusion – Compromised System Chain with Resilience

An extension of the *attack – intrusion – compromised system* chain (Figure 1) is presented in Figure 3 where the effects of intrusions with respect to resilience (see Definition 1 and Section II-C) and the layered resilience framework are also considered. Now, intrusions that are not detected nor handled by any of the mechanisms of the layered resilience framework may lead to a compromised system, which may result in either a *catastrophic failure* or *benign failure* of the system. However, there are three ways in which the mechanisms of the layered resilience framework may handle intrusions (if they were detected):

- *Intrusion Handled.* The intrusion may be handled by mechanisms in the HW/SW- or system-layers, i.e., *Errors handled* in Figure 2. In this way, the system operation will be kept nominal despite the occurrence of intrusions, e.g., through a system reconfiguration at the SW-layer, or a triple modular redudancy (TRM) system implementation at the system-layer that eliminates the impact of a malicious node.
- *Degraded Function.* The intrusion may be handled in a way causing some degradation of the system operation (*Graceful Degradation*), e.g., for a vehicle system, reconfiguration of the vehicle to limp home mode.
- *Disabled Operation.* The intrusion may be handled by disabling the operation of the system in a safe way (*Safe Shutdown*), e.g., for the adaptive cruise control system, disabling the operation.

According to Definition 1, benign failures, intrusions handled, and degraded functions characterises a resilient vehicle system, while catastrophic failures and disabled operations do not (marked in grey in Figure 3).

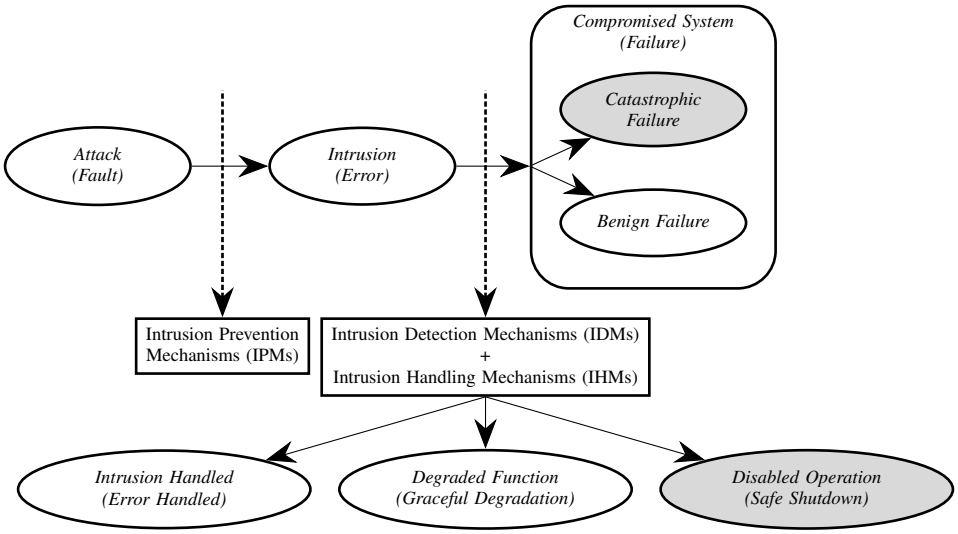

Figure 3. An attack – intrusion – compromised system chain with resilience. Benign failures, intrusions prevented or handled, and degraded function characterise a resilient vehicle system, while catastrophic failure and disabled operation are not (marked in grey).

IV. Conclusion and Future Work

In this paper, we presented an integrated safety and cybersecurity resilience framework that facilitates the analysis of mechanisms' capabilities to prevent, detect, and handle faults and attacks. Considering faults and attacks, we believe the framework may be useful to analyse how faults and attacks may propagate through the layered resilience framework with the purpose to identify which mechanisms may be useful to detect and handle faults and attacks, hence, should be implemented in a system. We note that faults and attacks may pass through all layers of the resilience framework to test the resilience mechanisms (i.e. resulting in either errors handled, benign failures, or degraded functions). Furthermore, given a set of attacks and a set of resilience mechanisms, an analysis may be conducted to identify whether all attacks are caught by some mechanisms or not, thus, if there are gaps to fill in the system design. This may further facilitate the identification of suitable test-cases for fault- and attack injections, to see whether the implemented mechanisms are effective or not. We are currently performing an analysis of the 17 security mechanisms listed in [1] using the framework and in the future, we also intend to use the framework to analyse the resilience of both safety and security mechanisms for automotive use-cases.

References

[1] B. Sangchoolie, P. Folkesson, P. Kleberger, and J. Vinter. "Analysis of Cybersecurity Mechanisms with respect to Dependability and Security Attributes". In: *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. June 2020, pp. 94–101.

[2] T. Rosenstatter, K. Strandberg, R. Jolak, R. Scandariato, and T. Olovsson. "REMIND: A Framework for the Resilient Design of Automotive Systems". In: *2020 IEEE Secure Development (SecDev)*. Sept. 2020, pp. 81–95.

[3] K. Strandberg, T. Rosenstatter, R. Jolak, N. Nowdehi, and T. Olovsson. "Resilient Shield: Reinforcing the Resilience of Vehicles Against Security Threats". In: *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. Apr. 2021, pp. 1–7.

[4] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. "Basic concepts and taxonomy of dependable and secure computing". In: *IEEE Transactions on Dependable and Secure Computing* 1.1 (Mar. 2004), pp. 11–33.

[5] T. Rosenstatter and K. Tuma. *A State-of-the-Art Investigation*. Deliverable CyReV D1.1, v1.0. Oct. 16, 2019.

[6] M. Bishop, M. Carvalho, R. Ford, and L. M. Mayron. "Resilience is more than availability". In: *Proceedings of the 2011 New Security Paradigms Workshop*. NSPW '11. New York, NY, USA: Association for Computing Machinery, Sept. 12, 2011, pp. 95–104.

[7] B. Sangchoolie, P. Folkesson, and J. Vinter. "A Study of the Interplay Between Safety and Security Using Model-Implemented Fault Injection". In: *2018 14th European Dependable Computing Conference (EDCC)*. Sept. 2018, pp. 41–48.

[8] Y. Cherdantseva and J. Hilton. "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals". In: *Organizational, Legal, and Technological Dimensions of IS Administrator*. Ed. by F. Almeida and I. Portela. IGI Global Publishing, Sept. 2014. DOI: 10.4018/978-1-4666-4526-4.ch010.

[9] D. Firesmith. *Common Concepts Underlying Safety, Security, and Survivability Engineering*. CMU/SEI-2003-TN-033. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.

[10] R. Barbosa. *Layered fault tolerance for distributed embedded systems*. PhD Thesis N.S., 2890. Göteborg: Chalmers University of Technology, 2008. 175 pp. ISBN: 978-91-7385-209-8.

[11] J.-C. Laprie. "Dependable computing: concepts, limits, challenges". In: *Proceedings of the Twenty-Fifth international conference on Fault-tolerant computing*. FTCS'95. USA: IEEE Computer Society, June 27, 1995, pp. 42–54.