

System Security and System Safety Engineering: Differences and Similarities and a System Security Engineering Process Based on the ISO 26262 Process Framework

Barbara J. Czerny
Chrysler Group LLC

ABSTRACT

Today's vehicles contain a number of safety-critical systems designed to help improve overall vehicle safety. Such systems may control vital vehicle functions such as steering, braking and/or propulsion independently of the driver. In today's vehicles, much emphasis has been placed on helping ensure that these safety-critical vehicle systems operate as intended. Applying rigorous system safety engineering principles in developing these safety-critical automotive systems helps ensure that they operate as desired and expected. Less emphasis has been placed to-date on helping ensure cybersecurity of cyber-physical automotive systems. However, this is changing as both the world and the automotive industry become more aware of the potential ramifications of cyber-attacks on vehicles.

As with system safety, applying a rigorous system security engineering process to the development of cyber-physical automotive systems is beneficial and will help reduce the likelihood of successful attacks on vehicles. System security and system safety interact with one another and cannot be considered in isolation. However, there are also differences between system security and system safety that require unique engineering activities to be performed to address these unique aspects. This paper describes some of the differences and similarities between system security and system safety, between safety-critical systems and security-critical systems, and between system safety and system security engineering, and presents a system security engineering process for applying to cyber-physical automotive systems that is based on the ISO 26262 process framework.

CITATION: Czerny, B., "System Security and System Safety Engineering: Differences and Similarities and a System Security Engineering Process Based on the ISO 26262 Process Framework," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 6(1):2013, doi:10.4271/2013-01-1419.

INTRODUCTION

Today's vehicles contain a number of systems that are designed to help improve overall vehicle safety and performance. These systems may control essential vehicle functions such as steering, braking, and/or propulsion, and they may control these functions independently of the driver to help the driver avoid potential hazardous driving situations. Such systems are commonly called safety-critical systems since there is a potential for safety-related issues if they are not operating as desired or expected. Much emphasis has been placed on helping ensure that these safety-critical vehicle systems operate as intended and help prevent potentially hazardous situations from occurring. Application of rigorous system safety engineering principles during the development of these systems helps ensure that they operate as desired and expected. This is common knowledge in the automotive industry today. However, less emphasis has been

placed to-date on helping ensure cybersecurity of security-critical automotive systems.

A security-critical automotive system is a system where losses could occur due to vulnerabilities in the system that could be exploited either directly or indirectly by either an external or internal entity. As awareness of the potential ramifications of cyber-attacks on vehicles increases, more emphasis is being placed on ways to help reduce the likelihood of successful attacks and on ways to help reduce the potential impact of potential attacks. To achieve this requires a broader thinking than has traditionally been applied to safety-critical automotive systems.

Traditionally, automotive systems (including safety-critical systems) have been referred to as embedded systems since the emphasis has focused on the computational aspects / control of these systems. However, as awareness of cybersecurity in the automotive domain increases, and as vehicle systems become more complex and interact more

tightly with both the physical elements of the vehicle and the physical environment around the vehicle, they are now more frequently being classified as cyber-physical systems or cyber-physical automotive systems. A cyber-physical system is one in which there exists a tight coupling between the computational elements and the physical elements of a system and the environment around the system. Cyber-physical automotive systems are becoming more tightly coupled both between vehicles (Vehicle to Vehicle) and between vehicles and infrastructure (Vehicle to Infrastructure). Viewing both safety-critical and security-critical automotive systems in the broader context of cyber-physical systems helps achieve more comprehensive analysis from a cybersecurity point of view.

The interconnectivity of today's and future vehicles creates the potential for cyber-attacks on both vehicles and the transportation infrastructure supporting vehicles and vehicle use (e.g., Intelligent Transportation Systems). Security-critical automotive systems are cyber-physical automotive systems. Cyber-attacks on security-critical cyber-physical automotive systems could lead to potential safety, operational, financial, and privacy losses.

Awareness of cybersecurity with respect to vehicles and the potential ramifications of cyber-attacks in the automotive community increased following the publication of two papers in 2010 and 2011, from researchers at University of Washington and University of California San Diego. These two papers were on experimental security analysis of a modern automobile [1] and experimental analyses of automotive attack surfaces [2]. These studies have raised awareness of the importance of cyber-security in cyber-physical automotive systems.

Given the automotive industry's experience and knowledge in developing safety-critical automotive systems, it would be beneficial to capitalize on this knowledge in addressing security-critical cyber-physical automotive systems. This knowledge and experience includes that safety cannot be added on to an existing design, but rather must be built in to a system. In the same way, security cannot be added on to a design, but must be built in to the system. Building safety into a system is done by following and applying a well-structured and well-defined system safety engineering process. In the same way, building security into a system may be done by following a well-structured and well-defined system security engineering process.

This paper discusses how the knowledge and experience gained from developing safety-critical automotive systems can be used to facilitate development of security-critical cyber-physical automotive systems. The paper describes some of the differences and similarities between system safety and system security, the differences and similarities between safety-critical and security-critical automotive systems, and the differences and similarities between system safety and system security engineering. Finally, the paper presents a system security engineering process based on the ISO 26262 Road Vehicles - Functional Safety process

framework [3], and describes why utilizing a familiar automotive process framework will help facilitate development and application of a system security engineering process for security-critical cyber-physical automotive systems, and how existing aspects of system safety engineering may be leveraged by system security engineering.

MOTIVATION

Security in the IT domain is more widely known, and though there are still some difficult areas, there is a great deal of experience with IT security. Some of this knowledge and experience may be able to be transferred into the automotive domain, however, there are some significant differences/considerations between IT security and cybersecurity with respect to cyber-physical automotive systems. For example, security of cyber-physical systems needs to address sensors and actuators that interact with the environment around the system, so unlike IT systems, security of cyber-physical systems must also consider the environment around the control system and cyber-physical system. This difference leads to different security countermeasures for cyber-physical systems than for IT systems.

There are a variety of ways today's vehicles are connected to extra-vehicle media (media that interfaces with a vehicle's infotainment system), including Bluetooth, CD's, USB's, etc. Some vehicles today, and more vehicles in the future, will not only be connected to extra-vehicle media, but also to other vehicles and vehicle infrastructure. This present and future interconnectivity creates the potential for cyber-attacks on vehicles and vehicle infrastructure. Given that potential safety, privacy, operational, and financial losses may occur as the result of an attack either directly or indirectly on vehicles and/or infrastructure, it is desirable to perform activities to reduce the likelihood of a successful attack.

Examples of potential losses in each of the categories associated with attacks on vehicles include [4]:

- Safety - a vulnerability that allows access, either directly or indirectly, to a safety-critical system that results in that system being compromised and potentially leading to a hazard.
- Operational - a vulnerability that allows access, either directly or indirectly, to a non-safety-critical system that leads to a denial of service of that operation.
- Financial - a vulnerability that allows multiple systems to be compromised and results in extortion. Warranty fraud is another example of financial losses.
- Privacy - a vulnerability that allows personal information to be compromised or that allows personal conversations in the vehicle to be monitored.

Reducing the likelihood of a successful attack can be likened to reducing the likelihood of potential hazards. To reduce the likelihood of potential hazards from occurring, the automotive industry applies the principles of system safety

engineering in the design and development of safety-critical systems. In a parallel way, to reduce the likelihood of successful cyber-attacks on vehicles, the automotive industry may apply principles of system security engineering to the design and development of security-critical cyber-physical automotive systems. The following sections of this paper describe some of the differences and similarities between system safety and system security, safety-critical systems and security-critical systems, and system safety and system security engineering. Finally, the paper presents a system security engineering process based on the ISO 26262 process framework. The paper describes the benefits of using a process framework familiar to the automotive industry and the ways using a process framework based on ISO 26262 will help leverage certain process elements and activities that may already be defined as part of a company's system safety engineering process.

This paper does not purport utilizing an existing system safety process and applying it to system security. As will be discussed in the paper, the two areas are unique and therefore require different considerations and activities. However, it is possible to capitalize on existing work that has been done with respect to system safety engineering in the automotive domain, and it would be beneficial to leverage what has been learned in automotive system safety rather than starting from scratch with respect to system security engineering.

SYSTEM SAFETY AND SYSTEM SECURITY

System safety is the state of a system that does not cause harm to life, property, or the environment. System security is the state of a system that does not allow exploitation of vulnerabilities to lead to financial, operational, privacy, or safety losses. All safety-critical systems are security-critical since a cyber-attack either directly or indirectly on a safety-critical system could lead to potential safety losses (Figure 1). Not all security-critical systems are safety-critical since cyber-attacks on security-critical systems can result in losses

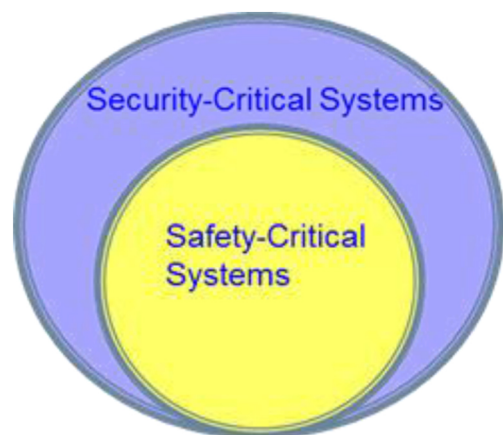


Figure 1. Relationship Between Safety-Critical and Security-Critical Systems.

other than safety losses; namely, privacy, operational, or financial. In addition, there is some overlap between the elements of system safety engineering and the elements of system security engineering, but the elements are not identical between the two engineering disciplines (Figure 2).

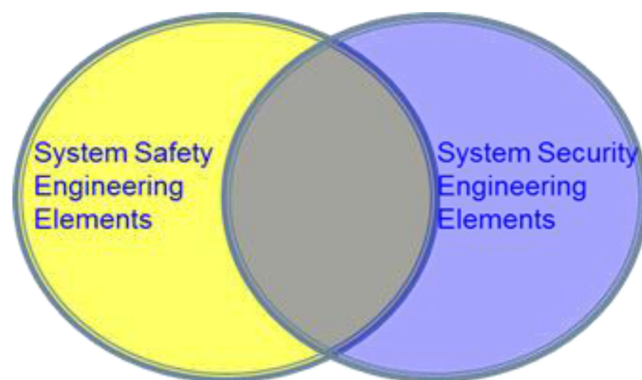


Figure 2. Relationship Between System Safety and System Security Engineering Elements.

System Safety and System Security Engineering Parallels

The objectives of system safety and system security engineering parallel each other. The goal of both engineering activities is, if possible, to build safety in to the design or to build security into the design, rather than attempting to add safety and security on to an existing design.

System safety and system security engineering process elements parallel each other. In the concept phase of a system safety engineering process a hazard analysis and risk assessment is performed. Paralleling this in a system security engineering process, a threat analysis and risk assessment is performed during the concept phase. In the requirements phase of a system safety engineering process safety requirements are derived and refined from the safety goals identified in the hazard analysis and risk assessment. Likewise, in the requirements phase of a system security engineering process, security requirements are derived and refined from the security goals identified in the threat analysis and risk assessment. In the design phase of a system safety engineering process detailed hazard analysis is performed on the highest risk hazards to help identify controls or safety mechanisms to help eliminate the potential hazards or to help mitigate the consequences should they occur. Likewise, in the design phase of a system security engineering process, detailed threat analysis is performed to help identify security countermeasures to help reduce the likelihood of a successful attack. Parallels between process elements continue through product development and verification. Though there are many parallels among the process elements between system safety and system security engineering, the underlying application of the process

elements may be unique between the two engineering disciplines.

Unique Aspects of System Safety and System Security

System safety and system security are unique from each other. Whilst system safety focuses on analyzing the system for potential hazards to identify safety mechanisms that can be integrated into the design to address the causes of the potential hazards to reduce the risk associated with the potential hazards, system security considers potential threats posed by a malicious attacker whose goal is to cause harm, wreak havoc, or gain financial benefits. With the exception of vehicle theft and odometer fraud, automotive engineers have historically not considered a malicious attack on an automotive system.

Though there are parallels between hazard analysis and risk assessment and threat analysis and risk assessment, the response to identified threats is different from the response to identified hazards. Since potential threats involve intentional, malicious, and planned actions, they are more difficult to address than potential hazards. Addressing potential threats fully, may require the analysts to think like the attackers and it is difficult to try to anticipate the exact moves an attacker may take in order to add appropriate security countermeasures to protect against attacker's options. In system safety, analysts can more readily identify the potential hazards, identify the potential causes and take appropriate action to mitigate the potential consequences, or to eliminate the potential hazards all together. The reason is that causes of potential hazards can be determined based on experience, knowledge of the system, components, and interactions, etc., and potential causes may be unique for particular systems, but are not unknown. In addition, with respect to safety, statistics may be used for claiming an acceptable level of risk. However, this may not be the case for security.

A further difference between hazard analysis and risk assessment and threat analysis and risk assessment is that additional factors are considered with respect to threats and the risks associated with threats, that need not be considered with respect to hazards and the risks associated with hazards. These additional factors to consider in assessing the risks of potential threats include the knowledge required by an attacker (proprietary or publically available), the experience level of an attacker, the access to the system that is required by an attacker, if special equipment is needed by an attacker, etc. None of these factors need be considered in assessing the risks of potential hazards.

Another unique aspect with respect to system security and system safety is that with system security a broader focus is considered. In system safety we look at subsystems, whereas in system security, both subsystems and electrical architecture are considered. In system safety we focus on safety-critical systems, whereas in system security, both safety-critical and non-safety-critical systems need to be

considered; it is possible to access a safety-critical vehicle system from non-safety-critical vehicle systems such as in-vehicle entertainment systems for example. In addition, it is also possible for a safe state identified as part of the system safety engineering analyses to be exploited by an attacker, and this needs to be considered with respect to security. Exploiting safe states seems acceptable and would not lead to a safety threat, but it could lead to denial of service of a feature. Thus, traditional hazard controls are not sufficient as security countermeasures and as stated, may be used against a system by causing a denial of service to occur.

With system security, we are not concerned with random hardware failures, whereas these are a concern in system safety. This is because attackers are looking for vulnerabilities in the system that could be exploited. A random hardware failure may result in a vulnerability, but given that it is random and cannot be anticipated, the random failure would have to occur before an attacker were trying to attack the system and they would have to figure out the random vulnerability to exploit it before the random failure was detected and action taken in response to the failure. Though security is not concerned with random hardware failures, it is concerned with systematic hardware vulnerabilities. Since these are vulnerabilities that would be persistent, system security engineering would attempt to identify these and eliminate them.

With respect to detailed hazard analysis and detailed threat analysis, the analysis techniques may parallel each other, however, the methodologies and goals are unique. For example, a detailed hazard analysis technique may utilize Fault Tree Analysis (FTA). Paralleling this in system security, a detailed threat analysis technique may utilize Attack Tree Analysis (ATA). Though the methodologies parallel each other, they are unique. In Fault Tree Analysis we are identifying potential causes of the top hazard event and we are looking for single-point and multi-point random hardware failures. With Attack Tree Analysis we are not concerned with single-point and multi-point random hardware failures, but rather with determining potential paths that an attacker could take through the system to lead to the top level threat. The underlying goals are synonymous - in FTA we want to identify single and multi-point random hardware failures that may lead to the top hazard so we can add safety mechanisms to detect and mitigate, and in ATA we want to identify potential vulnerabilities that could be exploited to lead to the top level threat so we can identify security countermeasures to incorporate to eliminate the vulnerabilities or to make them more difficult to exploit.

In the implementation and verification stages, static code analysis used in system safety is used to help identify bugs that directly affect primary functionality. In system security, static code analysis is used to identify potential security vulnerabilities in the code. Valid or correct code from a safety perspective may still have security vulnerabilities.

Finally, some verification methods for security are different and more difficult than verification methods used in