Towards Incremental Safety and Security Requirements Co-Certification

1st Morgagni Andrea
Cyber Security Division
Leonardo
Rome, Italy
andrea.morgagni@leonardocompany.com

2nd Massonet Philippe
Scientific coordination
CETIC research center
Charleroi, Belgium
philippe.massonet@cetic.be

3rd Dupont Sbastien
Model-Based Engineering and Distributed Systems
CETIC research center
Charleroi, Belgium
sebastien.dupont@cetic.be

4th Grandclaudon Jeremy
Model-Based Engineering and Distributed Systems
CETIC research center
Charleroi, Belgium
jeremy.grandclaudon@cetic.be

***Abstract*—The continuous technological developments and the growing connectivity of applications and infrastructures is leading to the new threats to the technological world in particular to the possibility of considering certain threats in environments that were not previously touched by them. Now that many safety critical systems are becoming connected, they need to be protected from security threats. Safety and security engineering and certification evaluation are processes that have evolved independently. However now that security issues may impact safety they need to be analysed together, yet the processes must become more flexible to encourage certification when it is not mandatory. In this paper we sketch an approach for incremental certification of security requirements with Common Criteria in the general context of security/safety co-engineering and certification. The approach is illustrated with a case study.**

***Index Terms*—cybersecurity, safety, certification, requirements, incremental**

1. Introduction

Nowadays in international contexts, various projects aim to integrate in a single engineering process the security of very different targets, such as products that are part of complex systems and processes. Among the most common problems is the attempt to reduce the distances between Safety and Security, starting from the assumption that both have the same priority and that the life cycle phases of a generic element from the point of view of Security or Safety are parallel to each other and structured in a similar way. Dependability studies [8] reliability, availability, safety, integrity, maintainability, etc in a system context. Dependability and security have followed different yet convergent paths: dependability has realized that restriction to non malicious faults was addressing only a part of the problem, 2) security has realized that the main focus that was put in the past on confidentiality needed to be augmented with concerns for integrity and for availability. [9]. Combining dependability and security fault-error-failure models is key to managing in a unified manner the threats to a system.

The topic of safety and security co-engineering and certification for cyber physical systems has many open research challenges [3]. Among them are challenges to find methods for safety and security co-engineering as well as methods for certification of safety and security, i.e. multi-compliance.

In this perspective, the Cape program of the SPARTA project is studying the convergence of Safety and Security aiming at a common process for the definition of a more agile assessment and certification framework.

2. Model for Co-Engineering and Certification

This section provides an overview of the SPARTA cybersecurity assessment framework. The approach builds on results from the AMASS research project where methods have been defined take into account the fact that systems are becoming more open and interconnected, and have new assurance requirements for multi-compliance for different dependability attributes [10].

2.1. V-Model

The SPARTA framework is composed of a list of assessment tools to that can be used during different phases of the security engineering lifecycle, a security engineering process description, that indicates in which phases each assessment tool can be used, a safety engineering process description and a security certification evaluation process (Common criteria). In this paper we focus on aligning security by design and Common Criteria phases in an iterative and incremental process. No specific security by design method is followed. The integration of safety certification with ISO 26262/SAE security guidelines is left for future work. In the CAPE research program a particular model, called V-model, has been introduced. It allows to parallelize a generic ”Security engineering model” and a generic Safety engineering model

Fig. 1 shows the SPARTA cybersecurity assessment framework. The process descriptions are shown in parallel, in order to highlight the time dependencies between

DOI 10.1109/EuroS&PW51379.2020.00019

the steps of a process, and between steps of different processes. The figure suggests that security and safety co-engineering can be performed, in parallel with cybersecurity Common Criteria certification. For example ”security requirements analysis” can be done in parallel with ”safety goals definition”, and finish with incremental certification of the ”security target evaluation (ASE)” (more specifically ASE REQ security requirements). The security engineering process covers both software and hardware development, however the focus is on software development. Each of these processes will be described in a separate section below. The framework covers the following phases of the software life cycle:

- the design phase covering requirements, architecture, design, development, unit testing, integration testing, acceptance testing and deployment,
- the operation phase when a system is running in its target environment
- the end of life phase when the system is taken out of operation

The design life cycle is assumed to be iterative. Fig. 1 uses the well known iterative V-Model development lifecycle to compare the different steps of the security engineering, safety engineering and cybersecurity certification processes. One of the main motivations in using the V-Model is to compare security and safety development processes. While software development models have evolved towards agile processes that describe the iterative nature of software development, the hardware nature of safety engineering processes is less adapted to an agile process model. Using the V-Model is a good compromise to compare security engineering and safety engineering processes as was done in the H2020 AMASS ECSEL project [3]. Safety, security and performance co-engineering are explored in the H2020 AQUAS ECSEL project [4].

For the cybersecurity certification process the Common Criteria is used. It is defined in ISO/IEC 15408 that defines the general model and evaluation criteria and ISO/IEC 18045 that defines the methodology for IT security evaluation. The use of the V-Model for describing the SPARTA cybersecurity assessment framework will continue to be revised. The safety engineering process is composed of the following phases: Safety goal definition, Functional and technical safety concept design, SW and HW safety requirements definition, SW and HW safety requirements verification, Functional and technical safety concept verification, Safety goal verification.

Once the system concept is defined, a Hazard analysis and a Risk assessment is done where the probability of exposure, the controllability and the severity of a hazardous event with regard to the system is determined. With these parameters the ASIL is defined and subsequently the safety goals, i.e. the top-level safety requirements are obtained.

During the subsequent phases and sub phases, some detailed safety requirements are derived from the safety goals. The functional safety concept is developed by taking into account the preliminary architectural assumptions. This safety concept is developed by deriving the functional safety requirements from the safety goals and allocating

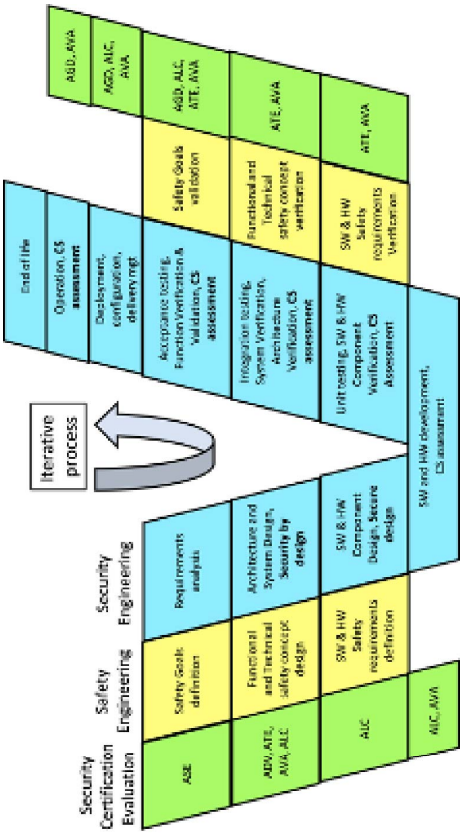

Figure 1. V-Model for cybersecurity, safety and certification

them to elements within the architecture and the necessary interactions to achieve to safety goal.

Then, the product development requirements at system level are specified, including the design of the system architecture, the development of the technical safety concept, and the allocation of the technical safety requirements to the elements of the system. To finish with the definition of the requirements, the lowest HW and SW requirements are established. At this point the hardware and software are developed.

Henceforth, safety verification and validation activities are executed, which include the validation of the functional safety concept aspects, the implementation of the safety goals and the validation of the assumptions concerning the effectiveness and the performance of external measures. The security engineering phases: Security requirements analysis, Security by design, Secure design, Code security assessment, Unit testing security assessment, Integration testing security assessment, Acceptance testing security assessment and Secure deployment

In addition to the (1) design and deployment phase cybersecurity assessment can also be made during the (2) operation and (3) end of life phases of a system.

2.2. Mapping of Security by Design and Common Criteria Assurance Classes

The cybersecurity certification process describes the phases that make up the evaluability for the purpose of

certification of a generic target (product, system, process, etc.), that indicate the expected elements (requirements) that the various procedures and the various tools must have in the various phases of the activities that make up the process of evaluability. The starting idea is to generalize what are the phases of a hypothetical certification process, which is by its nature adaptable to different elements (that we can define in general Target of Evaluation - TOE), but which also covers their entire life cycle.

In the initial hypothesis we focused on the idea of Cyber security seen as a process that accompanies a certain TOE throughout its life cycle naturally regardless of the need for a security certification of the TOE. If we then want to go within the scope of the certifications, we can immediately verify that the phases of a generic process of evaluation/certification of the security of a TOE are going to map perfectly with those of Cyber security process just mentioned.

Taking as an example Common Criteria (ISO / IEC 15408), a standard that has become established and consolidated in recent decades, in the next scheme we can note how the various assurance classes, that characterize the activities carried out during a process of evaluation/certification of a TOE, go perfectly to map the needs defined in the various phases of the introduced Cyber security process.

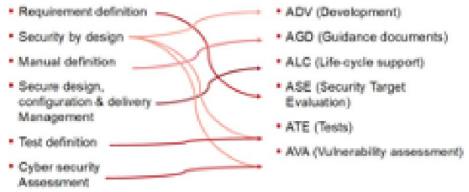

Figure 2. Security by design and Common Criteria Assurance Classes mapping

In this process of parallelization, the compatibility with the generic phases of an Evaluability process, with a generic target (product, system, process, etc.) certification purpose was checked, taking as reference the assurance classes of an evaluation process according to the Common Criteria (ISO/IEC 15408) [2], a standard that has become a reference for the cyber security certification. CC assurance classes are described below and the mapping to the security engineering process shown in Fig. 2:

- ASE (Security Target Evaluation): this class deals with the evaluation of the consistency of the Security Target which also contains the definition of the security requirements of the TOE, therefore it is closely linked to the security requirements management phase.
- ADV (Development): this class deals with the evaluation of the six families of requirements for structuring and representing the security functionality realized by the target of evaluation (TOE) at various levels and varying forms of abstraction that the developer must produce during the product development phase, naturally it is linked to the features of the Secure by design processes adopted by the supplier.
- AGD (Guidance Documentation): this class takes care of the evaluation of the manuals that are delivered to the customer. These manuals contain both the secure configuration process of the TOE in its user environment and its safe use methods for each category of defined end-user.
- ALC (Life-cycle support): this is a very important class that evaluates all aspects of the management of the TOE during its life cycle: in the development phase in which it is under the responsibility of the developer, during the transitional phase of transport in its final operating environment and of course the management in the operating environment under the responsibility of the customer and the developer, in the hypothesis of maintaining the certification (security patch management).
- ATE (Tests): it is the class that takes into consideration all the tests that demonstrate that security functionalities operate according to its design descriptions, both the functional ones proposed by the developer and the independent ones proposed by the evaluators.
- AVA (Vulnerability Assessment): this class takes care of vulnerability assessment activity to analyse vulnerabilities in the development and operation of the TOE. Development vulnerabilities are those introduced during its development and these can be minimized with the adoption by the developer of security by design processes. Operational vulnerabilities are those that could exploit the weaknesses of non-technical countermeasures to violate the TOE security functionality. This analysis is carried out by the evaluators during TOE evaluation deliverables analysis or from the classic vulnerability analysis performed also adopting automatic tools.

In the following scheme we can note how the various assurance classes, that characterize the activities carried out during a process of evaluation/certification of a target, go perfectly to map the needs defined in the various phases of the introduced V-model for safety and security engineering models. Moreover we have to consider that if we analyse the definition of safety and security for example in the new Oxford dictionary of English (Pearsall and Hanks, 2001) [1] where the words are described in the following way:

- Safety: The condition of being protected from or unlikely to cause danger, risk or injury. - Denoting something designed to prevent injury or damage, e.g. safety barrier
- Safe:1)Protected from or not exposed to danger or risk; not likely to be harmed or lost; Not likely to cause or lead to harm or injury; not involving danger or risk; (of a place) Affording security or protection
- Safe 2) Uninjured; with no harm done - From the Latin word saluses uninjured
- Security: 1) The state of being free from danger or threat, e.g. the system is designed to provide maximum security against toxic spills; the safety of a state or organizations against criminal activities such as terrorism, theft or espionage; procedures followed or measures taken to ensure such safety;

the state of feeling safe, stable and free from fear or anxiety

- Secure: not subject to threat; certain to remain or continue safe and unharmed; protected against attack or other criminal activity; feeling safe, stable and free from fear and anxiety

From this definition, it is evident that the differences between safety and security are not so noticeable. Both define situations where there is a situation of protection without risks.

2.3. Safety and Security Trade-off Analysis

There are many ways that safety and security requirements ca be co-engineered [5]. The figure below shows the planned approach for the SPARTA project, where safety and security analysis are re-reconciled during trade-off analysis to produce safety and security requirements that are linked together. To illustrate the above PP approach we are experimenting on an automotive case study using ISO 26262 [6] for the safety certification, and SAE J3061 [7] Cyber Security guidelines and ISO/IEC 15408 Common Criteria [2].

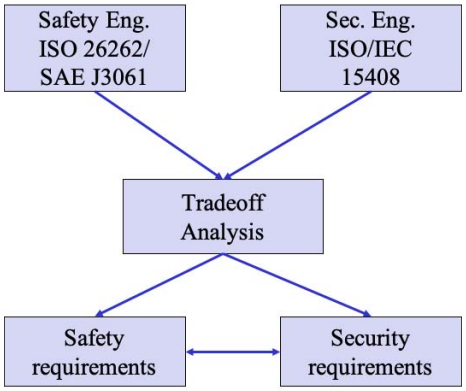

Figure 3. Safety and security tradeoff analysis

Fig. 3 above shows the approach that has been taken in the automotive vertical: safety analysis and cybersecurity analysis are being performed in parallel. A trade-off analysis then needs to be carried out to determine which trade-offs between safety and security need to be taken. The results of the tradeoff analysis are then documented in a common safety/security protection profile.

3. Safety and Security Requirements Challenges

Starting from these considerations, we now show see how it could be possible to approach, in a Safety and Security certification process, the first phase of the previously defined V-model, which is, the requirements definition phase. In particular the elements of the three parallel processes that characterize the first phase of the V model are:

1) Requirement analysis;
2) Safety Goals definition;
3) ASE (Security Target Evaluation).

About the certification process, considering the current cyber security certification schemes at a national and international level, Common Criteria (ISO / IEC 15408) has been taken as reference, a standard that has evolved and consolidated over the last decade.

Point 3 of the previous bulleted list contains the phase of the assessment on the Security Target which is the main document of an evaluation conducted according to the Common Criteria standard.

Among the contents of this document there is the precise definition of the security requirements that the TOE (Target of Evaluation - the object that is intended to certify, generally an ICT product, but can also be addressed to systems, processes and services) must satisfy.

So every time the supplier of a particular TOE intends to proceed to its certification it will have to start from scratch producing such document with a remarkable working effort.

In order to simplify this phase in a possible certification process, the idea is to adopt one of the solutions considered by the Common Criteria standard, the introduction of Protection Profiles (PP) for the categorization of Cybersecurity requirements.

But a further object is to try to merge together safety and security requirement in a single protection profile considering all the previous hypothesis on safety and security concepts.

In this PP definition has been considered the communication in connected and cooperative Car Cybersecurity (one of the SPARTA verticals) where safety and security are considered as target.

The purpose in the definition of the protection profile has been to introduce in a protection profile, normally adopted for security requirement definition also safety elements.

This action was deployed in all the elements that define a PP that are here listed for completeness in a new elaborated format:

- PP introduction
- Conformance Claims
- Security and safety problem definition
- Security and Safety objectives
- Extended components definition
- Security and Safety requirements

4. Lightweight Incremental Security Requirement Certification

From the perspective of certification, it is necessary to take into account the iterative nature of complex system development and long term evolution of systems, by providing iterative security certification processes. Such an incremental certification process should be lightweight, flexible to encourage security certification. Certification evidence should also be portable so that incremental certification can be performed by different evaluation facilities.

Fig. 4 sketches an incremental certification process for Common Criteria. The evaluation can be made by the same organization or by different evaluation organizations. The figure shows a target of evaluation (TOE) evolves in

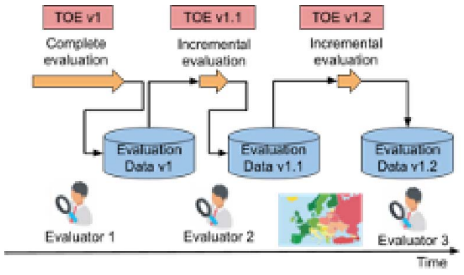

Figure 4. Incremental Evaluation Process

time from v1 to v1.1 and v1.2. TOE v1 is the subject of a complete certification of the TOE with respect to a protection profile (PP). The first evaluation is performed by an evaluation organisation evaluator 1 and evaluation data is stored as Evaluation Data v1 in a standard and shareable format between organisations. The TOE then evolves to v1.1 and some changes are made to requirements of the PP. Some of the changes made to the TOE impact some of the requirements in the PP. The TOE needs to be certified again with respect to the impacted requirements of the PP. This is the subject of an incremental evaluation on TOE v1.1 performed by evaluator Evaluator 2. Evaluator 2 could be an evaluation facility located in a different country than the first evaluation. It produces new evaluation data stored as Evaluation Data v1.1.

We illustrate the incremental certification process on an automotive platooning case study. Fig. 5 below shows an automotive car platooning scenario where the platoon is moving along the road behind a platoon leader car. In this V2C scenario the platoon leader is connected to an edge cloud. The platoon leader manager the platoon network with all the cars of the platoon, and is the unique connection point with the cloud/edge cloud network. This connection is protected by a firewall. The platoon leader car is connected to edge cloud 1. As the platoon advances edge cloud 2 becomes closer than edge cloud 1 with better response time. This triggers the switch from edge cloud 1 to edge cloud 2, initializes the handshake for authentication with edge cloud 2 and updates the firewall configuration to allow communication with edge cloud 2 and forbid communications with edge cloud 1.

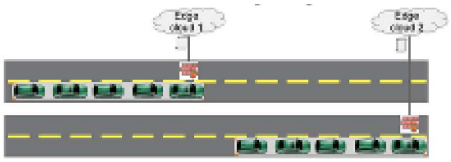

Figure 5. Automotive Platooning V2C scenario

The platooning firewall must also be protected with respect to a number of threats such as a user from one networks accesses the platoon network with malicious intent and starts sending false data that could jeopardize the safety property maintain a safe distance between platoon cars. Another threat is an attacker that obtains unauthorized remote access to the firewall and changes the configuration, adds unauthorized accesses, modifies audit traces, or saturates the firewall. Any data used to calculate the safe distance between cars needs to be protected, and the platooning firewall is part of that protection. Such a firewall should be highly secured and meet requirements defined in a high security firewall protection profile such as [11]. We now examine different types of changes to the platoon management firewall to illustrate the ones that should trigger incremental certification or not. When the platoon management changes from one edge cloud to another (1) this does not require any recertification because it is the normal functioning of the platoon management. However, auditing requirements in the platooning protection profile such as OT.AUDIT: the firewall must record all operator operations so that they can be analysed to detect attacks or attack attempts, and to detect configuration errors that could weaken the firewall must be respected. Such requirements should be monitored during firewall re-configurations. When a new version of the firewall is available and is ready to be updated on car with the platooning functionality (2), re-certification is required if the new firewall features are not already certified in a high secure firewall protection profile such as [11] that is part of the platooning protection profile. If this is not the case the new firewall features must be re-evaluated with respect to the impacted protection profile requirements. If the car manufacturer wishes to update the platooning management module with a different firewall product (3), then the firewall must be re-certified. If this different firewall product is already certified with respect to a high secure firewall protection profile such as [11] and is part of the platooning protection profile, then re-certification is not required.

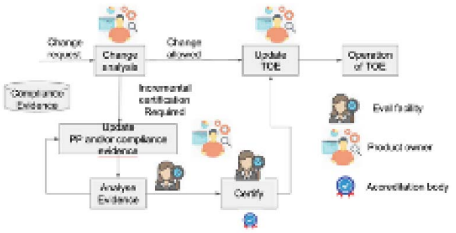

Figure 6. Incremental Evaluation Process

Fig. 6 sketches such an incremental certification process. If the change request analysis by the product owner determines that no re-certification is required, the TOE can be updated and be placed back into operation. If the change request analysis determines that re-certification is required, then the platoon management protection profile might have to be updated and the compliance evidence must be gathered by following the certification process for the impacted parts of the TOE. The evaluation facility then analyses the evidence. If the evidence is insufficient, then the product owner must complete the evidence, and present it again to an auditor of the evaluation facility. If the auditor determines that the evidence is sufficient, then the auditor presents this evidence to the accreditation body to obtain the TOE certification. Once certification is obtained, then the TOE can be updated and go back into operation.

5. Conclusion and Future Work

The increasing connectivity of safety critical systems is driving the need for safety/security co-engineering processes where safety and security are analyzed together. Even though there are many different ways to co-engineering safety and security [5], certification processes also need to be integrated.

The paper has described the effort in the SPARTA project to define safety and security requirements in the same Common Criteria protection profile. The approach is being experimented in an automotive case study with safety critical properties. The papers main contribution is that by integrating certification evaluation activities in the safety/security co-engineering process, it opens up the possibility for incremental certification. The paper has sketched a process for incremental certification of security properties. It was illustrated on the automotive case study where different changes were considered for incremental certification.

This paper had focused only on incremental security certification. Future work will cover incremental safety certification. This paper focused on the requirements phases. Future work will explore other lifecycle phases, e.g. testing, to complete certification evidence. Other challenges include understanding how to perform tradeoff analysis and how this can affect certification and incremental certification.

Acknowledgment

This paper is supported in part by European Unions Horizon 2020 research and innovation program under grant agreement No 830892, project SPARTA.

References

[1] Pearsall, J. and Hanks, P. (eds), The new Oxford dictionary of English, Oxford, Oxford, University Press, ISBN 0-19-860441-6, 2001.

[2] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, April 2017, Version 3.1, Revision 5 - CCMB-2017-04-001

[3] AMASS: Assurance and Certification of CPS. https://www.amass-ecsel.eu/

[4] AQUAS: Aggregated Quality Assurance for Systems. https://aquas-project.eu/

[5] Christophe Ponsard, Gautier Dallons, Philippe Massonet, Goal-Oriented Co-Engineering of Security and Safety Requirements in Cyber-Physical Systems, SAFECOMP Workshops, 2016.

[6] ISO26262. Iso 26262-1:2018 functional safety road vehicles. urlhttps://www.iso.org/standard/68383.html

[7] SAEJ3061. Sae j3061 - cybersecurity guidebook for cyber-physical vehicle systems. https://www.sae.org/standards/content/j3061_201601/

[8] Laprie, Jean-Claude, Dependability: Basic Concepts and Terminology, Springer, 1992.

[9] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, Carl E. Landwehr: Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Trans. Dependable Secur. Comput. 1(1): 11-33 (2004)

[10] Jose Luis de la Vara, Alejandra Ruiz, Barbara Gallina, Gal Blondelle, Elena Alaa, Javier Herrero, Fredrik Warg, Martin Skoglund, Robert Bramberger: The AMASS Approach for Assurance and Certification of Critical Systems. Proceedings Embedded World 2019.

[11] FIREWALL A EXIGENCES ELEVEES PROFIL DE PROTECTION, 1998, https://www.commoncriteriaportal.org/files/ppfiles/PP9905.pdf