HoliSec

Automotive Security and Privacy

Holistic Approach to Improve Data Security

Report type	**Deliverable D4.1.1**
Report name	**Tailoring the HEAVENS risk assessment methodology for improved performance**
Dissemination level	**Public**
Status	**Released**
Version number	**1.0**
Date of preparation	**2018-03-20**

Authors

Authors	E-mail
Christian Sandberg	christian.sandberg@volvo.com

Contributors	E-mail
Andreas Bokesand	andreas.bokesand@volvo.com
Urban Thorsson	urban.thorsson@volvo.om

TC Review	E-mail

Revision chart and history log

Version	Date	Reason
0.1	2018-01-30	Creation of the initial draft
0.2	2018-03-05	Draft for internal HoliSec review
1.0	2018-03-20	Created released version following review round

Table of contents

1 Introduction

This document corresponds to deliverable "**D4.1.1 Tailoring the HEAVENS risk assessment methodology for improved performance**" of the **HoliSec** project. The deliverable summarizes improvement activities related to the use of the HEAVENS risk assessment methodology within the scope of work package **WP4** (**Secure development & governance**) of the HoliSec project.

1.1 Background

Security engineering is an engineering discipline concerned with securing a system, encompassing the entire process from system design to deployment and maintenance; however the influence of data security mechanisms on safety still needs research and investigations.

To address this, the HoliSec project was launched in April 2016. The project targets a holistic approach to improve data security of safety-related embedded systems.

In 2014, Islam et al [1] presented the "HEAVENS Security Model", a methodology to facilitate deriving security requirements for the automotive E/E systems. Since its' first publication it has been described as a best practice methodology in the first industry standard for automotive cybersecurity engineering, SAE J3061 [2], been identified as one of the most applicable TARA methodologies for early development phases by Macher et al [3] and adopted by OEMs and suppliers to the automotive industry.

1.2 Objective

The objective of this deliverable is to describe the lessons learned from applying the HEAVENS risk assessment methodology in OEM projects and propose ways to tailor the methodology for improved performance. Rather than bringing up pros and cons of the methodology, the document focuses solely on the areas of improvement concerning risk assessment.

The document assumes knowledge about the HEAVENS security model and information will only briefly be repeated.

1.3 Document outline

The remainder of the deliverable is structured as follows. Chapter 2 identifies areas of the HEAVENS methodology that has shown costly, e.g. in terms of time consumption during risk assessment activities. Chapter 3 presents tailoring proposals to the HEAVENS methodology to address areas of concern identified in Chapter 2. Finally, Chapter 4 presents ideas for future methodology improvement.

2 Observations of the HEAVENS risk assessment methodology in real projects

Observing the use of the HEAVENS methodology for Risk assessment in multiple OEM projects have shown that certain parts of the process take an extraordinary amount of time compared to other parts, especially during concept phase of product development. These observations have been categorised and further described in the following chapter

.

Risk assessment in the HEAVENS methodology involves rating of a set of Threat Level (TL) (Expertise, Window of opportunity, Knowledge about TOE, Equipment) and Impact Level (Safety, Financial, Operational, Privacy/Legislation) parameters for each asset/threat pair as identified during the Threat analysis step in the workflow. As aid to the practitioners of the methodology, guidance is given as how to do the rating, however, organisations would likely tailor weights and definitions of the risk assessment to match the views of the business as well as risk appetite. Two main areas were identified as improvement areas, speed and consistency.

Speed

Risk assessment involves gathering people with different knowledge, a facilitator driving the risk assessment, security experts and domain experts, to discuss and rate a set of parameter for threats and assets. Prolonged discussions lead to multiple meetings, more time spent and increased lead time to finish the activity.

From the eight TL/IL parameters to be rated for each threat asset pair, the following showed need of significant more discussion among the Risk Assessment participants than the rest

- Window of opportunity
- Financial

Consistency

Comparing the results of different Risk Assessment teams showed consistency issues, even from the same team but at different points in time, such as risk assessments separated weeks in between. Risk assessment has a subjectivity component which ideally is minimized. The greatest inconsistencies were found in the rating of the same parameters that also triggered long discussions, Window of opportunity and Financial, but most of the parameters were identified as needing improvement in this area.

3 A tailored risk assessment approach for increased performance

The root cause of the issues related both the speed of the analysis and the consistency of the results was found to be in the definitions of the parameters; sometimes they were too vague or confusing in their descriptions, sometimes not easy to map to the problem being discussed, and were in need of clarification and tailored redefinition.

This chapter shows on per-parameter basis how tailoring/redefinitions have been made to improve speed of assessment and consistency of the result.

3.1.1 Threat level parameters

3.1.1.1 Expertise

The level of expertise required to mount an attack is dynamic over time and an attack that requires an Expert to perform at one point in time, may only require a Proficient or Layman person following the development of tools or detailed instructions. For this reason, “Expertise”, is tightly linked to all other Likelihood parameters, “Knowledge about TOE”, “Equipment” and “Window of opportunity”; and it is recommended that rating of “Expertise” is assessed after the other three, as indicated by Figure 1.

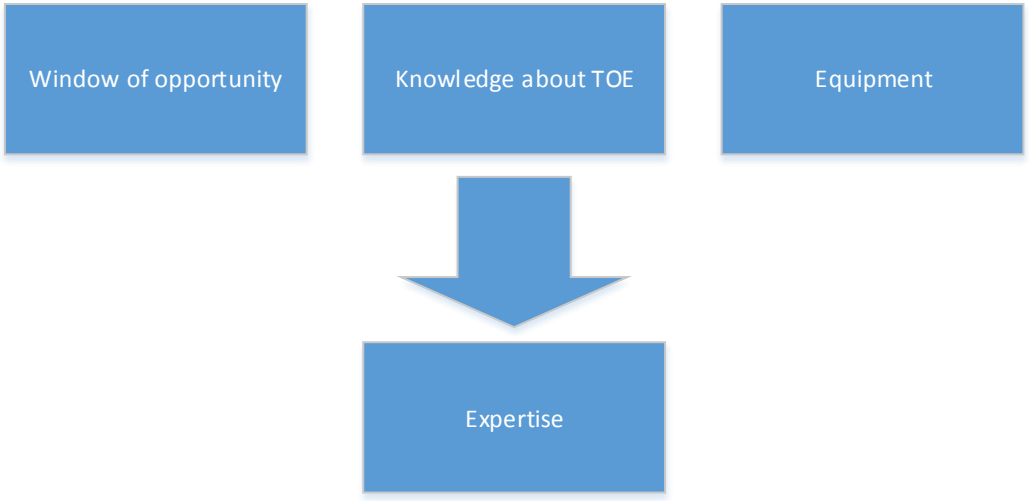


Figure 1Threat level parameter dependencies

3.1.1.1.1 Layman

HEAVENS definition

> *"Layman is unknowledgeable compared to experts or proficient persons, with no particular expertise; Examples may include persons who can only follow simple instructions that come with the available tools to mount simple attacks, but not capable of making progresses himself/herself if the instructions or the tools do not work as expected."*

A Layman has very limited knowledge about the electronics of modern vehicles, and may e.g. be a driver who wants to perform some operation on his own using a tool bought online with simple instructions, a fleet owner or a "script kiddie". A Layman is also not comfortable/able to disassemble/remove parts on a vehicle to be able to perform a hack. Furthermore, on the IT side, a Layman may install software applications in a PC, perform operations in the software given good instructions and connect cables between the PC and the vehicle, given that connectors are easily accessible. A Layman possesses average IT skills expected for domestic usage, e.g. how to connect standard connectors, connect to Wi-Fi networks, use Bluetooth and USB.

Links to other Threat Level parameters:

- A Layman uses "**Standard**" "**Equipment**"
- Since a Layman uses ready-made material that is likely to be purchasable online and documented, the "**Knowledge about TOE**" is to be considered "**Public**". Even if the information was initially Sensitive, if it has been leaked online, is documented and purchasable, it shall then be considered public.
- A Layman is not able to perform complex disassembly

3.1.1.1.2 Proficient

HEAVENS definition

> *"Proficient persons have general knowledge about the security field and are involved in the business, for example, workshop professionals. Proficient persons know about simple and popular attacks. They are capable of mounting attacks, for example, odometer tuning and installing counterfeit parts, by using available tools and if required, are capable of improvising to achieve the desired results. "*

A Proficient person is someone the Layman would hire to perform attacks he is not able to perform himself. The proficient person does not develop new attacks, but uses ready-made tools, is able to improvise, is not hindered by having to disassemble/remove parts of a vehicle, use multiple applications on a PC that may be poorly documented, and may have some basic knowledge about security mechanisms in place. The typical Proficient profile would be an advanced workshop professional; who is used to work with vehicles and tools used to interface with the vehicles. He may have downloaded/purchased tools made by experts and is performing services to modify vehicles for financial gain. The Proficient person may without trouble use tools developed by an expert and may, if needed, find more information using internet forums, websites and contacts to achieve the goals.

Links to other Threat Level parameters:

- A Proficient person uses "**Standard**" and "**Specialized**" "**Equipment"**
- A Proficient person may have "**Standard**" or "**Restricted**" "**Knowledge about TOE**". The reason is that as e.g., a workshop professional may have access to both these levels of information, and they are more likely to access information distributed in e.g. internet forums.

3.1.1.1.3 Expert

HEAVENS definition

> *"Expert is familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type."*

The Expert has the ability to analyse systems, exploit vulnerabilities and develop tools to perform attacks. An expert is typically an engineer with experience from working with automotive systems, or systems similar to that of the TOE and is knowledgeable in how these kinds of systems work. With the introduction of more and more parts from the IT domain in modern vehicles, such as Ethernet, Bluetooth, Android/IOS applications, an expert does not necessarily have automotive engineering experience, but at least in-depth experience with the components/protocols/algorithms used by the TOE. The main difference between the Proficient person and Expert is that the Expert is capable of developing tools and methods to accomplish a goal, whereas both Layman and Proficient persons use existing tools and methods.

Links to other Threat Level parameters:

- An Expert uses all kinds of equipment, "**Standard**", "**Specialized**", "**Bespoke**" and "**Multiple bespoke**".
- An Expert uses all kinds "**Knowledge about TOE**" information levels.

3.1.1.1.4 Multiple experts

HEAVENS definition

> *"The level "Multiple Experts" is introduced to allow for a situation, where different fields of expertise are required at an Expert level for distinct steps of an attack."*

The Multiple Experts profile is applicable when multiple fields of expertise are needed, to a degree that exceeds that normally expected from an expert specialized in a single field, such as e.g. if special hardware needs to be constructed by a hardware expert to intercept data from buses, to be later analysed by a software expert, or if key information needs to be extracted and then processed through a supercomputer cluster. Whenever analysis indicates that the expertise needed to mount an attack requires more than one field of expertise, this is the applicable profile.

Links to other Threat Level parameters:

- Multiple Experts use all kinds of equipment, "**Standard**", "**Specialized**", "**Bespoke**" and "**Multiple bespoke**".
- Multiple Experts use all kinds "**Knowledge about TOE**" information levels.

3.1.1.2 Window of opportunity

Window of opportunity is a parameter that incorporates many aspects, time, remote (logical) or physical access, and what degree of access is needed to mount an attack. Multi-dimensional characteristics made it difficult to determine a suitable level, instead it was found easier to create several sub parameters, rate them and then derive the Window of opportunity.

Sub parameters identified as suitable are “Accessibility means” and “Asset exposure time”, representing spatial and temporal dimensions respectively. This chapter contains definitions of the sub parameters as well as an example of how to combine and weigh them in order to derive Window of opportunity.

Furthermore, due to the definition of the sub parameters, the name of the parameter more closely resembles the definition of “Exposure”, but “Window of opportunity” will be used in this document for the purpose of simplified mapping to the HEAVENS security model.

HEAVENS definition

[Low]

“Very low availability of the TOE. Physical access required to perform complex disassembly of vehicle parts to access internals to mount an attack on the TOE.”

[Medium]

“Low availability of the TOE. Limited physical and/or logical access to the TOE. Physical access to vehicle interior or exterior without using any special tool (e.g., opening the hood to access wires).”

[High]

“High availability and limited time. Logical or remote access without physical presence.”

[Critical]

“High availability via public/untrusted network without any time limitation (i.e., TOE/asset is always accessible). Logical or remote access without physical presence and time limitation as well as unlimited physical access to the TOE/asset. Examples include wireless or via Internet (e.g., V2X or cellular interfaces).”

3.1.1.2.1 *Access means*

"Access means" represents the spatial dimension, proximity, or at what distance an asset is exposed from the vehicle. In itself, it does not correlate well to attack probability unless combined with an attacker model. For instance, it may be more likely that the owner of a vehicle changes parameters to bypass an enforced speed limiter than an internet hacker performing the same operation.

Access means	
Physical - Component Disassembly	**Definition:** Disassembly of a component is needed to reach an asset
	Examples: • Debugger connection to PCB • Access serial port on ECU • Read flash using flash reader
Physical - Vehicle Disassembly	**Definition:** Physical access to vehicle needed interior or exterior using tools
	Examples: • Replacement/installation of part • Communication with ECU on sub-network not reachable via external connections
Physical - No vehicle disassembly	**Definition:** Asset may be reached without any disassembly of parts outside the vehicle or inside the cab. No tools needed, although a cab key may be needed to reach interior parts.
	Examples: • Communication via external connectors such as Ethernet and OBDII • Vehicle BodyBuilder interface • NFC • USB
Remote – Direct wireless communication	**Definition:** Attack may be mounted using communication technologies communicating directly with the vehicle, i.e. close proximity.
	Examples: • Bluetooth • Wi-Fi (Vehicle is access point) • Wireless sensors • V2x, Car2Car
Remote – Indirect wireless communication	**Definition:** Attack may be mounted using communication technologies that does not need direct access to the vehicle, i.e. going via base stations
	Examples: • Mobile networks / Internet • WiFi (Vehicle connects to external access point)

3.1.1.2.2 Asset exposure time

Time is divided into four different increments, ranging from very low, meaning the TOE is accessible for a very short time until infinite amount of time.

Asset exposure time	
Very low **"Rare"**	**Description:** Utilization of a single rare event that cannot be triggered by the attacker. **Examples**: Factory programming, pairing of new part in a workshop, upgradable boot process, pairing of immobilizer and key fob
Low **"Sporadic"**	**Description:** Utilization of a sporadic event that may occur during a driving cycle, e.g. just at start-up or incoming remote connection from back-office. **Examples**: Using transients between steady states, diagnostics test, *specific vehicle modes where the mode is considered sporadic and not predictable even if the asset during the mode is of frequent and infinite exposure* (example factory)
High **"Frequent"**	**Description:** Utilization of frequent or periodic event during a driving cycle, yet asset is not accessible "at will" by the attacker. **Examples**: • Availability during steady states, but may disappear at any time. • Bodybuilder equipment while it is engaged (crane moving, pump running) • In-vehicle Android/IOS application while running • Tamper/denial of service of features while they are active (disable brake requests, interfere with radio, • Tampering/jamming on-going Cooperative Adaptive Cruise Control communication
Infinite **"Always"**	**Description:** Unrestricted exposure while the vehicle is operational, i.e. exposure can be triggered by attacker. **Examples**: Asset availability does not disappear. • Send data to receiver that is always listening (wireless gateway, Bluetooth receiver, diagnostics server, commands to actuators) • Offline processing of stored data • Leftover API

3.1.1.2.3 Deriving Window of opportunity

Table 1 presents an example approach how to combine the sub-parameters “Access means” and “Asset exposure time” in order to derive “Window of opportunity”. The mapping assigns higher degree of criticality the further away from the vehicle an asset may be reached, as well as how much time it is exposed. It can be seen as a proxy of the speed at which an attack may scale rather than likelihood (e.g. physical attacks may be described in web forums and repeated by Proficient people, but attacks over the internet may be automated and reach a fleet of vehicles in seconds or minutes).

	Physical			Remote	
Asset access means **Asset exposure time**	Component Disassembly	Disassembly of vehicle	No vehicle disassembly	Direct wireless access	Indirect wireless access
Very low “Rare”	Low	Low	Low	Low	Medium
Low “Sporadic”	Low	Low	Low	Medium	High
High “Frequent”	Low	Low	Medium	High	Critical
Infinite	Low	Medium	High	High	Critical

Table 1 Mapping sub-parameters to Window of opportunity

3.1.1.3 Knowledge of the TOE

No tailoring has been performed for this parameter. See Islam et al [1] for definition.

3.1.1.4 Equipment

The Equipment parameter caused low amount of discussions, however for speed and consistency reasons it is important for the organisation to maintain and update a master list of “Equipment” classifications for quick lookup. New tools identified during risk assessment should be rated and added to the master list.

This chapter contains examples of tools mapped to different equipment levels.

3.1.1.4.1 Standard

HEAVENS definition

> *"Standard equipment is readily available to the attacker, either for the identification of vulnerability or for an attack. This equipment may be a part of the TOE itself (e.g. a debugger in an operating system), or can be readily obtained (e.g. Internet downloads, protocol analyser or simple attack scripts). Examples include simple OBD diagnostics devices, common IT device such as notebook."*

The key thing about the Standard equipment is that it has to be readily available. Easily accessible, or purchasable for a low or moderate amount of money to count as Standard tools.

Examples:

- Cheap OBD devices
- CAN adaptors (while being mostly Automotive specific, this equipment has become inexpensive and readily available)
- Open source/Free software
- All communication equipment applicable to both automotive and IT domain, such as Ethernet tools, common Wi-Fi protocols, Bluetooth and USB
- Downloadable tools or scripts made with the purpose of modifying/reading data in a vehicle
- Tools for CPU families and operating systems also used by IT/Telecom domain, such as Linux tools, x86 and ARM CPU families (for instance, disassemblers/debuggers)
- Radio jammer

3.1.1.4.2 Specialized

HEAVENS definition

> *"Specialized equipment is not readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g. power analysis tools, use of hundreds of PCs linked across the Internet would fall into this category), or development of more extensive attack scripts or programs. Examples include in-vehicle communication devices (e.g., CAN cards), costly workshop diagnosis devices. If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack this would be rated as bespoke."*

Specialized equipment is more automotive domain specific, targeting the special communication buses, hardware or protocols used, or are standard tools but available at high prices. Modifying/extending existing tools, albeit to limited extent, falls into this category.

Examples:

- Disassembler/Debugger targeting automotive specific CPU families
- CAN FD/MOST/FlexRay/LIN equipment
- Computer cluster for calculations (cloud services)
- Equipment to monitor cell phone networks
- Radio frequency monitoring/broadcasting equipment targeting automotive specific frequency spectrums

3.1.1.4.3 Bespoke

HEAVENS definition

> *"Bespoke equipment is not readily available to the public as it may need to be specially produced (e.g. very sophisticated software), or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive."*

Bespoke equipment is produced for a specific purpose, may be one-of-a kind, or very expensive. If new tools need to be developed to mount an attack, it counts as bespoke. The latter is typically performed by an "Expert" or "Multiple Experts".

Example:

- Software or hardware tools that need to be developed
- Tools available by custom order (such as circuit boards)
- Tools considered expensive even for companies, and if used, only by few people even in a large enterprise.

3.1.1.4.4 Multiple bespoke

HEAVENS definition

> *"The level "Multiple Bespoke" is introduced to allow for a situation, where different types of bespoke equipment are required for distinct steps of an attack.*

The "Multiple bespoke" level keeps the definition of the "Bespoke" level but adds further requirements on the number of tools that need to be developed within this category.

3.1.2 Impact level parameters

3.1.2.1 Safety

No tailoring has been performed for this parameter. See Islam et al [1] for definition.

3.1.2.2 Operational

The HEAVENS definition of the Operational parameter brings up the concepts of Primary and Secondary features in the vehicle [1].

What constitutes a Primary and Secondary function may be different for each organisation, and perhaps for each brand within a multi-brand organisation. For instance, a question the passenger car OEM might ask to determine whether a feature falls into a primary or secondary category could be “is the driver able to complete the journey in a safe manner, albeit at some discomfort?”, whereas the truck industry might ask “is the vehicle operational for a working day without being a safety risk or cause damages to the goods, albeit at some discomfort to the driver/business?”. An example of the latter case could be a fleet management system not working and the driver needs to communicate work orders over cell phone with the back office, but is able to transport the goods and avoid downtime.

Table 2 presents a high level example of how a business providing transport solutions may adapt the description and weight of effects within the Operational parameter.

Table 2 Example of "Operational" impact parameter adapted for transport solutions

Severity of Effect on Service (transport solution)	Severity of Effect on Product (Effect on Customer)	Effect	Severity Rank Error! eference source not found.	HEAVENS Value
No discernible effect	No discernible effect	No effect	1	No Impact (0)
Appearance item or audible noise (vehicle still operates, but does not conform)	Appearance item or audible noise (vehicle still operates, but does not conform, annoys more than 25% of customers)	Minor disruption	2	Low (1)
	Appearance item or audible noise (vehicle still operates, but does not conform, annoys more than 50% of customers)		3	
	Appearance item or audible noise (vehicle still operates, but does not conform, annoys more than 75% of customers)	Moderate disruption	4	
Degradation of secondary function (transport solution still operable, but comfort or convenience functions work at a reduced level of performance or are non-functional)	Degradation of secondary function (vehicle still operable, but comfort or convenience functions work at a reduced level of performance)	Moderate disruption	5	Medium (10)
	Loss of secondary function (vehicle still operable, but comfort or convenience functions do not work)		6	
Degradation of primary function (transport solution still operational, but at a reduced level of performance)	Degradation of primary function (vehicle still operates, but at a reduced level of performance)	Significant disruption	7	
Loss of primary function (transport solution inoperable)	Loss of primary function (vehicle inoperable, but does not affect safe vehicle operation)	Major disruption	8	High (100)

Severity of Effect on Service (transport solution)	Severity of Effect on Product (Effect on Customer)	Effect	Severity Rank Error! eference source not found.	HEAVENS Value
	Potential failure mode affects safe vehicle operation with some warning or noncompliance with government regulations		9	
	Potential failure mode affects safe vehicle operation without warning or involves noncompliance with government regulations	Fails to meet safety or regulatory requirements	10	

3.1.2.3 Financial

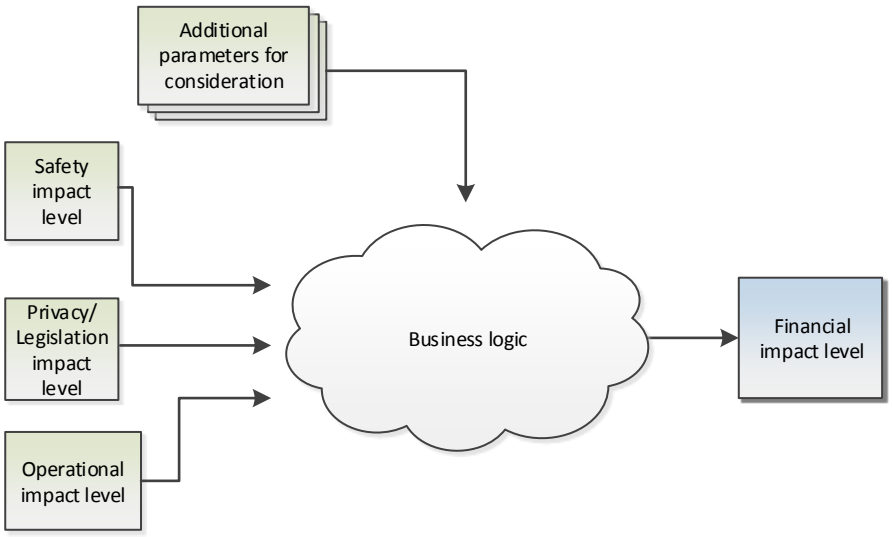
The financial parameter is heavily dependent on all other Impact parameters as everything may be linked to a financial impact. For this reason it is suitable that the Financial parameter is the last to be rated among the impact level parameters.

It is also a parameter that contains many factors to consider at a single time and is a cause for long discussions during risk assessment sessions, as well as generating greater than average uncertainty in the output.

A way to improve speed and consistency in rating this parameter is to split it up into several sub-parameters, rate them, and use a model to derive the financial parameter level.

A Financial Impact Level Model is linked to the business and may consider factors such as:

- Combinations of the Safety, Privacy/Legislation, Operational parameters
- Estimate of affected vehicles if an incident occurs
- Cost of correction (e.g. Over-the-air updates vs. workshop visits)
- Loss of sales or intellectual property (e.g. unsolicited activation of soft features)
- Reputational loss for the organization



3.1.2.4 Privacy/Legislation

No tailoring has been performed for this parameter. See Islam et al [1] for definition.

4 Future work

This chapter presents ideas how to further adapt the risk assessment methodology to derive a more stable security level value that may be used to determine process rigor for development projects.

4.1 Determining development process rigour using security levels

The HEAVENS security model provides a systematic approach to derive security requirements for the automotive Electrical and/or Electronic (E/E) systems.

Threat analysis and risk assessment are activities that may be performed iteratively several times during a products lifecycle. The earlier the activity is performed the greater the uncertainty for the parameters will be. In the Concept phase for instance, it may not have been decided exactly what operating system to use or exact distribution of a feature that is implemented over several Electronic Control Units (ECU). This uncertainty especially affects the threat level parameters, which are more dynamic in nature than the impact level parameters.

Table 3 shows the Threat level and Impact level parameters along with an indication of their relative dynamic sensitivity. In the impact level parameter category, legislation may change and be retroactively applied, showing some dynamic behaviour, and due to parameter dependencies it would also affect the financial parameter. Equipment becomes more readily available and cheaper over time, as well as the knowledge about the product, and along with improved tooling and information it may be expected that the expertise needed to perform an attack is reduced over time. Window of opportunity however is not expected to change drastically.

Table 3 Parameter relative dynamic behaviour

Threat level parameters	
Expertise	High
Window of opportunity	Medium
Knowledge about TOE	High
Equipment	High
Impact level parameters	
Safety	Low
Privacy/Legislation	Medium
Financial	Medium
Operational	Low

Due to the dynamic behaviour of the parameters, several instances of risk assessment over the lifecycle are likely to produce different security levels as result of new information being incorporated into the assessment.

For some use of the security level, such as determining development process requirements, i.e. the rigour of a development process for an Item, achieving security level stability is desirable.

For instance, would the security level used to determine to amount of process rigour change from a lower to higher value during the course of a project, it may cause disruption in the project and trigger rework in areas such as design review, code review, level of testing, documentation.

Process rigour determines to what extent activities are performed, such as the degree of design or code review, the amount of fuzzing or pen test, or whether to test the system internally or let an external party perform an independent analysis. The degree of process rigour is determined early in a project, during concept phase, where parameter uncertainty is at its greatest, in order to set project budget and plan activities going forward with the project.

Figure 2 presents' concept ideas how to determine the level of process rigour during concept what by splitting Threat Level and Impact Level in the Security Level derivation, and to a greater extent consider the parameters dynamic sensitivity.

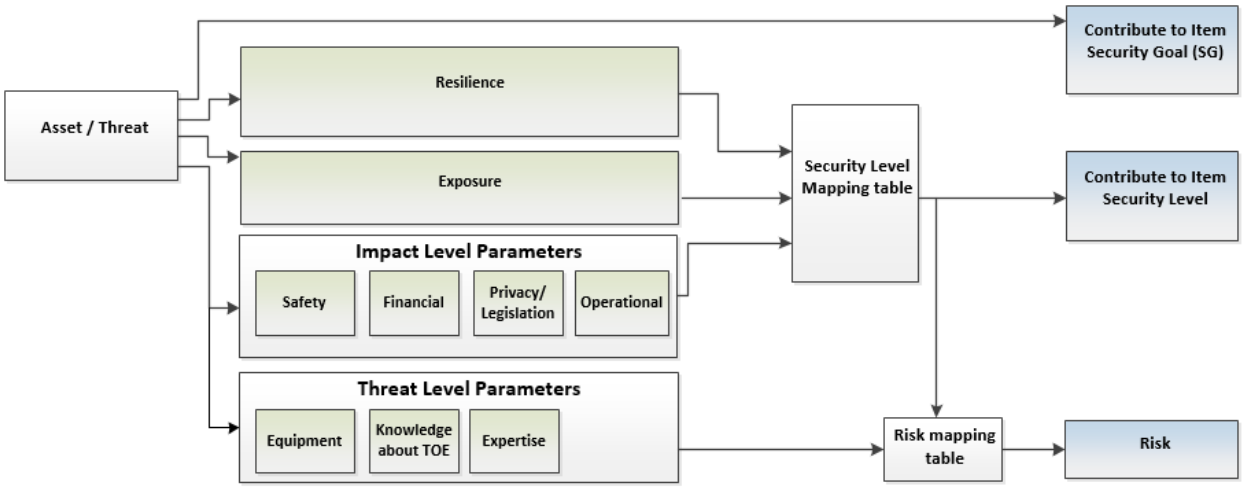


Figure 2 Concept overview for security level and risk separation

By splitting up the different parameter groups a separation may be made between security level and risk, where the former is more stable and tightly linked to impact, whereas the latter represents a snapshot of the current risk at the time of the assessment.

Basing Security Level entirely on Impact Level may lead to over-engineering of the Item and process requirements that are unreasonably high, which is why Exposure (Window of opportunity) and Resilience are introduced as parameters that provide aspects of likelihood, speed at which attacks may scale, and the ability to cope with an attack that has successfully penetrated the security countermeasures protecting an asset.

In the extreme case, if a single ECU has high impact on e.g. the Operational parameter, but is completely disconnected from the rest of the electrical system apart from power connector, requires complex disassembly to be reached for physical tampering, it would likely get a too high Security Level relative to other ECUs unless Exposure is considered.

In a similar way, an Item under e.g. the monitoring of an Item-external strong monitor device, such as an intrusion detection system, which provably would be able to detect a certain set of attacks and take controlling actions, may not need as high security level as a system without such mechanism in place.

4.1.1 Cyber security Resilience

ISO26262, Functional safety, considers Controllability as one of the factors next to Severity and Exposure when determining Automotive Safety Integrity Level (ASIL), and is defined as:

"ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures " [4]

In a similar sense as Controllability for Safety, Resilience describes a systems ability to recover from an attack after it has happened. This may occur at different levels, it may be the business ability to mitigate and resolve an attack or inside a vehicle it might be the ability to detect an attack, warn the driver, isolate the attack and try to recover.

Figure 3 presents a view of how Resilience may be seen in an Item context; as the ability to bring back an Item from an Undesired attack state and to a Desired state, either fully or partially. An example of the latter case would be the Item operating in a state of reduced functionality, such as limp home mode for the rest of the driving cycle. A full recovery from an attacked state to the initial state would incorporate logging of the event and regaining full integrity of the Item under consideration.

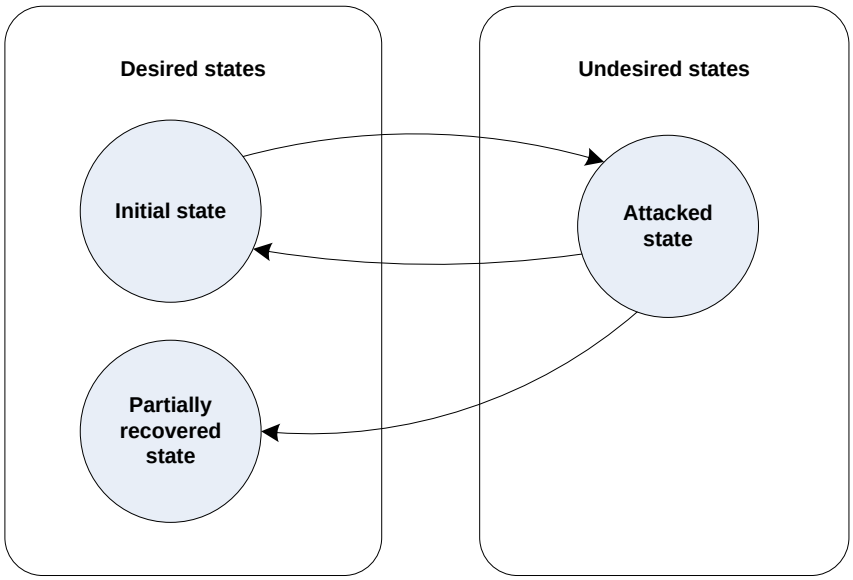


Figure 3 Item Resilience states

5 References

[1] M. Islam, A. Lautenbach, C. Sandberg, M. Olsson, A. Bokesand, T. Olovsson, H. Broberg et al. Deliverable D2 Security Models. HEAVENS Project, Deliverable D2, Release 1. Dec. 2014

[2] Society of Automotive Engineers. SAE Standard J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, Jan 2016

[3] Macher et al, “A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context”, International Conference on Computer Safety, Reliability, and Security, Sept 2016

[4] ISO (International Organization for Standardization). Road vehicles—Functional safety (ISO 26262:2011). ISO 26262:2011, 2011