D4.4

VESSEDIA in Common Criteria evaluations

Project number:	731453
Project acronym:	VESSEDIA
Project title:	Verification engineering of safety and security critical dynamic industrial applications
Start date of the project:	1st January, 2017
Duration:	36 months
Programme:	H2020-DS-2016-2017

Deliverable type:	Report
Deliverable reference number:	DS-01-731453 / D4.4 / 1.0
Work package contributing to the deliverable:	WP 4
Due date:	October 2019 – M34
Actual submission date:	03rd January 2020

Responsible organisation:	TUAS
Editor:	Emmanuel Querrec
Dissemination level:	PU
Revision:	1.0

Abstract:	In this deliverable, we develop a contribution to the Common Criteria (CC) evaluation scheme in the form of a complementary light conformity assessment scheme (CAS) called Verified in Europe (ViE). The ViE CAS can contribute to policy-making in cybersecurity in the EU.
Keywords:	Conformity assessment, certification, label, security, safety, Common Criteria

The project VESSEDIA has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 731453.

Editor

Emmanuel Querrec (TUAS)

Contributors (ordered according to beneficiary numbers)

Pekka Forselius (TUAS)

Timo Mieskonen (TUAS)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

In this deliverable, we develop a contribution to the Common Criteria (CC) evaluation scheme under the form of a complementary light conformity assessment scheme (CAS). After a brief presentation of the CC, we introduce the main elements of the VESSEDIA project that form the basis of the CAS. Namely, the ISO/IEC standard that includes the notion of Target of Verification (TOV), the VESSEDIA verification tools, verification metrics, the notion of Object of Verification (OOV) and the notion of Result of Verification (ROV).

The ViE CAS introduces the trace-card which acts as a "passport of verification" for the software. It documents which verification tools that have been used and where/when with regards to the SDLC. It is an important step in the context of a smart Society that needs to lift up software requirements towards safety and security from a tool perspective.

The ViE CAS proposes three levels for indexing the degree of verification, following the extensiveness of static analysis applied, if any. We also take in consideration the possibility of self-conducted SSSV or externalized SSSV, for example to an evaluator.

Altogether, the ViE CAS requires light efforts in documentation during the SDLC that supports visibility, and traceability throughout the verification value chain, while promoting the use of verification tools, with an emphasis on program analysis tools.

The ViE CAS has been presented to the IACS thematic group[1] with the purpose of being integrated to IACS recommendations to ENISA and the EU commission, alongside references such as ISO/IEC 15408 (CC), ISA/IEC 62443 and documentation under ISO/IEC JTC 1/SC 27. Ultimately those recommendations will influence ENISA and EU Commission final orientations for the IACS Cybersecurity Certification Framework (ICCS).

[1] See at https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs last consulted 11.12.2019

Contents

List of Figures

List of Tables

Chapter 1 Introduction

Under Task *T4.4 Contribution to Common Criteria process (M18-M36; Task Lead: TUAS)*, the public deliverable *D4.4 VESSEDIA in Common Criteria evaluations*, reports on the potential contributions expected from VESSEDIA in the context of the Common Criteria (CC) process. The D4.4 report is complementary to other VESSEDIA deliverables presented in the end of this introduction.

We will study what extra support can be brought by the VESSEDIA tools and methodology to the CC activities. The study is based on results from WP1 Safety and Security Verification Methodologies, WP2 metrics and tools, WP5 use-cases and essentially on WP6 Standardization plan outcomes.

A developing company can expect a positive return on investment by using static analysis, however only at the right level of static analysis corresponding to a certain criticality level and depending on market conditions (see VESSEDIA D1.6). In addition, there is a gap as there is no guide for using formal methods for using in assessment for EAL validation which "depends on evaluator" (see VESSEDIA D4.2 page 19).

Insights on direct contributions to CC from a ***VESSEDIA tools*** point of view can be found in:

- The cost benefit analysis and vulnerability methodology, respectively D1.6 and D1.7 in WP1 Safety and Security Verification Methodologies (both public deliverables)
- D3.4 Design proposal for integrating Frama-C. More precisely, this deliverable contains the proposal to cover semi-formal and formal development and evaluation tasks in a Common Criteria certification scheme (confidential), from WP3 High-level models for software verification.
- D4.3 Benchmark for evaluating VESSEDIA Tools (public)
- D4.5 Quality tests and limits of VESSEDIA tools regarding security vulnerabilities detection (public)
- D6.4 The standardization plan (confidential), from WP6 Standardization plan outcomes
- D6.6 Proposal for enhancement of CSPN and Common Criteria schemes (confidential)

Additionally, key elements of the VESSEDIA methodology with regards to the metrics and tools can be found in WP2 deliverables (Integrated Verification Toolbox development and WP4 Quality assurance and certification).

The VESSEDIA project aims at initiating a "Verified in Europe" label. This label will contribute to make safety and security tools (e.g. Frama-C) as widely recognized by the developer and security communities. The label will be discussed, defined and designed as a new standard to be supported by the members of the VESSEDIA Advisory Board.

This report is complementary to the deliverables listed above, builds strongly on the standardization plan, and aims at proposing a light weight conformity assessment scheme (CAS). The CAS fulfils the following VESSEDIA project objectives:

- Promoting the overall use of verification tools so as to build less vulnerable applications running in Internet of Things (IoT) environments/systems, and therefore making those IoT systems more reliable
- Getting the developers and evaluators to use those verification tools

- Increase transparency, traceability and comparability of verification efforts in software development

In the following sections, we will discuss the CC, the building blocks of the VESSEDIA methodology and present the details of the CAS that we propose as a complement to the CC, which is the current mainstream framework for security evaluation process.

Chapter 2 Elements of safety and security evaluation process

2.1 The Common Criteria

The ISO/IEC 15408 Standard is a set of guidelines that define a common framework for evaluating security features and capabilities of Information Technology security products against functional and assurance requirements. The ISO 15408 defines the Target of Evaluation (TOE) as the product or system that is the subject of the evaluation against security functional requirements (SFR)[2] and security assurance requirements (SAR)[3]. There are seven levels of confidence in that the SFR have been met, and corresponding to a degree of extensiveness of verification efforts done to ensure the SAR, as presented in the table below:

EAL1: Functionally Tested	Applies when you require confidence in a product's correct operation, but do not view threats to security as serious. An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation and that it provides useful protection against identified threats.
EAL2: Structurally Tested	Applies when developers or users require low to moderate independently assured security but the complete development record is not readily available. This situation may arise when there is limited developer access or when there is an effort to secure legacy systems
EAL3: Methodically Tested and Checked	Applies when developers or users require a moderate level of independently assured security and require a thorough investigation of the target of evaluation and its development, without substantial reengineering.
EAL4: Methodically Designed, Tested, and Reviewed	Applies when developers or users require moderate to high independently assured security in conventional commodity products and are prepared to incur additional security-specific engineering costs.
EAL5: Semi-Formally Designed and Tested	Applies when developers or users require high, independently assured security in a planned development and require a rigorous development approach that does not incur unreasonable costs from specialist security engineering techniques

[2] See https://pdfs.semanticscholar.org/f553/d790104dc1d0b49b6d7e4347e71eb370b6a2.pdf last consulted 29.11.2019

[3] See https://www.jtsec.es/common-criteria-cheatsheet.pdf last consulted 29.11.2019

EAL6: Semi-Formally Verified Design and Tested	Applies when developing security targets of evaluation for application in high-risk situations where the value of the protected assets justifies the additional costs
EAL7: Formally Verified Design and Tested	Applies to the development of security targets of evaluation for application in extremely high-risk situations, as well as when the high value of the assets justifies the higher costs

Table 1: table of EAL levels[4]

In a CC certification process, the SAR/SFR are requirements which are verified with the help of verification and testing, using well-established benchmarks and documentation (Protection Profiles, Security Target), and to some extent depending on the knowledge and experience of the CC evaluator. With regards to the tools we develop and promote in VESSEDIA, some SFR/SAR can be claimed as fulfilled by the CC applicant based on the use of specific verification tools.

Tools can be used for example for the purpose of *Life-cycle support* related requirements, which is referred to as the *ALC* Assurance Class. The applicant can claim and give evidence on the use of certain verification tools capabilities at the time of development, in order to fulfill the so called *ALC_DVS: Development Security* Assurance Family.

Moreover, verification tools are used by the evaluator during the CC certification process, possibly with the help of verification tools such as those developed in VESSEDIA. For example, static analysis tools are possible to use for the purpose of *Vulnerability* related requirements, which is referred to as the *AVA* Assurance Class. Within the so called *AVA_VAN: Vulnerability Analysis* Assurance Family.

The connections with CC have already been discussed within VESSEDIA deliverables Clear linkage between VESSEDIA methodology and CC components can be found in the following reports:

- The list of security functional requirements (SFR) is presented in D1.2 for the three VESSEDIA use-cases (confidential)
- The methodology how to use Frama-C to perform a security audit is thoroughly presented in D1.7 *Vulnerability discovery methodology* (public)
- The general presentation of the Evaluation Assurance Levels (EAL) is in in D4.2 Chapter 2 (public)
- The proposal to cover semi-formal and formal development and evaluation tasks in a common criteria certification scheme is thoroughly presented in D3.4 *Design proposal for integrating Frama-C* (confidential)
- The Benchmark for evaluating the quality of VESSEDIA Tools regarding security vulnerabilities is presented in D4.3 (public)
- Application of Frama-C static analyzer to the above benchmarks is presented in D4.5 *Quality tests and limits of VESSEDIA tools regarding security vulnerabilities detection* (public)
- Finally, methodologies to enhance current certification and evaluation approaches by relying on formal methods and tools during static analysis of source code is presented in D6.6 *Proposal for enhancement of CSPN and Common Criteria schemes* (confidential).

[4] See at https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria , last consulted 15.12.2019

The contribution from VESSEDIA in D6.6 which is complementing existing security evaluation schemes is a suggestion of an extension of the CSPN scheme. The D4.4 and D6.6 proposals have in common the emphasis on formal methods. However, while the D6.6 CSPN extension would require the developer to provide additional documents and information, the conformity assessment scheme proposed in D4.4 imposes more constraining requirements with regards to evidences supporting claims made on software safety and security verification (SSSV).

In order to further contribute to the CC scheme, it is important to understand the structure and requirements of the CC process, in view of the potential for added value from VESSEDIA. Added-value through applying formal methods is central to the VESSEDIA methodology and explored in deliverables D3.4, D4.5 and D6.6. The CC requirements impose to find sufficient evidence and justification so that the evaluation determines that the TOE is CC conformant and meets the assurance requirements at a given level. The certification scheme can be illustrated as in the following figure:

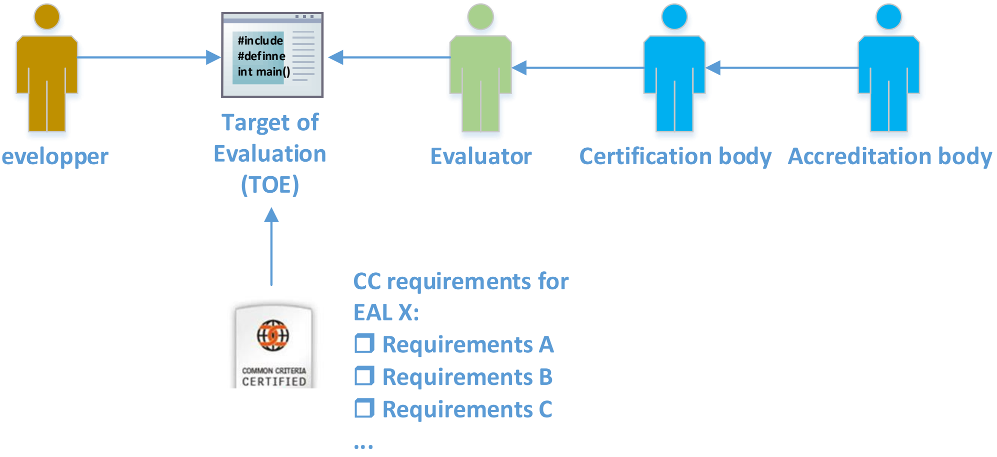

Figure 1: structure of the CC scheme

VESSEDIA experts are interested in applying the VESSEDIA methodology and VESSEDIA tools for levels below than 5, for IoT Verification and Validation (V&V). Discussion with CC experts support this statement as formal security policy model is required from EAL 6. In conclusion. Given the sparse use of higher levels EAL certification (5 and above), the use of formal methods is not that common, all the more that they are not explicitly required[5]. There is an argument on whether the developers and evaluators are actually sufficiently skilled in using them, and whether the time would be well spent[6]. Those questions are recurrent among CC experts. Therefore, from the CC community perspective (Common Criteria Scheme organisations), instead of spending all that time on examining the TOE design, wouldn't the time be better spent at doing the actual testing of the product?

The EAL levels where formal methods are typically considered most applicable, as commented by CC experts[7], are EAL levels 5-6-7 (grey shading in the following table). This would leave a large proportion

[5] See in *Mind the Gap: Formal Verification and the Common Criteria* (Discussion Paper by Bernhard Beckert, Daniel Bruns and Sarah Grebing, 2010, 6th International Verification Workshop, VERIFY-2010, Edinburgh; see https://easychair.org/publications/open/PM last accessed on 15.10.2019

[6] Same reference as above, Beckert et Al. (2010)

[7] Source: International Common Criteria Conference 2019 https://www.iccc2019.com/, see in addition dissemination event report

of CC evaluations (level 4 and below) without benefits from formal methods, as developed and promoted in VESSEDIA. However, VESSEDIA project concludes that despite formal methods can be time consuming, when they are used in a CC context, they should be configured by the developer, and the evaluator has just to check the configuration and replay the test [8] (this will be later referred to as the so–called *self-conducted* verification case in the context of the conformity assessment).

Additionally, we have tested semi-formal tools on some use-cases and connected them to complement formal methods in VESSEDIA (see WP2 and WP3). We have found out that:

- Semi-formal methods, e.g. using UML and its derivatives, are applicable at EAL5;
- Testing, using e.g. AFL, is applicable at EAL5 and below and
- Control-flow graph analysis can be used for testing at EAL5.

The typically considered most applicable EAL levels for formal methods are shown as shaded in the following table.

[8] Source: VESSEDIA outputs in D3.4 and D6.6

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 2: table of assurance components by evaluation assurance levels

Additionally, the laboratories which perform the CC evaluation face the recurrent issue that claims from applicant that the TOE has undergone formal verification regularly lack the evidences[9]. This aspect

[9] Source: International Common Criteria Conference 2019 https://www.iccc2019.com/

could be tackled better if there was a simple set of requirements on how to document the efforts done in verification during the software development life-cycle (SDLC). This is a gap that we try to fill in this report.

2.2 Other certification schemes:

With regards to software security assessment, the CC dominates the certification landscape. It is however difficult to engage in a CC certification process for cheap, short life spanned IoT devices. There exists country-specific light-weight “derivatives” (for example in France, the CSPN and Security Visa from French Certification Body ANSSI, or BSZ from German Certification Body BSI).

For addressing security and privacy threats in IoT environments, there exists a variety of frameworks such as OWASP, oneM2M, GSMA, ANASTACIA and ARMOUR[10] which address the specifics of security in IoT. Those models list surface areas, vulnerabilities, problems, attack vectors, impacts, elements to be secured and/or countermeasures. They generally have a holistic scope that encompasses the devices, data, connectivity, platforms, applications and services.

A list of public and restricted publications from standardization and regulatory bodies on IoT security can be found in an ARMOUR European H2020 project report[11]. Security certification must overcome different obstacles that are inherent to IoT contexts, such as heterogeneity of devices and changing conditions. A conformity assessment scheme must therefore be capable to adapt to regulatory and market changes, so as to not not become obsolete. Similarily H2020 project ANASTACIA presents a holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and Cloud architectures[12].

In the VESSEDIA project we are concerned by the capabilities of verification tools, and as such, we do not intend to propose a holistic certification scheme. We concentrate on the issue that verification efforts are, in most cases of medium criticality IoT, not formally reported along the software development life-cycle and not valued throughout the software value chain untill end markets.

Some interesting research and results done by EU sister projects on the development of certification are:

- Giving importance to “human rights and European values” (TRUESSEC)[13]
- Taking into consideration the challenges cause by the multiplication of certification requirements that apply to cloud service provider, for example with regards to data protection (EU-SEC)[14]
- Coping with the limits of “point-in-time” certification and promote “continuous” certification (EU-SEC).

In VESSEDIA we focus on the operating systems, middleware layers and applications that are parts of the larger IoT eco-system, and whose vulnerabilities can be better taken care of with enhanced verification effort at the time of development.

[10] Internet of Things Security and Data Protection; Editors: Ziegler, Sébastien; Springer publications; 2019

[11] See at https://www.armour-project.eu/wp-content/uploads/2018/01/white_paper_ARMOUR-IoT-Certification.pdf last consulted 04.12.2019

[12] See at http://www.anastacia-h2020.eu/ last consulted 05.12.2019

[13] See at https://cyberconnector.eu/web/truessec last consulted 05.12.2019

[14] See EU-SEC deliverables at https://www.sec-cert.eu/eu-sec/deliverables last consulted 05.12.2019

The future of certification with regards to cybersecurity, safety and privacy is currently an important topic in the EU. Under the EU Commission, the Joint Research Center (JRC) called EU Science Hub acts as the European Commission's science and knowledge service. Under that organisation, the Project Platform called European Reference Network for Critical Infrastructure Protection (ERNCIP) oversees those matters. The ERNCIP network aims at improving EU critical infrastructure protection. The ERNCIP collaborates with all types of CIP stakeholders, focusing particularly on the technical protective security solutions.

ERNCIP has 12 thematic groups among which 6 are "in progress". One of those is the IACS Cybersecurity Certification Framework (https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs). The IACS focuses on:

- extracting common good practices from existing standards and requirements towards setting new certification;
- defining Generic IACS Cyber-security Profiles, product classes and target levels;
- defining a common process for each of the levels of the proposed European IACS components Cyber-security Compliance & Certification Scheme;
- developing a prototype of a database of Certification and Compliance evaluated IACS products.

More information on certification for IoT devices can be found in D4.2. For the VESSEDIA team, as a conclusion, it is interesting to consider the IACS Thematic group as a beneficiary of our certification related output, as it will influence future EU policy on certification for Cyber-security.

2.3 Elements of the VESSEDIA methodology

Among the main elements of the VESSEDIA methodology that are important and that provide added value to the existing certification programmes, are the following:

- The ISO/IEC standard that includes the notion of Target of Verification (TOV)
- The verification tools
- The verification metrics
- The notion of Object of Verification (OOV)
- The notion of Result of Verification (ROV).

We provide explanations and details in the following sections.

2.3.1 The ISO/IEC Standard 23643

The ISO standard developed in VESSEDIA, within the ISO JTC1/SC7 WG 4 is named Software and Systems Engineering- Capabilities of Software Safety and Security Verification Tools. It is identified as the ISO/IEC DIS 23643[15]. The scope of ISO/IEC DIS 23643 includes Software safety and security verification tools based on static and dynamic methods and use cases. Therefore, it excludes both data and system safety and security verification. It also excludes testing and verification methods and processes.
The ISO/IEC DIS 23643 is planned to be published in its final version after its last developments, following the Spring 2020 ISO/IEC JTC 1/SC 7/Working Group 4 Interim Meeting and the Final Draft

[15] At the time of writing of this report, the standard is in *final draft international standard* status (FDIS).

International Standard ballot. Meanwhile, information supporting common understanding in the area of software safety and security verification tools can be found among the following standards:

- ISA/IEC 62443 series on *security capabilities for control system components*[16]
- ISO/IEC JTC 1/SC 27. Information security, cybersecurity and privacy protection. This series aim at the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects
  - More precisely, the ISO 14508, ISO/IEC 15408 series on *Information technology — Security techniques — Evaluation criteria for IT security* and more precisely — *Part 1: Introduction and general model*, widely recognized as 'Common Criteria' (CC)
- IEC 61508 international standard on functional safety. This standard provides information on software requirements and certification for tools[17].

The standardisation plan D6.4 is a confidential deliverable in VESSEDIA unlike the present D4.4 report. The ISO/IEC DIS 23643 is a document that is copyrighted by the ISO organization. We can only refer to some aspects of the standard in this report.

The main elements of the ISO/IEC DIS 23643 are[18]:

- Terms and definitions: analyzing the state of the art in standardization for software security and safety verification tools
- Categories of software safety and security verification tools
- Use cases of software safety and security verification tools: these are usage scenarios for different levels of criticality
- Entity relationship model of software safety and security verification concept
- Capabilities and requirements of software safety and security verification tools.

We can now look more closely at the VESSEDIA tools.

2.3.2 Verification tools

The tools developed in VESSEDIA can perform analysis that support a security evaluation process. More information can be found in VESSEDIA D4.2 where verification tools are presented with more details. The following table illustrates the main tools developed or used in the VESSEDIA project. The tools are characterized following guidance of the ISO/IEC FDIS 23643.

[16] See at https://www.isa.org/intech/201810standards/

[17] See https://www.iec.ch/functionalsafety/faq-ed2/ and https://www.perforce.com/blog/qac/what-iec-61508-plus-safety-integrity-level-basics Last consulted 20.12.2019

[18] See full table of contents at https://www.iso.org/obp/ui/#iso:std:iso-iec:23643:dis:ed-1:v1:en . Last consulted 10.12.2019

Tool name	Tool capability	Indicative SDLC Stage
Frama-C	Program Analysis	Code (implementation)
FlowGuard	Program Monitoring	Testing (unit testing, verification and validation)
Diversity	Modeling	Design (implementation)
Papyrus	Modeling	Design (refinements)
SecuRate	Program Analysis	Code (implementation)
VeriFast	Program Analysis	Code (implementation)
EVA (plugin)	Program Analysis	Code (implementation)
WP (plugin)	Program Analysis	Code (implementation)
RPP (plugin)	Program Analysis	Code (implementation)
E-ACSL (plugin)	Program Monitoring	Code (implementation)

Table 3: table of VESSEDIA tools

VESSEDIA tools are examples of the many tools available for Software Safety and Security Verification (SSSV). Those tools may apply at different stages of the SDLC for a given software. They can be characterized by using categories, capabilities and requirements of SSSV Tools (SSSVT) from the ISO/IEC 23643.

2.3.3 Verification metrics

VESSEDIA metrics are presented in D4.1. The following list illustrates the main metrics developed or used in the VESSEDIA project.:

Metrics name	Technical implementation	Type	Related plugin/tool
SecuRate	Fingerprint matching	Numeric value	SecuRate, EVA
CriticalDepth	Call stack depth	Numeric value	EVA
Liveness Metrics	Taint analysis	Numeric value	EVA
Size Definition Distance Metrics	Taint analysis	Numeric value	EVA
Dangling Pointers Persistence Metrics	Taint analysis	Numeric value	EVA
Cryptographic Secrets Persistence Metrics	Taint analysis	Numeric value	EVA
Static Analysis Coverage Metrics	Abstract Interpretation	Ratio	EVA
Quantitative assessment for deductive verification tools	Deductive Verification	Numeric value	WP
“CWE scoring of an alarm” Metric	Classification	Numeric value	Report/MDR
“Criticality of an alarm” taint analysis Metrics	Taint analysis / Control-flow assessment	Boolean / Numeric value	EVA
“Statistics” Metric	Collection of existing metrics	Set of numeric values	Metrics

Table 4: Table of VESSEDIA metrics

These metrics determine and prioritize the most crucial vulnerabilities to analysts and developers. As we will see in the conformity assessment scheme later, the metrics are meant to be presented with their computed value whenever used for the purpose of verification.

2.3.4 Objects of Verification

For the purpose of creating the CAS, we need an extension of the notion of TOV, as can be found in ISO/IEC 23643, through the notion of object of verification (OOV). The TOV is the software product to be verified and integrated into a product, and is granted the certificate, while the OOV specifies precisely the elements on which verification is implemented (e.g. program files). The OOV, for example in the case of use of a program analysis tool, will state which code segment has been covered by the use of verification tools and on which metrics have been stated.

2.3.5 Results of Verification

For the purpose of creating the CAS, we also need to characterize the elements that can be consulted by the conformity assessment body so as to validate that a tool has been used and has generated elements that provide input and/or output in a software security and safety verification process. Those elements are referred to as the Result of verification (ROV).

Chapter 3 Proposal for contribution of VESSEDIA to Common Criteria

3.1 Overview of the proposal

3.1.1 Rationale

Negligence at the time of executing software safety and security verification efforts during the software development life-cycle (SDLC) leads to vulnerable applications, and thus IoT devices and IoT/smart systems and their integrated environments (e.g. smart homes).

In VESSEDIA we aim at developing the Verified in Europe (ViE) Conformity Assessment Scheme (CAS), to propose light steps and rewards for building more reliable and secure IoT. This is done through improved traceability and by rewarding for taking care of safety and security risks during the SDLC.

Despite the ViE CAS can be used as a stand-alone CAS, it is meant to be complementary to CC by providing useful information on V&V to the CC evaluators.

3.1.2 Concept of the Verified in Europe Conformity Assessment Scheme (ViE CAS):

The ViE CAS proposes a lightweight documentation, a list of tool capabilities (as can be found in ISO/IEC 23643[19]) that have been used in verification related activities along the SDLC stages. Only authorised parties (developers and evaluators) can consult it. The ViE CAS contributes to building more robust smart environments. The idea is represented in the figure below:

[19] See at https://www.iso.org/standard/76517.html

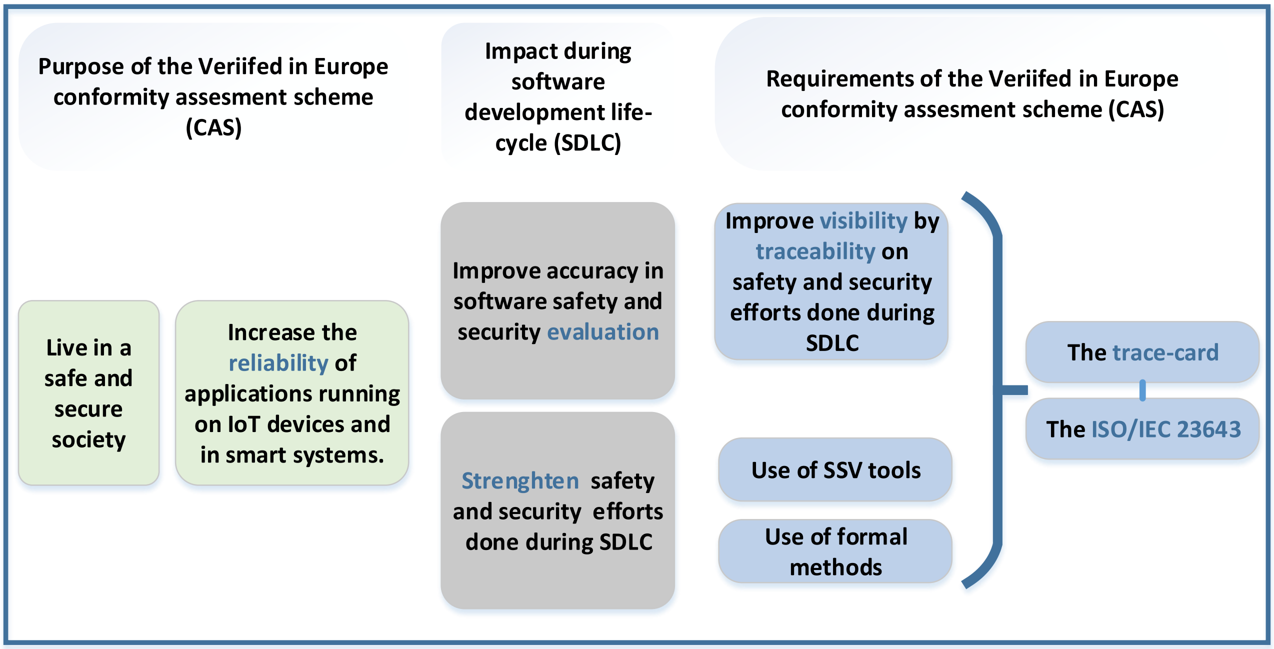
Purpose of the Veriifed in Europe conformity assesment scheme (CAS)
Impact during software development life-cycle (SDLC)
Requirements of the Veriifed in Europe conformity assesment scheme (CAS)
Live in a safe and secure society
Increase the reliability of applications running on IoT devices and in smart systems.
Improve accuracy in software safety and security evaluation
Strenghten safety and security efforts done during SDLC
Improve visibility by traceability on safety and security efforts done during SDLC
Use of SSV tools
Use of formal methods
The trace-card
The ISO/IEC 23643

Figure 2: mindmap of the ViE CAS

3.1.3 Elements of the Verified in Europe Conformity Assessment Scheme (ViE CAS):

The required documentation, called the *trace-card,* acts as a SDLC “passport” with regards to software safety and security verification (SSSV) efforts. All tools which have been used during the SDLC, for the purpose of safety and/or security verification, are named in a matrix with two dimensions:

The SDLC stages

The software safety and security verification tool capabilities (ISO/IEC 23643)

3.1.4 Certification:

A company that provides the evidences to the third party with regards to documented safety and security verification efforts is eligible for the Verified in Europe certification. Evidences are:

- A clearly defined *Target of Verification (TOV):* the product version and components to receive the certificate
- Named effectuated *tools*
- *Metrics* delivered by the tools
- Clearly defined *Object(s) of Verification* (OOV): the files and documents, e.g. the code segment on which tools apply)
- A clearly documented set of *Result(s) of Verification* (ROV): the evidences supporting the claim that the use of the verification tool was successfully completed.

3.1.5 Trademark:

The following trademark has been conceptualized for the purpose of providing market visibility for those products which guarantee traceability on the use of SSV tools during their SDLC. The trademark is protected and owned by member of the VESSEDIA project consortium.

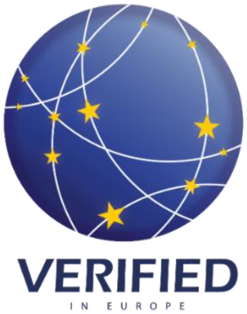

Figure 3: trademark of the ViE CAS

3.1.6 Support to the use of formal methods and level of certification

The ViE CAS offers an easy entry level for compliance with documentation on SSSV, and two higher levels when formal methods are applied. The CAS process offers two paths:

- Production of evidences by the applicant, then validated by a third-party *evaluator*.
- Production of evidences and validation fully delegated to a third-party *evaluator*.

3.1.7 Conclusion

The ViE CAS is a promising development towards supporting software security and safety verification efforts done by the community of IoT applications developers, evaluators as well as tool vendors. It is complementary to currently available certification practices and supporting the efforts put by the VESSEDIA project for promoting formal methods for V&V. We believe that the ViE CAS crystalizes the efforts done by the actors of the community towards making our society less vulnerable to threats and incidents. The ViE CAS can be influential to policy-making in the EU. We will provide more details on the CAS in the following sections.

3.2 Details of the contribution to Common Criteria: The Verified in Europe Conformity Assessment Scheme

3.2.1 Introduction:

The structure of this section presenting details of the ViE CAS is based on Conformity assessment. Fundamentals of product certification and guidelines for product certification schemes (ISO/IEC 17067:2013).

3.2.2 How ViE CAS relates to the concept of certification

3.2.2.1 Attestation that requirements are fulfilled in reference to existing standards

Impartial third-party organizations[20,21] carry out product certification on the so-called *Target of Verification* (TOV). The TOV is a software, or a set of software items or units, to be verified (e.g. in terms of safety and security), see *ISO/IEC 23643 DIS*. The TOV's Software Development Life-Cycle (SDLC) must have undergone verification by the means of software safety and security verification tools.

Certification organizations thereby attest that specific *software safety and security verification tool capabilities (SSSVTC)* have been effectuated during the SDLC of a given TOV.

3.2.2.2 Activity that provides confidence that products comply to requirements

When granted, the Verified in Europe Conformity Assessment Scheme (ViE CAS) provides visibility and confidence to consumers, regulators and industry that specific *SSSVTC* have been effectuated during the SDLC of a given TOV.

The effectuated SSSVTC on the TOV must be valid for the target software that is sold on the market. Therefore, any change in the software with a ViE CAS certificate shall be monitored whether it invalidates the effectuated SSSVTC on the TOV. It is the responsibility of the applicant to ensure continuation and validity of the effectuated SSSVTC by asking follow-up service from the certifying third-party organizations.

3.2.2.3 Benefits to markets and consumers

Effectuated *SSSVTC* reduce the risk of vulnerabilities in the TOV and its related target software sold on the market. The ViE CAS gives visibility, raise awareness and supports common understanding on those verification efforts. This results in less vulnerable software and applications, therefore in more secure and safer IoT environments. This results in improved trade, market access, fair competition and consumer acceptance of products on a national, regional and international level.

3.2.2.4 Fundamental objective of product certification

The ViE CAS addresses the issue of traceability and fulfilment of SSSV requirements in the SDLC. The ViE CAS offers awareness, visibility and common understanding to the entire SSSV value chain with regards to effectuated SSSVTC, i.e. towards the following stakeholders:

- The society at large (characterized as "smart society"[22] in the context of IoT)
- Clients/sponsors
- Developers
- Evaluators and providers of safety and/or security evaluation services
- Certification bodies
- Accreditation bodies
- CAS owner

[20] Conform to ISO/IEC 17065.

[21] See in https://www.iso.org/sites/cascoregulators/documents/Annex%203%20-%20Conformity%20assessment%20techniques%20-%20Accreditation.pdf last consulted 26.11.2018

[22] See in Smart society: a winding road towards the future by youris.com EEIG, on https://cordis.europa.eu/news/rcn/128878_en.html last consulted 01.11.2018

- Tools providers.

Effectuated SSSVTC may be done by the developers themselves or externalized to evaluators and providers of safety and/or security evaluation services. In both cases the third-party body certifies the validity of the effectuated SSSVTC on the TOV.

3.2.2.5 Confidence in fulfilment of requirements:

Actors of the entire SSSV value chain have an interest in fulfilment of requirements. They benefit from the common understanding, improved awareness, and visibility on the extent of effectuated SSSVTC. Ultimately, SSSV efforts result in less vulnerable TOV, thereby improving software safety and security (SSS).

3.2.2.6 Value of the ViE CAS:

The customers and SSSV value chain actors' perception and sensibility to SSS risks depends on the business and criticality of the domain considered. The reduction of vulnerability and the improved SSS yield sufficient value for suppliers to effectively market products containing a TOV with effectuated SSSVTC.

Actors	Benefits
The society at large ("smart society")	Improved reliability, safety and security
Client/sponsor	Confidence, acknowledgement
Developers	Product quality, visibility
Evaluators	Complementary service, more business
Certification bodies	Complementary service
Accreditation bodies	Complementary asset, more business
CAS owner	Strategic asset, more business
Tools providers	More business

Table 5: Table of actors of the verification value chain and their expected benefits

In VESSEDIA, we have presented cost/benefits considerations in D1.6. We have been able to demonstrate that given certain characteristics of the SDLC, evaluation, and certain market conditions, it can be profitable for a developing company to use program analysis tool capabilities, i.e. formal methods, in the verification process.

3.2.3 The ViE CAS in practice

Below we present details on the ViE CAS.

3.2.3.1 General model of the CAS

The figure below illustrates where the ViE CAS stands and how it connects with end-users' (client/sponsor), giving visibility on the product quality with regards to verification efforts, as opposed to a non-labelled product. The label reflects the efforts put into the security and safety verification and the documentation about which tool capabilities have supported it.

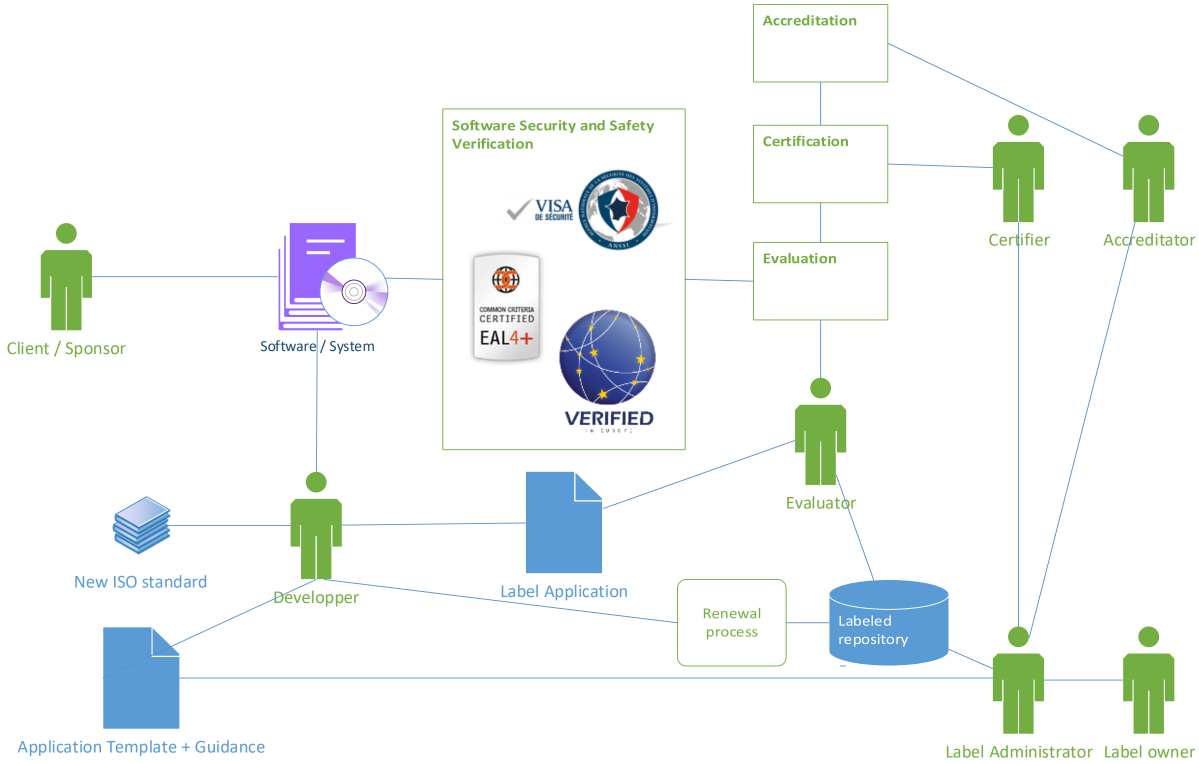

Figure 4: Labelling scheme of the Verified in Europe label

Generally, the label and its requirements for certification shall improve safety and security in industrial applications, support the competitiveness of software/systems, and improve end users' trust in such applications. The label trademark, as shown in Figure 4 characterizes European expertise in software security and safety verification.

During the SDLC of a given software, with pre-requisite on a *risk assessment*, the developing company and/or an external service provider such as an evaluator, make use of safety and security verification *tools*. Those tools deliver logs, report and metrics on specific object(s) of verification that belong to the TOV. The applicant must provide truthful information and input for the certifying third party to determine the conformance of the effectuated *SSSVTC on* the TOV during *the SDLC*, with the help of explicit Result of Verification that are bookmarked on the SDLC. From there, a decision on effectuated tool capabilities can be taken by the certifying third party.

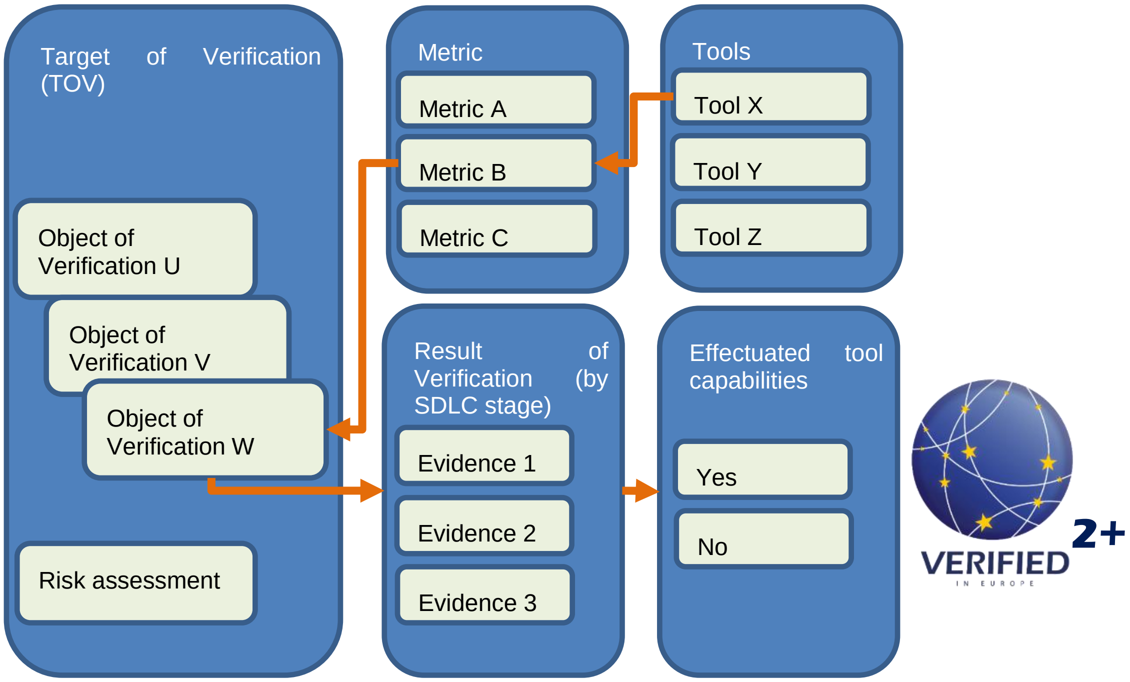

Figure 5: elements of the ViE CAS

There are two alternative scenarios for the third-party to determine the conformance of the effectuated *SSSVTC on* the TOV during *the SDLC*:

3.2.3.2 Risk assessment:

Most IoT products already have existing security claims, prior to any certification process through the ViE CAS, and they have undergone a risk assessment process that is aligned with those existing schemes. The ViE CAS comes as a complement to those existing schemes such as the Common Criteria Evaluation or lighter versions such as German BSZ or French CSPN. In that case, the ViE CAS does not add any extra work with regards to the risk assessment part. It is possible to integrate this already existing element as an input in the ViE CAS certification process.

However, for a product that has no pre-established risk assessment it is necessary to perform one. Risk assessment is presented in details in the ISO 31000-series. It is an activity in the scope of risk management and of information security risk management, as presented in the ISO/IEC 27000-series.

We would recommend performing risk assessment work using for example the evaluation methodology that can be found in VESSEDIA WP4 for:

1. Asset valuation: the use of the Confidentiality – Integrity – Availability framework
2. Threat identification: the use of the STRIDE framework
3. Risk estimation: to compute vulnerability levels

Specifically, for risk assessment, four techniques provide interesting features with regards to applying them on IoT devices, which are:

- Environmental risk assessment

- Structure “What if?” analysis (SWIFT)
- Reliability centered maintenance
- Failure mode effect analysis (FMEA/FMECA)

Depending on the IoT devices considered, those techniques provide various advantages. We recommend consulting deliverable D1.1 of VESSEDIA project for complementary information on risk assessment.

3.2.3.3 Selection in the ViE CAS

Firstly, in the case of **self-conducted SSSV**, the applicant conducts the SSSV independently, and at the end of the SDLC, provides evidences of the effectuated *SSSVTC on* the TOV during *the SDLC*. The applicant must provide:

a. A **risk assessment** of the safety and security critical TOV
b. Characteristics of the **Object of Verification** (OOV) e.g. files, documentation and technical support on which tool capabilities are effectuated
c. The information expressing the **stage(s) of the SDLC** where the OOV has been verified, namely:
    1. Requirements (definitions)
    2. Specifications (details)
    3. Design (refinements)
    4. Code (implementation)
    5. Test cases (unit testing, verification and validation)
    6. Target software (integration and integration testing)
    7. System integration, testing and validation
    8. Other (e.g. related to life-cycle activities such as Project management, Configuration management, Quality assurance, Documentation, Training and support, Evaluation And testing / Verification and Validation – V&V)
d. the list of tools used for verification (vendor, version)
e. the list of effectuated tool capabilities during verification (see *ISO/IEC 23643 DIS*)
f. the list of metrics, reports and logs produced (measurement, measurement unit, scale, definition)
g. the information that expresses the Result of Verification (ROV) e.g. files, documentation and technical support, necessary to control the validity of effectuated tools and metrics on the OOV.

The following diagram displays the self-conducted SSSV process. This process is based on internal competences in verification, and guarantees independence of the verification efforts.

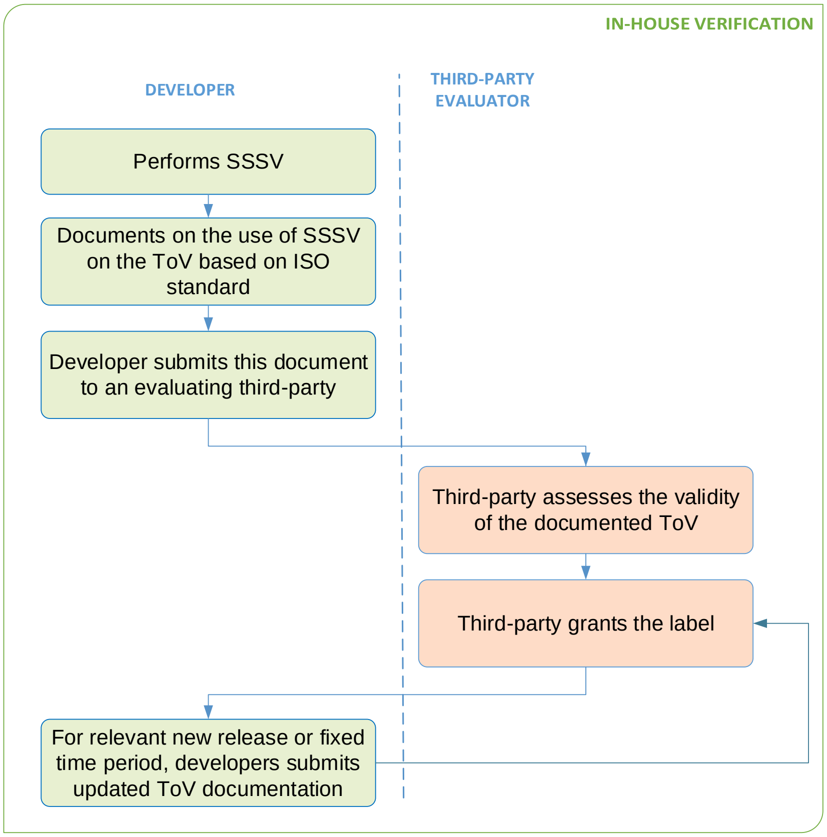
IN-HOUSE VERIFICATION
DEVELOPER
THIRD-PARTY EVALUATOR
Performs SSSV
Documents on the use of SSSV on the ToV based on ISO standard
Developer submits this document to an evaluating third-party
Third-party assesses the validity of the documented ToV
Third-party grants the label
For relevant new release or fixed time period, developers submits updated ToV documentation

Figure 6: self-conducted SSSV

Secondly, in the case of **externalized SSSV**, the certifying third party effectuates SSSVTC on the TOV during the SDLC and produces evidences. The applicant must provide the information and input (e.g. files, documentation and technical support) that enable the certifying third party to effectuate the SSSVTC on the TOV during the SDLC and enable the production of truthful evidence.

The following diagram displays the externalized SSSV process. This process is based on value adding service provided by the certifying third party. Competence of the certifying third party in verification allows for reducing software vulnerabilities without the needs for the software development company to purchase licence and train of developers.

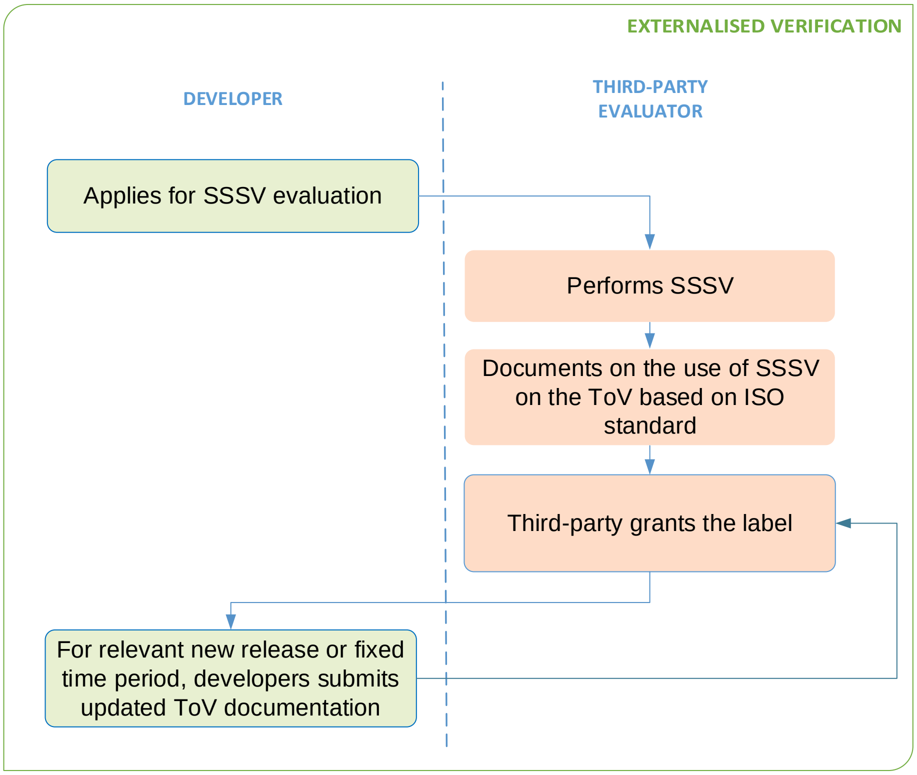
EXTERNALISED VERIFICATION
DEVELOPER
THIRD-PARTY EVALUATOR
Applies for SSSV evaluation
Performs SSSV
Documents on the use of SSSV on the ToV based on ISO standard
Third-party grants the label
For relevant new release or fixed time period, developers submits updated ToV documentation

Figure 7: externalised SSSV

3.2.3.4 Determination in the ViE CAS

There are two scenarios for determination:

- In **self-conducted SSSV**: the applicant lists the effectuated SSSVTC and provides truthful evidences for each effectuated capability.
- In **externalized SSSV**: the certifying third party applies SSSVTC and produces the evidences. The determination of effectuated SSSVTC is done by referring to the list available in ISO/IEC 23643 DIS, for all stages of the SDLC. The effectuated tool capabilities are listed in a table called the SSSVTC Trace-card (see below).

The trace card shows two dimensions: the SDLC stages in lines and the SSSVTC in columns.

SDLC Stage (V-model)	**Effectuated safety and security verification tool capabilities**									
	Safety capabilities						**Security capabilities**			**Common capabilities**
	Specification and refinement	Model-checking	Program analysis*	Proof	Monitoring	Programming rules checkers	Vulnerability analysis	Security modeling	Threat modeling	
a) Requirements (definitions)									☑ **STRIDE**	☑ **Risk Analysis**
b) Specifications (details)										
c) Design (refinements)								☑ **Papyrus**		
d) Code (implementation)			☑ **Frama-C**							
e) Test cases (unit testing, verification and validation)					☑ **Flowguard**					
f) Target software (integration and integration testing)										
g) System integration, testing and validation										
h) Other than above**										
i) Update 1, 2,…										

Table 6: Table of effectuated safety and security verification tool capabilities (the SSSVTC Trace-card):

* Program analysis verification levels are incremental and set as: 1) No analysis 2a) Use of compiler diagnostic 2b) Heuristic static analysis 3) Sound static analysis. Those levels are defined in VESSEDIA Project's *Vulnerability Discovery Methodology* D1.7 Public Report (see https://www.vessedia.eu/). VESSEDIA project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731453.

**In software development projects, safety and security verification tool capabilities may be effectuated across stages of the SDLC. If connecting an effectuated capability to a single or a series of stages of the SDLC is misleading, this additional category may be used for listing those effectuated capabilities. This may the case for example for capabilities effectuated during life-cycle activities such as project management, configuration management, quality assurance, documentation, training and support, and evaluation and testing.

3.2.3.5 Review in the ViE CAS

In both **self-conducted SSSV** and **externalized SSSV**, the effectuated SSSVTC Trace-card and its evidences are reviewed by the certifying third-party. As availability and truthfulness of evidences are validated, a decision on certification can be taken.

3.2.3.6 Decision in the ViE CAS

On the basis of availability of evidences, the certifying third-party rejects or grants the following levels for the ViE CAS (levels are indexed on the level of effectuated program analysis):

Self-conducted SSSV as a base for the ViE CAS	Decision on certification	Externalized SSSV as a base for the ViE CAS
Rejected	The evidences on effectuated SSSVTC during the SDLC are not available, incomplete or their truthfulness could not be established.	Rejected
Level 1	The SSSVTC Trace-card and truthful evidences on effectuated SSSVTC during the SDLC are both available.	Level 1+
Level 2	In addition to the above, truthful evidences on effectuated program analysis capabilities up to the level of ***use of compiler diagnostic*** or ***Heuristic static analysis*** are available.	Level 2+
Level 3	In addition to the above, truthful evidences on effectuated program analysis capabilities up to the level of ***Sound static analysis*** are available.	Level 3+

Table 7: Table of ViE CAS levels

3.2.3.7 Attestation in the ViE CAS

Once granted the applicant has the right to use the trademark associated with the ViE CAS.

3.2.3.8 Surveillance in the ViE CAS

In order to maintain its certification, the beneficiary of the ViE CAS has the obligation to submit the SSSVTC Trace-card and make its evidences available to an accredited CAB within one year after last validation of the Trace-card.

Following the granting of the ViE CAS, if there has been some modifications on the TOV, for example in the case of patches or new releases, the Trace-card and its evidences are updated and mention any additional verification effort implemented, if any.

If not, the target software attached to the TOV loses conformance to the ViE CAS requirements, the claim is not validated anymore and the applicant has to withdraw all trademarks or reference to ViE for the given modified TOV.

3.2.3.9 Details on the functions of the ViE CAS

Functions of the scheme characterize the steps to be followed by the CAB to deliver the CAS. In this scheme, the TOV is subjected to the determination activities. A certificate of conformity is issued for the TOV, the characteristics of which are detailed in the certificate. The TOV is representative of manufacturer as being manufactured in accordance with the certified type. Details on the TOV are given in the following sections.

3.2.3.9.1 Scope

The scheme covers a software or module of software's code specified as the *Target of Verification* (TOV). It guarantees that the TOV has undergone *software safety and security verification tool capabilities (SSSVTC)*.

3.2.3.9.2 Requirements

The product is evaluated against the requirements by reference to the SSSVTC as listed in *ISO DIS 23643*. The SSSVTC are listed with all evidence needed to support the claim as listed in section 3.2.3.3 *Selection in the ViE CAS*.

3.2.3.9.3 Selection of the activities

Especially, the OOV must be precisely formulated so that there is no misunderstanding on the extent of coverage of the used SSSVTC. If the OOV corresponds to the portion of a whole, the applicant must provide metrics that explicitly defines the OOV as a proportion of the whole. For example, a code segment on which SSSVTC have been used will be expressed in a metric, such as lines of codes, alongside with the whole of the software expressed in the same metric as well as the percentage in proportion.

3.2.3.9.4 Other requirements

The certification body involved in the process of evaluation must have the competence to assess the truthfulness of the evidences that support the claim. This means that if the certification body does not have such competence, i.e. expert having the knowledge for validating an evidence that supports the claim of a used SSSVTC, it has the obligation to ask for validation of this specific evidence from another conformity assessment body that has the competence.

3.2.3.9.5 Procedure

The certification body validates one by one each of the evidence claimed to sport the use of SSSVTC by the applicant of the ViE CAS.

3.2.3.9.6 Content of the statement of conformity

The certificate presents the clearly the TOV and lists the following elements in a table that contains information on the tools, metrics, Object of Verification and Results of Verification, and a validation mark for each SSSVTC. The table shows clearly which elements and evidences validate which SSSVTC.

3.2.3.9.7 Conditions of use of the statement of conformity

Once the validation is granted, the applicant can make use of the statement of conformity, refer to the associated ViE CAS level, and make use of the trademark in association with the TOV (for example on the packaging of the software, on web environment in association with the product or within its documentation).

3.2.3.9.8 Resources required for the operation of the scheme

The personnel in charge of the validation of the Trace-card must have competence in understanding each of the verification capabilities that have been used in order to be able to validate them.

3.2.3.9.9 Determination and surveillance reporting and use by the certification body and the scheme owner

Information about the validated SSSVTC (summarised in the Trace-card) are to be kept strictly undisclosed to the public, it is only to be seen by the applicant and the validator. Such information can be critical as it gives an idea on which vulnerabilities have been well addressed during the SDLC, and which vulnerabilities may therefore not have been sufficiently addressed. This is very useful information for testing in the context of another conformity assessment scheme (e.g. CC) but can also give hint to hackers for exploiting neglected sources of vulnerabilities.

However, a company that has been granted the statement of conformity can make use in discretion of the validated SSSVTC towards its own stakeholders. The company can for example show the Trace-card to its own customers, as it may increase the perceived value of the software characterized by the TOV.

3.2.3.9.10 Non-conformities

As long as the truthfulness of an SSSVTC cannot be proven with the help of the evidence provided, the Trace-card cannot be validated and the CAS is not granted.

3.2.3.9.11 Publication of the directory of certified products

National certification bodies hold a central/shared list of products that have been validated as conform TOV by the CABs. The CABS make edit directly in the list.

3.2.3.9.12 Extension of scope

Future developments in the scheme may add to the scope of the ViE CAS some ranges of values for key metrics in a given capability to be used as a criterion for validation.

3.2.3.9.13 Marketing

It is common for actors in the verification value chain to display the label of a CAS for recognition, https://www.primx.eu/en/about-primx/). The Verified in Europe trademark can be used in documents for the purpose of Marketing activities.

Chapter 4 Summary and Conclusion

In this deliverable, we developed the Verified in Europe Conformity Assessment Scheme (ViE CAS). It is a light scheme complementary to the Common Criteria. Its trademark is awarded when the requirements are completed. The verified in Europe conformity assessment scheme fulfills the gap and needs which have motivated the development of the ISO/IEC 23643 (see section 2.3.1 The ISO/IEC Standard 23643). It harmonizes knowledge throughout the verification value chain, improves visibility and traceability of use of SSSVT. The ViE CAS also promotes verification as a value adding activity towards more secure and safer society.

The ViE CAS introduces the trace-card which acts as a “passport of verification” for the software it relates to. It documents which verification tools have been used and where/when with regards to the SDLC. It is an important step in the context of a smart Society that needs to lift up software requirements towards safety and security from a tool perspective.

A software development team can collaborate with an evaluator to track the application of SSSVTC, whether engaged in the process of a CC evaluation or not. The ViE CAS can also support the CC evaluation process by providing interesting information to the evaluator on the extent of efforts used to spot vulnerabilities and faults and fix them. The claim made by the applicant for certification is awarded to a software in a given version, which we refer as the *Target of Verification* (TOV – see ISO/IEC 23643) on which a risk analysis must have been performed.

The claim follows the use of verification tools during the SDLC, more precisely, of tool capabilities as listed in the ISO/IEC 23643 list. Clearly designated elements, such as code segment(s), a file, or a set of files corresponds to the so-called *Object of verification* (OOV). The so called Results of Verification (ROV) contain evidence on the use of verification tools, and give way to the certification.

There exist three levels of verification, following the extensiveness of using static analysis, if any. In level 1, there is no static analysis is applied, but there is visibility and traceability on verification through a validated trace-card. In level 2, the application of static analysis corresponds to so called compiler diagnostics, programming rules checks or Heuristic static analysis levels. In level 3, the application of static analysis corresponds to so called Sound static analysis level, which is relevant for applications with highly critical risks

In case of contribution for the production of evidences, supporting the claim of verification, by an evaluator, we refer to levels 1+, 2+ and 3+ representing a higher level of confidence than levels 1, 2 and 3 respectively. Moving up the levels of the ViE CAS offers an opportunity for return of investment as robustness increases due to the power of programme analysis tools.

Altogether, the ViE CAS requires light effort in documentation during the SDLC that supports visibility, and traceability throughout the verification value chain, while promoting the use of verification tools, with an emphasis on program analysis tools.

The ViE CAS has been presented in the 4th Meeting of ERNCIP’s IACS thematic group [23]. The meeting was a technical and review meeting for planning and producing the IACS Cybersecurity Certification Framework (ICCS). ENISA and EU Commission will write the final version of ICCS on the basis of the recommendations of the IACS group. The ViE CAS corresponds to ERNCIP objective of being agnostic as it does not impose its principles, it is a referral, and encourages SSSV and its documentation. Also, the ViE CAS corresponds to ERNCIP objective of being unequivocal as it reduces ambiguity through enhanced visibility and traceability of SSSV. Therefore, the ViE CAS was relevant to propose for being taken in consideration in making recommendations for the ICCS

[23] See at https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs last consulted 11.12.2019

(for example in its section 5[24]), alongside the benchmarks of ISO/IEC 15408 (CC), ISA/IEC 62443 and documentation under ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection.

[24] In reference to the draft version consulted during IACS meeting on 08.11.2019

Chapter 5 List of Abbreviations

Abbreviation	Translation
CAB	Conformity Assessment Body
CAS	Conformity Assessment Scheme
CC	Common Criteria
ENISA	European Union Agency for Cybersecurity
ERNCIP	European Reference Network for Critical Infrastructure Protection
EU	European Union
IACS	Industrial Automation and Control Systems
ICCS	IACS Cybersecurity Certification Framework
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IoT	Internet of Things
OOV	Object of Verification
ROV	Result of Verification
SAR	Security Assurance Requirements
SDLC	Software Development Life-Cycle
SFR	Security Functional Requirements
SSS	Software Safety and Security
SSSV	Software Safety and Security Verification
SSSVT	Software Safety and Security Verification Tool
SSSVTC	Software Safety and Security Verification Tool Capability
TOE	Target of Evaluation
TOV	Target of Verification
V&V	Verification and Validation
ViE	Verified in Europe