HEAVENS

HEAling Vulnerabilities to ENhance Software Security and Safety

Project within FFI Fordonsutveckling

Mats Olsson, Volvo Technology AB

2016-04-29

This page is intentionally left blank

Content

FFI in short

FFI is a partnership between the Swedish government and automotive industry for joint funding of research, innovation and development concentrating on Climate & Environment and Safety. FFI has R&D activities

worth approx. €100 million per year, of which half is governmental funding. The background to the investment is that development within road transportation and Swedish automotive industry has big impact for growth. FFI will contribute to the following main goals: Reducing the environmental impact of transport, reducing the number killed and injured in traffic and Strengthening international competitiveness. Currently there are five collaboration programs: **Vehicle Development, Transport Efficiency, Vehicle and Traffic Safety, Energy & Environment and Sustainable Production Technology.**
For more information: www.vinnova.se/ffi**.**

1. Executive summary

Safety is traditionally regarded as one of the most important attributes in the automotive industry. In contrast, unfortunately security has hardly been addressed in software-intensive automotive systems, considering the initiation phase of the HEAVENS project. This is where the HEAVENS project comes into the picture: the project aims to identify security vulnerabilities in automotive systems and define methodologies along with tools to evaluate security. A common way of assessing security will improve the industry's ability to deliver safe and secure vehicles. The target of the HEAVENS project is to equip the "owners" with "countermeasures" to facilitate protecting their "assets" by minimizing the "risk" associated with the "vulnerabilities" that can be exploited by the "threats" originated from the "threat agents". Furthermore, the project intends to investigate the interplay of safety and security in the context of the automotive E/E systems.

Initial activities such as identifying automotive security related needs and requirements, identifying a set of use cases along with one or more misuse cases, establishing a common understanding of the related concepts, terminologies and security engineering processes alongside baseline architectures, provided the basis for the subsequent work.

We then investigated and critically reviewed state-of-the-art threat analysis and risk assessment methodologies along with processes, frameworks and tools related to various industrial domains, such as IT security, telecommunications, software engineering and defense. A harmonization to the automotive domain was performed and resulted in a systematic approach, including methods, processes and tool support, of deriving security requirements for automotive Electrical and/or Electronic (E/E) systems. We call it the **HEAVENS security model**. Similarly, a systematic approach, including framework to perform security testing and evaluation for automotive E/E systems was proposed.

Furthermore, a secure software development lifecycle for the automotive industry has been proposed with the goal of producing "**Security Case**" which is conceptually similar to the notion of "Safety Case" as described in the functional safety standard ISO 26262. A security case consists of security requirements along with arguments and evidence to establish that the security requirements are fulfilled while developing software. We suggested a set of activities, including testing and evaluation methods, to be performed during different phases of the development lifecycle and how the different activities can be performed to systematically construct a security case. In our aspiration trying to understand the applicability of existing standards in the context of the automotive domain we investigated a set of standards such as Information and IT Security (Common Criteria, ISO 27000), functional safety (ISO 26262) and industrial control systems security (IEC 62443). And based on the above we presented a secure coding and testing guideline, which aims to reduce the likelihood of implementing vulnerabilities as well as reducing the number of residual vulnerabilities in a released product.

Finally, we investigated the interplay of safety and security, considering ISO 26262, AUTOSAR and other relevant standards used in the automotive area. Common methods for risk assessment, design and architectural considerations, implementation aspects as well as techniques and tools for verification and validation are discussed from both safety and security perspectives. Safety and security considerations of in-vehicle network architectures such as domain-controlled network architectures and hypervisors are discussed. Safety mechanisms listed in the ISO 26262, AUTOSAR and IEC 61508 standards are identified and their applicability for security is considered. Correspondingly, security mechanisms listed in the IEC 62443 standard for industrial automation systems are identified and their applicability for safety is discussed. Tools for verification and validation of system safety and security are also discussed and a model level tool for performing attack injection based on fault injection techniques is presented.

The HEAVENS consortium consisted of the following companies and institutions: Arccore, Chalmers University of Technology, Combitech, Omegapoint, SP, Volvo Cars, Sectra Secure Solutions and Volvo Technology AB (below called Volvo GTT-ATR). The project, with a total budget of 11 041 685 SEK, started in April 2013 and ended in March 2016. Volvo GTT-ATR was the coordinator and main applicant.

2. Background

Electronics have invaded virtually all vehicle functions. It has been estimated that already today more than 90% of all vehicle innovations are centered around software and hardware [3]. In line with the trend, the concepts of safety are central in the automotive industry. On the contrary, unfortunately security is traditionally considered being of less importance compared to the safety issues. However, security and safety are highly intertwined. As a result, security must be considered more seriously alongside safety to achieve overall improvement in safety and security.

Automotive software security

Security is one of the attributes of dependability as shown in Figure 1 [15]. However, one fact has emerged from the security field: *Software will always have security problems* [4]. At the same time, an increasing degree of computerized control in the automotive industry brings with it a corresponding array of potential threats [5]. Compounding this issue, the attack surface for modern automobiles is growing swiftly as more safety mechanisms, sophisticated services and communication features are incorporated into vehicles. Finally, emerging vehicle-to-X (V2X) communications will only broaden the attack surface further [5].

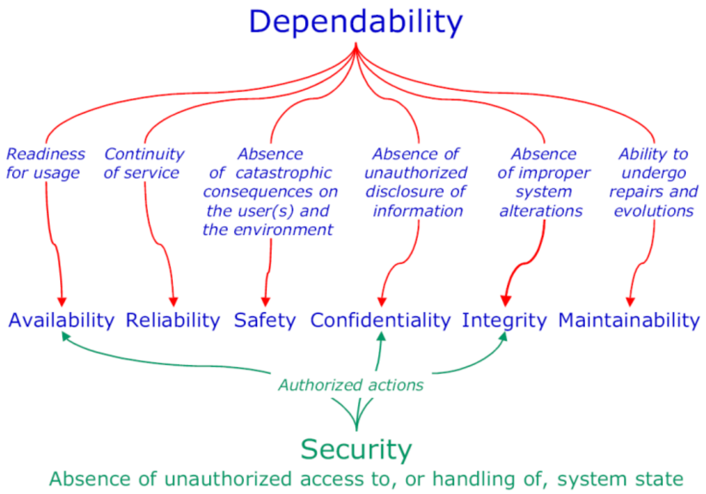
Dependability
Readiness for usage
Continuity of service
Absence of catastrophic consequences on the user(s) and the environment
Absence of unauthorized disclosure of information
Absence of improper system alterations
Ability to undergo repairs and evolutions
Availability
Reliability
Safety
Confidentiality
Integrity
Maintainability
Authorized actions
Security
Absence of unauthorized access to, or handling of, system state

Figure 1: Dependability attributes and security [15].

Overall, these trends suggest that a wide range of attack vectors will be available by which an attacker might gain access to internal vehicular networks— with unknown consequences [5]. *Unfortunately, very little is known about the practical security issues in road vehicles.* In the past, automotive software systems did not need security functions as there was very little incentive for malicious manipulation in traditional applications. Also, security tends to be an afterthought [1], i.e., not part of the original development process. Hence, adding security to legacy system as well as incorporating security features to new design constitutes multifold challenges.

Security and safety

Safety (active safety and passive safety) is a relatively well-studied field in the automotive industry. Security, on the other hand, has hardly been addressed in the context of automotive software. *Safety features are intended to protect against technical failures whereas security features are expected to protect against malicious manipulations* [3]. Software security is thus ensuring expected behavior of software in presence of malicious attacks. ISO 9126 defines security as a software quality attribute that bears on its ability to prevent unauthorized access, whether accidental or deliberate, to programs or data [12]. Figure 2 shows the interplay of safety and security in the automotive industry.

Security aspects are tightly coupled with safety aspects. A vehicle is most often closely related to a human being and this implies that security threats against the vehicle could potentially affect the safety of the human being involved [6]. Indeed, it has been demonstrated that it is possible to systematically control a wide array of components including engine, brakes, lights, etc. and combine these to mount attacks that represent potentially significant threats to personal safety [5]. For example, forcibly and completely disengage the brakes while driving, making it difficult for the driver to stop. Consequently, safety and security issues must be considered simultaneously.

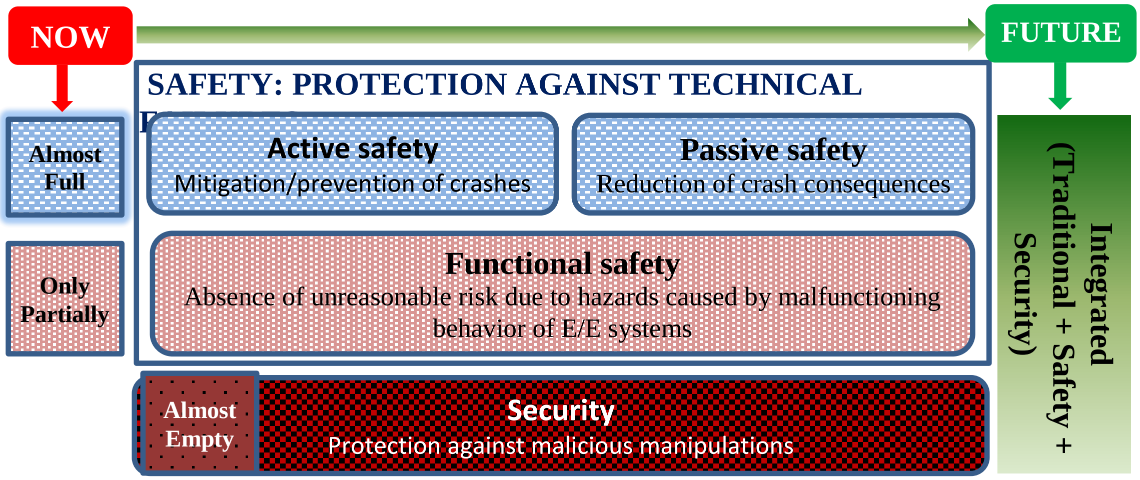
NOW
FUTURE
SAFETY: PROTECTION AGAINST TECHNICAL
F
Almost Full
Active safety
Mitigation/prevention of crashes
Passive safety
Reduction of crash consequences
Only Partially
Functional safety
Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems
Almost Empty
Security
Protection against malicious manipulations
Integrated (Traditional + Safety + Security)

Figure 2: Interplay of safety and security in the automotive industry: now and future.

Security, competitive advantage, uptime and revenue

Security issues and cases can potentially lead to increased revenue and uptime in the automotive industry. *Competitive advantage* can be maintained by preventing sensitive business data being read from internal systems by third parties. *Revenue* from aftermarket soft products can be increased by preventing illicit activation and/or modification of purchasable features. *Uptime* can be increased by avoiding illicit modifications that can make the system run out of specification as well as increase wear and tear. Finally, *integrity* of legislation regulated data, for example, related to emissions can be ensured.

3. Objective

Project goals

The project will focus on security aspects of the electrical and/or electronic (E/E) systems within automotive systems. The project goals are as follows:

- Study and identify state-of-the-art in security in the automotive industry.
- Identify needs and requirements of security in the automotive industry.
- Identify potential threats, threat agents and vulnerabilities to construct security models.
- Define methodologies and identify tool support for evaluating software security.
- Investigate the interplay of safety and security in the E/E architecture, considering ISO 26262, AUTOSAR and other relevant standards.
- Demonstrate proof of concepts.

Security vulnerabilities and security testing

Vulnerabilities are flaws that an attacker can exploit either intentionally or unintentionally to cause security breaches in terms of confidentiality, integrity and availability. As per CVE [14], security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network. Security vulnerabilities in software systems range from local implementation errors to much higher design-level mistakes [1]. Vulnerabilities typically fall into two categories – bugs at the implementation level and flaws at the design level [1].

Software security testing has recently been moved beyond its traditional goal to include probing software behavior as a critical aspect of system behavior [1]. Security testing can point to the areas of code which are most vulnerable by identifying risks in the system and creating tests driven by those risks. This eventually can provide a higher level of quality assurance than possible with classical testing. Consequently, *security testing* must involve two diverse approaches: (a) testing security mechanisms to ensure that their functionality is properly implemented and (b) performing risk-based security testing motivated by understanding and simulating the attacker's approach [1]. This project aims at performing risk-based security testing.

Security vulnerabilities and Software Development Lifecycle (SDLC)

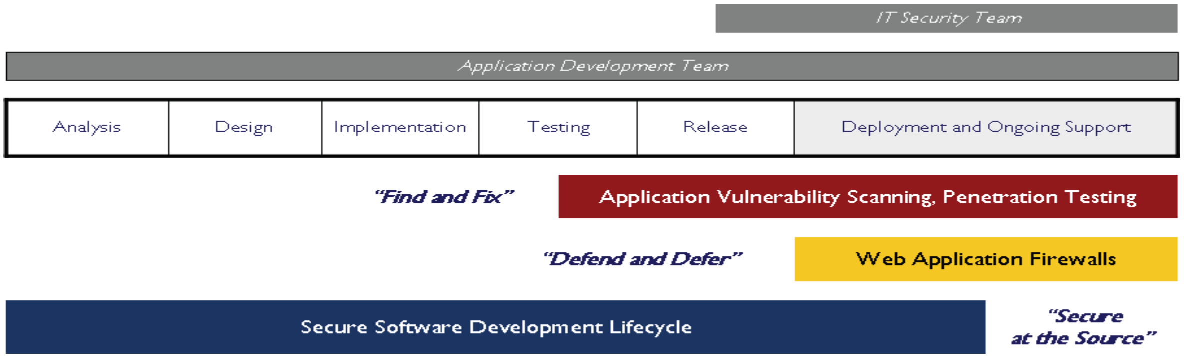
IT Security Team
Application Development Team
Analysis
Design
Implementation
Testing
Release
Deployment and Ongoing Support
"Find and Fix"
Application Vulnerability Scanning, Penetration Testing
"Defend and Defer"
Web Application Firewalls
Secure Software Development Lifecycle
"Secure at the Source"

Figure 3: Securing Your Applications – Three High-Level Strategies [7].

Based on current practices, Aberdeen found that companies leverage three distinct strategies to address the security threats and vulnerabilities associated with software [7]. In contrast to *find and fix* as well as *defend and defer* approach, *secure at the source* integrates tools and practices into the SDLC to increase the likelihood of eliminating security vulnerabilities even before applications are deployed. Aberdeen's analysis has revealed that companies adopting the *secure at the source* strategy realized *4.0 times return on their annual investments* in application security and higher than that of both the *find and fix* and *defend and defer* approaches [7]. The reason is that more application vulnerabilities were identified and remediated prior to deployment.

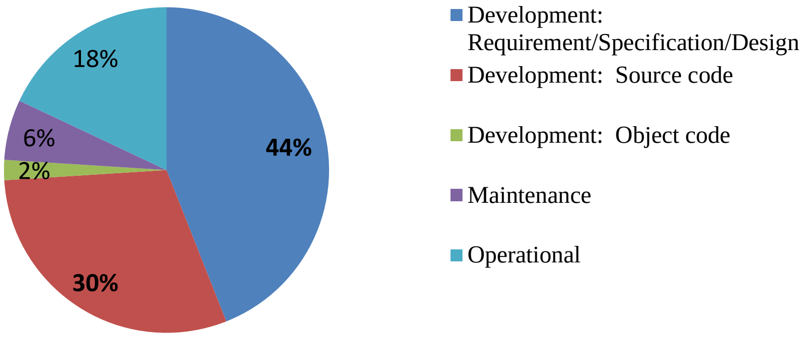

Figure 4: Taxonomy of security vulnerabilities: by time of introduction [2].

On the other hand, software engineering literature investigated the general question of *how and when* security vulnerabilities are introduced into software [2]. Carl et al [2] showed that about 76% of the total numbers of security vulnerabilities are introduced during the development phase – 44% at requirement/specification/design, 30% at source code and 2% at object code. Figure 4 shows the findings. Another recent study shows that approximately 50% of all security bugs or vulnerabilities occur at program code level [13]. *This clearly shows that we should primarily focus on software development phases that include software unit design and implementation*.

Security vulnerabilities, ISO 26262 and AUTOSAR

ISO 26262-6 (Part 6 of the standard) [10] states that mechanisms such as control flow monitoring and external monitoring facility shall be applied for error detection of safety-critical components. Furthermore, AUTOSAR [11] suggests implementing program flow monitoring related features while developing safety-critical software components. However, in addition to safety, control flow monitoring is closely related with detection and mitigation of security vulnerabilities because most security attacks aim to modify control flow maliciously. If the control-flow of a program can be determined statically, the actual control flow of the program then can be monitored at run-time. Hence *run-time monitoring and integrity checking of control flow can be beneficial to discover properties of control flow during testing and to detect malicious behavior during operation*.

At the same time, memory errors, including buffer overflows remain as leading cause of security vulnerabilities. These affect almost all applications, including embedded systems. Buffer overflows are one of the most commonly and widely exploited security vulnerabilities in programs in the history of computer security [8]. In a buffer overflow attack, the attacker’s aim is to gain access to a system by changing the control flow of a program. The US-CERT [9] shows that 11 out of 20 most widely exploited attacks are indeed buffer overflow attacks and reports over 200 buffer overflow vulnerabilities in 2011, many of which are in products of Microsoft, Adobe and Google. As a result, countermeasures must be developed to address such vulnerabilities. *To this end, the* *project will investigate control flow monitoring mechanisms to facilitate run-time monitoring and integrity checking of AUTOSAR-based systems*.

Approaches and methodologies

While there are standard ways to measure performance such as the SPEC CPU benchmarks, there is virtually no standard way of testing software security and comparing the defense coverage of any given method against a given set of vulnerabilities. *In this respect, the project aims to develop standard approaches of security testing and evaluate defense coverage of a given method*. The project intends to work with all the different components of security (Figure 5). The target is to equip the **"owners"** with **"countermeasures"** to facilitate protecting their **"assets"** by minimizing the **"risk"** associated with the **"vulnerabilities"** that can be exploited by the **"threats"** originated from the **"threat agents"**.

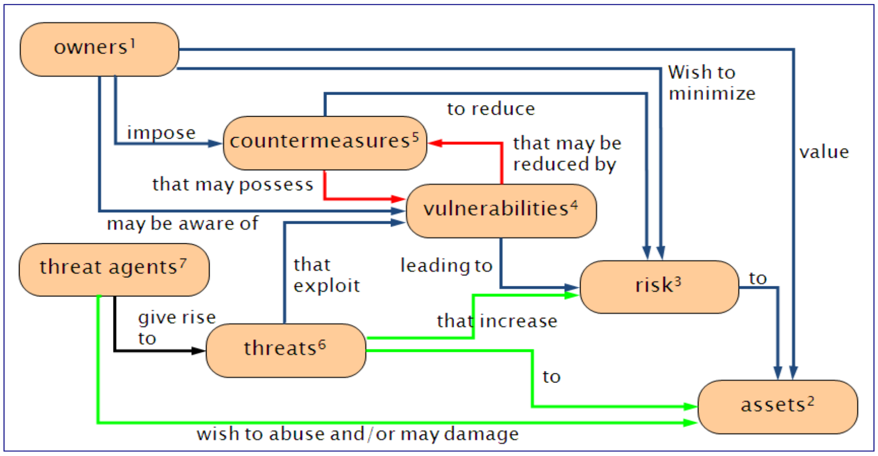

Figure 5: Components involved in security. Source: Information technology security techniques evaluation criteria for IT security part 1: Introduction and general model, International Standard ISO/IEC 15408-1, 2005.

This project emphasizes software unit design, implementation and testing phases of software development lifecycle as per Part 6 of ISO 26262 to identify potential vulnerabilities and evaluate their impact on software as well as on system. In particular, the project will investigate threat models and attack surface of the E/E system. Next, the project will perform studies to develop risk-based security test cases and methods of applying those test cases. Based on the results, the project will propose methods of reducing vulnerabilities to enhance security and incorporating the security related processes into the traditional SDLC. The project will define methods to deal with software security issues as early as possible in the traditional software development lifecycle. Finally, similar to the design and coding guidelines for using the programming languages in safety-related systems, the project will define guidelines for using the programming languages to support the security requirements of automotive embedded systems.

In this project, a number of different approaches, including the followings will be investigated:

- As most security attacks aim to modify control flow maliciously, run-time monitoring and integrity checking of control flow are valuable to detect malicious behavior during operation. Several control flow monitoring approaches will be investigated to find a suitable method of healing security vulnerabilities, considering ISO 26262 and AUTOSAR.
- Fault injection is a well-accepted technique of evaluating system behavior in presence of faults. Traditionally, fault injection is tightly coupled with reliability. In this project, suitability of fault injection will be investigated from security perspective to evaluate software behavior against a set of vulnerabilities and various relevant matrices will be measured.
- Use of signatures of software – both for securing the origin of the creator of information that is received over a communication link and also, before starting an application in an ECU.
- Applications of security aspects from other domains, for example, IT security in the context of the automotive E/E architecture.

While the methods that will be developed in the project are in general applicable to any software, the project will primarily focus on AUTOSAR-based systems. Similar to the concept of *Safety Element out of Context (SEooC)* as described in ISO 26262 [10], security testing in a target-independent way will be considered. The project will identify AUTOSAR and ISO 26262 specifications and requirements to identify the requirements that could be related to security.

Use cases of security testing

Software security testing and the derived results may be exploited in many different ways. The project will however focus on the following four specific use cases of security testing:

- *Profiling.* Profile software for identifying and highlighting strengths and weaknesses with respect to security vulnerabilities. For example, if a particular weakness in terms of vulnerabilities is found, efforts can be made to mitigate the vulnerability.
- *Comparison.* Compare suitability of an element with respect to security, during system development/integration. Several implementations of a given component might be available which are identical from functionality and safety perspectives. Then, methods and results of security testing can be used to select the most “secure” component.
- *Requirements.* Security-related requirements can be identified and communicated across OEM and suppliers using a common understanding of security vulnerabilities and their potential impact.

- *Safety properties.* Identification and evaluation of security vulnerabilities will assist in pinpointing the relationship between security and safety to provide valuable feedback to understand certain safety properties of software.

4. Project realization

The project consists of a number of work packages (WP) as shown in Figure 6. The project is detailed in WP1. The main technical works will be performed in WP2, WP3 and WP4. The developed concepts and methodologies will be demonstrated in WP5. The results will be exploited and disseminated in WP11 whereas the project coordination activities are part of WP10. Table 1 provides more details about the work packages and their contents along with the partners who will lead a particular WP and a sub-WP.

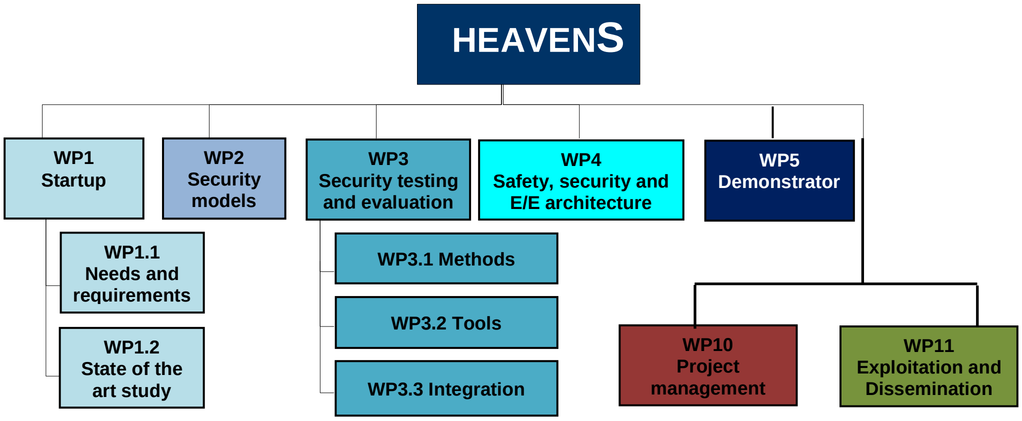
HEAVENS
WP1 Startup
WP2 Security models
WP3 Security testing and evaluation
WP4 Safety, security and E/E architecture
WP5 Demonstrator
WP1.1 Needs and requirements
WP1.2 State of the art study
WP3.1 Methods
WP3.2 Tools
WP3.3 Integration
WP10 Project management
WP11 Exploitation and Dissemination

Figure 6: Structure of the project.

Table 1: Work package details: title, contents and leaders.

WP1 Startup – Leader: VTEC	
Defines the requirements for the subsequent work packages, including overall goals; establish state of the art study and practice, investigate needs and requirements, identify use cases.	
WP1.1	Needs and requirements (VTEC). WP1.1 investigates how security models and testing could be used by different stake holders. The needs of the identified stake holders will be mapped to the use cases of security testing. Defines the details of the project plan, the goals and vision of the project, and ensures cooperation among the project partners.
WP1.2	State of the art study (Chalmers). Objective is to identify different methods and tools to evaluate different dimensions of software security and to establish the state-of-the art within this area in the context of the automotive industry.
WP2 Security models – Leader: CHALMERS	
Identifies owners, assets, risks, vulnerabilities, countermeasures, threat agents and threats. All the aspects will be put together to establish security models for the automotive industry. Security issues from software engineering and traditional networking as well as from other domains will be considered to map those in the context of the automotive domain.	
WP3 Security testing and evaluation – Leader: CHALMERS	
Defines methods and tools that are required to perform security testing and evaluation. Also, defines how to carry out	

experiments to evaluate the security aspects of software/system and how to utilize the results to improve overall security. The contents of this WP at the end will provide a framework, including guidelines and examples, for evaluating security. The relevant standards and software architectures such as ISO 26262 and AUTOSAR will be considered.	
WP3.1	Methods (Chalmers). Defines methods for security testing, analyzing the results and aspects related to experimentation.
WP3.2	Tools (Chalmers). Defines the necessary tools needed to implement the test cases and their interactions.
WP3.3	Integration (ARCCORE). Defines how to integrate security related processes and methods into the standard software development lifecycle. Defines design, coding and testing guidelines related to security.
WP4 Safety, security and E/E architecture – Leader: SP	
Identifies the interplay of safety and security in the context of the E/E architecture. The interactions among safety mechanisms and security mechanisms will be analysed to understand the impact (positive and negative) of safety mechanisms on security and vice versa. The goal is to understand the best possible trade-offs between safety and security requirements.	
WP5 Demonstrator – Leader: ARCCORE	
The concepts and methods that are developed in the previous WPs (WP2 – WP4) will be demonstrated by applying those to a set of selected uses cases to establish proof of concepts.	
WP10 Project Management – Leader: VTEC	
Overall project management. This work package also performs wrap-up activities at the end of the project.	
WP11 Exploitation & Dissemination – Leader: CHALMERS	
Deals with disseminating results and exploiting relevant and applicable results at the various project partner organisations, as well as in academia. In particular, we plan to have project workshops and seminars.	

5. Results and deliverables

The project will provide a framework to assist in assessing security of automotive E/E systems and an environment to demonstrate proof of concepts. Table 2 lists the deliverables and planned release dates in month (M). We consider two iterations of most of the deliverables so that lessons and experiences learned from the first evaluation can be exploited to achieve the project goals.

Table 2: Deliverables: title, contents and timeline.

Deliverable	Description	Release 1	Release 2
D1.1 Needs and requirements	Describes the needs and requirements that could be used by different stake holders in the product creation process. The needs of the identified stake holders are mapped to the uses of security testing and evaluation (comparison, profiling, requirements, and safety properties). Also, lists and describes the uses cases selected for the project.	M6	M18
R1.0 Project Terminologies	Attempts to harmonize the terms and definitions that will be used in the HEAVENS project. The goal is to establish a common view on definitions, usage and application of different terms within the project consortium to minimize ambiguities during the project lifetime. The definitions are collected from multiple sources, including relevant standards and specifications.	M6	M22
D1.2 State of the Art	A state of the art study and practice (methods, tools and so on) related to software security in automotive industry, other domains and other application areas, as well as scientific results in academia.	M6	M18
D2 Security	Describes different actors of security in automotive E/E systems. The actors	M12	M24

Deliverable	Description	Release 1	Release 2
models	include owner, asset, risk, vulnerabilities, countermeasure, threat agent and threats. The knowledge from other domains will be put into the context of the automotive industry.		
D3.1 Security evaluation framework	Framework to assist security evaluation in automotive E/E systems. This describes processes as well as methods and tools for performing security testing and evaluation. Links to ISO 26262, AUTOSAR and other relevant standards. Also, the integration of security aspects into the traditional software development lifecycle will be discussed.	M24	M36
D3.2 Coding and testing guidelines	Similar to the guidelines for the usage of programming languages in safety-critical systems, guidelines for using C programming language will be prepared from security perspective, including guidelines for performing security testing.	M36	
D4 Interplay of safety and security in E/E architecture	The relationship between safety and security, and the impacts of safety and security mechanisms on each other will be addressed. Approaches of integrating safety and security mechanisms in the E/E architecture to improve the overall dependability.	M24	M36
D5 Demonstrator	Developed concepts and methods will be demonstrated via a prototype and applications from the automotive domains.	M36	
D11.1 Workshops	After each major part of the project, we will have a project workshop for disseminating the major results from the project up until that point. These workshops may include a project internal part, and an open part.	Will be defined in WP1.	
D11.2 Seminars	Seminars on topics within the scope of the project will be held. Participants from both within and external to the project will be invited. Internal and external speakers and experts will be invited. Also, students related to the project will give presentations.	Will be defined in WP1.	

Delivery to FFI-goals

Table 3: Contribution to targets (Source: “Programbeskrivning för Fordonsutveckling”, Version 2011-02-01).

Vision and goal (English translation is made in-house.)	**Brief motivation**	**Level**
Specific for FFI Fordonsutveckling		
Fordonsel och elektronik. Gröna, Säkra och Anslutna fordon kräver hög nationell kompetens vilken är kapabel att utveckla komplexa elektriska system som nyttjar både ett nationellt och ett globalt utbud av forskning och teknik. *Green, Safe and Connected vehicles require high national competence which is able to develop complex electrical system that uses both a national and a global range of research and technology*	A corner stone in the development of green, safe and connected vehicles is the ability to ascertain that electrical system and software are indeed safe. However, if the underlying vehicle electronics does not provide the required level of security, the vehicles neither will be safe nor can be connected, regardless of the advancements in safety systems. HEAVENS provides the fundamental basis for this, enabling evaluation of concepts and solutions with respect to security.	High
Inbyggda system och mjukvara. Etablera nationell kompetens som förmår att utveckla komplexa inbyggda mjukvarusystem. Gröna, Säkra och Anslutna fordon kräver hög nationell kompetens vilken är kapabel att utveckla komplexa elektriska system som nyttjar både ett nationellt och ett globalt utbud av forskning och teknik *Establish national skills able to develop complex embedded software system. Green, Safe and Connected vehicles require high national skills which is capable of developing complex electronic systems that*	HEAVENS will come up with methods of evaluating security and provide a framework to support security testing and provide skills that are necessary to develop automotive embedded software in a more efficient way. Also, the project will study the interplay of safety and security in the automotive E/E architecture. This will provide technology at the national level to facilitate the development of safe and connected vehicles. HEAVENS will also continuously	High

Vision and goal (English translation is made in-house.)	**Brief motivation**	**Level**
utilize both a national and a global range of research and technology	disseminate results to increase national skills in security.	
Materialteknik för effektivare fordon. Fordonsindustrin har fått användbara och innovativa material samt tillgång till nydanande materialanvändning	The project does not deal with material technology.	Low
Metoder och verktyg för fordonsutveckling. Etablera världsledande metoder och verktyg för fordonsutveckling. Säkerställa att den svenska fordonsindustrin bidrar och får tillgång till metoder, verktyg och kompetens i världsklass för att möjliggöra snabb och effektiv utveckling *Establish a world-leading methodologies and tools for vehicle development. Ensure that the Swedish automotive industry contribute and access methods tools and world-class expertise to enable rapid and effective development*	HEAVENS will identify and apply new methods and tools for assessing security of software-intensive automotive systems. The project will propose methods and processes to be integrated into the traditional product development lifecycle. Also, the project will provide guidelines for using the commonly used programming languages to develop software in line with the security requirements. These will assist Swedish automotive industry with methods, tools and world-class expertise to enable rapid and efficient development.	Medium
Overall for FFI, in the areas Climate & Environment and Safety		
Höja den tekniska mognadsgraden (genom att mäta ”technology readyness level”, TRL) samt effektivisera metoder inom produktutveckling för att snabbare kunna industrialisera resultaten och öka kundvärdet *Improve the technical maturity (by measuring the "technology readiness level ", TRL), and streamline practices in product development for more rapidly industrialize results and increase customer value*	The project identifies needs and requirements of the Swedish automotive industry, derives security models and proposes methods as well as tools for security testing and evaluation. All these increases the TRL in the area of vehicle development. Furthermore, the project will integrate security aspects into traditional product development. Finally, HEAVENS will actively disseminate results and knowledge.	High
Genom ökad forsknings- och innovationskapacitet i Sverige säkra fordonsindustriell konkurrenskraft och arbetstillfällen på lång sikt och helst även på kort sikt *Through increased research and innovation capacity in Sweden secure competitiveness and jobs in the automotive industry in the long term and preferably also in the short term*	Because of in-vehicle networks and emerging vehicle-to-X communications, security issues will have profound impact on vehicle electronics and development in foreseeable future. Efficient handling of security issues will thus increase the competitiveness of the Swedish automotive industry.	High
Utveckla internationellt uppkopplade och konkurrenskraftiga forsknings- och innovationsmiljöer, i vilka bland andra akademi, institut och industri samverkar *Develop internationally connected and competitive research and innovation environments, in which among others academia, institutes and industry collaborate*	HEAVENS brings together several Swedish automotive players along with academia and research institute in the area of security and safety to find a common view on how security shall be assessed in automotive electronic systems as well as how to develop an integrated view on safety and security in the E/E architecture.	Medium
Främja internationell forsknings och innovationsverksamhet där förutsättningar för medverkan i EU:s ramprogram och annan internationell forsknings- och innovationssamverkan noga värderas *Facilitate international research and innovation collaboration where prerequisites for participation in the framework programmes of the EU and other international research and innovation collaboration is scrutinized*	Security assessment is a well-established area in the networking community. However, the automotive industry has not come together in their ways to perform and interpret security assessments. HEAVENS will provide the partners with strong results combining research and industrial relevance. This increases their attractiveness in future international research and collaboration projects.	High

Uniqueness, new values and Technology Readiness Level (TRL)

Safety has since long been at the core of the Swedish automotive industry. However, security testing and evaluation along with the adoption of security models in the context of the Swedish automotive industry is still in its infancy. Importantly, the intertwining relationship between security and safety in relation to the E/E architecture has hardly been investigated and established. To this end, the HEAVENS project attempts to bring in new values by:

- Uniting several Swedish automotive players (OEM and tool provider) and academia as well as research institute to identify and evaluate the needs and requirements in relation to security, and thus develop efficient communication across the partners in the automotive industry so that everyone *speaks the same language in terms of security*.
- Creating a consolidated view on how to derive security model and perform security testing in the context of automotive embedded systems to increase national competences and skills. This will not only facilitate cost- and time-effective realization of automotive embedded systems but also increase the overall awareness of security and related aspects.
- Investigating interweaved relationship between safety and security in the E/E architecture and contributing to the skills and tools required to develop “Green, Safe and Connected vehicles”.
- Aiming to reach the technical maturity level TRL 4.

All in all, the above creates positive impact on the competitive advantages of the Swedish automotive industry, and assists in guiding Swedish automotive industry to be an internationally leading force in dealing with security issues.

6. Dissemination and publications

Knowledge and results dissemination

Information, i.e. deliverables and other reports, that describes results and findings in the HEAVENS project is available for all employees within the Volvo Group, for project partners and for certain selected third parties. A number of activities for the dissemination of project results have been arranged as external and/or internal seminars and workshops. In addition, a new FFI project within the automotive security area, called HOLISEC, started in April 2016. It is based on the HEAVENS project and its main goal is to further develop the process of deriving security requirements and to perform security testing and evaluation for the automotive domain.

Security standardization initiatives have been carried out, which have caught a lot of attention from SAE J3061, AUTOSAR WP-X-SEC and NHTSA.

AUTOSAR WP-X-SEC has decided to use the HEAVENS deliverable R1.0 Project Terminologies as their glossary.

The dissemination activities performed within the project timeframe are as follows (Table 4).

Table 4. Performed dissemination activities in the HEAVENS project.

Date	Event	Main Topics
2013-05-20	First open seminar	• A Crash Course on Security (Tomas Olovsson, Chalmers) • Electrical System Security Context and Security Engineering for C2X (Henrik Broberg, Volvo Cars) • Securing the Connected Car Security (Tomas Olovsson, Chalmers) • Exploring Vulnerabilities - A Brief Hacking Overview (Mattias Jidhage, Omegapoint) • License Protections & Software Cracking (Peter Magnusson, Omegapoint)
2013-09-25	AUTOSAR seminar	• AUTOSAR Introduction (Tobias Johansson, Arccore) • ArcCore Tools (Tobias Johansson, Arccore) • AUTOSAR in Product Development at Volvo (Jens Svensson, Volvo)
2013-12-04	Internal seminar	• State-of-the-art in security in the automotive industry (Mafijul Islam, Volvo GTT-ATR) • Data security: A GTT perspective (Andreas Bokesand, Volvo GTT-VE) • Security evaluation and testing using static analysis (Christian Sandberg, Volvo GTT-ATR)
2014-03-04	Data security seminar	• Security in the Telecom Area (Ulf Larsson, Ericsson) • Automotive Penetration Testing (Mattias Jidhage, Omegapoint)
2014-04-17	External presentation for SAE	• HEAVENS, Overview of Activities and Results (Mafijul Islam, Christian Sandberg, Volvo GTT-ATR, Henrik Broberg Volvo Cars)
2014-10-10	Second open seminar	• Overview of HEAVENS (Mafijul Islam, Volvo GTT-ATR) • State-of-the-Art and Terminologies (Anders Hansson, Sectra Secure Solutions) • Needs and Requirements (Andreas Bokesand, Volvo GTT-VE) • Heavens Security Model (Aljoscha Lautenbach, Chalmers) • Workflow and Tool Demonstration (Christian Sandberg, Volvo GTT-ATR) • Summary and Future Work (Mafijul Islam, Volvo GTT-ATR)
2015-01-15	Announcement by AUTOSAR WP-X-SEC	• Proposal to use the HEAVENS glossary on Security In AUTOSAR (Marc Stoettinger)
2015-02-12	AUTOSAR WP-X-SEC meeting	• ETAS presented HEAVENS Security Model and how it can be applied to use-case “Secure Storage” (Bernard Bavoux, Armin

		Happel, Hamit Hacioglu)
2015-06-09	Third open seminar	• Introduction to HEAVENS –Background and Progress (Christian Sandberg, Volvo GTT-ATR) • Vehicle Control Unit Security using Open Source AUTOSAR (Anton Bretting and Mei Ha, Chalmers) • Testing and Evaluation to Improve Data Security in Automotive Embedded Systems (Filip Hesslund and Johannes Weschke, Chalmers) • A framework for software security testing and evaluation (Rahul Kumar Dutta, LiTH) • Security Evaluation of Automotive Ethernet (Linus Book, Chalmers)
2016-04-07	Fourth open seminar	• HEAVENS –Project summary (Mafijul Islam, Volvo GTT-ATR) • Secure Software Development (Christian Sandberg, Volvo GTT-ATR) • Penetration Testing (Mattias Jidhage, Omegapoint) • Safety, Security and E/E Architecture (Peter Folkesson, SP) • Secure Onboard Communication (Karl Erlandsson, Arccore)

Publications

A Risk Assessment Framework for Automotive Embedded Systems **(**Mafijul Islam, Aljoscha Lautenbach, Christian Sandberg and Tomas Olovsson)**.**
2nd ACM Cyber-Physical System Security Workshop (CPSS 2016), May 30, 2016.

Master Thesis Works

Vehicle Control Unit Security using Open Source AUTOSAR (Anton Bretting and Mei Ha). This thesis report presents a case study where two variants of Microsoft's threat modeling technique STRIDE are applied to a limited part of the AUTOSAR platform.

Testing and Evaluation to Improve Data Security in Automotive Embedded Systems (Filip Hesslund and Johannes Weschke). This thesis conducts a threat analysis and risk assessment for the DCM module inside AUTOSAR. Also an evaluation of the security of an engine control ECU by investigating how a possible intrusion can affect the overall safety.

A framework for software security testing and evaluation (Rahul Kumar Dutta). Implements a security evaluation framework that allows us to improve security in automotive software by identifying and removing software security vulnerabilities that arise due to input invalidation reasons during SDLC.

Threat Modelling and Risk Assessment Within Vehicular Systems (Sathya Prakash Kadhirvelan and Andrew Söderberg-Rivkin).
This thesis conducts an analysis of current threat modeling and risk assessment methodologies, the adaptations created to make these methodologies applicable to vehicular systems and a comparison of each. From these described activities a process for threat modeling and risk assessment has been created.

Security Evaluation of Automotive Ethernet (Linus Book). Ongoing.

7. Conclusions and future research

We have presented the HEAVENS security model, which is a systematic approach, including methods, processes and tool support, of deriving security requirements and to perform security testing and evaluation for automotive Electrical and/or Electronic (E/E) systems. Although the security model has attracted quite a lot of interest from standardization organizations such as SAE J3061, AUTOSAR WP-X-SEC and NHTSA, we believe that more research and refinement is needed before it can reliably be integrated into a generic secure software development lifecycle for the automotive industry. Therefore, a new FFI project, called HOLISEC, was started in April 2016. It is based on the results from the HEAVENS project and its main goal is to further develop the process of deriving security requirements and to perform security testing and evaluation for the automotive industry.

Below we summarize the findings from the HEAVENS project as well as points to potential future works.

- Introduces basic dependability and security concepts, including security attributes and security objectives that shall be considered in the HEAVENS project.
- Introduces basic concepts of system engineering processes from security perspective. Identifies potential stakeholders, assets, application characteristics, threats and attackers along with approaches of threat analysis, risk assessment and risk mitigation. Defines various means (forecasting, prevention, detection, isolation, recovery, and forensics) of risk mitigation.
- Establishes a common view on relevant definitions and terminologies that shall be applied consistently in the HEAVENS project.
- Provides baseline architectures of ITS, in-vehicle network and in-vehicle software to be used in the HEAVENS project.
- Identifies and explains a set of use cases to have a better understanding of security needs in the automotive E/E systems and consequently, derives security requirements based on needs.

Potential future works include:

- In-depth study and analysis of potential stakeholders, assets, vulnerabilities, threats, attacks, attackers, risks and countermeasures to systematically establish relationship among those to address the identified needs and requirements.
- Exploring state-of-the-art study and practice to determine how risk mitigation can be done based on what is available today and to identify the gaps.
- Refining the use cases to provide more information in operational descriptions and scenarios as well as associated misuse or abuse cases.

8. Participating parties and contact persons

Volvo Technology AB
Mafijul Islam
mafijul.islam@volvo.com
+46 31 3228296

Volvo Technology AB
Christian Sandberg
christian.sandberg@volvo.com
+46 31 3226094

Volvo Technology AB
Mats Olsson
mats.olsson.2@volvo.com
+46 31 323 59 11

Chalmers Tekniska Högskola
Tomas Olovsson
tomas.olovsson@chalmers.se
+46 31 772 16 88

Combitech AB
Daniel Eriksson
daniel.eriksson@combitech.se

SP Technical Research Institute of Sweden
Jonny Vinter
jonny.vinter@sp.se
+46 10-516 53 59

Arccore AB
Mårten Hildell
marten.hildell@arccore.com
+46 31 301 28 30

Volvo Car Corporation
Jörgen Borg
jorgen.borg@volvocars.com
+46 31 59 26 61

Sectra Secure Solutions AB

Anders Hansson
anders.hansson@sectra.se
+46 13-23 52 76

Omegapoint AB
Anders Mutén
Anders.Muten@omegapoint.se
+46 766-27 54 57

9. References

[1] B. Potter and G. McGraw, “Software Security Testing”, IEEE Security and Privacy, pp.32 - 36, 2004.

[2] C. E. Landwehr et. al., “A Taxonomy of Computer Program Security Flaws, with Examples”, *ACM Computing Surveys 26*, 3, September 1994.

[3] K. Lemke et. al., “Embedded Security in Cars”, Springer-Verlag Berlin Heidelberg, 2006.

[4] A. Takanen et. al., “Fuzzing for Software Security Testing and Quality Assurance”, ISBN 13: 978-1-59693-214-2, ARTECH HOUSE, INC., USA, 2004.

[5] K. Koscher et. al., “Experimental Security Analysis of a Modern Automobile”, In *Proc. of IEEE Symposium on Security and Privacy*, 2010.

[6] D. Nilsson, “How to Secure the Connected Car”, PhD Thesis, Chalmers, 2009.

[7] Aberdeen group, “Securing Your Applications: Three Ways to Play”, Research brief, December 2010.

[8] J. Wilander et. al., “RIPE: Runtime Intrusion Prevention Evaluator”, In *Proc. of ACSAC*, 2011.

[9] US-CERT, Vulnerability notes database, http://www.kb.cert.org/vuls.

[10] ISO 26262 Road Vehicles – Functional Safety

[11] AUTOSAR – AUTomotive Open System Architecture. http://www.autosar.org.

[12] ISO 9126 Software engineering – Product quality

[13] H. Shahriar and M. Zulkernine, “Mitigating Program Security Vulnerabilities: Approaches and Challenges”, *ACM Computing Surveys 44*, 3, Article 11, June 2012.

[14] CVE, Common Vulnerabilities and Exposures, http://cve.mitre.org/

[15] A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing”, IEEE Trans. on Dependable and Secure Computing, 1(1):11-33, Jan 2004.