D1.6 - Economic rationale and metrics report of the effectiveness and efficiency of the use of VESSEDIA outcomes

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 / D1.6/ V1.0
Work package contributing to the deliverable:	WP1
Due date:	December 2018 – M24
Actual submission date:	1st April 2019

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

Abstract:	The VESSEDIA methodology promotes verification tools towards enhanced software safety and security verification efforts throughout the developing community. Also, it initiates the supporting label “Verified in Europe”. Related investments for enhanced verification are well spread out between the actors of the verification value chain, and each actor faces its own challenges on its business model. While the logic of investing in higher levels of static analysis for high criticality applications is commonly agreed, the rationale shows that a breakeven point is reachable at a lower criticality level for medium level of static analysis. This is encouraging for broadening the use of static analysis among the developing community.
Keywords:	Costs and benefits, Value chain.

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)

Purna Bahadur Baral (TUAS)

Pekka Forselius (TUAS)

Timo Mieskonen (TUAS)

Disclaimer

Executive Summary

The building blocks of the VESSEDIA methodology are the developments on the toolbox based software verification, as well as the supporting ISO standard IEC 23643 along with the “Verified in Europe” label.

Implementing the VESSEDIA methodology therefore relates to promoting and supporting enhanced verification efforts during the software development life cycle and along the software safety and security verification value chain. The value chain is characterised by:

- Client/sponsor
- Developers
- Evaluators
- Certification bodies
- Accreditation bodies
- Label owner
- The society at large, characterized as “smart society”[1] in the context of IoT

However, there is uncertainty with regards to the costs and benefits of applying the VESSEDIA methodology throughout the software verification value chain. Therefore, we analyse the cost structure of the methodology and of the use of the developed tools. For cost-benefit analysis in the context of software security and safety verification, the economic rationale should take in consideration each of the actors of the value chain.

The short term affordability of the VESSEDIA methodology is therefore critical for reaching interest and commitment throughout the software verification value chain. Given the economic rationale case-based assumptions, the breakeven is reached at the point of using heuristic static analysis on medium criticality software. There is a potential loss to expect in any case where a lower criticality software undergoes static analysis. However, if static analysis is applied for low criticality software the breakeven is very close or even reached in some cases if the training costs of developers is considered as an amortized investment (for example on 10 years).

While the logic of investing in higher levels of static analysis for high criticality application is common practice, showing that a breakeven point is reachable at a lower criticality level for medium level of static analysis supports the methodology. This is encouraging for broadening the use of static analysis among the developing community.

[1] 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

Contents

List of Figures

List of Tables

Chapter 1 The VESSEDIA methodology and the software safety and security verification value chain

1.1 IoT software safety and security verification tools

There is growing societal concern over IoT safety, security and privacy issues mostly from a data and device perspective[2]. While the global market for automated software and security testing tools is expected to grow, there is a lack of awareness among embedded/IoT software engineers towards security[3].

For IoT applications developers, providing secure and safe applications to be used on IoT devices is actually challenging. Applying advanced verification tools and methodologies surely helps but it may imply prohibitive constraints in terms of time, training and other types of costs or resources.

Those efforts yield specific advantages, such as improved efficiency through standardized verification efforts, as well as risk mitigation. In first place, it is challenging to budget for certifications[4]. Moreover, it may be difficult to justify the efforts spent for conformity to a demanding verification methodology such as the one introduced in VESSEDIA. The requirements may be perceived as non-revenue generating activities, or under constraints in terms of date of delivery[5]. Following the development of the VESSEDIA methodology (toolbox based software verification), and with the support of the candidate ISO standard IEC 23643, we analyse the cost structure when applying the methodology. We also want to investigate expected benefits from the VESSEDIA security and safety verification toolbox.

1.2 Evaluating costs and benefits for the Economic Rationale

Implementing the VESSEDIA methodology relates to enhancing verification efforts during the software development life cycle. However, there is uncertainty with regards to the costs and benefits of applying the VESSEDIA methodology throughout the software verification value chain.

Within “Task 1.5 Cost structure, scalability and metrics of the methodology (M01-M24)”, we analyse the cost structure of the methodology and of the use of the developed tools. Consequently, we have to consider the ***costs savings*** and ***avoided costs*** that the approach yields by increasing safety and security. Therefore, we are interested in both costs and benefits. As a note, all figures displayed in financial tables are expressed in Euros, unless specified otherwise.

Cost savings[6] refers to the impact on resource consumption and efficiency (e.g. does VESSEDIA reduce the time spent in verification?), while avoided cost refer to an expense not yet incurred (cost of the realization of a risk that the VESSEDIA approach mitigates). We will also consider gains and other types benefits (e.g. brand value, market visibility) yielded by the VESSEDIA approach.

The costs and benefits analysis unrolls through the following cost estimating steps:

1. information/feedbacks gathered/measured in the VESSEDIA project use-cases,

[2] See CHARIOT EU Project https://www.chariotproject.eu/About and TRUESSEC EU Project https://truessec.eu/library
[3] See http://blogs.grammatech.com/static-analysis-is-gaining-ground-in-security-despite-some-developers-still-ignoring-the-issue
[4] See in https://www.corsec.com/certification-budgeting/ last consulted 08.01.2019
[5] See in https://www.jrothman.com/articles/2000/10/what-does-it-cost-you-to-fix-a-defect-and-why-should-you-care/ last consulted 26.02.2019
[6] Source at https://www.business-case-analysis.com/avoided-cost.html

2. an analogy estimate using a value chain and cost breakdown structure (CBS[7]) and relevant cost factors information through secondary data research
3. information/feedbacks gathered/measured in the test case analysis proper to D1.6

The analysis will be synthesized and help establishing estimates for future implementation of the VESSEDIA methodology, for example when using a safety and security verification toolset, that is benchmarked on the ISO standard as stated in D6.4, on any software verification effort.

1.3 Introduction to the software verification value chain

The context of implementing the VESSEDIA approach can be simply illustrated as the following: *clients/sponsors* use a software/system built by *developers*. The software/system is prone to undergo intentional (security related) or unintentional (safety related) misuse, corruptions, bugs or attacks possibly executed by *threat agents* (see Figure 1).

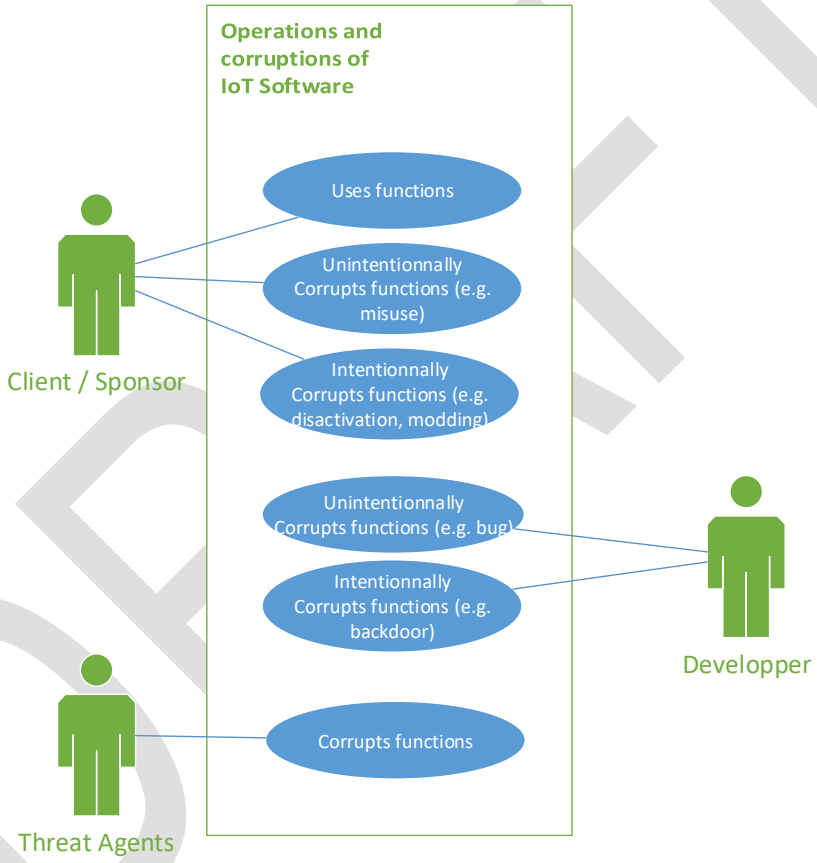

Figure 1: actors of operations and corruptions of IoT software

The developer ensures that both the development and verification processes will satisfy the security and safety functional requirements of the coded software/system. See in Figure 2.

[7] See in W.J. Fabrycky and B. S. Blanchard, Life-Cycle Cost and Economic Analysis, Chapter 6, Prentice Hall, 1991 and adapted materials at http://www.emc.ufg.br/~lguedes/moodle/get/7.pdf last consulted 23.11.2018

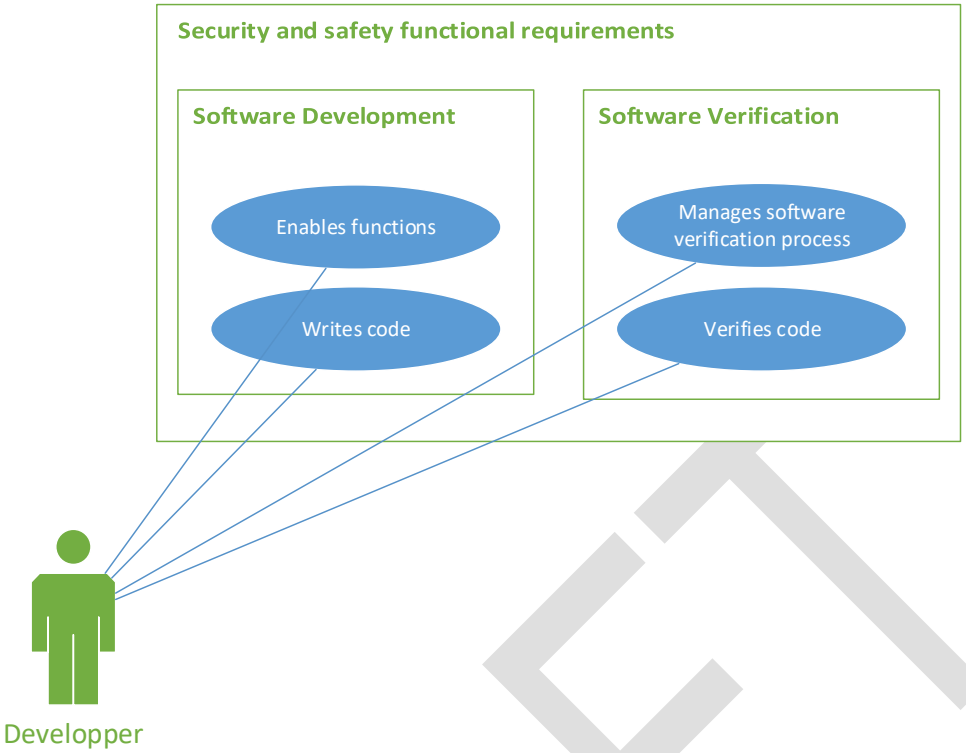

Figure 2: the developer's efforts towards safety and security

For a developer, making the code safe and secure by applying the VESSEDIA methodology implies certain constraints. Indeed, the developer must perform and demonstrate that specified requirements relating to his software / system are fulfilled. Note that the developer may perform and demonstrate itself or delegate to a third party.

An output from VESSEDIA, task 6.4 “Standardization Plan”, introduces a taxonomy of *software safety and security verification tool capabilities*. Then, the “*Verified in Europe*” label, another output of the VESSEDIA project, proposes specifications for *conformity assessment*[8] arrangements.

It may be difficult to justify the efforts for conformity to the VESSEDIA methodology, thus leading to risk of suspicion. VESSEDIA requirements may be “perceived as non-revenue generating activities” (Computer Security Handbook, Volume 1, 5th Edition, by S. Bosworth, M.E. Kabay and E. Whyne, 2009).

Through efforts done in VESSEDIA work package four (WP4 - the verification metrics and tools) and work package six (WP6 –Standardization), it appears important to have a comprehensive vision on the software verification process. Therefore, for cost-benefit analysis in the context of software security and safety verification, the economic rationale should take in consideration:

- The society at large (characterized as “smart society”[9] in the context of IoT)
- Client/sponsor
- Developers
- Evaluators
- Certification bodies
- Accreditation bodies
- Label owner

In the upstream verification value chain, we expect the following relationships:

[8] See in ISO/IEC 17007/2009, Conformity assessment – Guidance for drafting normative documents suitable for conformity assessmenyt

[9] 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

Figure 3: the upstream software verification value chain of applying the VESSEDIA methodology

In the downstream software verification value chain, we expect the following relationships:

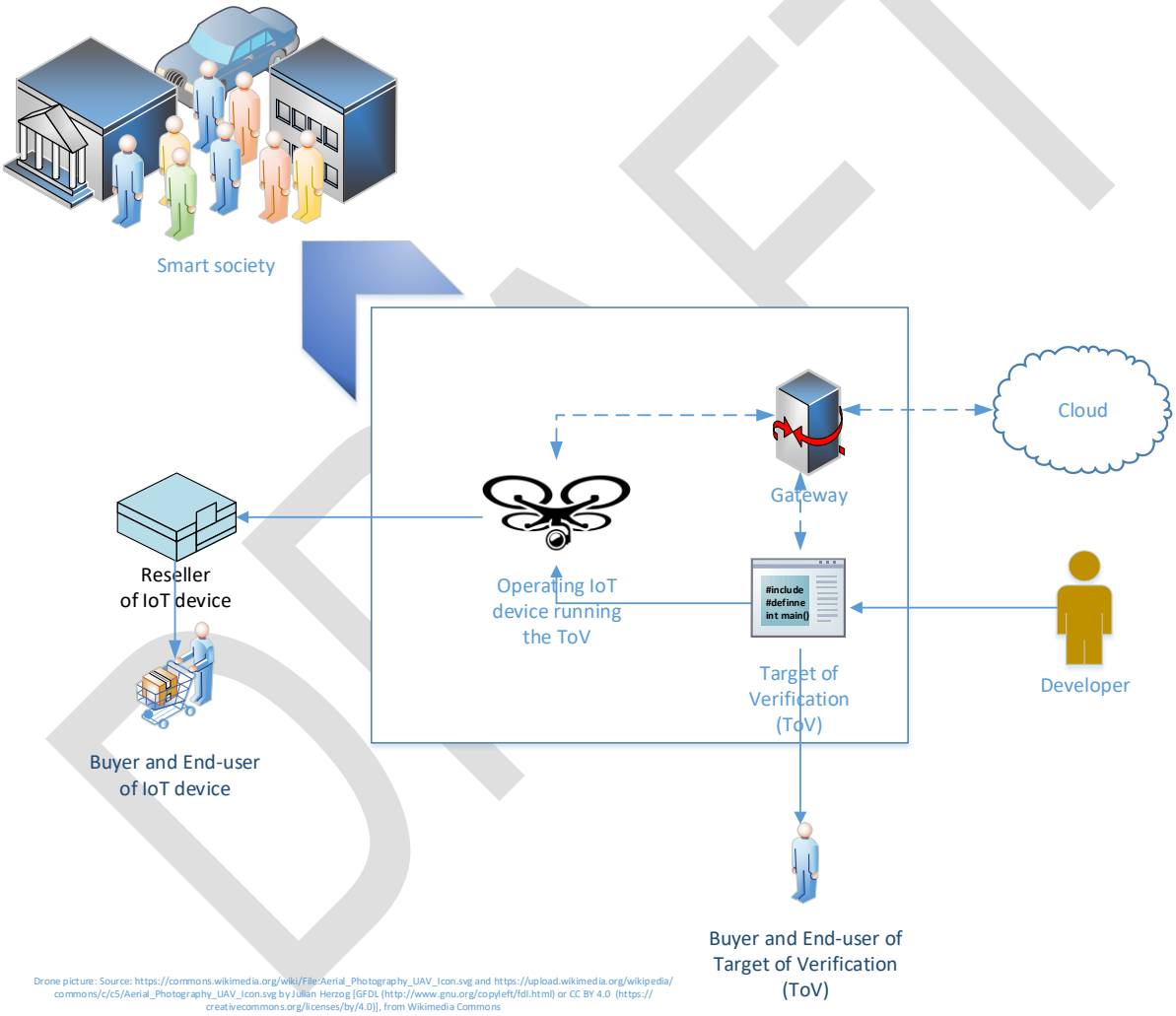

Figure 4: the downstream software verification value chain of applying the VESSEDIA methodology[10]

We want now to analyse the costs and benefits associated with the methodology. The following section applies engineering build-up and analogy methodology for costs estimates (See in Systems Life Cycle Costing – Economic Analysis, Estimation, and Management by J. V. Farr – CRC Press – 2011), as well as gathered information from VESSEDIA use-case owners.

[10] Note: the cloud is indicative as it is not within focus of the VESSEDIA methodology

1.4 Strategic options in software verification and scope/limitations of the economic rationale

A software development company can choose between three different validation and verification strategies. Validation and verification effort can be done as:

- **In-house operated open-source verification tools**: the verification efforts are undertaken by own developers who are using open-source verification tools. There are no license cost but some costs are necessary (e.g. training) for the own developers to be able to operate the verification tools to reach a certain level of verification.
- **In-house operated licensed verification tools**: the verification efforts are undertaken by own developers who are using licensed verification tools. There are license cost and some costs are necessary (e.g. training) for the own developers to be able to operate the verification tools to reach a certain level of verification.
- **Externally operated verification tools**: the verification efforts are undertaken by an external service provider who may be using open-source and/or licensed verification tools. There are no license cost, no training costs but there is a cost for the validation and verification service.

As we have gathered data on the cost of licensed verification tools, we have been able to estimate that licensed tools can offer various levels of analysis, with a relatively volatile licence cost spanning from free-of-charge to 100,000 € and more, depending on the version and capabilities of the tool (e.g., Sonarqube, CodeSonar). There is a lot of uncertainty and volatility when considering the cost of licensed verification software, which may depend on the tool, the options and configuration of the verification tool considered, as well as the training needed, the support and the related maintenance.

The VESSEDIA methodology intends at promoting enhanced verification effort throughout the developing community as a whole, including SME's developing IoT applications. Therefore the present report primarily considers the case of **in-house operated open-source verification tools**, so that we can estimate the affordability of the methodology. The economic rationale shall provide a simple and robust scheme for supporting the developing community in enhancing verification efforts during the software development life cycle. The economic rationale shall demonstrate if enhanced verification efforts can be done in a cost efficient manner.

Chapter 2 Cost breakdown structures (CBS) for actors of the software safety and security verification value chain

VESSEDIA methodology brings a new element in the software verification value chain. Intuitively, the application of VESSEDIA methodology increases the developers' short term fixed costs (e.g. training on the verification tools) and variables costs (e.g. lengthier verification process). For cost analysis, a life-cycle costing (LCC) perspective may be recommended. LCC is typically categorized as through the following stages[11]:

- research, development and design,
- primary production,
- manufacturing,
- use and
- disposal.

Within those stages, it is important to estimate as exhaustively as possible the costs, and especially giving attention to spotting those which may not be easily visible or intuitive, beyond the *acquisition costs*. Estimates need to consider the cost centres related to[12]:

- System operating
- Distribution
- Computer resources
- Maintenance
- Test and support equipment
- Training
- Supply support
- Retirement and disposal
- Technical data

The VESSEDIA methodology imposes constraints under the form of costs that may lead to increase of market price for applications. Such costs represent a burden that would possibly and ideally be shared by the actors of the verification value chain. The costs and benefits horizon differ from one actors of the value chain to another. For example, an evaluator is involved to the extent of the terms of the contract signed with the developer, as well as for possible renewals. This is done within the scope of obligations as stated in the process set jointly by the accreditation and certification bodies (the conformity assessment scheme). As efforts and benefits are to be bear by the actors of the value chain with a different horizon and different CBS, we are estimating the costs and benefits for each actor in the following sections. As short-term profitability is a key motivator for actors of the value chain, and a key success factor for dissemination of the VESSEDIA methodology, we move away from traditional LCC and will not consider costs such as costs for disposal. As the increase of horizon makes the cost model more complex, and less reliable, we will try to consider a one-year horizon for all actors of the value chain. Whenever relevant, we will notify the importance of more

[11] See in Life Cycle Costing and the Environment by G., van Rooijen M., Kleijn R., Heijungs R., de Koning A. and van Oers L. CML (2004) and Life Cycle Costing State of the art report by Helena Estevan and Bettina Schaefer available at http://www.sppregions.eu/fileadmin/user_upload/Life_Cycle_Costing_SoA_Report.pdf

[12] See in Life-Cycle Costing. The Technology Management Handbook by Fabrycky J. and Blanchard BS. Pg 8-63 to 8-70. 8.13. CRC Press (1998)

than one-year horizon costs. We start with the CBS for the label owner (or conformity assessment scheme owner).

2.1 CBS for the label owner

Given the context of development of the VESSEDIA methodology, the steps in estimating the label owner cost would unfold into aggregated costs centres based on the following activities[13]:

- Creation and selection
- Trademark clearance and registration
- Accreditation bodies clearance and registration for 11 countries
- Renewal, watch and database
- Promotion
- Other administrative costs

As for the creation and selection stage[14], we have been developing some sketches of the trademark within the VESSEDIA project in the first year of the project, and we have had an agreed upon visual trademark in second year. As for the requirements and specifications of the label, the grounds have been set through deliverable 6.4 and are still under development through work package 6 and deliverable 4.4.

For the trademark clearance and registration stage[15], it is possible, through WP6 and WP4 efforts, to estimate those costs. The extent of the geographical coverage of the trademark protection can greatly affect this cost.

The accreditation bodies clearance and registration stage is estimated as an office worker[16] working 40% of its time over the first year (0.4*12*3,877=18,609.60 €) in one country. Building on the success met by the ISO combined NP and CD ballot in October 2018 (in relation to D6.4) with the approval from 11 countries, we forecast that the label would be available in 11 countries. The cost of clearance and registration is therefore multiplied by 11 (18,609.60*11=204,705.60€) and in the Benefit Breakdown Structure of the Label Owner, we will observe that royalties can be collected from those countries.

For the renewal, watch and database cost centre, cost estimation is difficult, it implies to make assumptions on:

- The requirements for renewal, which have not been yet formally set through the VESSEDIA project. A strong assumption is that based on the state of *Target of Verification* (ToV) at the time of verification (ToV concept as defined in the VESSEDIA ISO standard draft), the ToV can remained labelled as long as the ToV fulfils the requirements set in the conformity assessment scheme.
- The efforts for watching the market and controlling that there is no counterfeiting or misuse of the label can be estimated taking in consideration that the workload would gradually

[13] See at https://www.slideshare.net/Events4Sure1/trademark-life-cycle-and-outsourcing-49257665 and https://karich.net/wp-content/uploads/2014/02/Trademark-Development-and-Registration.pdf last consulted 23.11.2018

[14] Trademark initial graphic design development estimated 600€. Initial conformity assessment development and labelling scheme development costs are internal to VESSEDIA project (see deliverable 6.4)

[15] See at https://www.wipo.int/madrid/en/fees/calculator.jsp?Lang=E&ForDate=20181119&Origin=FI&Classes=1&ServCd=EN&AU=Y&BX=Y&CN=Y&DZ=Y&EG=Y&EM=Y&IN=Y&JP=Y&PAINAU=263&PAICBX=424&PAICCN=747&PAICEM=1531&PAININ=148&PAINMX=167&PAICNO=278&PAINNZ=102&PAINOA=704&PAINUS=388&TOTAL=5755 for a selection of high GDP countries as for 6,992 Swiss Francs (6,180 €). A full global coverage would cost 25,521 Swiss francs (22,563 €). We take the average between the two as an estimate.

[16] See at https://www.investinfinland.fi/cost-calculator by taking average from “office assistant” (2585 €) and “office manager” (5,169 €) total monthly cost for employer (3,877 €).

increase as the label becomes more spread and popular. This is estimated as an office worker working 20% of its time over the first year (0.2*12*3,877=9,304.80 €)[17].

- The efforts for maintaining the database of labelled ToV can be estimated as an office worker working 40% of its time over the first year (0.4*12*3,877=18,609.60 €).
- Therefore the total for Renewal, watch and database is 9,304.80+18,609.60=27,914.40 €.

In addition, if the label is well accepted by the value chain, there would be an increase of administrative costs, but the economic model of the labelling scheme will act as a guarantee against such a risk. On the other hand, if the label has difficulties to penetrate the label market, there may be promotion and efforts (presentation in conferences and trade fairs). We will add an additional cost for promotion of 2 trade fairs at 44,400 € [18] and 4 conferences for a total cost of 12,000 €[19].

Finally, we add the *other administrative costs* category for taking in consideration hidden costs, and costs not directly related to renewal, watch and database, but occurring for example because of meetings at specific organisations such as ISO.

In the case of the label owner, we consider the occurred costs prior to launch of the label and up to the **first year** of administration of the label, which give the following costs:

Table 1: CBS for label owner (year one)

Value-chain entity	Cost centre	Cost
Label owner	Creation and selection	2,000.00
	Trademark clearance and registration	14,371.00
	Accreditation bodies clearance and registration for 11 countries	204,705.60
	Renewal, watch and database	27,914.40
	Promotion	56,400.00
	Other administrative costs	8,000.00
	TOTAL	**313,391.00**

For the following years, the renewal, watch and database costs are most likely to increase up to a certain level while promotion efforts will decrease (e.g. a reduction to 1 conference and 1 trade fair per year starting from the second year for a total of 25,200 € per year). A yearly budget of about one full time person for *renewal, watch and database* would be sufficient (12*3,877=46,524.00 €), in addition to a yearly 8,000 € for *other administrative costs*. Note that it would be possible to fine-tune

[17] See at https://www.investinfinland.fi/cost-calculator by taking average from "office assistant" (2,585 €) and "office manager" (5,169 €) total monthly cost for employer (3,877 €).
[18] See at http://www.exhibitsusa.com/average-costs-to-display-attend-trade-shows for an estimate of 25,200 Dollars (approximately 22,200 €) and https://www.businessfinland.fi/en/for-finnish-customers/services/funding/startup/trade-fair-grant/ for an indicative range between 10,000 € to 60,000 € of fundable expenses.
[19] See at https://cyberseries.io/nordx/#parallax_1080 for an estimate of 2,000 € fee plus 500 € flight plus 300 € hotel plus 200 € other costs = 3,000 € times 4 conferences.

the CBS through a more detailed analysis using detailed structures from ISO conformity assessment schemes[20,21].

2.2 CBS for accreditation bodies

Accreditation activity relates to the attestation that conformity assessment bodies (*CABs)*, also referred to as *certification bodies* later in the report, can demonstrate their "competence to carry out specific tasks"[22] to the accreditation body.

As the accreditation body designs and organises the accreditation process for CABs, it goes through the "front-office" process of clearance and registration with the label owner. Only then can the accreditation body work "back-office" with the new conformity assessment scheme (CAS) towards CABs. This preparation includes designing and organising the process for accreditation and the process for its renewal.

There are variables costs that will occur for each time a new CAB goes through the process of application for accreditation. For example, an assessment manager from the national accreditation body consults with the applicant for accreditation. In our model we consider that the accreditation body needs to run one and only one accreditation process to a national (generally *public*) certification body. The national certification body then delegates the responsibility to other actors (e.g. other private certification bodies and evaluators) that are substituting in this stage of the software safety and security verification value chain.

Therefore, in order to verify CABs "competence to carry out specific tasks", the accreditation body has two sets of fixed costs centres as through the *recognition of competence* and *recognition of specific tasks*.

There is a cost centre for "Other efforts". That refers to efforts other than related to a CAB's tasks or competences (e.g. related to developing guidance to timescale, policies, procedures and complementary documentation, guidance for substitution of certification) in certification capability for the "Verified in Europe" label, reflecting the VESSEDIA methodology. The "Verified in Europe" label is an extension of scope of certification for certification bodies. This category can be viewed as a provision for costs that may have been neglected or unexpected at the time of the cost/benefit analysis.

[20] See in SO/IEC 17067 Conformity assessment – fundamentals of product certification and guidelines for product certification schemes and in IEC presentation regarding ISO /IEC 17067 at https://www.iecex.com/archive/committee_docs/ExMC_898_Inf_introducing_ISO-IEC_17067.pdf last consulted 27.11.2018

[21] See at https://www.iso.org/sites/cascoregulators/documents/Annex%202%20-%20Conformity%20assessment%20-%20Conformity%20assessment%20schemes.pdf last consulted 26.11.2018

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

This means that there is a cost for accreditation bodies as through the processes of extension of accreditation[23]. Those costs are absorbed as through the accreditation bodies' regular activities[24] and consequently invoiced to certification bodies or other applicants for accreditation.

Table 2: CBS for accreditation bodies

Value-chain entity	Cost centre	Cost
Accreditation bodies	Front-office accreditation body clearance and registration in collaboration with label owner[25]	18,609.60
	Back-office procedure of verification and validation of the VESSEDIA "Verified in Europe" conformity assessment scheme[26] to be used by CAB's	27,914.40
	Recognition of specific tasks (for 1 CAB)	
	Assessment manager from the national accreditation body consults with the applicant for accreditation[27]	15,507.00
	Define the documentation requirements for the application to accreditation[28]	12,405.60
	Define the independence and impartiality requirements for accreditation[29]	6,202.80
	Recognition of competence (for 1 CAB)	
	Define the staff training and competence requirement for accreditation[30]	15,507.00
	Define new locations requirements for accreditation if any	00.00
	Other efforts[31]	15,507.00
	TOTAL	**111,653.40**

2.3 CBS for certification bodies

[23] See at https://www.ukas.com/customer-area/preparing-to-apply-for-an-extension-to-scope/ last consulted 26.11.2018
[24] See at https://www.unido.org/sites/default/files/2017-07/Accreditation_Bodies_final_0.pdf last consulted 26.11.2018
[25] Collaboration with the label owner is estimated as an office worker, working 40% of its time over the first year (0.4*12*3,877= 18,609.60 €).
[26] This is estimated as an office worker working 60% of its time over the first year (0.6*12*3,877=18,609.60 €).
[27] This is estimated as an office manager (5,169 € see at https://www.investinfinland.fi/cost-calculator) working 25% of its time over the first year (0.25*12*5,169=15,507.00 €).
[28] This is estimated as an office manager (5,169 € see at https://www.investinfinland.fi/cost-calculator) working 20% of its time over the first year (0.20*12*5,169=12,405.60 €).
[29] This is estimated as an office manager (5,169 € see at https://www.investinfinland.fi/cost-calculator) working 10% of its time over the first year (0.10*12*5,169=6,202.80 €).
[30] This is estimated as an office manager (5 169 € see at https://www.investinfinland.fi/cost-calculator) working 25% of its time over the first year (0.25*12*5,169=15,507.00 €).
[31] This is estimated as an office manager (5,169 € see at https://www.investinfinland.fi/cost-calculator) working 25% of its time over the first year (0.25*12*5,169=15,507.00 €).

The certification bodies (CABs) in the software development industry, have the competence and can undertake specific tasks to verify that an applicant complies with a given conformity assessment scheme.

For the CABs, the VESSEDIA methodology and its related *software safety and security verification conformity assessment scheme* represent an extension of service. It is a new conformity assessment scheme that develops the certification bodies' certification portfolio. It will generate additional incomes as it spreads among the software development community and throughout the verification value chain.

Costs related to the verification for certification[32,33] are fully invoiced to the applicants for compliance with the conformity assessment scheme.

There are national certification models which are structured so that certification bodies delegate the verification activities to other entities (for example the *evaluators* as referred to in this report).

The requirements[34] set for certification bodies by accreditation bodies imply costs[35,36] presented in the following table. We kept consistency with the rest of the value chain model by replicating the formula:

*Cost estimate=time proportion in percentage*12 months*monthly salary*

rather than using one-off price list of accreditation service[37], and we controlled that estimates are in line.

We kept consistency also with the accreditation body's perspective by using the two categories of requirements (the *recognition of specific tasks* and *recognition of competence*). In addition there is a special cost centre for preparation and training for evaluators towards applicants for certification, which is needed for evaluators, especially in the case of no prior knowledge in verification tools. We create a fixed learning effort of 2 weeks to get familiar with the requirements for compliance towards the *recognition of specific tasks* and *recognition of competence*:

0.5*3 877= 1,938.50€

As from our research in D1.6 on the training required for learning the VESSEDIA methodology, we have found out that a junior developer needs about 324 hours to learn the methodology and practice the tools for the so-called *use of compiler diagnostic* level of analysis (see Table 5). We consider that evaluators are seniors, and we therefore apply an arbitrary reduction of training time of 60%, which brings the training time for senior to 194.40 hours, giving us:

(194.40/(52*38.50))*(12*3,877)= 4,517.62€

Therefore the preparation and training costs for learning the VESSEDIA methodology becomes:

1,938.50€ + 4,517.62€ = 6,456.12€

For certification bodies, we have the following CBS:

---

[32] See ISO/IEC 17067:2013(E) CONFORMITY ASSESSMENT. FUNDAMENTALS OF PRODUCT CERTIFICATION AND
GUIDELINES FOR PRODUCT CERTIFICATION SCHEMES.

[33] See the CBS details and annotations in the developer's section regarding the activities to be invoiced by the performer of the third-party verification and validation

[34] See in IAF Guidance on the Application of ISO/IEC 17024:2003 Conformity assessment - General Requirements for Bodies operating Certification of Persons by International Accreditation Forum, Inc. at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=2ahUKEwi-jJKe5_LeAhXKAxAIHfF-ANQQFjADegQICRAC&url=http%3A%2F%2Fwww.iaf.nu%2FupFiles%2F327597.IAF-GD24-2003_Guidance_on_ISO_17024_new_doc.doc&usg=AOvVaw1LyPdxdwwlfZS3IP6a0d91 last consulted 27.11.2018

[35] See in What are the costs for accreditation service? by UKAS at https://www.ukas.com/services/accreditation-services/apply-for-accreditation/what-are-the-costs-of-accreditation/ last consulted 27.11.2018

[36] See at https://www.sac-accreditation.gov.sg/Resources/sac_documents/Documents/Management_System_And_Products_Certificaton/Related_Documents/PDOC04.pdf

[37] For example see FINAS costs of service per hour at https://www.finas.fi/Tiedostot%201/Julkaisut/finas_hinnasto_englanti.pdf last consulted 08.01.2019

Table 3: CBS for certification bodies

Value-chain entity	Cost centre	Cost
Certification bodies	Applying certification body's manager consults with the assessment manager from the national accreditation body for accreditation[38] within the scope of *recognition of specific tasks*	15,507.00
	Preparation for certification process documentation through efforts for compliance towards the *recognition of specific tasks*[39]	31,014.00
	Preparation for certification process documentation through efforts for compliance towards the *recognition of competence*[40]	15,507.00
	Preparation and training for own evaluators to handle applications for certification	6,456.12
	Service invoiced by accreditation bodies for preparation of the CAS	27,914.40
	TOTAL	**96,398.52**

2.4 CBS for developers

Developers, along with evaluators, are central to the VESSEDIA methodology as they represent a primary target for improved efforts in software safety and security verification along the value chain. In the cost structure, we use a *generic* category of cost centres, a *V-model* based category for software development life-cycle (SDLC - as presented within VESSEDIA deliverable 6.4), as well as a *training* category. The V-model is well spread in the industry[41,42].

Similarly to the smart society, the risk of delay or longer delivery times is difficult to estimate as a cost towards the developers. The delay may result in loss of competitiveness and loss of market share. We decided to not include a best guess for delays caused by enhanced verification approach. Possible costs of delay or longer delivery times are also expected to be balanced by the gains of attractiveness of the software on the market as it is **visibly**, with the help of the Verified in Europe label, more secure and safe as compared to software which would not have undergone enhanced verification efforts.

[38] This is estimated as an office manager (5,169 € see at https://www.investinfinland.fi/cost-calculator) working 25% of its time over the first year (0.25*12*5,169=15,507.00 €).
[39] This is estimated as an office manager (5,169 € see at https://www.investinfinland.fi/cost-calculator) working 25% of its time over the first year (0.50*12*5,169=31,014.00 €).
[40] This is estimated as an office manager (5 169 € see at https://www.investinfinland.fi/cost-calculator) working 25% of its time over the first year (0.25*12*5,169=15,507.00 €).
[41] See http://www.clarotesting.com/page11.htm last consulted on 19.11.2018
[42] See in An Economic Analysis of Software Development Process based on Cost Models by E. Şaykol at International Conference on Eurasian Economies 2012. Available at https://www.researchgate.net/profile/Ediz_Saykol/publication/281270700_An_Economic_Analysis_of_Software_Development_Process_based_on_Cost_Models/links/55ddaf8b08ae79830bb525b1/An-Economic-Analysis-of-Software-Development-Process-based-on-Cost-Models.pdf?origin=publication_detail last consulted on 15.01.2019

For establishing the CBS, we consider a software product example case with a required effort of 240 person day[43] for delivery. Using a V-model based costing structure, we use the categories as can be found in Table 4. The example case has originally a total cost for software development of 106,650 €, of which 54,900 € are allocated to the phases and the remaining to the on-going activities of the V-model. In the on-going activities we consider the *Evaluation and Testing cost*, of 22,500 €. We then allocate the Evaluation and Testing costs (verification) in proportion to the percentage of total cost of the development phases. Note that the distribution of costs may variate depending on the industry and the software considered.

Table 4: case-based costs for software development phases and the verification effort

Software phases of the V-model	Cost of the phase	Percentage of total cost of the phases	Evaluation and Testing cost allocation (Verification)	Total allocated by software phase
Requirements definition, global specifications	8,550.00	15.57	3,504.10	12,054.10
Detailed specifications	8,550.00	15.57	3,504.10	12,054.10
Refinement/design	11,400.00	20.77	4,672.13	16,072.13
Code implementation	10,200.00	18.58	4,180.33	14,380.33
Unit testing, verification and validation through test cases, integration and software integration testing	8,100.00	14.75	3,319.67	11,419.67
System integration, testing and validation	8,100.00	14.75	3,319.67	11,419.67
Total	**54,900.00**	**100.00**	**22,500.00**	**77,400.00**

While doing software safety and security verification, developers want to demonstrate that specified requirements relating to his software / system are fulfilled. Depending on the properties they want to verify, they could also have to express these specifications in a formal language, and this task may require an additional workload.

The extent of verification may be considered from an SDLC perspective and very importantly from a level of analysis. A commonly referred list of levels of security analysis comes from the Common Criteria[44]:

- EAL1: Functionally Tested
- EAL2: Structurally Tested
- EAL3: Methodically Tested and Checked
- EAL4: Methodically Designed, Tested and Reviewed
- EAL5: Semi-formally Designed and Tested

[43] See in in International Journal of Computers, Issue 1, Volume 5, 2011 see at http://www.naun.org/main/NAUN/computers/19-651.pdf last consulted on 26.02.2019

[44] See in ISO/IEC 15408 https://www.iso.org/standard/50341.html

- EAL6: Semi-formally Verified Design and Tested
- EAL7: Formally Verified Design and Tested

In VESSEDIA, we refer to levels of analysis as presented in VESSEDIA D1.5, and indicatively, to the verification levels as found in VESSEDIA D6.4 (See more detail in the following section):

- **Use of compiler diagnostic** (see D1.5) is a basic static analysis relevant in verification for low criticality software (see D6.4)
- **Heuristic static analysis** is a Simple / Advanced static analyses relevant in verification for medium criticality software (see D6.4), and
- **Sound static analysis** is similar to formal static analysis (see D1.5) relevant in verification for high criticality software (see D6.4).

Experts in the VESSEDIA team found it difficult to exactly, explicitly and quantitatively formulate the correlation between costs from using static analysis and the full set of benefits to expect from it. However, there were hints on the degree of effort to invest and hints on the degree of benefits. Therefore, the following costs factors were set through discussions with VESSEDIA experts and are prospective. They should be considered with caution. Further research could aim at verifying the extent and correlation of costs and benefits.

The table of costs and benefits factors are presented in the following table:

Table 5: factors representing the increase in resource spent and benefits yielded, for increasing the level of static analysis

Level of verification analysis	Cost factor (expressing the increase in spent resources from the former level – e.g. in Euros or time)	Cumulated cost factor	Benefit factor (expressing the increase in cost savings and cost avoidance from the former level – e.g. in Euros or time)	Cumulated benefit factor
No analysis	1	1	1	1
Use of compiler diagnostic	1.1 (=10% increase)	1.1	2	2
Heuristic static analysis	1.5	1.65	3	6
Sound static analysis	5	8.2	5	30

Figures on costs obtained by the application of a level of static analysis, i.e. formal methods, were difficult to obtain given that:

- Open-source and collaborative type use-case in VESSEDIA methodology application could not deliver relevant costs figures (no process or resource usage data available),
- Highly critical and confidential type use-case in VESSEDIA methodology application could not deliver costs figures (no process or resource usage data available),
- The same critical and confidential aspects hinder the gathering of cost data on application of formal methods which is typically applied in high criticality software,
- Applying the VESSEDIA methodology in the VESSEDIA use-cases is an on-going problem-solving process. It is hard at M27 of the project to distinguish the “pure” VESSEDIA methodology application process costs from the overall VESSEDIA methodology development costs (which may be possible when the methodology is fully ready applicable).

We can now provide estimates of the costs of the VESSEDIA methodology for the developer. We consider that the VESSEDIA methodology does not affect the *Requirements definition, global specifications* stage of the V-model[45]. Therefore, we apply the costs factors from Table 5 on the costs for development and verification from Table 4.

Table 6: case-based costs for software development phases and the enhanced verification effort

Software phases of the V-model	**Cost of the phase**	**Verification cost allocation** (Evaluation and Testing)			
		No enhanced analysis	**Use of compiler diagnostic** (for low criticality software; cost factor 1.1)	**Heuristic static analysis** (for medium criticality software; cost factor 1.65)	**Sound static analysis** (for high criticality software; cost factor 8.2)
Requirements definition, global specifications	8,550.00	3,504.10	3,854.51	5,781.77	28,733.62
Detailed specifications	8,550.00	3,504.10	3,854.51	5,781.77	28,733.62
Refinement/design	11,400.00	4,672.13	5,139.34	7,709.01	38,311.47
Code implementation	10,200.00	4,180.33	4,598.36	6,897.54	34,278.71
Unit testing, verification and validation through test cases, integration and software integration testing	8,100.00	3,319.67	3,651.64	5,477.46	27,221.29
System integration, testing and validation	8,100.00	3,319.67	3,651.64	5,477.46	27,221.29
Total	**54,900.00**	**22,500.00**	**24,750.00**	**37,125.00**	**184,500.00**

[45] Presented in VESSEDIA Leuven Meeting presentations, 2018 under Tools – big picture by Armand Pucetti

Table 7: case-based cost impact of enhanced verification efforts

	Cost of Verification without enhanced analysis	Cost impact of enhanced verification by level		
		Use of compiler diagnostic (for low criticality software; cost factor 1.1)	Heuristic static analysis (for medium criticality software; cost factor 1.65)	Sound static analysis (for high criticality software; cost factor 8.2)
Amount	**22,500.00**	**2,250.00**	**14,625.00**	**162,000.00**

In addition, based on the research within D1.6 on the training required for learning the VESSEDIA methodology for developers, a junior developer needs about 324 hours to learn the methodology and practice the tools for the *use of compiler diagnostic* level of analysis (see Table 5). We assume that evaluators have senior developer knowledge, therefore we apply an arbitrary reduction of training time of 60%. We also assume that there is an increase of training costs of 25% for developing the competence up to undertaking *heuristic static analysis* as well as another 25% for developing the competence up to undertaking *sound static analysis*. This gives us the following table of training costs:

Table 8: training costs per developer experience and capability in level of analysis

	Use of compiler diagnostic	Heuristic static analysis[46]	Sound static analysis[47]
Junior	7,529.36[48]	9,411.70	11,764.62
Senior[49]	4,517.62[50]	5,647.02	7,058.77

Table 9: training costs for a team of four developers

	Use of compiler diagnostic	Heuristic static analysis	Sound static analysis
Junior	30,117.43	37,646.79	47,058.49
Senior	18,070.46	22,588.08	28,235.09

Using the calculations presented in the tables above as inputs in the CBS gives the following:

[46] Cost increase of 25% as from use of compiler diagnostic
[47] Cost increase of 25% as from heuristic static analysis
[48] (324/(52*38.50)=0.1618 and then 0.1618*(12*3,877)= 7,529.36€
[49] We consider that senior developers have an arbitrary reduction of training time of 60% as compared with juniors
[50] (194.40/(52*38.50))*(12*3,877)= 4,517.62€

Table 10: case-based CBS of enhanced verification efforts for developers[51]

Value-chain entity	Cost centre	Cost
Developers	*Generic*	
	Computer resources[52]	11,200.00
	Licences[53]	0.00
	Cost impact of V-model based[54] enhanced verification[55]	
	TOTAL without training for use of compiler diagnostic analysis	2,250.00
	TOTAL without training for heuristic static analysis	14,625.00
	TOTAL without training for sound static analysis analysis	162,000.00
	Total with training included[56]	
	TOTAL for junior developer (x4) for use of compiler diagnostic analysis	**43,567.43**
	TOTAL for junior developer (x4) for heuristic static analysis	**63,471.79**
	TOTAL for junior developer (x4) for sound static analysis	**220,258.49**
	TOTAL for senior developer (x4) for use of compiler diagnostic analysis	**31,520.46**
	TOTAL for senior developer (x4) for heuristic static analysis	**48,413.08**
	TOTAL for senior developer (x4) for sound static analysis	**201,435.09**

[51] The cost estimates are done on a 200,000.00€ development project
[52] VESSEDIA methodology may impose the developers to purchase complementary hardware, for example Mac OS operated hardware. Here two 5,000.00£ computer (about 11,200.00€ in total)
[53] We consider that the developer installs and uses open-source tools, for example Frama-C, and its plug-in architecture as well as VeriFast, thereby no cost.
[54] All V-model based costs are proportional to the size, quality and the complexity of the code. Based on data gathered among the VESSEDIA project use-cases through questionnaire, the VESSEDIA methodology is most likely to reduce development speed (Development speed = software size/duration) and increase duration/development time, even though this depend on the use of the tools for verification. Efforts in the verification process include for example additional manual debugging, and the use of debugging tools such as Valgrind see at http://www.valgrind.org/info/about.html (which can present high variability in slowdown factor, see in Valgrind: A Framework for Heavyweight Dynamic Binary Instrumentation by Nicholas Nethercote and Julian Seward see at http://valgrind.org/docs/valgrind2007.pdf last consulted on 27.11.2018).
[55] We use effort distribution on activities figures as in Effort and Cost Allocation in Medium to Large Software Development Projects by Kassem Saleh, in International Journal of Computers, Issue 1, Volume 5, 2011 see at http://www.naun.org/main/NAUN/computers/19-651.pdf (we take in consideration the "software phases" cost allocation only for proportion) and at https://it.toolbox.com/blogs/craigborysowich/project-management-lite-distribution-of-effort-by-phase-sdlc-031612 last consulted on 15.01.2019
[56] We add the figures from the above table of *training costs for a team of four developers*. We note that verification tools require efforts in training the users, and the learning curve effect provides with advantages on the medium/long term. We distinguish two types of learners where the junior developer needs more efforts for learning the methodology.

In addition to the costs above, and based on the simulated case presented in the evaluator benefit breakdown structure section, the developer is most likely to bear the cost of validation for certification and/or verification.

2.5 CBS for evaluators and other verification service providers

Evaluators and other verification service providers (for example security firms) provide validation and verification service to developing companies. Along with developers, evaluators and other verification service providers are central to the VESSEDIA methodology as they represent a primary target for improved efforts in software safety and security verification along the value chain.

For the remaining of the report, we use the word evaluators while still encompassing external verification service providers. The costs related to the verification efforts are fully invoiced with a margin of profit to the customer, therefore we discard the costs of running a verification from the CBS. The VESSEDIA methodology proposes that whether done by itself or whether externalised to an evaluator, the beneficiary of enhanced verification efforts can apply for certification[57] through the conformity assessment scheme that awards the Verified in Europe label.

Similarly to the certification body, we create a fixed learning effort of 2 weeks for a team of 4 software developers to get familiar with the requirements for compliance towards the *recognition of specific tasks* and *recognition of competence*:

0.5*3,877*4= 7,754.00€

[57] See the CBS details and annotations in the developer's section regarding the activities to be invoiced as a verification and validation service provider

Table 11: CBS for evaluators and other providers of verification services

Value-chain entity	Cost centre	Cost
Evaluators	*Generic*	
	Computer resources[58]	11,200.00
	Licences[59]	0.00
	Yearly fee invoiced by certification body	20,000.00
	Training for certification process	
	Training on requirements for compliance towards the *recognition of specific tasks* and *recognition of competence*	7,754.00
	Training on enhanced verification tools	
	Training costs for evaluator[60] (x4) for compiler diagnostic analysis	**18,070.46**
	Training costs for evaluator (x4) for heuristic static analysis	**22,588.08**
	Training costs for evaluator (x4) for sound static analysis	**28,235.09**
	TOTAL costs for evaluator (x4) for compiler diagnostic analysis verification and certification capability	**57,024.46**
	TOTAL costs for evaluator (x4) for heuristic static analysis verification and certification capability	**61,542.08**
	TOTAL costs for evaluator (x4) for sound static analysis verification and certification capability	**67,189.09**

2.6 CBS for the client/sponsor

The client/sponsor can also be referred to as the *consumer* or end-*user*[61] in the business-to-consumer (B2C) or business-to-business (B2B) market. Following VESSEDIA methodology, the enhanced efforts in software safety and security verification are visible on the B2B and B2C markets as through the label Verified in Europe carried by ToV. In practice, and from an end-user perspective, the ToV is a software or module of a software that is installed on:

- an IoT device sold to the end-user by the final IoT device re-seller/retailer or,
- an IoT device sold between B2B intermediaries in the chain.

[58] VESSEDIA methodology may impose the evaluator to purchase complementary hardware, for example Mac OS operated hardware, as seen in the CBS for developers
[59] We consider that the evaluator installs and uses open-source tools, for example Frama-C, and its plug-in architecture as well as VeriFast, thereby no cost.
[60] We consider that evaluator are specialists in the field of security evaluation, so that they are considered as senior in terms of learning capability
[61] See in Official Journal of the European Union Volume 59 26 July 2016 C272 The 'Blue Guide' on the implementation of EU products rules

All intermediaries in the chain will pass a price rise caused by enhanced software verification, if any, on to the next, in a similar fashion as *carbon pricing* – the umbrella term for taxes and levies based on emissions – in the transportation industry. The demand will be inelastic to price increase as long as consumers perceive the added value of efforts done during development towards increasing software security and safety.

We distinguish two cost centres, linked with application of the VESSEDIA methodology in the software verification value chain for the client/sponsor: an increase of purchase price due to enhanced verification efforts and an increase of purchase price due to the efforts in complying with the conformity assessment scheme *Verified in Europe*.

In VESSEDIA, we can refer to levels of analysis as presented in VESSEDIA deliverables D1.5, D6.4 and also as detailed in the above section dedicated to the developers' CBS.

The market price of the IoT device that contains the ToV bears the passed on costs that occur in the upstream value chain. The new market price would also reflect the "premium" price due to the value of a system containing a ToV that has undergone enhanced verification efforts, and that is possibly labelled with "Verify in Europe". However, it is important to keep in mind that market perception on the value of a label is complex and can lead to confounding situations[62].

For the CBS, we run the cost estimate through the simulated case. In practice, such case could be an end-user that purchases a software to be installed on a drone (e.g. recreational or for farming, a fast growing market for IoT applications[63]). There are multiple usage scenarios for end-users to buy pre-installed or off-the-shelf drone software. A farmer may buy a one-off software worth 154.80€[64], up to purchasing monthly full package software based services worth between 1,000.00€ and 3,000.00€ or more in the case of customized solutions[65].

In order to estimate the price increase due to enhanced verification efforts, we refer to the case software as described in the developer CBS, therefore making **assumption** of:

- A total development cost for the software without enhanced verification effort of 106,650.00€
- An original target market selling price of 1,000.00€
- Original target sales in volume of 200 units on the first year, with the costs of applying the VESSEDIA methodology to be totally amortized on the first year of sales
- A price increase on a device containing a ToV that has undergone enhanced efforts in verification and /or certification as can be found in the evaluators' BBS (section 3.4) with an effectuated evaluation for certification under medium criticality software analysis by the evaluator.

[62] See in Eco-Labeling Strategies and Price-Premium: The Wine Industry Puzzle by M.A. Delmas and L.E. Grant in Business & Society 2014, Vol 53(1) 6–44. SAGE Publications. Can be found at https://cloudfront.escholarship.org/dist/prd/content/qt0w96p15x/qt0w96p15x.pdf last consulted 15.01.2018
[63] See at https://www.n-ix.com/how-to-reap-benefits-agriculture-drone-software/ last consulted 04.03.2019
[64] See at https://shop.prodrones.fr/pix4d/157-75-pix4d.html last consulted 15.01.2019
[65] See at https://prismic-io.s3.amazonaws.com/dronedeploy-www%2F0fac4d0d-769c-4faa-8e45-7a3c96b50f78_dronedeploy_pricing-11_2018.pdf last consulted 15.01.2019

The costs with enhanced verification are presented in the table below:

Table 12: case-based impact on software cost for the client/sponsor

	TOTAL cost impact for the customer base in case of in-house verification by the developer team (x4) per developer expertise and per level of analysis[66]	Cost impact on a single customer with in-house verification	Cost impact passed on to the customer base for certification service by evaluator[67]	Cost impact passed on to a single customer for certification service by evaluator	Cost impact on software selling price from verification and certification effort
Junior - compiler diagnostic analysis	**43,567.43**	217.84	5,430.90	27.15	**244.99**
Junior - heuristic static analysis	**63,471.79**	317.36	3,468.39	17.34	**334.70**
Junior - sound static analysis	**220,258.49**	1,101.29	6,076.94	30.38	**1,131.68**
Senior - compiler diagnostic analysis	**31,520.46**	157.60	5,430.90	27.15	**184.76**
Senior - heuristic static analysis	**48,413.08**	242.07	3,468.39	17.34	**259.41**
Senior - sound static analysis	**201,435.09**	1,007.18	6,076.94	30.38	**1,037.56**

The above costs are best guess estimates with calculations that are made with the help of assumptions and the case-based simulations. The impact on the client/sponsor is affected by multiple variables:

[66] See section on developers' CBS
[67] Given the assumption done on the size of the customer base.

- The conditions in which the purchased or already installed ToV on an IoT device has undergone enhanced efforts in verification (self-made verification by developer or subcontracted to evaluators, and level of expertise of the verification team),
- If the verification is certified under a set conformity assessment scheme or not,
- The level of analysis effectuated,
- The complexity of the code to undergo verification is also a non-negligible variable, but there are difficulties to find agreement on the correct metric to measure code complexity as a factor of cost per level of static analysis (e.g. function point, Lines-of-code, Halstead's metrics, McCabe cyclomatic number, and Maintainability Index)
- The costs to be expected for the client/sponsor are difficult to assess in the generic case as the amortisements of fixed costs invested by the developer will depend on the size of the market.

2.7 CBS for the society at large (characterized as "smart society"[68] in the context of IoT)

For the smart society, there is a risk that the implementation of the VESSEDIA methodology means longer delivery times for making applications and software available to the market as it imposes more efforts at the software verification stage. Consequently, IoT devices which contain those applications may also be delivered with longer lead times. Despite a cost model that is sustained by actors of the software verification value chain upstream, VESSEDIA methodology represents a risk for delay in the value chain and thereby the availability of secure and safe IoT product.

The risk of delay or longer delivery times is difficult to estimate as a cost towards the smart society as well as for the developers. We decided to not include a best guess for delays or longer delivery times caused by enhanced verification approach, especially if the delay is due to fixing a vulnerability that would otherwise not have been spotted and that is essential for ensuring product liability.

There is no clearly identifiable and measurable cost of delay or longer delivery times associated with implementing the VESSEDIA methodology towards the smart society.

[68] 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

Chapter 3 Benefits breakdown structures (BBS)

We want to consider the impacts of the VESSEDIA methodology, in terms of benefits, for each actor of the software verification value chain (see Figure 3 and Figure 4). Verification activities are executed by the developer and/or by the certification body/evaluator. VESSEDIA related conformance assessment scheme guarantee the level of effort and quality of the tools applied to verifying security and safety of the ToV. Given the value chain perspective, we want to find out how benefits may spread out throughout the value chain, and not only be restricted to the owner or user of the ToV.

We are using a benefit breakdown structure (BBS) to present categories and estimates of benefits for the actors of the value chain.

3.1 BBS for the label owner

The label owner is meant to sustain the new conformance assessment model. The label owner needs to cover costs implied as detailed in the label owner's CBS, i.e. for year one: 129,295.00€ (see in 2.1). The ideal model for the label owner is to collect a fixed royalty based on each ToV application that is handled by a certification body/evaluator. The amount of the royalty shall support the administration of the conformity assessment scheme.

There has already been 11 countries which have approved the ISO combined NP and CD ballot in October 2018 (in relation to D6.4). We expect the number of interested countries to grow by the time the ISO standard is further developed. Therefore we are confident in the support from accreditation and other national bodies interested in standards related to verification tools.

We assume that there will be about 150 applications for certification in each of the 11 countries considered above. The timeline for receiving the royalties is uncertain and there may be a lag between setting the conformity assessment scheme throughout the verification value chain and collecting the royalties. The royalty to be collected by the label owner is of 190.00 €. We will consider that the cost is supported by the evaluator even if the label may yield premium price increase in the downstream value chain, and the evaluators are most likely to pass the cost on to their customers. As we can see in the evaluator BBS, the amount of the royalty (190.00€) is negligible given the considered margin for profit at the evaluators level in the value chain. The total amount of royalties collected is equal to (11*150*190.00=313,500.00€)

Table 13: BBS for the label owner

Value-chain entity	Benefit centre	Income generated
Label owner	Royalties	313,500.00
	TOTAL	313,500.00

3.2 BBS for accreditation bodies

Accreditation bodies need, at least, to cover costs implied as detailed in the accreditation bodies' CBS (see in 2.2). Accreditation bodies generally operate following the self-financing principle[69]. Accreditation bodies are very interested in the benefits brought to the actors of the software safety and security verification value chain.

Table 14: BBS for the accreditation bodies

Value-chain entity	Benefit centre	Income generated
Accreditation bodies	Invoicing to Label Owners[70]	18,609.60
	Preparatory work re-invoicing to CABs (Certification And verification Bodies)[71]	65,129.40
	Service invoicing to CABs for the preparation of the CAS[72]	27,914.40
	TOTAL	**111,653.40**

3.3 BBS for certification bodies

In some countries, certification bodies need, at least, to cover costs implied as detailed in the certification bodies' CBS (see in 2.3), close to the economic model of an accreditation body. If it is not the case, the certification body's economic model is closer to the one of an evaluator. We consider certification bodies as public institutions working with the objective of providing responses to cybersecurity issues. With the implementation of the VESSEDIA methodology, the objective is fulfilled through improving practices in software safety and security verification. The certification body will collect a yearly fee from evaluator and other verification services providers of an amount of 10,000.00 €.

Table 15: BBS for a certification body

Value-chain entity	Benefit centre	Income generated
Certification body	Fees collected in the country of competence of the certification body[73]	100,000.00
	TOTAL income	**100,000.00**

[69] See in https://www.finas.fi/Tiedostot%201/Julkaisut/finas_hinnasto_englanti.pdf last consulted 08.01.2019
[70] See in Label Owner CBS in section 2.1 and for control see price list at https://www.finas.fi/Tiedostot%201/Julkaisut/finas_hinnasto_englanti.pdf
[71] In reference to re-invoicing costs from the CBS of the accreditation body in section 2.2 where the assessment manager from the national accreditation body consults with the applicant for accreditation, and consequently invoices the applicant.
[72] In reference to the CBS of the Certification body in section 2.3
[73] The number of licensed laboratories in a country variates from one country to another as from https://european-accreditation.org/promotionals/document-ict-certification-laboratories/ last consulted 13.03.2019. We may consider that for a given country there is an average number of laboratories or evaluators of 5. That may be considered as a pessimistic figure, given that in some countries, "minor" schemes more comparable to the Verified in Europe, for example French CSPN are offered by more laboratories (10) than "larger" schemes such as the Common Criteria (6 laboratories). With a fee of 20,000.00 € per applying evaluator for being able to certify on the Verified in Europe conformity assessment scheme, it gives 5*20,000.00= 100,000.00 € of incomes for the certification body.

3.4 BBS for developers

Some of the benefits to be expected using the VESSEDIA methodology are the avoided costs related to the reduction of security vulnerabilities and safety issues. The enhanced verification process allows to find and to fix bugs that would otherwise not have been found. A concrete example of unsatisfying verification effort is the Intel Pentium chip bug with a total cost of 475 million dollars[74] (for a yearly turnover of 16 202 million dollars, i.e. a 3% loss). In terms of costs savings, and to consider smaller scale actors of the value chain and low criticality software, it is important for us to consider how the VESSEDIA methodology applies. Common usage IoT devices are very likely to be under attack, including "software attacks"[75]. It is difficult to give customized figures for a company with regards to cost savings due to avoidance of loss of turnover due to cyberattacks. However, some figures show that the problem is very relevant, as with turnover losses in Asia, Europe and US of respectively 81, 62 and 61 Million dollars[76].

With regards to increase of incomes, by reinforcing consumer trust in IoT operated devices through the *Verified in Europe* label, one can expect higher growth on the IoT software market. One could also expect a price premium for labelled software. However, to maintain pessimistic assumptions for the economic rationale, we will consider that there is no such premium.

Other benefits relate to the improvements in terms of accessibility and efficiency in the formal methods applied for software verification. Those methods are constantly improved, which allow to increase the quality of verification without increase of costs. The cost savings are generated by the spotting of vulnerabilities which would otherwise be not possible or at a greater cost, as discussed in D3.3 in relation to CURSOR methodology (p13) and in the article *Verification Coverage for Combining Test and Proof* in Annex 1).

It is important to notice that there are no fixed training costs on the next software development, once the methodology and knowledge in doing enhanced verification is assimilated. Training costs could be amortized on an estimate of number of projects as the developer is likely to work on for the time spent in the company. The advantage is of course lost in case of high staff turnover in the developing team.

We can apply an analogy to IoT by looking at figures in product liability problems, and figures in the toy industry. Our assumption is that it is possible to use enhanced verification for decreasing vulnerabilities thereby decreasing risks of malfunction and therefore injuries. For a developing company the cost of a problem related to product liability (due to a vulnerability in the software) can be estimated as close to 60,673.00 €[77]. Product liability is a growing concern for software developers and IoT device manufacturers[78]

Additionally, in reference to Table 1Table 5, we have an informal appreciation on the benefits of using enhanced verification. The benefit factors presented in the following Table 16 were set through discussions with VESSEDIA experts and are prospective. The benefit factors were also discussed

[74] See https://money.cnn.com/1997/05/06/technology/intel_bug_pkg/ last consulted on 04.01.2019

[75] Bako A. and Ali I. A. *Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes*. Sensors 2018, 18, 817; doi:10.3390/s18030817 www.mdpi.com/journal/sensors

[76] See in Cybersécurité - Protégez vos produits et les données associées at http://www.lcie.fr/medias/cadre_reglementaire_sur_la_protection_des_donnees.pdf (CAP'TRONIC, Bureau Veritas ; 2018) last consulted on 04.03.2019

[77] See figure on midpoint plaintiff award in personal injury cases at https://www.iii.org/fact-statistic/facts-statistics-product-liability last consulted on 11.03.2019. Other estimate is the actualized 47,500$ (as found in in *Software Product Liability* by J.Armour and W.S. Humphrey, 1993 available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a272570.pdf) which give 72,883.26€

[78] See in https://i.blackhat.com/us-18/Thu-August-9/us-18-Palansky-Legal-Liability-For-IoT-Vulnerabilities.pdf last consulted on 13.03.2019 and in Crashed Software: Assessing Product Liability for Software Defects in Automated Vehicles by Sunghyo Kim in Duke Law & Technology Review (2018) available at https://scholarship.law.duke.edu/do/search/?q=author_lname%3A%22Kim%22%20author_fname%3A%22Sunghyo%22&start=0&context=1022222&facet= last consulted on 11.03.2019

with verification tools experts[79]. Further research could aim at verifying the extent and correlation of costs and benefits to levels of verification analysis.

For the cost saving percentage, we express the cumulated benefit factor as a cost saving percentage in proportion of the 100% of avoidance of liability costs with a sound static analysis level. We assume that:

- the requirements provided for the ToV have been correctly translated to formal statements and,
- that all kinds of flaw have been considered for verification, and as well
- with pending risks related to third party software vulnerabilities (for example if we rely on a technology which may have a flaw).

The cost saving percentage on forecasted product liability costs becomes:

Table 16: expressing the cost saving percentage on forecasted product liability costs

Level of verification analysis	Benefit factor (expressing the increase in cost savings and cost avoidance from the former level – e.g. in Euros or time)	Cumulated benefit factor	Cost saving percentage
No analysis	1	1	**0.00**
Use of compiler diagnostic	2	2	**6.67**
Heuristic static analysis	3	6	**20.00**
Sound static analysis	5	30	**100.00**

We need an estimate as to the possible number of liability cases to occur for a given software. This is most likely to depend on multiple factors, and very strongly related to quality aspects (such as code complexity). In our case-based simulation, we have a software that is sold to 200 customers. The cost savings depend on the probability of presence of flaws, the probability of exploitable vulnerabilities and the realization of risks through probabilities of attacks. This is difficult to estimate. The cost savings will range from 0 (no occurrence of damage or with no liability of the developer) up to an amount close to average product liability case costs (60,673.00€), or even more, increasing with the criticality of the software and multiplied by the number of liability cases. Other case based cost estimates such as the 3% net revenue loss in the example of the Intel bug, or other cost in value mostly publicized by large companies[80] and for high criticality software[81] are difficult to use as analogies for low and medium criticality situations.

For the estimates, we make the following assumptions:

- There is one forecasted case of product liability problem declared among the customer base
- The 60,673.00 € product liability cost is relevant for low criticality software.
- A medium criticality software brings product liability cost up to 10*60 673.00 = 606 730.00 €

[79] In the context of dissemination event at Software Quality Days 2019 https://www.software-quality-days.com/en/ last consulted 14.03.2019

[80] See https://crossbrowsertesting.com/blog/development/software-bug-cost/ last consulted 13.03.2019)

[81] See Zhivich, Michael, and Robert K. Cunningham. "*The Real Cost of Software Errors*." IEEE Security & Privacy Magazine 7.2 (2009): 87–90. © 2012 IEEE

- A high criticality software brings product liability cost up to 100*60 673.00 = 6 067 300.00 €

Making those assumptions weakens the economic rationale model but is a best guess that we can use for making a simulation and projection of benefits for the developer. The BBS for developers relates to costs savings made on product liability costs. We apply the cost saving percentage on the forecasted product liability costs in the following table:

Table 17: potential cost savings based on level of analysis and per software criticality level

Level of verification analysis	Potential cost saving impact per software criticality level		
	Low criticality	Medium criticality	High criticality
Use of compiler diagnostic	4,044.87	40,448.67	404,486.67
Heuristic static analysis	12,134.60	121,346.00	1,213,460.00
Sound static analysis	60,673.00	606,730.00	6,067,300.00

If we relate the forecasted cost savings to the costs for the team of 4 developers in the case-based simulation from the CBS section of the report, we obtain:

Table 18: potential net value at given expertise level of the developing team

Level of verification analysis	Potential net value per software criticality					
	Low criticality		Medium criticality		High criticality	
	Junior	Senior	Junior	Senior	Junior	Senior
Use of compiler diagnostic	-39,522.57	-27,475.59	-3,118.77	8,928.21	360,919.23	372,966.21
Heuristic static analysis	-51,337.19	-36,278.48	57,874.21	72,932.92	1,149,988.21	1 165 046.92
Sound static analysis	-159,585.49	-140,762.09	386,471.51	405,294.91	5,847,041.51	5 865,864.91

When training is taken as a fixed cost on year one, like it is in our current model, the breakeven is reached at the point of using heuristic static analysis on medium criticality software. There is a potential loss to expect in any case where a lower criticality software undergoes static analysis. However, if static analysis is applied for low criticality software the breakeven is very close or even reached in some cases if the training costs of developers is considered as an amortized investment (for example on 10 years).

While the logic of investing in higher levels of static analysis for high criticality application is common practice, this shows that a breakeven point is reachable at a lower criticality level for medium level of static analysis. This is encouraging for broadening the use of static analysis among the developing community.

3.5 BBS for evaluators and other verification service providers

Evaluators invoice *validation* and/or *verification* effort for a given applicant's Target of Verification (ToV). In the case of the validation of the *applicant's self-verification* and its associated *certification* service, the evaluator does not verify (i.e. it does not apply the tools itself), but validates the proofs and documentation provided by the applicant for certification. It is a service of validation of enhanced efforts and its associated certification service. However, in the case of *verification and certification*, the tools are actually used by the evaluator on the ToV, thereby higher costs are of course invoiced to the applicant with a margin of profit.

We analyse the costs and incomes generated for the evaluator based on a simulated first year of activity with customer service estimates of 30, 10 and 2 customer contracts for the respective levels of low, medium and high analysis[82]. The costs correspond to the figures found in the evaluator CBS, with costs under assumptions made for evaluators (e.g. for a team of 4 evaluators).

[82] Those sales projection estimates have been discussed with companies providing service in the field of security evaluation. The fixed costs invested are then spread only to the level of analysis to which it is relevant.

Table 19: costs per service for certification and/or verification amortized to yearly service estimate

Degree of capability in criticality software analysis	**Total fixed costs to invoice on year one for the certification service only** (under assumptions made for evaluators)	**Yearly service estimate** (in number of contracts for evaluation)	**Costs to invoice per certification service** (including when it is only validation of self-made verification by developer)	**Cost of enhanced verification**[83] **to invoice per verification service**	**Costs to invoice per service in case of both verification and certification service**
Low	57,024.46	30	**1,357.73**[84]	2,250.00	**3,607.73**
Medium	61,542.08	10	**1,734.19**[85]	14,625.00	**16,359.19**
High	67,189.09	2	**4,557.70**[86]	162,000.00	**166,557.70**

Depending on customer sensitiveness to price, amortization of high criticality software analysis capability fixed costs may be challenging if set to a one-year payback.

If we assume that on the first year, the number of enhanced verification and certification service represents 80% of the customer contracts[87] (thereby 20% of contracts deal with certification only – with enhanced verification done by the developers themselves).

The profit margin on service offered has to be adjusted to the type of service, given the increasing amount invoiced as the analysis level increases. The margin itself is meant to cover for costs of validation for certification.

We assume that the profit margin per level of analysis is:

- Low: 75% profit margin
- Medium: 50% profit margin
- High: 25% profit margin

[83] As taken from the estimates done in the report for the developer
[84] 57,024.46 / 42 = 1,357.73 €
[85] 1,357.73 + (61,542.08-57,024.46)/12 = 1,734.19€
[86] 1,734.19+ (67,189.09-61,542.08)/2= 4,557.70€
[87] Rounded to lowest in the calculations

Table 20: invoicing by evaluators on verification and certification services

Degree of criticality software analysis	Number of contracts for certification service (20%)	Costs to invoice per certification service	Invoiced amount with profit margin per certification service only	Number of contracts for verification and certification service (80%)	Costs to invoice per verification and certification service	Invoiced amount with profit margin per verification and certification service
Low	6	1,357.73	**5,430.90**	24	3,607.73	**14,430.90**
Medium	2	1,734.19	**3,468.39**	8	16,359.19	**32,718.39**
High	1	4,557.70	**6,076.94**	1	166,557.70	**222,076.94**

Table 21: total invoiced by evaluators

Degree of criticality software analysis	Total Invoiced for certification service only	Total Invoiced for verification and certification service
Low	32,585.41	346,341.62
Medium	6,936.77	261,747.09
High	6,076.94	222,076.94
TOTAL	**45,599.12**	**830,165.65**

In our case-based simulation, given the assumed customer service estimates for the different levels analysis, the evaluator makes a total income of **875,764.77 €.**

3.6 BBS for client/sponsor

For the client/sponsor, at the end of the downstream value chain, we want to find out the benefits and whether they outreach costs as detailed in its CBS (see in 2.6). However, it may be difficult to measure the cost savings through avoidance of technical flaws[88] or avoidance of cloud infrastructure vulnerabilities[89,90] that may be found in IoT devices.

With regards to enhanced software safety and security, we may use two trivial examples: a smart TV and a flying drone. We consider vulnerabilities on IoT devices[91], for example an attack that may target a smart TV[92]. A possible outcome may be that volume could be set at its highest. In that case,

[88] See https://www.bbc.com/news/technology-46032019 last consulted on 27.11.2018
[89] See https://dronelife.com/2017/11/16/dji-flawed-bug-bounty-program/ last consulted on 27.11.2018
[90] See https://www.wired.com/story/dji-drones-bugs-exposed-users-data/ last consulted on 27.11.2018
[91] See http://www.ece.cmu.edu/~koopman/ladc2007.pdf last consulted on 15.01.2019
[92] See in Bako A. and Ali I. A. *Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes*. Sensors 2018, 18, 817; doi:10.3390/s18030817 www.mdpi.com/journal/sensors

when users, for example children, operate the device, they may suffer ear damage. In that case, security vulnerability would lead to safety issues[93]. The drone software is more critical in the sense that if operated outdoor, with people in its surroundings, in case of loss of control due to software vulnerability, there may be injuries to human beings. In general, any vulnerable smart/IoT device may lead to dangers or disturbance in a cause-to-effect manner.

Benefits to consider are:

- Avoidance of damages due to incidents with the IoT device (e.g. farming drone collisions)
  - Related repair costs
  - Related temporary replacement solution costs
  - Related idleness costs
- Reduction of insurance cost[94]

The benefits to be expected by the client/sponsor are however difficult to measure financially. We can however apply an analogy to the IoT devices market by looking at figures in the toy industry. For example in 2016, 240,000 injuries and 7 deaths associated with toys have been reported in the USA, although not mentioned if it was related to the manufacturer's responsibility only. The consequences from IoT devices incidents and the exploitable vulnerabilities can be lethal. Making IoT software more secure and safer is likely to decrease incidents and accidents as well as increasing consumers' confidence.

While the loss related to product liability can be estimated as close to 60,673.00 €[95] it is difficult to estimate its probability. It is also difficult to estimate the benefit to the client/sponsor from a risk avoidance perspective. Quantifying financially risk avoidance for the client/sponsor implies assumptions on its awareness and aversion to risk. Moreover, the type of IoT device and the environment in which it is operated may also affect risk aversion. Multiple factors should be considered for evaluating perceived benefits of risk avoidance for the client/sponsor. A strength of the *Verified in Europe* label is to create awareness about safety and security risk while also providing a reassuring message:

> "*this software/device has undergone enhanced verification,*
> *so it is most likely less vulnerable than a non-labelled one*".

We will therefore not make assumptions which would be very volatile from one device and one client/sponsor to another. We will hold the product liability average as a representative cost. This cost would otherwise be paid to the client/sponsor as a compensation to damage done because of negligence in making IoT software robust to vulnerabilities, due to an insufficient verification effort from the developer.

3.7 BBS for the society at large (characterized as "smart society"[96] in the context of IoT)

The smart society, beyond the costs as detailed in its CBS (see in 2.7), is interested in the benefits brought to the actors of the software safety and security verification value chain and to the society at large. It may be difficult to estimate in Euros the qualitative benefits as well as the avoided costs (e.g. consequences to the society from damages to client/sponsors[97]).

[93] See at https://users.ece.cmu.edu/~koopman/ladc2007.pdf last consulted on 15.01.2019
[94] See insurance coverage costs at https://uavcoach.com/drone-insurance-guide/#CoverageTypes last consulted on 11.03.2019
[95] See figure on midpoint plaintiff award in personal injury cases at https://www.iii.org/fact-statistic/facts-statistics-product-liability last consulted on 11.03.2019
[96] 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
[97] See shoppers loss at https://www.kaspersky.com/about/press-releases/2018_the-nightmare-before-christmas-a-third-of-shoppers-have-had-their-financial-credentials-compromised. Last consulted on 06.01.19

Among qualitative benefits, VESSEDIA methodology offers traceability[98] through the available documentation on effectuated verification efforts on the Target of Verification. In addition, IoT devices operating with less vulnerable software are most likely to reduce incidents, accidents and related breakdowns, as well as medical treatments and insurance expenses. This results in increased safety and security in the smart society. This is especially true as the latest estimates suggest that the number of globally operating IoT devices by 2020 will rise to more than 30 billion[99].

[98] See in Official Journal of the European Union Volume 59 26 July 2016 C272 The 'Blue Guide' on the implementation of EU products rules 2016

[99] See https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ last consulted 27.03.2019

Chapter 4 Summary and Conclusion

We have considered the building blocks of the VESSEDIA methodology, namely:

- A software verification toolset that is accessible and supported with guidance and tools,
- A list of software safety and security verification tool capabilities that sets a new standard for referral (VESSEDIA deliverable 6.4),
- A proposal for developers and evaluators to increase the use of formal methods for verification (with the evidence of VESSEDIA use-cases),
- A notion of Target of Verification, that includes the already well-established notion of Target of Evaluation (Common Criteria)
- A conformity assessment scheme that supports the application of formal methods for verification (the Verified in Europe label).

The report provides a cost/benefits analysis of the application of the VESSEDIA methodology through its building blocks. This cost/benefits analysis is done on the value chain for year one with given assumptions throughout the verification value chain. A similar analysis can be made with any other assumptions representing different software development settings.

Recent development of the conformity assessment scheme indicate that the expected fixed costs expect after year 1 should be minimal, and that benefits will sustain. The short-term affordability of the VESSEDIA methodology is therefore critical for reaching interest and commitment throughout the software verification value chain. The following table shows the summary of costs and benefits in Euros for year 1:

Table 22: summary of costs and benefits in Euros for year 1

Value chain segment	Costs	Benefits	Net Value
Label Owner[100][101]	313,391.00	313,500.00	109.00
Accreditation bodies	111,653.40	111,653,40	00.00
Certification bodies	96,398.52	100,000.00	3,601.48
Developers[102]	31,520.46 to 220,258.49	4,044.87 to 6,067,300.00	-159,585.49 to 5,865,864.91
Evaluators[103]	400,189.09 [104]	875,764.77	475,574.20
Client / Sponsor (per usage of installed ToV on IoT device)[105]	184.76 to 1,131.68	60,673.00	-1,131.68 to 60,497.77
Smart society[106]	Delay in products/services availability	Increased safety and security	Welfare and well-being

A crucial condition for keeping the balance in the economic rationale is to keep enhanced verification efforts to a relevant and efficient level. Verification should not be done at a too high level in order to maintain a satisfactory, but not invasive number of alerts in the Validation and Verification. As current static analysis techniques may yield “too many” alerts, this may compromise the delivery time frame of the software undergoing enhanced verification and jeopardize cost control and expected incomes.

The initial investment from the label owner requires to set up an organisation acting as the scheme owner, to ensure investment capability and success in developing as well as settling the conformity assessment scheme in the software verification community. Additionally, the VESSEDIA economic

[100] The costs estimates are very pessimistic with 11 clearance and registration procedure costs added whereas there would be shortcuts between countries (e.g. EU countries) for adapting the label from one accreditation body zone of influence to another, thereby decreasing the costs in clearance and registration procedure.
[101] The economic balance is optimistic on the short term as there is most likely a delay between investment in the setting the conformity assessment scheme and collecting the royalties.
[102] Calculations are made on the case-based simulation.
[103] Calculations are made on the case-based simulation.
[104] The calculation goes as the fixed costs for certification capability added to variable costs for certification: Total fixed costs for certification service capability only for 4 evaluators (67,189.09) + Total cost of enhanced verification for the simulated case study (24*2,250.00 +8*14,625.00+1*162,000.00)= 400,189.09
[105] Calculations are made on the case-based simulation.
[106] Cost and benefits estimate at the extremity of the downstream value chain are difficult to measure. The benefits are expected to cover substantially the costs. Costs are mostly present through the delay in availability of software and installed IoT devices while benefits are ubiquitous through reduction of incidents, accidents and related breakdowns, medical treatments and insurance expenses.

methodology and rationale is currently based on open source tools for verification in view of making the methodology accessible for a wider audience. Licensed software would increase costs at the level of the developer and evaluator in the verification value chain, and consequently passed on costs downstream.

Nevertheless, the VESSEDIA methodology and the associated conformity assessment scheme (CAS) offer increased visibility on enhanced verification across the verification value chain, especially towards end markets (downstream). The VESSEDIA methodology also supports the use of static analysis and other tools or techniques for automation of verification to the software development community and industry through the ISO standard IEC 23643, while improving the tools themselves. This is done in a way that is sustainable for the actors of the software verification value chain.

Also, in the most sensitive segment of the value chain, were costs are high (developer, evaluator), the benefits from the VESSEDIA methodology are most quickly reached and with minimal risk in the investment when of using ***heuristic static analysis level*** on ***medium criticality software***.

Chapter 5 List of Abbreviations

Abbreviation	Translation
BBS	Benefits Breakdown Structure
CAB	Conformity Assessment Body
CAS	Conformity Assessment Scheme
CC	Common Criteria
CD	Committee Draft (document status in ISO standards development)
CBS	Costs Breakdown Structure
EAL	Evaluation Assurance Level (category ranking in Common Criteria security evaluation)
ISO	International Organisation for Standardization
IoT	Internet of Things
LCC	Life-Cycle Costing
NP	New Project (document status in ISO standards development)
SDLC	Software Development Life-Cycle
SME	Small and Medium Enterprises
ToE	Target of Evaluation
ToV	Target of Verification