Ecossian

D7.11

Societal and ethical impact analysis

Project number:	607577
Project acronym:	ECOSSIAN
Project title:	ECOSSIAN: European Control System Security Incident Analysis Network
Start date of the project:	1st June, 2014
Duration:	36 months
Programme:	FP7/2007-2013

Deliverable type:	Report
Deliverable reference number:	SEC-607577 / D7.11/ 1.0
Work package contributing to the deliverable:	WP7
Due date:	MAY 2017 – M36
Actual submission date:	31st May, 2017

Responsible organisation:	CESS
Editor:	Reinhard Hutter
Dissemination level:	PU
Revision:	1.0

Security Sensitivity Committee Review performed on:	15th May, 2017
Comments:	N/A

Abstract:	Measure for improving security such as the ECOSSIAN system need to work and regard their positive and possibly negative ethical impact and socio political implications they may cause. These factors need to be systematically analysed, weighted and assessed. A set of relevant criteria are developed and an evaluation methodology and tool were developed and validated in a set of possible future decision makers, application topologies and threat levels in which the ECOSSIAN system may operate.
Keywords:	Ethical, legal, political, societal: Methodology; Evaluation samples; Criteria; Methodology

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 607577.

Editor

Reinhard Hutter (CESS)

Contributors (ordered according to beneficiary numbers)

Jessica Schroers, Erik Zouave (KUL)

Hans Kühl, Uwe Nerlich (CESS)

Executive Summary

Beside the need to improve security, reduce risks and to use budgets in a cost-efficient way, decisions on security measures in general and on CIP measures in particular are often strongly driven by and/or have impact on political, societal, ethical, legal, administrative and related factors and restrictions. They are mostly of qualitative nature, not expressible in monetary or physical units. These factors may range from political appropriateness, social perception, privacy violations and acceptance by people or fears on environmental impacts, to name only a few examples.

Supposing that the ECOSSIAN framework will develop into an operational system, it needs to be evaluated against how it will influence and how it may be influenced by such socio-political factors.

This paper provides a general rationale on the need to include these factors in decision making, and a methodology and application approach for assessing in a systematic way how the utility of security measures in Critical Infrastructures is influenced by intangible factors as opposed to tangible or quantitative factors like money, loss of supplies, number of fatalities or similar. Such intangible factors are also called here qualitative criteria. Typical qualitative criteria are fear, freedom of movement, loss of time, but factors like subjectively perceived security, data privacy or compliance with existing rules of law, political concepts etc. as well.

A methodology and a comprehensive catalogue of qualitative criteria is presented. It is derived from a former EU project [4] and other resources, and modified for the purposes of ECOSSIAN. The methodology EELPS[1] is demonstrated with a selection of basic parameter variations like application scenarios or type and objective of stakeholders. Recommendations are given for a full-scale evaluation with the tool to accompany and support the implementation of the ECOSSIAN system in Europe in the future.

[1] Ethical, Economic, Legal, Political, Societal (impact assessment)

Contents

List of Figures

List of Tables

Chapter 1 Introduction and History

Decisions in industry and politics are often driven by criteria which cannot or are hard to be expressed in quantitative terms such as physical units, years of life or money. They are usually named as "intangibles", "soft criteria" or "qualitative" attributes of a decision. In security matters we have to deal with cost, benefits – which mostly is the reduction of risk – and a large number of qualitative "socio-political criteria"

Dealing with qualitative criteria in economy, enterprises, administrations etc. is not a new issue. It has been introduced by Zangemeister as Utility Analysis UA in the 1960s [2] . A further developed approach is the AHP[2] introduced by Thomas Saaty in the 1980s [1]. These two approaches are the main cornerstones in the whole area of qualitative assessment, also often named MCDA[3]. Both, UA and AHP have been used since then in various fields at least in the US, in Europe and Japan as well. AHP and UA concepts have been implemented in many software solutions, e.g. AHP in Expert Choice [13] and UA in the QCA tool of ValueSec [4] and CIRAS [5] .

A good definition of MCDA is given in [18]:

"MCDA introduces sound procedures for problem structuring and criteria aggregation, which can be used to rank and classify a set of alternative options or to choose the best ones. Except for the normative and descriptive aspects of decision-making, MCDA also adds a constructive perspective, in which a decision model is built through a progressive learning process that enhances the decision maker’s understanding of the problem and ultimately facilitates the construction of a good model. Thus, a decision model is interactively constructed with the active participation of the decision-makers, taking into account their system of values and judgment policy as well as their expertise on the particular problem under consideration".

A very profound discussion of various approaches, methodologies and application samples can be found in [17], an overview of its emergence and basic features can be found in [27]. MCDA methods and tools have been in use in many disciplines: Research, business, political and societal/sociologic problems, even in psychology applications. In security, however, it has not been found so far, apart from some MCDA elements in econometric solutions for security investments, also known as ROSI[4]- approaches. In an ENISA analysis [20], not only the benefits of the methodology but also the risk of manipulating "to justify a decision rather than enlightening it" is discussed.

The need for a broader or general employment of qualitative criteria in the assessment of security measures needs some explanation, which also refers to the recent EU/FP7 project ValueSec [4] and its deliverables 3.3 and 5.3.

Developing and applying a Qualitative Criteria Assessment (QCA)-tool is an important innovation in the context of security decision-making. In that ValuSec project and several successive ones, the methodology and supporting tool was both welcomed by decision-makers and stakeholders, but they also had to go through a process of understanding its dimensions and limits, its functionality, its utility and its potential impact. While the QCA was

[2] Analytical Hierarchical Process

[3] Multi Criteria Decision Analysis: see also [17]

[4] Return On Security Investment

both tested in ValueSec at stakeholder workshops and in 5 different use cases, for ECOSSIAN, its content and architecture naturally had to undergo some refinements in order to incorporate the specifics of an advanced system for CIP.

As a result, out of originally 122 different criteria, 48 were selected and refined: Content, explanations and descriptions were detailed. In addition, each criterion was provided with a utility function that transforms the qualitative value of utility of a criterion into a value on a scale between -10 and +10. One question of an evaluation session could e.g. be: Does the measure promote trust in fellow the political stem? Substantial increase in trust would result in the generic impact of +10, Moderate increase in trust in +5, no affect in 0, and risks of vigilantism may lead to -10). Each of these 48 utility functions was developed individually for each criterion.

While the translation of single answers into numerical values was an important step for the functionality of the QCA tool, the team has also discussed and is aware of the limits that this imposes. These limits refer to the fact that most of the raised societal, ethical, political etc. problems are complex and cannot always be summarized in one number because that may imply over-simplification of the problem. At the same time the results are still highly dependent on whoever assesses the problem and who decides on a final solution option or political a statement. Thus, the use of the QCA-tool has to be introduced and contextualized thoroughly before it is put into action, mostly in order to make comprehensible how the specific results come about and what that implies. It is also recommended to use the tool in a group environment for better mutual understanding and improving statistical confidence. In addition to the evaluation, the QCA tool supports awareness-raising and consensus-building about the specific societal and political problems that security decision-making may entail. One topic also addressed in the DoW and included in the criteria is the need for public-private partnership (PPP) as a composite of political and economic drivers. Details of a PPP concept for ECOSSIAN, however, have been worked out in D7.10.

The following terms for the methodology are used in this report, describing the same methodology within different contexts of implementation:

MCDA- Multi Criteria Decision Analysis: General term used in Literature

QCA – Qualitative Criteria Assessment: Used in the source FP7 project ValueSec

EELPS – Ethical/Economic/Legal/Political/Societal: Concrete instantiation of data and tool for the ECOSSIAN project

The complete list of terms and abbreviations can be found in Chapter 7.

Chapter 2 A General Rationale for QCA in Security

2.1 Planning of and Decisions on Security Measures

2.1.1 Measures to improve security

The field of security measures is extremely manifold, planning and decisions of security measures can be very complex, and the needs to improve security faces changing scenarios of vulnerabilities, threats, political and societal frameworks and societal perception. Measures to improve security may comprise legislation, strengthening of law enforcement and of first responders, international agreements, improving preparedness by training and exercising, adapting organizations, improving underlying disaster and crisis management processes, introducing new surveillance, hardening or recovery technologies, or alerting people through social media. Also "negative" measures may occur and need to be evaluated, e.g. when it comes to reduction of security personnel due to budgetary limits or needed confinement of civil rights.

2.1.2 Decisions on security measures

Although these scenarios for possible security measures are so versatile, there is one underlying model which describes the three main drivers of planning and deciding on security measures:

- The need for improving security, mainly by avoiding or reducing, likelihood of threats, risks of damages and consequences of anticipated adverse, hostile, dangerous etc. incidents.
- The cost involved, both, investments for planning, design, implementation and operation as well as possible savings.
- A huge number of societal and political factors which are widely intangible in the sense that we cannot directly translate them into monetary or physical terms.

These findings hold for security measures generally and for measures concerning CIP, which is the subject of ECOSSIAN.

Figure 1 gives a summary of these factors influencing decisions on security (the A in the top line acronyms standing for Assessment).

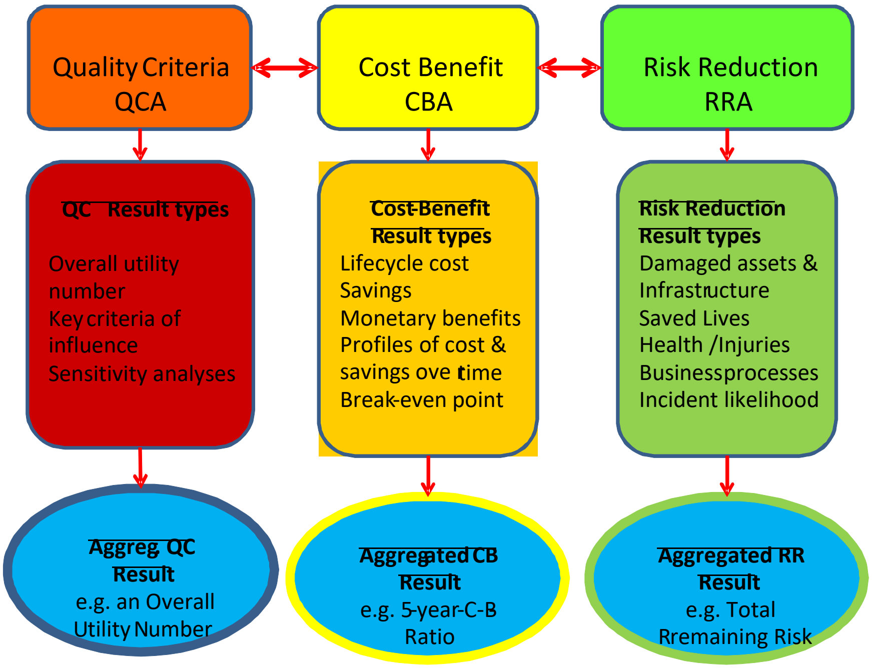


Figure 1: Decision Analysis of security measures

Risk reduction is the reduction of damages and/or the reduction of the probability of an adverse event to happen.

Cost are usually the cost for planning, preparation and procurement plus the operational, maintenance and consequential cost. Often also cost of measures for system enhancement and disposal at the end of the life cycle of the system need to be regarded. RRA[5] and CBA[6] have since long been addressed by sound research and covered by known analytical methodologies and supporting econometric tools.

Qualitative Criteria Assessment (QCA) methods are also around since long. But they are often neglected or treated unprofessionally: Lack of courage to name the risks of societal aversion, hidden politcal agendas, complexity of legal restrictions or ignorance against environmental risks are but a sample few obstacles entrapping decision makers not to regard the qualitative factors to the extent and attention they should deserve.

Few examples may illustrate the facts of unqualified preparation of security measures because of neglecting (od even ignoring) qualitative factors: In the wake after 9/11, a huge number of new regulations passed national legislation but many were ultimately rejected by supreme courts [9], obviously becaus legal and constitutional restrictions have not been properly regarded. CCTV surveillance or capturing of communications data is creepingly widened in our statehoods, often without sufficient information and consultation of the public. Attention and actionism of politicians use to dramatically explode after spectacular security incidents, but unfortunately the engagement then suffers from rather fast deterioration.

[5] Risk Reduction Assessment

[6] Cost-Benefit-Assessment

2.2 The Role and Importance of Qualitative Criteria

Though the public discussion about CI related security measures often shows that intangible factors are as important as e.g. financial costs it is not transparent how they have been or will be incorporated into the decision-making process. Moreover, up to now analytical methods of problem structuring and qualitative assessments are not systematically applied in security. There are numerous examples that demonstrate three things: (a) Intangible factors are often more important than cost and security risks, (b) intangible factors are not respected at all or not to their importance, and (c) theories and methods and in particular methods of qualitative assessment are treated step motherly in security research and security planning. This leads to security decisions which are suboptimal to say the least. Often they turn out to be obsolete after a short time and the real drivers of the decisions made remain unclear and are not made transparent.

2.2.1 The need of QCA

There is, however, growing perception of this fact: The EU has launched projects on societal factors in security, e.g. [3] and [4] in FP7. The current projects ECOSSIAN [6] and CIRAS [7], both on the improvement of critical infrastructure protection (CIP), and PULSE [8] on enhanced healthcare all contain work packages on methods and tools for assessing the societal, ethical, legal etc. factors of security measures. The Horizon 2020 program explicitly and generally emphasises stronger inclusion of **societal actors and factors** in its projects [10]. Germany e.g. operates the Centre for Security and Society at the University of Freiburg [11] which includes the disciplines of law, humanities, philosophy, economics and behavioural science and technology. Another example showing the growing integration need of security and society can be found in [12].

In the domain of CIP, questions to be evaluated by a QCA approach may include e.g.

- What kind of societal reactions will a new technology provoke (e.g. denial; protests; better "feeling" of security)?
- Will the measure fit into an existing legal framework (e.g. the country's constitution)?
- Is the measure compliant with or supporting the national and the EU security strategy (e.g. the EPCIP [14])?
- Does the measure promote the technological and/or scientific ambitions in the country?
- Will the measure support or hamper the establishment of public-private partnerships (PPP)?

In practice, there is a large amount of this type of questions. They can be broken down into several driving qualitative factors. In 5 different use case experiments in [4], the number of relevant criteria was in the order of 30(!) for a certain use case, out of a total catalogue of approximately 100 criteria.

2.2.2 The benefits

Compared to cost calculation and risk reduction estimation (see Figure 1), the systematic treatment of the "intangibles" is different and difficult.

This can also be observed in the various and different forms of impact assessments (for an overview on social-, privacy- and surveillance impact assessments see [15], furthermore ethical impact assessment as described by [22]. These impact assessments have as a common characteristic that they handle ‘vague’ factors, which might be influenced by the context in which they are considered. E.g. in some cases of PIA (Data Protection Impact Assessments) this is less the case; however, these are often criticised as a mere check of compliance with the European data protection framework [15].

There have also been approaches for MCDA to considering soft criteria e.g. by Banville et.al. [23] and Munda [24], proposing the involvement of stakeholders and stressing the importance of transparency.

Treating qualitative factors can lead to endless discussions and frustrating unsolved contradictions. This can drastically be mitigated if QCA methods and tools were available and became common and accepted in security planning, procurement, operation and administration.

When it comes to supporting tools, qualitative assessment needs to translate qualitative factors into pseudo-quantities such as rankings, weightings, scorings, relative importance between criteria etc. But although these processes to some extent can be arbitrary and subjectively biased, they inherently support to mitigate these shortcomings and offer a number of benefits:

- The methodology facilitates a systematic structuring of the problem and of the factors of relevance, by individuals or within a group;
- The methodology eases consensus building on the problem, its structure and the basic questions to be answered, within a group, particular when group members have different agendas, objectives and preferences;
- The evaluation process and related discussions make aware how important societal, political etc. factors really are;
- Once consensus is reached on the methodology and problem structure, e.g. in a group of diverging interests or opinions, the chances of reaching agreement on the assessment results and on the security measure itself dramatically increase;
- The consensus is based on a tedious but transparent selection, definition, finally agreed and jointly assessed criteria. After that process they will not easily be questioned any longer;
- After that agreement and a joint assessment, there is in principle no further need for debating the final outcome;
- The outcome of the process is transparent[7] and the process can be rehearsed if needed for justification or if doubts arise later (similar but even more systematic as with brainstorming results).

Wright [22] e.g. concludes when proposing an ethical impact assessment, "*while consulting and engaging stakeholders is important, ultimately in most cases the decision-maker – the technology developer or policy-maker – will need to take the final decision*". The QCA method provides decision-makers with the tools to support a decision which takes into account qualitative views of different stakeholders involved.

These great benefits have been proven and appreciated in a large variety of management processes and decisions, in social science and psychology. In the field of security, however, we are at infancy of exploiting QCA methods.

2.2.3 Different roles and views of evaluators

Before doing an evaluation of this kind, it is necessary to start with a few basic questions that need to be discussed and decided upon beforehand. Otherwise the potential "space of evaluation"- the number and variety of parameters- is most likely too large and even confusing. In our case, of course, parameters should be limited to ECOSSIAN-specific ones.

Questions to be clarified in advance may include but will surely not be limited to:

1. What do we want to find out and "Measure" by applying such evaluation?
    - Benefit for society?

[7] there are, however, decision processes and decision makers who prefer confidentiality and concealment over transparency

- Scepticism/ mistrust of society?
- Security increase as anticipated by society?
- Impact of political preferences and compliancy with the government's security strategy?
- Potential conflicts with the rules of law (which ones)?
- Different "attitudes" of different societies/societal groups towards the measure-the ECOSSIAN system?
- Expected constraints to and limitations of, the application of the ECOSSIAN system?
- Supporting arguments for the EU to introduce a system like ECOSSIAN?
- More options possible?

Depending on which questions under 1. above we will consider the most important ones, the criteria and methodology will differ substantially, and we have to ask

2. Who will be the real or assumed evaluators? Type and importance of criteria are substantially different, depending on who is doing the evaluation and which view, objectives, preferences etc. the evaluator has. It doesn't make much sense to have a "Joint" evaluation of groups with different interests and objectives unless they are willing or forced to jointly work out and agree on the setup of the methodology and to jointly accept the results finally. Just an example: Expectations of society will lead to completely different results than expectations of politicians, than those of CI operators, than those of a specific NGO, than those of a research professor. Candidate evaluators in ECOSSIAN could be
   - The project team and possibly external scientists;
   - Society/societal groups;
   - Political planners and decision makers;
   - Operators or potential future operators of the PULSE Platform;
   - Beneficiaries of the ECOSSIAN platform, e.g. national and EU officials, CI management.
3. Which is the assumed scenario or spectrum of scenarios? – assuming an "every day" threat environment will lead to different results than if we assume highly dramatic catastrophic events.
4. How far can or should we break down and detail the evaluation? e.g. evaluation of the whole system or different topologies, or broken down to individual tools or modules.
5. How far can and should we formalize the evaluations? Do we want to prefer verbal discussion over formal scoring schemes or vice versa?

A good evaluation requires a well-prepared guideline for the evaluators and a professionally moderated process.

These points, at a first glance, appear somehow strange and manipulative compared to other more straight-forward analytical methods and tools. QCA does not deliver "objective" results. Nevertheless, the benefits of working with such a methodology, particularly in a team, as described before in 2.2.2 prevail.

In past real application cases (e.g. for the military), after realizing the complexity of the problem and decision space, the methodology helped to avoid ending up with endless discussions and hundreds of pages of verbal descriptions of pros and cons: ethical, societal, political, scientific, legal, etc. arguments.

Within a single project such as ECOSSIAN it is unfeasible to cover all the above views and parameters in a systematic way. What we finally do is to offer a transparent methodology and a limited set of criteria and of assessments examples out of the large "evaluation space" discussed above.

It is probably not necessary to prove the full ethical, legal etc. compliance of the ECOSSIAN system now but rather offer a methodology and provide guidance on how to appreciate and how to use it, for future evaluators (whoever they will be), to do this evaluation in the context of the then actual decision situation (actual country, anticipated threat situations, societal attitude, rule of law, role and responsibility of decision makers, …), and in the context of scenarios the decision makers will then have in mind.

2.2.4 Cost-benefit and cost-effectiveness

In the economic world, QCA methods are often integrated within cost-benefit analyses. They, in principle compare cost of an investment with the non-monetary benefits of an investment. The latter part of this analysis is similar to the QCA methodology described here. This can make sense for decisions in the commercial industry. For security planning and decision making, however, we strongly recommend to strictly separate the qualitative assessment of socio-political factors from the monetary view. This "model" has been intensively discussed and advocated for in the ValueSec project (see [4], D6.2) and is continued in another CIP project of the EU/DG HOME [5].

2.2.5 The hurdles to do it

By definition, qualitative factors are first place not directly expressible in numbers. They don't have quantifiable physical or economical dimensions or attributes like loss numbers, fatalities, saved property or reliability of business processes. They deal with human perception, ethical impact, political correctness or adequacy, civil rights or data protection. Qualitative factors of influence have some characteristics which complicate or sometimes even deny systematic evaluation. They are often badly defined, vaguely understood and give room for different interpretation.

Successful approaches therefore require a number of thorough analyses and preparatory steps and agreement among the community which will do the assessments:

- Clear definition of the hierarchy system of criteria;
- Clear definition of the terms and criteria to be used;
- Understanding of interdependencies between criteria;
- Avoidance of overlaps and redundancies among the criteria to be applied;
- Where they are unavoidable, clear description of the overlaps and dependencies between criteria;
- Analytical support in handling overlaps and interdependencies;
- Agreement on the weighting schemes;
- Understanding of, and agreement on the utility functions.

If a decision is supposed to be supported and carried out by different individuals or organizations, it is required to reach a common understanding of the methodology, of the evaluation process, and agreement on the role and importance of this part of decision support. Otherwise, separate independent evaluation rounds may help. An in-depth discussion of these aspects can be found in [3], demonstrated there for the scenario of introducing public surveillance technologies like CCTV.

A more detailed application guideline and recommendations are given in Chapter 4.

2.3 The ECOSSIAN System in View of Society

The ECOSSIAN System (ES) according to its design objectives, if implemented at large scale in Europe, would provide a quality jump in governing and controlling European Critical Infrastructures (ECI). Any novel technology or technical solution of scale usually implies advantages for the whole society, economy, and security politics. At the same time (or later), however, they also bring along a number of socio-political risks and pitfalls. Innovative security measures are often based on new technologies and systems which require organizational changes, new procedures, effects on society or individuals, need to cooperate differently with people, conflicts with existing rule of law, international embedding etc. In this sense, **the ECOSSIAN (ES) System is a complex "security measure"** which needs to be evaluated not only with respect to its effectiveness, commercial benefits, mitigated damages, cost etc. but also in reflection of the spectrum of its wider societal impacts, which can be both, positive and negative.

Possible categories of qualitative societal factors describing impact on society on one hand and factors which characterize a possible evaluation (critical or appreciating) of a measure by society on the other, are summarised in Table 1. These categories are usually further broken down into criteria. Some typical qualitative criteria in the sample category "individuals" which may be of importance for the assessment of the ES are shown in Table 2 (both are samples from[4].

Rauschmeyer proposed an ethics approach in multi-criteria decision making, but noted that the building of criteria is a challenge [25]. The classical point of view on criteria is formulated by Bouyssou [26] "*In a multiple-criteria approach, the analyst seeks to build several criteria using several points of view. These points of view represent the different axes along which the various actors of the decision process justify, transform and argue their preferences*". Rauschmeyer declares that it might be difficult to fulfil this condition in an ethically profound debate: "*Whereas the condition of understanding and acceptance seems to be no fundamental problem in a superficial MCA*[8]*, it cannot be fulfilled in each ethically profound MCA. The responsibility of the analyst to the public and to the decision-maker(s) demands him/her to report as best as he/she can the different values affected by the decision*"[25].

As a practical solution a comprehensive catalogue of criteria has been developed in the FP7 project ValueSec [4], see also Annex 1: Categories and Annex 2: Comprehensive Criteria Catalogue It is thought to be a general baseline of qualitative criteria generally of potential relevance in the security domain for all kinds of security measures. In a concrete decision case, the user/evaluator can choose from this catalogue, but also can add or modify categories and criteria.

For the evaluation of the ECOSSIAN system, a first selection from this catalogue has been made. Descriptions have been modified and formulated in the form of typical questions. Further detailing will continue during the preparation of the experiments and of the evaluation sessions.

This catalogue of categories and criteria is given in chapters 3.3 and 3.4, respectively

[8] Multi-Criteria Asseement

Table 1: Categories of Qualitative factors

Categ. ID	Name	Helpful question
1.	SOCIETY as a whole	How will the measure impact societal life or societal reaction?
2.	INDIVIDUALS	How will the measure impact on individuals and individual reactions?
3.	LAWS AND REGULATIONS	Is the measure compliant with existing national and international rules of law?
4.	RIGHTS AND ETHICS	Is the measure compliant with or in conflict with fundamental rights?
5.	POLITICS	How does the measure influence the political level or cause specific political reactions?
6.	SOCIO-ECONOMICS	Will the measure influence the economic situation?
7.	TECHNOLOGY AND SCIENCE	How does the measure relate to scientific and technological development?
8.	ENVIRONMENT	Will the measure impact on the environment?
9.	GENERAL PRINCIPLES	Is the measure in line with basic principles of good governance?

Table 2: Sample qualitative criteria

2.	Category: INDIVIDUALS	How will the measure impact on individuals? What reactions may this cause?	A measure may alter the lives of individuals and may cause different reactions that are important for the success of the measure's implementation.
2.1	Perceived security	How does the measure influence perceived security?	Example: Vigilantism can create higher perceived security – or the opposite.
2.2	Risk appetite	Does the measure nurture or hamper risk appetites?	Example: Some technologies convey a false impression of being safe and nurture risky behaviour.

2.	Category: INDIVIDUALS	How will the measure impact on individuals? What reactions may this cause?	A measure may alter the lives of individuals and may cause different reactions that are important for the success of the measure's implementation.
2.3	Individual risks and opportunities	Does the measure produce any risks for individual citizens?	Example: with regards to the replacement of some analogue security measures through technological procedures, risks are being created for single citizens to lose access passes, etc.
2.4	Mental health/ well-being	Does the measure have consequences for individual mental health and well-being?	Example: The visibility of military/arms might influence the mental well-being of the population.
2.5	Physical health	Does the measure have consequences for individual physical health?	Example: Screening, X-Rays may have impacts on the individual health.

Benefits of the ES will be proven and demonstrated in a series of experiments in simulated scenarios and selected use cases with attacks/incidents in the CI sectors Energy, Transportation and Finance. Details can be found in D1.5. On the other hand, the project is tasked in WP7 with an accompanying critical assessment of the "Legal, Ethical and Social Foundations". While the legal frameworks and information sharing policies are extensively analyzed and evaluated in the deliverables D7.1, 2, 3, 6 and 7, this D7.11 provides the methodology for systematically and concisely evaluating the ES against the huge number of societal and other soft, i.e. qualitative factors of influence. Also, some sample results of applying this methodology are discussed.

Chapter 3 The QCA Methodology for ECOSSIAN

In a first order view, the QCA methodology is based on a 3-level hierarchical structure of attributes. First level is a security measure or measure alternatives, second level a set of evaluation categories and level 3 a set of criteria for each category. Criteria are weighted relative to each other. In the evaluation process, verbally described criteria properties are transformed into numbers on a scale between minus 10 (negative impact) and plus 10 (positive impact). The basic results are weighted sums over the three hierarchies.

Supporting functions help the evaluator select or define new categories and criteria, defined killer thresholds for specifically critical criteria and help avoiding or diminishing overlaps of criteria and visualizing dependencies between criteria. Overlaps and dependencies tend to produce double counting of same or similar effects.

3.1 The Adaptation Process of the QCA Tool

The core element of the tool is the criteria scheme in which the criteria are defined and explained, and grouped into different categories.

The ES is assumed to be a "security measure" (SM), a very complex one though, a term used in the definitions and descriptions of the methodology.

The objective of the ValueSec project was to develop decision support methodologies for public security planners and decision makers. The methodologies were to be suited for a large range of possible security measures which could comprise legislation, investment into technology, reorganization of security agencies, qualification of personnel and many more. The full Catalogue of Categories and Criteria from ValueSec is given in Annex 1: Categories and Annex 2: Comprehensive Criteria.

In ECOSSIAN, we will evaluate only one system, possibly in a limited number of different installations and applications. Therefore, the ValueSec criteria, 98 in total [4], are taken as the starting point for ECOSSIAN Task 7.5 from there

- Definitions and descriptions have been modified according to the specifics of the ES;
- Recommendations are made and criteria selected that appear important for the ES evaluation.

Additional categories and criteria may be defined which are typical for the ECOSSIAN environment but which were not included in the source material.

3.2 The Specifics of Applying QCA in ECOSSIAN

The characteristics, needs and benefits of such a qualitative criteria assessment have been discussed in chapter 2.2. From the application in ECOSSIAN we do not expect to generate a one-and-forever "true" evaluation result. The main aim of T7.5 and this deliverable D7.11 is to offer future developers, sales and marketing organizations, purchasers and users of a system like the ES a tool and a guideline for rationalizing their planning and procurement decisions not only from a risk reduction and economic perspective but also with respect to its socio-political implications. This will support several processes helpful for an efficient decision process, including:

- Awareness on the importance of societal, political etc. factors;
- The clear definition of those socio-political factors;
- The building of consensus between groups of diverging interests and agenda, on criteria and importance of criteria (e.g. between industry and government);
- The chances of reaching agreement on the assessment results and on the security measure itself will substantially increase;
- After that process criteria as well as results will not easily be questioned any longer;
- After that process, there is in principle no further need for debating the final outcome;
- The process and criteria are transparent[9] and the process can be rehearsed if needed for justification or in case that doubts about the decision arise later;

In summary, the decision maker will own a clear, systematic, solidly documented, and hard to dispute basis of her/his decision.

3.3 Categorization of EELPS

As already shown in Table 1, ValueSec, according to its broad application spectrum, handled nine different categories. They have been developed to serve as a starting platform for all types of decisions on security that need socio-political regards. For concrete security measures, usually only a subset from this catalogue apply, and in some cases categories and criteria may be of relevance that are not included yet in the list. For ECOSSIAN, five categories will be used, subsuming criteria of relevance to the ECOSSIAN system design, implementation and operation. These Categories are

1. **E**thical and psychological;
2. **E**conomic (factors which cannot be expressed in numbers , e.g. in Euros);
3. **L**egal;
4. **P**olitical and
5. **S**ocietal.

In the remaining part of the project and deliverable, we call the methodology **EELPS**.

3.4 Criteria

The 98 ValueSec [3] have been taken as a starting basis for selecting those which appear relevant for a System like ECOSSIAN. But also other resources from projects such as SURPRISE [3], PULSE [8] and ASSERT [15] have been analysed and searched for applicable criteria. This was a cross-project exercise analysing the application of the QCA methodology to three different EU projects in which CESS, the leader of ECOSSIAN T7.5, is currently involved.

This detailed analysis of sources, the tentative selection of criteria and the assignment to these three different projects has been documented at Annex 3: Tentative Criteria Selection .

The revised criteria, their definitions and descriptions for ECOSSIAN are further detailed in the following chapter 3.5.

[9] there are, however, decision processes and decision makers who prefer confidentiality and concealment over transparency

3.5 Analysis of Categories and Criteria

The criteria of course have varying meanings and importance depending on the subject of evaluation. For example, the protection of personal data in a system for improving healthcare in cases of pandemic will have characteristics which are different from data protection in energy supply of households. In the following chapters, the categories and criteria are discussed with respect to their characteristics and features they will show in ECOSSIAN. Societal criteria often need to be addressed in two ways: (a) describing how systems like the ES may impact on society and individuals and (b) how society, societal groups or individuals will perceive and react to such a system. The scales may reach from positive (welcome, appreciation ...) to negative (fear, rejection, protest ...) reactions.

The need, relevance and expected effects related to the criteria discussed may in certain cases (e.g. on ethical or legal issues) be seen differently by different stakeholders' organizations, by individuals, by social groups, by CI providers or by politicians. It is one of the strengths and benefits of the QCA methodology that these differences become obvious during the preparation of an evaluation and that the methodology facilitates open discussion and consensus-building on these differences. Handling of these phenomena is further discussed in chapter 4.3 and more profoundly in [17].

The interpretation of the criteria below and of their possible benefits and shortfalls assumes a situation in the future when the ECOSSIAN System (ES) would be implemented in Europe. The model of which and how many infrastructures and nations will participate, and the role of the EU in the implementation and operation still need to be discussed but will not be fully clear and fixed by the end of the ECOSSIAN project.

The criteria below were based upon the results of other projects but were adjusted to ECOSSIAN and influenced by the research in other tasks of WP7. The legal but also the ethical and societal criteria draw upon T7.1 (Applicable legal framework) and T7.4 (Information sharing policies). These tasks influenced not only the questions regarding adherence to or conflict with national and European regulations, but also considered fundamental rights such as the right to privacy. Criteria regarding political and economic aspects on the other hand were considered alongside the tasks T7.2 (Business Framework conditions) and T7.3 (Public-Private Partnerships). The main aspects in this regard are the possibility and need of cooperation of industry and government agencies and business considerations such as potential business improvement created by better industry cooperation, improved business image or market opportunities.

3.5.1 Ethical criteria

Under the category of ethical criteria, criteria are collected which address possible impact of a system like the ES on ethical values, principles and rules, and on quality of life of the society.

Table 3: Ethical Criteria

No.	Category & Criterion	Description	**Interpretation & commenting** These are ECOSSIAN "internal" comments that may not be given to external evaluators in this form-in order to avoid à priori bias.
1. Ethical Criteria			
1.1	Change of social values	Could the SM potentially positively or negatively change societal values?	The general prospect towards an improved resilience of CI-related supplies and services to citizens may improve quality of life in Europe. This will not become aware in peaceful operations, but could be drastic under massive threat scenario conditions. It could also foster negative values, e.g. egoism

No.	Category & Criterion	Description	**Interpretation & commenting** These are ECOSSIAN "internal" comments that may not be given to external evaluators in this form-in order to avoid à priori bias.
1.2	Privacy	Do security measures respect private and family life, ensure or endanger (physical) privacy?	There is the risk of undue penetration and violation of privacy when the ES handles/ uses personal data (e.g. if smart meters become mandatory or when banking or travel data will be used for operating the ES)
1.3	Equality, discrimination	Does the SM support equal treatment or rather prefer certain groups or individuals?	Maybe in a pilot phase, certain categories of people will be preferred. Generally, the risk of discrimination exists but is not supported by ES
1.4	Confidentiality	Does the SM protect or endanger personal information (e.g. medical; consumer)	Consumer information need to be protected and rules for using this information need to be clear, established and supervised. The rules should be documented in the related WP7 deliverables, in cooperation with the development of the ES confidentiality IT concept.
1.5	Trust	Does the measure enhance trust in institutions, infrastructure, or does it decrease trust?	Depending on the strategy of implementation, this may be seen positive and negative. If the ES is transparent to the end-customers and clearly contributes to enhanced CI services and supply, the reaction can be positive. If it is handled as a "political secrecy" (as many security and other measures such as TTIP are), the perception and reaction may become very negative.
1.6	Control of citizens	Will citizens be more controlled by the SM or will they be less controlled because of the SM?	The risk of abuse of ES's consumer and personal data, e.g. for targeted/ aggressive marketing and advertising is there. The capability of undue profiling of customers may be supported by ES. Evaluation of the potential of undue abuse may lie outside the scope of the ECOSSIAN project.
1.7	Organizational/ grouping	Can the measure lead to formation and action of special societal groups and initiatives (positive and/or negative)?	This, again, depends on the policy of implementation and operation and relates to the criterion "Trust" above. Beyond a certain level of mistrust, a tendency of building and acting of protest groups can develop
1.8	Integrity	Is the integrity of the decision maker on the SM verified?	The ES can become operational only under the governance of trilateral PPPs between EU, National governments and CI providers and operators. This is some facilitating measure prerequisite but no guarantee for the integrity of the partners and decision makers involved, on political as well as on industry level.
1.9	Truthfulness	Is the SM a response to a real risk or only/partially pretending it? Is it supposed to follow hidden agendas?	The ES will contribute to counter assumed realistic threats. Serious scenario forecasts of this types of threats to escalate or even contribute to "Cyber War" strongly suggest to improve CI security concepts. Other policy agendas may evolve and need to be critically observed. They will be driven by national policy and preferences and by the role and competence the EU will develop in the security and CIP domain.

No.	Category & Criterion	Description	**Interpretation & commenting** These are ECOSSIAN "internal" comments that may not be given to external evaluators in this form-in order to avoid à priori bias.
1.10	Transparency concerning the system	Are the procedures of the SM transparent to society or are they camouflaged or hidden? Is the balance of security improvement vs. privacy intrusion fully transparent to people or is it unclear?	Transparency of functions (what does the system do) should be seriously observed and regarded when implementing the ES. A concrete transparency policy needs to be regulated in a PPP (see also D7.10). Processes directly affecting society/ individuals need to be clearly described and communicated. This is especially important regarding the choices and procedures that can have an adverse effect on privacy.
1.11	Controlling by citizens	Will citizens get better (feeling) of being empowered to control or do they feel less in control	The potential for improving "subjective" security perception is given. The empowerment of citizens to contribute to control of the system is limited. A good solution could be an operational advisory board which includes societal representatives which supervises processes that may be critical for individuals, families, social groups

3.5.2 *Economic qualitative criteria*

Generally, a dominating economic decision driver is usually return on investment (ROI). In security, however, ROI calculations are very difficult or even impossible. We owe this to the fact that main factors of economical influence such as type of threats and likelihood of occurrence exhibit high uncertainties, and that the implementation process of a system like the ES may be mainly driven by political rather than by economical objectives and motivation. For these and other reasons it is very hard to directly translate security investments into quantified monetary benefits for the business. Economic factors at political level, e.g. "investment climate", again, cannot be directly expressed in revenue increase or tax return.

Therefore, the QCA offers a platform that nevertheless facilitates to regard the main "qualitative" economic drivers in the evaluation, although they cannot be expressed in Euros.

Table 4: Economic Criteria

2. Economical Criteria			
2.1	Economic stability	Does the measure influence economic stabilities (positive and/or negative)?	In "regular" peacetime operations, the contribution of the ES to economic stability may be limited. From a political point of view, however, at both the national and the EU level, the contribution of systems like the ES to economic stability may be substantial. This will become even more important in future possible cyber war scenarios or other events of major disruptions.

2. Economical Criteria			
2.2	Compensation of side effects	Can (unwanted) side effects be controlled, tolerated or compensated (e.g. via insurance)	There are many uncertainties on the operation of ES pending, which cannot all be solved in the project. One will be the sharing of information and of responsibilities across the three levels O-SOC, N-SOC and E-SOC, and peer to peer, between O-SOCs and between N-SOCs. Breach of confidentiality or unclear liability in cases of damages are but few side effects whose compensation and regulation may be unclear. Some recommendations will be given in D7.10 on PPP.
2.3	Cost-benefit	Is the economic benefit of the SM vs. cost clear/ transparent?	As mentioned in the introduction, clear cost-benefit ratios are impossible to calculate presently, as implementation and operation cost, cost sharing models etc. are outside the scope of ECOSSIAN and it would be too early to try them now. A QCA, however, dedicated to cost-vs.-benefit effects would facilitate a first order scaling of the ratio between expected cost and expected benefit in assumed scenarios and use cases.
2.4	Economic beneficence	Who benefits from the SM? Does the SM confer benefits on some groups but not on others?	Will the SM be only beneficial (in an economic sense) to specific companies or also to society in general? Can individuals benefit from it?
2.5	Validation	Does the introduction of the SM foresee measurement and evaluation of the SM's effectiveness and benefits regular base?	The direct measurement of technical performance, such as detection rates, rates of false positives and/or false negatives will be measurable. The effect of the whole system on the resilience of the subjected infrastructure and on the supply of society can only be guessed at best. The ES, however, should provide a scheme and method for capturing lessons learned which should contribute to such validation.
2.6	Environment	Does the SM have significant (pos./neg.) impact on environmental or environmental factors?	No environmental impacts can be related to the ES in the foreseen scenarios. This may be different when a system like ES would be applied to other infrastructures such as Water supply, flood disaster control or healthcare.
2.7	Cooperation	Will the SM support or block/hamper cooperation (e.g. among peer stakeholders, between nations, with international bodies)	Cooperation models still need to be worked out. Generally, assuming that CIs, nations and the EU to expect economic (and political) benefits from the ES, the cooperation between all levels will be fostered. Or the other way: Well functioning cooperation is a decisive prerequisite for the success of the ES. Cooperation between peer stakeholders may suffer from competitive attitudes and from proprietary and confidentiality restrictions. The risk and chance of an ES to contribute to monopolization or even to building a "government-industry complex" need to be regarded.

2. Economical Criteria			
2.8	Market	Does the SM support/increase /decrease market advantage?	The market advantage of ES partners will develop, compared to competitors not participating in the ECPOSSIAN-like system operation. Market advantages will further grow if a system like the ES becomes a role model for the EU.
2.9	"foreign" sectors	Will the SM require involvement of "other" sectors (e.g. private security org's., foreign org's)?	The ES will need the cooperation of all partners affected. This includes different but dependent CIs, national and EU organizations for security and crisis management. But also the cooperation with interest groups of society, possibly NGOs, partners, subcontractors and suppliers of the CIs may need to be involved. Depending on the cases, this may result in supporting or hampering cooperation.
2.10	Dependency	Is the measure dependent on "foreign technology"; how critical?	The ECOSSIAN project has its proprietary architecture. But he hardware to operate ECOSSIAN is COTS and so are the basic operating systems. This means that the ES can become subject to numerous security exploits offered by the security gaps in these systems. The risks implied may be substantial and needs to be evaluated.

3.5.3 Legal criteria

A system like ES is a sophisticated technical platform but needs to be embedded in political and business will and rules and legal and regulatory framework. On the one hand, it will require dedicated contractual agreements among partners and on the other hand the ES needs to comply with existing national and international rule of law, and with related EU regulations and EU policies (e.g. concerning standardization). The main criteria of "legal" (in this sense) relevance for introducing and operating an ES are discussed.

The need for and a model of partnerships among different CI sectors, between industry and governments, and altogether with the EU (PPP) is analysed in D7.10. Selected legal attributes are also included here and in the political criteria catalogue (next chapter).

Table 5: Legal Criteria

3. Legal Criteria			
3.1	Legal conformity/ compliance	Doe the SM comply with existing regulations and rule of law	Which is the basic legal framework the ES follows? Have legal prerequisites and possible gaps been clearly identified and assessed? Does ECOSSIAN assume certain national legislation? Is this adequate as a role model? How easy can it be adapted to different rules of law? Has this been verified with examples?
3.2	International compliance	Does the measure comply with international guidelines, regulations, treaties etc.?	Have the EU regulations (e.g. directive 114, anti-terror strategy; cyber security strategy, ...) been properly regarded? Which are the main objectives of the EPCIP that will be supported by the ES? Do we or expect to face basic problems with legal compliance. How serious are they and how easy to implement ES as a compliant solution?

3. Legal Criteria			
3.3	Justice	Is there a fair and just system for addressing SM failure with appropriate compensation to affected Stakeholders?	Partners working jointly with the ES need a system of mutual assurance and possibly of insurance of covering risks and damages attribute to one stakeholder to another one.
3.4	Standards	Does or doesn't the measure comply with standards (if requested)?	Application of standards may have different motivations at political than at industry level. Which are the "Standards" applied in the ES? Are they real standards (e.g. ISO, IEE, ENISA supported, or rather proprietary, national? What is the effort to make the ES a real European standard? How does it compare to other European or global standard solutions (e.g. in aviation or healthcare)?
3.5	Contracts/ Policies	Can possible gaps be solved with contracts or policies?	e.g. differences in national data protection or in national procedures may be bridged by special system specific regulations.

3.5.4 Political criteria

A system such as the ES should comply with the political will, political security strategies at national and EU level, and it should support the interests of political decision makers.

Table 6: Political Criteria

4. Political Criteria			
4.1	Responsibi lities	Is a shift of responsibility needed to implement the measure? with pos./neg. effects? [2]	It is to be expected that the ES can work rather smoothly in every-day operations. Conflict potential arises when it comes to serious infrastructure disruptions with cascading effects and massive impairment of economy and society. Then the focus is no longer on the routine prevention and mitigation of threats and smaller damages but rules and contracts must be in place on who will be taken accountable for deaths and damages in the high millions.
4.2	Strategy & political relevance	Does the SM fit into related security strategies (if existing); national, EU and other international	Is the ES supposed to be of political relevance? Do we have measurements to evaluate the political relevance of the ES? Do e have role models used for the operational concept of the ES.
4.3	Media reactions	Will the media respond to the SM upon its introduction positive or negative?	The ES may become a highly "visible" system. The implementation concept must provide clear regulations for the treatment of the public media and the information, early warning and alerting of the public. These regulations may be different for different threat scenarios.

4. Political Criteria			
4.4	Partnerships	Does the SM imply/ require special partnerships, particularly PPPs, including NGOs? Are risks of failure or misconduct of these partnerships to be expected?	By definition, the ES is a three-tier system serving at CI, at national and at EU level. Due to this character, it requires rather rigorous partnership regulations. The PPP concept has been described in D7.10. Do we expect major obstacles against implementing such PPP and against operationally implementing the ES? Which are the supporting, which are the endangering factors? Do useful role models exist?
4.5	Reputation	Will the SM improve or reduce political reputation (e.g. locally, nationally, internationally)?	The ES has the potential of becoming a showcase for PPP, for European cooperation in security and for efficiency of coordinated CIP. Will these possible effects be taken up by the political community or will they rather be seen sceptically?
4.6	Acceptance	What is the potential for the measure to be politically accepted or to produce (counter-) movements/ scepticism/opposition? [3]	Politicians may be reluctant to embark on such a system with joint responsibility. Industry will be afraid of becoming more or over-regulated by the government through the ES operation. How broad or narrow will be the acceptance on both sides, and at EU level? If acceptance is perceived differently by industry and politics, this criterion may be split in two
4.7	Opportunism	Is the SM opportune to political agenda(s) & objectives other than strategy (e.g. pol. reputation, imminent elections)	Politicians tend to support solutions which give them public visibility, often with a rather short-term perspective. Would a decision to implement the ES be opportune from a political p.o.v.? Political motivations may be different in individual states and at the EU (Council; Commission; Parliament).
4.8	NGOs reactions	Will NGOs or other societal groups react positively or negatively? [4]	Will a system like the ES raise the attention of NGOs or even motivate the building of NGOs? Will NGOs be rather supporting or rather rejecting? Is the reaction of NGOs or similar groupings expected to be positive or negative?
4.9	Political risks	Does or doesn't the SM imply the potential of creating political risks? (e.g. o. prosecution at high courts)	Political and/or legal risks may be raised by a system such as ES, e.g. risk of operational failure in case of severe crises, risk of being sued by constitutional/supreme courts or regulatory bodies?

3.5.5 Societal criteria

Societal criteria may have overlaps with ethical criteria. While under 3.5.1Ethical criteria have been discussed under ethical aspects and moral grounds, here we discuss effects of an ES-like system on society more from an economic and material point of view of morale and way of living. Both aspects, the ethical and the more materialistic one cannot be fully separated and defined independent of each other.

Table 7: Societal Criteria

5. Societal Criteria			
5.1	Fundamental rights	Does a measure respect or endanger fundamental rights, e.g. family life, personal dignity, liberty, health, integrity, freedom of information, etc.? [5]	New systems may unduly penetrate the private sphere of people or rights of civil liberty. The risk of this to happen (deliberately or by chance) is particularly high with complex ICT systems that have direct influence on social life. Could there be cases in which these rights may be or need to be limited or impaired through the ES? Will these effects be motivated politically, economically, technologically? (see also next criterion)
5.2	Technology intrusiveness to society	Does the SM support (in the positive sense) or enforce (in the negative sense) intrusion of technology into society / into the private sphere, e.g. dedicated HW/SW installations	The ECOSIAN system may foster or even enforce intrusion of technology into the private sphere. Examples are online banking or ticketing and introduction of smart meters. Positive effects of intrusiveness could be cost savings for customers via flexible and optimized tariff rates.
5.3	Direct benefits to the needs of society	Will people/ society have direct benefits or detriments from the SM	Society/people may have different expectations and criteria to measure the benefit of a system. E.g. during peaceful regular operations, the benefits of the ES may not even be visible. In cases of major disaster and crisis, even in cases of war, benefits may become paramount. Are these benefits (e.g. sustained supply) adequately communicated to and appreciated by people and society as a whole?
5.4	Perceived security	How does the measure influence societal feeling of security [8]? How will be the effects and effectiveness of the SM on perceived security? Does the measure influence societal feeling of security positively or negatively?	Real security and perceived security are two different things. How will the ES contribute to the perceived and subjective feeling of security? Which are the means (e.g. via media) to enhance subjective security perception through an ES?
5.5	Health impact	Does/can the SM have (negative/positive) impact on mental and/or physical health of individuals or societal groups?	Are there any direct or indirect factors identified which may have an influence on the physical and/or psychic health of people? Have these factors been identified, analysed and will they be communicated before implementing the system?
5.6	Attitude towards technology	Will society reject / welcome the technology and processes which would be implemented by the SM?	Experiences with introducing new technologies show that they can create a certain attitude in societies or societal groups. With the ubiquity of IT/internet in society, the attitude towards an ES may be positive. However, can we learn from positive and negative cases similar to ES of the past (e.g. SWIFT/ online banking)?

5. Societal Criteria			
5.7	Preparedness	Does the measure enhance preparedness of society to cope with (new; unexpected) risks or does it make society less prepared?	People tend to better cooperate and accept new systems when they feel to be a respected part of the system. Does the ES have the potential to create or improve the educational state of societies to become better aware of potential risks and to voluntarily invest into pro-active measures (e.g. building livestock reserves, redundant heating systems, ...)
5.8	Risks to society	Beside its primary purpose: Does the measure imply or create any additional risks to or additional positive security and safety impact on society or individuals?	Possible risks to society can be additional cost of living (?), the wrong and unrealistic assumption about security, carelessness, Impact on social/social order (?) On the other hand, generally improved sustainability of supplies when operating the ES reduces certain risks for society e.g. of not maintaining jobs, SMEs etc..
5.9	Exploitation	Does the SM exploit information on the system) to the extent possible and/or necessary? [9]	What are the basic information material, style and media on how to inform the public about the benefits of (and maybe impairment by) the ES (e.g. by addressing of individuals, public discussions, media campaigns, ...?)

3.6 Capturing the Views of Stakeholders

Stakeholders - CI operators/ providers and future decision makers concerning ECOSSIAN use - were included in the analytical work on EELPS via

1. Early stakeholder workshops with national external stakeholders;
2. Including internal stakeholders in the process of criteria descriptions;
3. Feedback from the ECOSSIAN advisory Board (Notes from AB on PPP.docx, 17. May 2017;
4. Including internal stakeholders in the sample evaluations (see Chapter 5);
5. Including the external ethical advisor (EEA) in the sample evaluations (see Chapter 5.2.2.2).

Early stakeholder involvement in the ECOSSIAN project have been planned, handled and reported in WP8. Discussions with external stakeholders addressed a multitude of issues of ECOSSIAN to be regarded when implemented in the future. Feedback concerning EELPS can be summarized as follows:

- A lack of trust in systems or fear of control (by governments) was identified as possible unwanted side effect.
- Societies' reactions will most likely depend upon how the ECOSSIAN implementation will be communicated as it could be seen as a controlling system. Society should be informed clearly and the objectives, benefits and how the information is handled should be clear and transparent.
- Acceptance will further depend upon the credibility of the N-SOC/E-SOC entities. It was recommended that they should be managed by public organizations such as police authorities or governmental entities that will have better credibility than private corporations.

- Concerning political acceptance and feasibility, the role of N-SOC (and also that of E-SOC) needs to regard the specific national organizations and rules. E.g. in a federal constitution like that of Germany, responsibilities are distributed across divers national and state ministries. Responsibilities for incident and disaster management may be very fragmented across federal, state and local authorities. So the interface and communication structures need to be clearly defined.
- As long as the information is anonymized, no potential impact on fundamental rights or potential to increase control over people was expected.
- As long as privacy is kept, no legal obstacles were foreseen and rules of law were considered sufficient.
- It was furthermore recommended that the ECOSSIAN solution should be subject to an external independent audit.

As to the future discussion with stakeholders of socio-political factors of a system like ECOSSIAN, a catalogue of questions has been prepared which contains questions addressing the qualitative criteria categories above as well as questions addressing the need of a public-private partnership (PPP[10]). These questions are to support the understanding of the need of ECOSSIAN, and the development of a reasonable criteria scheme agreed among stakeholders of different interests. The full list of questions and the typical stakeholders to be addressed is documented in Annex 3: Tentative Criteria Selection for ECOSSIAN.

This is a guide for future decision makers who will be in charge of planning and implementing the ECOSSIAN system at an operational scale. At this stage of the ECOSSIAN project, the demonstrations still ongoing, the feedback of stakeholders from the demonstrations was limited to some dedicated discussions with internal and external stakeholders and a reduced set of evaluation questions. These questions were subject of the feedback rounds as organized for the four demonstrations of the ECOSSIAN system in certain scenario use cases. The result of these feedbacks is documented in D5.8.

In addition, the evaluators of sample evaluations gave valuable discussions on the criteria applied in these evaluations. This includes the External Ethical Advisor (EEA). For more details on concrete evaluations, see Chapter 5.

[10] PPP is analysed in T7.3 and documented in D7.10.

Chapter 4 Application Process and Guide

4.1 Possible Tools

This chapter guides the user of the EELPS methodology and tool through the preparation of evaluations of the ECOSSIAN system. The menus samples given are based on the Excel tool which was partially developed in the ECOSSIAN project, based on the preceding work of ValueSec [4] and CIRAS [5].

Beside or instead of this xls tool, the JAVA version implemented on the server of the ValueSec and CIRAS partner ATOS Spain may also be used, but the functionalities of both are basically identical.

The ATOS platform also offers a modified version under the acronym MAHP[11] which has implemented a different methodology of ranking and weighting of the criteria. A licence agreement has been put in place that allows the use of the ATOS platform for EU research projects at no cost. This may become attractive when it comes to the implementation of the ECOSSIAN system. For the purpose of validating and demonstrating the methodology in this project, the .xls-version was fully sufficient.

4.2 General Preparation Guidelines

A good guidance on the necessary steps of an MCDA evaluation process is given in the ASSERT project [15] on "Criteria for Assessing and Mainstreaming Societal Impacts of EU Security Research Activities".

That project, however, is limited to the assessment of privacy (and surveillance) impact assessment (PIA) and to some extent also discusses social and societal impact assessment (SIA) and constructive technology assessment (CTA). There is a rather comprehensive list of steps to be generally taken for such assessments (derived from [16], A step by step guide to privacy impact assessment):

1. Determine whether a PIA (or surveillance impact assessment) is necessary;
2. Identify the PIA (or surveillance impact assessment) team and set the team’s terms of reference, resources and time frame;
3. Prepare a PIA (or surveillance impact assessment) plan;
4. Determine the budget for the PIA (or surveillance impact assessment);
5. Describe the proposed project to be assessed;
6. Identify stakeholders;
7. Analyse the information flows and other impacts;
8. Consult with stakeholders;
9. Determine whether the project complies with legislation;
10. Identify risks and possible solutions;

[11] Modified Analytical Hierarchical Process

11. Formulate recommendations;

12. Prepare and publish the report, e.g., on the organisation’s website;

13. Implement the recommendations;

14. Ensure a third-party review and/or audit of the PIA (or surveillance impact assessment);

15. Update the PIA (or surveillance impact assessment) if there are changes in the project;

16. Embed privacy awareness throughout the organisation and ensure accountability.

These sources contain a sound analysis of different aspects and needs for such kind of assessments, and provide a number of very useful references ECOSSIAN can benefit from. ECOSSIAN, however, goes an essential step further beyond verbal discussion by providing an analytical methodology and tool that allows to systematically push the analysis and the evaluation process beyond verbal discussion.

For the purpose of ECOSSIAN, the points 2, 3, 5, 6, 9 and 10 of the above list are of importance. They will be discussed in the following chapter. The other points, in "reality" also need to be considered, however not so in a research project like ECOSSIAN.

Before doing further preparation of using this methodology, it is suggested to start with a few basic questions that should be discussed and decide upon beforehand. Otherwise the potential "space of evaluation"- the number of options and the variety of parameters- becomes too large. Parameters should be limited to the ECOSSIAN-specific needs.

Questions may include but will surely not be limited to:

1. Which will be the main objectives to be addressed by such evaluation: e.g. benefit for society? scepticism / mistrust of society? Security increase as anticipated by society? Political preferences? Potential conflicts with the rules of law (which ones)? Different "attitudes" of different societies/societal groups? Expected constraints to and limitations of, the application of the ECOSSIAN platform and tools? Depending on which objective or mix of objectives we choose from above, the criteria, the methodology setup and the evaluation process will differ substantially.
2. Who will be the real or assumed evaluators: The project team? Society/societal groups; which ones? Political planners and decision makers? Operators or anticipated operators of the ECOSSIAN Platforms? Beneficiaries of the platform, e.g. CI operators, first responders, victims, affected society, politicians….? Just an example: Expectations of society will lead to completely different results than expectations of politicians than those of hospital operators than those of CSOs in critical infrastructures and so on.
3. How far can or should we break down and detail the evaluation; e.g. by individual tools (e.g. see ECOSSIAN architecture elements in D1.7)?
4. How far can and should we formalize and organize the evaluations? Do we prefer verbal discussion, brainstorming, or scoring schemes? A profound evaluation will probably need all.

There will be more aspects to be discussed and decided upon during the planning and setup of experiments and the preparation of the evaluation.

4.3 The EELPS Setup Process

For setting up evaluations, the following guide operates with a number of terms defined in Table 8 and referred to in the coming chapters, in a somewhat logical sequence.

Table 8: Terms used in the evaluation Guide

Term	Defined as	Limit/range of the EELPS Tool
Campaign	A set of evaluation sessions	unlimited
Session	A number of evaluations with parameter variations	unlimited
Case	One parameter set within a session	3 per session
Category	Group of evaluation criteria	5
Criterion	Subject to scoring	10 per category
Weighting	Scaling of the relative importance of categories within a session And of relative importance of criteria within a category	0 to 100%
Descriptors	A qualitative scale verbally describing the possible range of a criterion in the utility functions	20 per criterion
Utility function (UF)	A function transforming descriptors into a numerical scale of -10 to +10	1 for each criterion
Evaluation[12]	Assigning a descriptor to a criterion	
Results	(a) Numerical table showing a summary of scores (b) Bar charts of scores for each criterion and averaged for each category	Range of scores normalized to -10 to +10
Analysis[13]	Interpretation of results	See chapter 5.2

4.3.1 *Campaign and Session Parameters*

The methodology uses a number of operational terms for defining a session, which need to be clear and kept unchanged. These definitions include few basic parameters:

1. Security Measure (SM): The measure planned to be applied and which will be evaluated. Usually, in one evaluation session one can/will compare alternative measures in order to find indications on which one to prefer (e.g. the installation of CCTV cameras as opposed to intensifying personal screening. In the case of evaluating the ECOSSIAN system, individual components or the whole system in different configurations could be taken as SMs and compared.
2. Evaluator type: The individual or group of evaluators. Choosing different evaluator types would show how the socio-political evaluation may differ depending on the basic priority settings and objectives of different individuals or groups. An NGO may come to completely different results than a CI manager.

[12] here in the narrow context of an evaluation campaign

[13] here in the narrow context of an evaluation campaign

3. Main evaluation objective category: Objective of an evaluation could be e.g. to evaluate the perception of a new system by a critical society, The expected acceptance in a certain political constellation, the expected risks from incompliance with international law etc. This "main objective is usually closely correlated with the type of evaluator (parameter 2. above).
4. Scenario: Assumptions on the basic characteristics of the scenario in which the security Measure is assumed to operate and against which its effectiveness will be evaluated.[14]
5. Other important parameters, which may dominate a certain measure and the decision to be made, e.g. alternative political framework conditions or strategies, basic cultural differences of countries in which the same system/ measure should be operated.

For the sake of clear separation of effects, in one Evaluation Session only one of these basic parameters should be varied, the others should be kept the same. Exception may be parameter 2 and 3 which are often correlated.

The following Tables give some examples of typical candidates of evaluation sessions. Samples are taken from another EU security project, PULSE [8], on a complex IT system for healthcare improvement, where sample evaluations were demonstrated in 2016. We show these samples from another project here in order to also **highlight the inter-project cooperatio**n (more details can be found in D8.4/ D8.6, the dissemination reports).

Tentative Session/Case descriptions for ECOSSIAN will be given in chapter 4.3.2, the final session parameter setups in chapter 0.

Table 9: Comparison of Measures- sample from the PULSE project

Session Name: PULSE Eval.			
CASE Parameter	**Case 1: National**	**Case 2: EU**	**Case 3: Reference**
Measure	PULSE national/local level	PULSE incl. international level (EU+WHO)	Status Quo; no PULSE System
Evaluator type or individual	National healthcare authorities	national healthcare authority	national healthcare authority
Main evaluation objective	Public acceptance	Public acceptance	Public acceptance
Scenario	SARS	SARS	SARS
Other parameters to be varied			
Other			

In this session, the sophisticated security system (PULSE platform) will be evaluated assuming different application environments (national, case1 and EU-level, case2), against the status quo (case 3).

[14] Evaluation of effectiveness is not part of a QCA analysis but needs to be performed with a different mathodology based on Measures of Effectiveness (MoEs)

Table 10: Comparison of an SM by different groups of interest

Session Name: PULSE Eval.			
CASE Parameter	**Case 1:** National	**Case 2:** EU	**Case 3:** Reference
Measure	PULSE on national and international level (EU+WHO)	PULSE on national and. international level (EU+WHO)	PULSE on national and international level (EU+WHO)
Evaluator type or individual	Hospital operators authorities	national healthcare authority	EU healthcare authority
Main evaluation objective	Satisfaction of victims	Public acceptance	Political role model
Scenario	Major flood disaster	Major flood disaster	Major flood disaster
Other parameters to be varied			

This evaluation session would show the differences when the same system would be evaluated by three different stakeholders: Hospital operators (case1), national authorities (case2) and EU healthcare authorities (Case3).

Table 11: Comparison in different scenarios

Session Name: PULSE Eval.			
CASE Parameter	**Case 1:** National	**Case 2:** EU	**Case 3:** Reference
Measure	PULSE on national and international level (EU+WHO)	PULSE on national and. international level (EU+WHO)	PULSE on national and international level (EU+WHO)
Evaluator type or individual	National first responders	National first responders	National first responders
Main evaluation objective	Cooperation willingness of society	Cooperation willingness of society	Cooperation willingness of society
Scenario	Major flood disaster	Major pandemia	Major terror attack with international effects
Other parameters to be varied			

In this session, the SM will be evaluated under the aspect of public in three different scenarios, a flood (Case1), a pandemic (case2) and a terrorist attack (case3).

4.3.2 Setup of Session parameters for ECOSSIAN

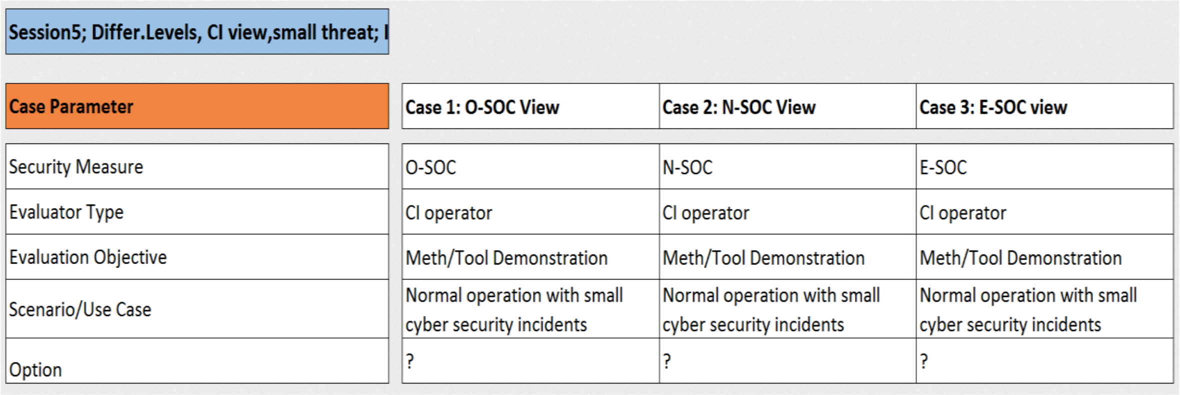
Usually, in MCDA type analyses, the main objective is to compare different options or "Measures" and help the decision maker(s) find the "best" option, and embed this in a consensus and compromise-building process between stakeholders of diverging interests. In security in general and in the ECOSSIAN project in particular, the scene is different: The main objective of this experiment here is to raise awareness and to make transparent the different intangible factors which may be of importance for the ECOSSIAN system and its application. That means, we don't look at alternatives to the ECOSSIAN system, maybe except for comparing it to a status-quo situation with no system like ES in place. Furthermore, we may want to evaluate and compare the system from different stakeholders' points of view. E.g., a CI enterprise will have different preferences and objectives than a national crisis management organization. This implies that a potential operator of the ES at E-SOC level will have different or partially differing objectives and political preferences than a national government, and a scientific community or societal representatives, again may have different views on an ES-type system.

In ECOSSIAN, the SESSION parameters offer a range of variations:

1. Measures: It should comprise application and configuration of the ECOSSIAN system. Variations can be: Full scale or partial system, application at local, national or EU level or at all levels. Many subsets of system configuration and application appear possible.
2. Evaluator type: There are at least five basic different types of evaluators: (a) Society, societal groups or individuals, (b) CI operators and managers, (c) National security organizations, (d) EU/ international security organizations, and (e) the scientific community including the ECOSSIAN project team itself.
3. Main evaluation objective: The spectrum can be very large, ranging from public acceptance or appreciation to legal compliance, from national preferences to EU policy implications, from national commercial interest to improving international standards.
4. Scenario: The basic ECOSSIAN scenarios have been defined in the deliverable D1.5, covering energy, finance, transportation, smart grid attack, and CI supply chain management scenarios.

Combinatorial grouping of all parameter variations (and there may be more) results in an estimated total of between 160 to 480 cases which of course cannot be handled. It will therefore be necessary to limit the effort to those sessions which appear most appropriate in support of ECOSSIAN on one hand and for critical evaluation on the other. Presently, it appears likely that we will have basically one type of ECOSSIAN system to be implemented as a whole in a European environment and to be compared to the status quo, three stakeholder groups (CI operators, national and EU-level authorities) doing the evaluation, one main objective which is to evaluate ethical impact and social acceptance, in two or three scenarios. A sample of possible parameters variations is given in given in Table 12.

Table 12: Sample ECOSSIAN case settings



Session5; Differ.Levels, CI view,small threat; I

Case Parameter	Case 1: O-SOC View	Case 2: N-SOC View	Case 3: E-SOC view
Security Measure	O-SOC	N-SOC	E-SOC
Evaluator Type	CI operator	CI operator	CI operator
Evaluation Objective	Meth/Tool Demonstration	Meth/Tool Demonstration	Meth/Tool Demonstration
Scenario/Use Case	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents
Option	?	?	?

If we allow 6 sessions and 3 cases[15] per session, this will result in a total of 18 cases. This amount seems to be manageable. The concrete sessions used in the ECOSSIAN evaluation campaign are discussed in chapter 5.2 and Annex 5: ECOSSIAN EELPS Evaluation Sessions, finally comprising seven different evaluation sessions.

4.4 Preparing the Assessment Process

Evaluations with the EELPS methodology and underlying tool require a basic understanding of the principles of utility analysis and MCDA. A good discussion on strengths and weaknesses, myths and practical examples can be studied in [17]. This is particularly necessary for setting up a concrete evaluation campaign. The evaluation itself needs some introductory briefing of the evaluating persons but evaluation can be done without detailed methodological knowledge. It is therefore recommended to do the parameter definitions of a session and setting the system by an experienced person or group separated from the evaluation round(s) which can then be done by "stakeholders" with less methodological knowledge. A detailed description of the individual steps can also be found in [4], a most recent EU/FP7 project result, which is briefly summarized here. In [17], e.g. it is even suggested that the problem analysis and tool preparation and setup should be supported by a facilitator external to the decision maker's organization and that the evaluation is done by the decision maker or people of his/her organization with the possible moderation by this consultant. This process eases common understanding and solving of conflicts of interest.

4.4.1 Setting the system

4.4.1.1 Categories and criteria

Criteria are the "factors of influence, in our case qualitative factors out of the societal, individual and ethical, Legal and political domain. They are grouped into the five categories E-E-L-P-S. A set of categories and criteria is available. The tool, however, allows to extend, reduce and modify both, categories and criteria.

[15] present tool limitation

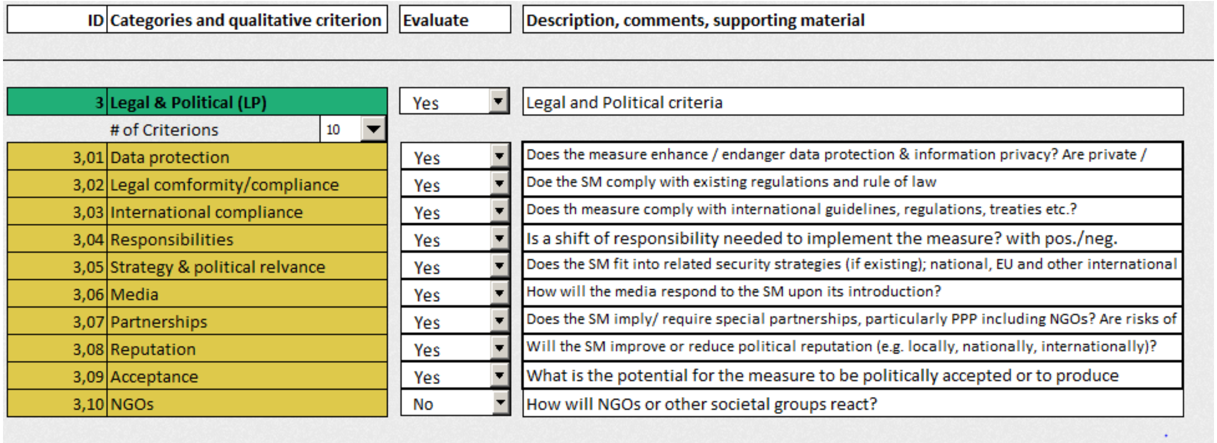
When structuring the criteria hierarchy, the following recommendations should be followed [19]. The criteria should

- Be complete (no important criterion missing);
- Not complex (Too complex criteria be better split into different independent simple criteria;
- Measurable (Here not in physical or monetary scales but in a clear set of descriptors, the simplest one being e.g. "high, medium low". The number[16] and type of descriptors can be chosen different for each criterion;
- Be understood by all and be operational (clearly defined and agreed);
- Be decomposable (structuring in a tree);
- Have no or limited and identified redundancies to other criteria (see "overlaps" and "dependencies below");
- Be as far as possible "judgmental independent" [17];
- Be concise and reasonable in number (cover all important aspects but don't get lost in too many details and fine-structuring).

The system offers a set of predefined categories and criteria described in chapters 3.3 and 3.4, respectively. The user can choose those which appear relevant to the evaluation context which we have called "Session". The user can also insert additional categories and criteria if the available ones are not sufficient or exhaustive. Thus the steps necessary are:

1. Selection of categories and criteria;
2. Inserting new categories and criteria (optional);
3. (Specify overlaps of criteria);
4. (Specify dependencies between criteria).

Steps 3 and 4 are not yet implemented in the software. They are recommended to be regarded in future full-scale evaluations.



ID	Categories and qualitative criterion		Evaluate	Description, comments, supporting material
3	Legal & Political (LP)		Yes ▾	Legal and Political criteria
	# of Criterions	10 ▾		
3,01	Data protection		Yes ▾	Does the measure enhance / endanger data protection & information privacy? Are private /
3,02	Legal comformity/compliance		Yes ▾	Doe the SM comply with existing regulations and rule of law
3,03	International compliance		Yes ▾	Does th measure comply with international guidelines, regulations, treaties etc.?
3,04	Responsibilities		Yes ▾	Is a shift of responsibility needed to implement the measure? with pos./neg.
3,05	Strategy & political relvance		Yes ▾	Does the SM fit into related security strategies (if existing); national, EU and other international
3,06	Media		Yes ▾	How will the media respond to the SM upon its introduction?
3,07	Partnerships		Yes ▾	Does the SM imply/ require special partnerships, particularly PPP including NGOs? Are risks of
3,08	Reputation		Yes ▾	Will the SM improve or reduce political reputation (e.g. locally, nationally, internationally)?
3,09	Acceptance		Yes ▾	What is the potential for the measure to be politically accepted or to produce
3,10	NGOs		No ▾	How will NGOs or other societal groups react?

Figure 2: Categories and Criteria

[16] present tool limit is 10

4.4.1.2 Utility functions and thresholds

The possible effects, in some literature also called the performance of a criterion regarding the problem to be evaluated, in our case the ECOSSIAN system in the specified evaluation session (defined in chapters 4.4.1 and 4.4.2) are described in verbal attributes. E.g. the user acceptance of a system may have the range: -not usable -difficult to use -needs extensive training –need some instruction - easy to self-learn – perfect. The Utility Function transforms this verbal scale into a numerical scale between -10 and +10 (see Figure 3).

Source:
Eval. Session #1
Criterion # 2.02
Compensation of side-effects

Threshold level: -3

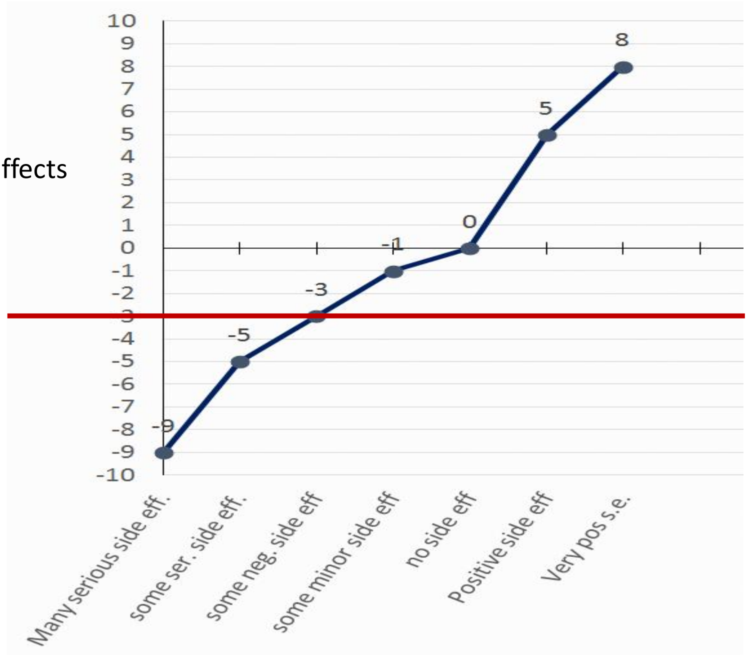


Figure 3: A typical Utility Function

In addition, the user has the option to set a threshold. Thresholds can be defined as e.g. warning indicators or for "k.o. Criteria". If the set threshold in the evaluation process is exceeded (usually the evaluated criterion staying below the set threshold, the user of the tool receives a notification. Then the evaluator may discuss the criticality, modify (not manipulate) the evaluation or abandon the security measure evaluated as not compliant wit set minimum standards (killer criteria). The user marks the criterion as "Killer" Criterion and sets a value in the UF.

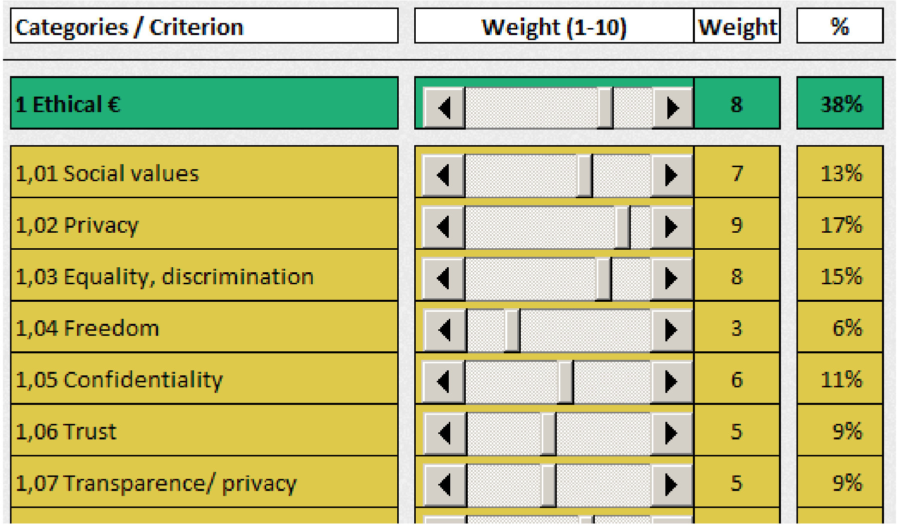
4.4.1.3 Weightings

Weightings characterize the importance of a category relative to the other categories, within one session, and the importance of a criterion relative to the other criteria within one category. The user can choose (using the slider) from a scale between 0 and 10. Weightings of all categories are automatically normalized to add up to 100%, weightings of all criteria within one category also add up to 100% (right column in Figure 4).

There are two options of generating weights, depending on the cases set according to chapter 4.3.2:

(a) If the objectives and the evaluators are of similar type, it is suggested that weightings of categories and of criteria are the same across all cases.

(b) If we have different evaluators or groups of evaluators, each one may want to set his/her own weighting values because they have differing mind sets of preferences.

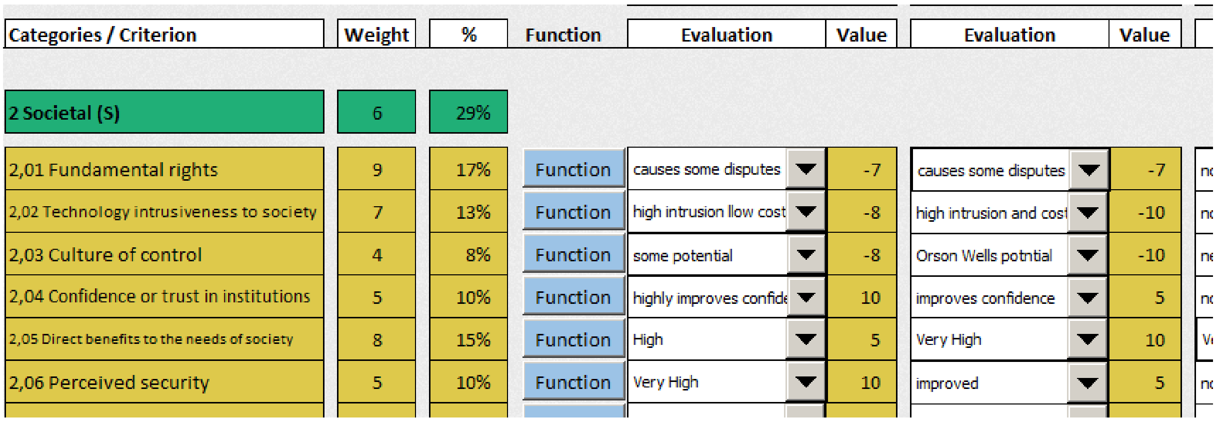


Categories / Criterion	Weight (1-10)	Weight	%
1 Ethical €		8	38%
1,01 Social values		7	13%
1,02 Privacy		9	17%
1,03 Equality, discrimination		8	15%
1,04 Freedom		3	6%
1,05 Confidentiality		6	11%
1,06 Trust		5	9%
1,07 Transparence/ privacy		5	9%

Figure 4: Weighting Input

4.4.2 Evaluation

Evaluation is done for each "case" in a session (right columns in Figure 5). Hitting the down arrow, a pop-up menu shows the verbal descriptors of the possible effects of a criterion. The evaluator chooses the descriptor he believes is appropriate. In the column to the right, the corresponding value from the UF appears. For explanation purposes he can view the UF (button "Function"). Do not re-iterate for purposes of manipulation!



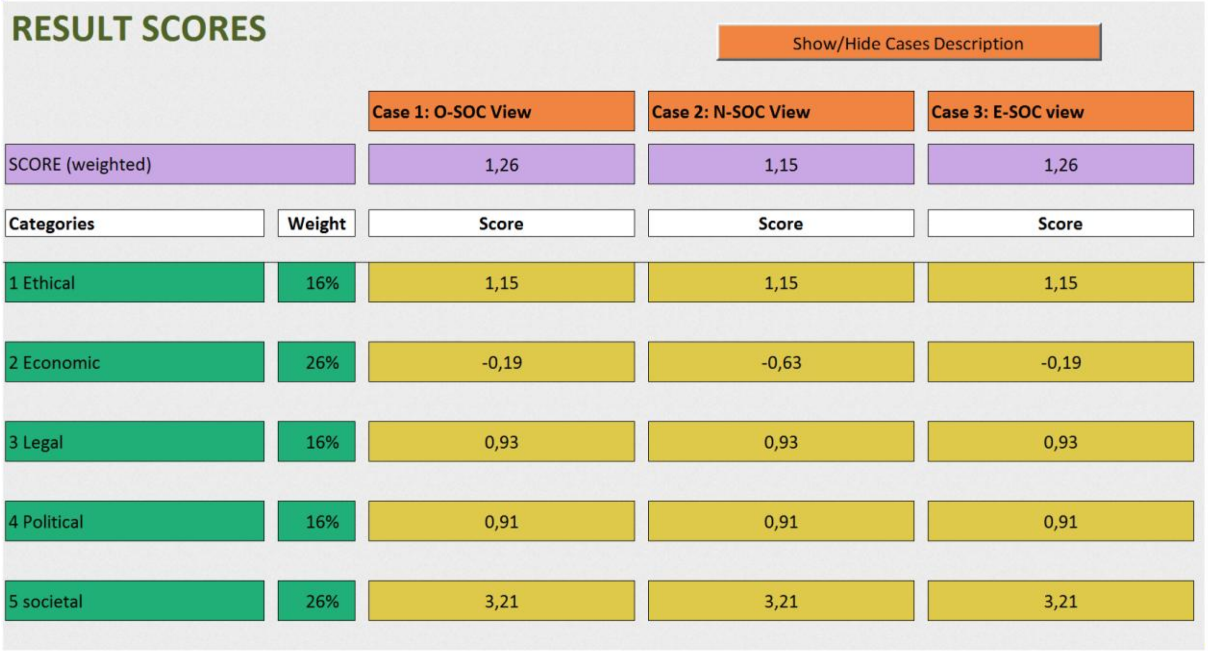
Categories / Criterion	Weight	%	Function	Evaluation	Value	Evaluation	Value	
2 Societal (S)	6	29%						
2,01 Fundamental rights	9	17%	Function	causes some disputes	-7	causes some disputes	-7	nc
2,02 Technology intrusiveness to society	7	13%	Function	high intrusion llow cost	-8	high intrusion and cost	-10	nc
2,03 Culture of control	4	8%	Function	some potential	-8	Orson Wells potntial	-10	ne
2,04 Confidence or trust in institutions	5	10%	Function	highly improves confide	10	improves confidence	5	nc
2,05 Direct benefits to the needs of society	8	15%	Function	High	5	Very High	10	Ve
2,06 Perceived security	5	10%	Function	Very High	10	improved	5	nc

Figure 5: Evaluation

4.4.3 View Results

4.4.3.1 Numerical results

The numbers presented in Figure 6 are summaries of the weighted scores per category.



RESULT SCORES

		Case 1: O-SOC View	Case 2: N-SOC View	Case 3: E-SOC view
SCORE (weighted)		1,26	1,15	1,26
Categories	Weight	Score	Score	Score
1 Ethical	16%	1,15	1,15	1,15
2 Economic	26%	-0,19	-0,63	-0,19
3 Legal	16%	0,93	0,93	0,93
4 Political	16%	0,91	0,91	0,91
5 societal	26%	3,21	3,21	3,21

Figure 6: Result numbers

4.4.3.2 Graphics

Figure 7 is a sample of score results of individual criteria within one category (Ethical) showing the unweighted scores and the scores multiplied with the weighting factors. These types of results are generated for all 6 Sessions and Cases as evaluated in Chapter 5.

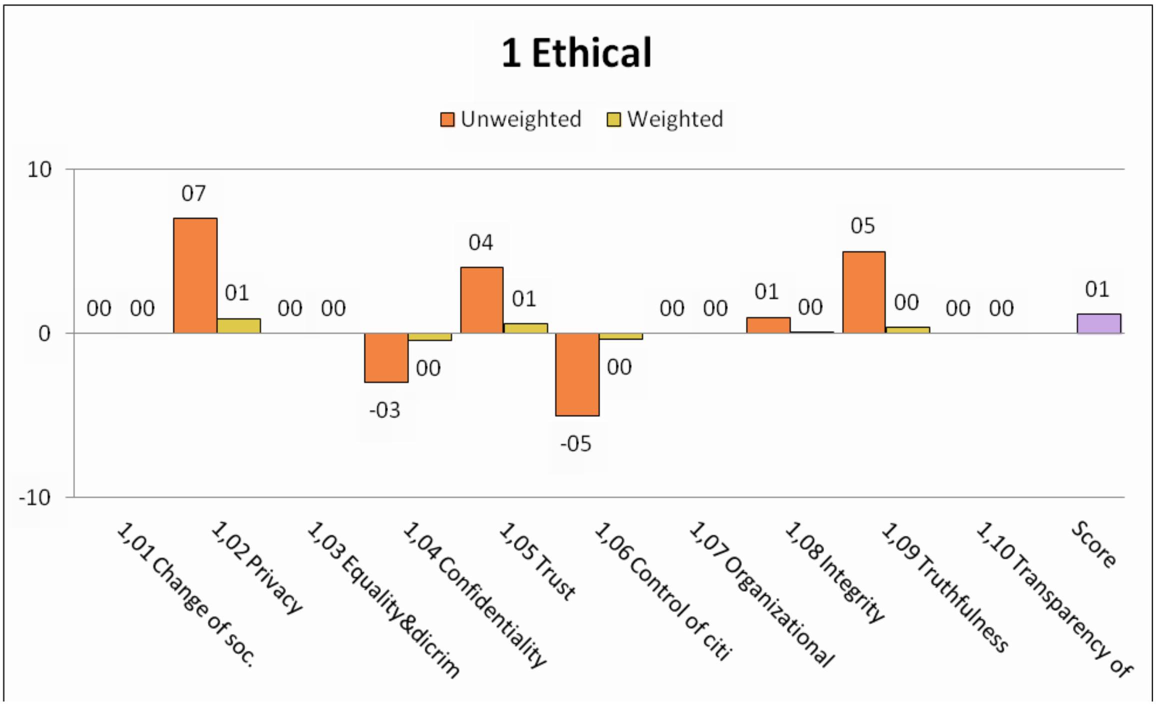


Figure 7: Result bar charts

4.4.3.3 Threshold treatment

Thresholds are defined as indicators or for so called "Killer Criteria". If the threshold in the evaluation process is exceeded, the user of the tool receives a notification. Then the evaluator should discuss the criticality, the evaluation has for the measure evaluated as not compliant with set minimum standards (k.o. criteria). Solutions may be redesign and re-evaluation of the measure or its complete abandoning. In any case, the user needs to be aware of the manipulation potential when tailoring solutions.

4.5 Exploration Analyses and Manipulation

The EELPS offers for tailoring the type of evaluation to the needs of the decision makers and other framework conditions.

- Sensitivity analysis e.g. of parameters which involve uncertainties. The results will show the impact if the parameters would change;
- Parametric analyses by varying system parameters and related criteria that the decision maker is entitled to still change;
- Varying parameters of the cases, e.g. by stepping into the role of a potential opponent and create some perception of how (s)he may evaluate;
- Allowing different weightings and evaluations by different users e.g. for testing the stability of results for preferred options;
- Backtracking, finding pressure points, e.g. if outcomes are too drastic and would jeopardize any solution;
- **Manipulation:** Be very aware of the difference between exploration and manipulation
    - With exploration analyses (bullets above), someone is interested in more detail, wants to see specific impacts, cause and effects, thinks he has forgotten something important etc.
    - With manipulation, someone wants to change results in the direction of his interest or bias.

It is therefore strongly suggested to perform EELPS evaluations under the supervision of an experienced and commonly accepted absolutely neutral moderator.

Chapter 5 Exemplary ECOSSIAN Evaluations

The evaluations of the ECOSSIAN system in this chapter serve several objectives in terms of

1. Demonstrating and validating the EELPS methodology and of the underlying tool in a sets of different framework conditions as stakeholder/evaluator type, different threat assumptions etc.
2. Comparing and rationalizing different evaluation samples.
3. Validating a prepared set of tool parameters – the criteria scheme, weightings, utility functions etc.
4. Deriving practical guidance for preparing sound and successful evaluations in addition to the more formal and technical evaluation steps described in Chapter 4.
5. Gathering input from the ECOSSIAN system demonstrations that address EELPS topics that appear interesting for external stakeholders.

The basic technical processes for evaluating the ECOSSIAN system have been discussed in Chapter 4. It became obvious, that within the scope of task 7.5 with 5.4 PMs, only some selected demonstrations of socio-political evaluation can be given. The main deliverable of this WP is to provide this methodology. It will be available and should be adopted and applied in full scale for the implementation process of the ECOSSIAN system, before huge investments would be done for introducing the ECOSSIAN system in Europe. This full-scale evaluation is estimated to require about 30 to 40 PMs.

5.1 Preparing the Evaluations

5.1.1 Main purpose(s)

These are sample evaluations for demonstrating the system of categories and criteria, and the methodology and tool for evaluating the EELPS implications of the ECOSSIAN system. The different sessions will show the differences in "Views" of the various evaluators and their perspectives. The selected evaluators were asked to assume certain roles of the CIP world.

In real world evaluations, before a sound evaluation can start, it would require a huge effort

(a) for creating common understanding and consensus among evaluators from different organizations about the selected criteria and the definitions, and

(b) of detailed analysis of the (expected) impact of the ECOSSIAN with regard to the individual criteria.

5.1.2 Framework conditions

These above mentioned detailed analyses, however, are outside the scope of the ECOSSIAN project. But the analyses of the Session sample evaluations should give an impression on the power and limitations of the EELPS method. Conclusions and some guidance for future application will be drawn.

There are also still some methodological limitations (e.g. overlaps, dependencies, killer – criteria) that need to be mitigated before future "real life" evaluations.

CESS has the option to use the full-scale JAVA-based version that has been developed in the projects ValueSec and CIRAS, and implemented on a platform at the company ATOS, Spain. Full scale professional use, however, would require separate agreements with ATOS.

In order to limit the effort of the evaluations, it was recommended to keep the scheme of criteria, the relative weightings and the pre-designed utility functions unchanged. In future "real world" conditions, they will be selected and set, respectively, by the evaluating community.

5.1.3 EELPS evaluation preparation

The main technical steps to be performed for arriving at this EELPS evaluation have been discussed in Chapter 4. The process for this applied evaluation consisted of:

- Basic discussion and agreement on the need and benefits of doing such an EELPS evaluation;
- Development of the scheme of categories and criteria (see chapter3.5);
- Development of the tool;
- Implementation of data into the tool;
    - Categories and Criteria;
    - Relative weightings;
    - Utility functions;
- Discussion of the quality of the input;
- Guidance for application of the tool.

Finally, the 6 Sessions for evaluation were specified in order to demonstrate the scope of the tool in different parameter settings (see chapter 5.2).

5.1.4 Process of evaluation

The evaluation started with setting evaluation Sessions and agreeing them in WP7.

In the WP7 Workshop on 6th July 2016 at KU Leuven, the evaluation approach was presented and agreed. Selected team members ("Moderators"), different for each session, were tasked to perform the evaluations. Moderators were asked to adopt certain evaluator roles as set in the sessions.

Also the EEA was asked to also perform at least one session evaluation.

The moderators were tasked via e-mail message of 14th September 2016, supported by further guidance on 3rd October 2016, as follows (quotation):

> ***Dear (Moderator Name),***
>
> *"You or someone of your organization should act as a moderator of preparing and performing individual session evaluations. You should either be able to adapt/emulate the role of the evaluator type you will find in the XLS template (explained below), or you may consult persons from your organizations or from any stakeholder network, to assist you.*
>
> *The assessment method was taken from another EU project (http://www.valuesec.eu). It is a classical "Multi-Criteria Decision Analysis" (MCDA) that can be applied to complex planning and decision processes in security. It has been adapted to the ECOSSIAN specifics, in Task7.5. In addition, an EXCEL based tool has been developed to support efficient evaluation.*
>
> *In its main sense, the ECOSSIAN system when it came to its implementation, would be an implementation of a highly complex security measure across EUROPE that*

needs to be seen and evaluated against its benefits, but also against its ethical, qualitative economical, legal, political and societal implications.

This evaluation can be seen from very different views (session parameters):

- *The system (the "Security Measure") deployment and type of operation (e.g. local, EU-wide etc.)*
- *The category of evaluator (e.g. CI-operator, politician, societal interest group, …)*
- *The objective of the evaluation (e.g. expected societal or political acceptance)*
- *The assumed threat and scenario in which the system might operate and show its benefits (and also its possible deficits)*

Variations of these parameters are set in 6 "Sessions". The sessions are documented in the attached "Different EELPS Sessions & Case Parameters.docx".

It is evident that a sound and full-scale evaluation in the end would need substantial preparation and solid analyses of the different factors of influence. These factors can be positive (e.g. improving economic resilience of the CI in question) or negative (e.g. causing protests and scepticism in society).

Consequently, within the ECOSSIAN project we can only demonstrate a selected number of evaluation "Sessions", and finally offer the methodology to the future decision makers for supporting the planning and decision process of implementing an ECOSSIAN-type system.

Where are we TODAY?

The method has been prepared for this task since the start of ECOSSIAN

1. *A set of defined EELPS* ***categories and criteria*** *has been agreed between KUL and CESS*
2. *An EXCEL-based tool for the EELPS evaluation of the ECOSSIAN system has been developed. Attached is the template "ECOSS-EELPS-valuation on V37-Templ.f.sessX …" (your session), and a sample evaluation session for session 1 " ECOSS-EELPS-valuation-Session1 CESS.xlsm"*
3. *Presentation and discussion of this approach, the criteria and the tool in the WP7* ***workshop on 06. July*** *in Leuven (minutes on SVN)*
4. *Documentation of the methodology, the criteria (incl. definitions and explanations), the tool and an* ***application guide*** *(Chapter5) in the draft D7.11, V1.7 (in SVN under WP7). The tool also contains in its main menu a shortened version of the guide (upper right button)*
5. *Preparation of a set of 6 different evaluation* ***sessions*** *tool-templates that facilitate the evaluation of the ECOSSIAN system in different threat environments, different deployments and from different user points of view. One session has 3 "Cases" with variations of a main parameter*
6. *Assignment to these sessions, of ECOSSIAN staff ("Moderators") who should perform such evaluations (see attachment "Different EELPS Sessions & Case Parameters.docx")*
7. *We asked TEC to facilitate the support of the EELPS evaluations by the Ethical Advisor (pending)*

In case you are not a moderator but interested in this tool, we invite you to have a look at it and provide us your feedback!

Each MODERATOR *is asked to perform these steps:*

1. *If this is all too strange and abstract, pls. familiarize with the rationale, approach and methodology (chpts. 2 and 3 in D7.3, V1.7 on SVN)*
2. *Open your XLS Template; View your session parameters which are already pre-set under "Set Eval. Session"*
3. *Familiarize with the tool and the criteria. When first opening it, you may need to activate the Macros ("Options" in the top line at security warning; "activate…" in the pop-up menu). Some distortions of buttons may show in the tool, which are produced by different XLS-versions, but have no influence on functionality*
4. *Read the Guide (Guide Button); if this is too short, see chpt.4 in D7.11, V1.7 on SVN*
5. *"Set Cat.& Crit.":Sort out criteria you think are irrelevant for your session, by clicking "no". At this phase, we do not recommend to insert new criteria at the moment as this would complicate the comparison between sessions*
6. *Ignore at the moment "Utility Functions" (they are pre-set) and "Killer Criteria" (We don't use them now; samples can be visited in the attached session1)*
7. *"Weighting" (means relative importance in your decision (session) situation): 1. chose the relative weightings of the 5 Categories (EELPS), 2. Chose the relative weightings of the Criteria within each category*
8. *"Evaluation": Select in each Case column the attribute which fits best to the individual criterion in that case. Do it per case and for each criterion*
9. *View numerical and graphical results.*
10. *You my run a copy of the XLS template and do any experimentation if you like.*

Please feel free to ask any questions and ask for any support.

Concerning schedule, after a likely process of iterations, we aim at having the first consolidated set of session evaluations finished by early December" (2016).

-End quotation -
Verbal feedback in terms of questions, comments and recommendations were also requested.

5.2 Terms used:

In the following chapters, we use the term "Evaluation" for the application of the tool to the individual sessions and the underlying Cases. The term "Analysis" is applied to the process of extracting and interpreting results from the evaluations.

Analysis of all Evaluations

The evaluations **demonstrate** the capabilities of the methodology but also give sample results that can be used as baseline for future evaluation in the real world.
Parametric variations will include

1. The main ES operational application setting (O-SOC/N-SOC/E-SOC);
2. The type of evaluator, e.g. planners, decision makers, lawyers, NGO, ...
3. The different evaluation background and focus (correlated to 2.), e.g. system resilience, cost-effectiveness, political implications;
4. Threat assumption: e.g. small "every day" incidents, medium size events, massive attack with catastrophic impact.

For all 6 sample evaluation sessions, the evaluation objective (3.) was kept the same, namely the demonstration and validation of the capabilities of the EELPS methodology and tool. In future, real life evaluations this will be replaced by the objectives of the decision makers.
The analysis of results of the sessions (high and low marks) is a summary concentrating on relative high and low marks and differences between the 3 Cases within a session. The full-scale evaluations are documented in the EXCEL tool sets. For full understanding of the

extracted findings below, it is also helpful to visit the criteria definitions in the tool and the explanations given in D7.11.
The analysis comprises mainly

- Extraction of significant findings of the ES evaluations;
- Comparison of Cases within a session;
- Discussion of important comments concerning both, the evaluations and the methodology/tool itself;
- A summary evaluation and conclusions.

An analysis has been performed for each individual evaluation session. The first table in each session shows the parameters as set for the session. Usually, one parameter is varied in a Session, forming three different Cases per session. A summary of the sessions is given in Table 13 below. The full description of all Sessions is given Annex 5: ECOSSIAN EELPS Evaluation Sessions.

Table 13: Overview of Evaluations sessions

Session #	Evaluator	Variable Parameter	Case 1	Case 2	Case 3	Other settings
1	CESS	Evaluator type	System designer/researcher	CI provider	Political stakeholder	Massive cyber terror attack
2a	KUL	Evaluator type	Lawyer	Human rights activist	CI operator	Normal operations; small incident
2b	EEA[17]	Evaluator type	Lawyer	Human rights activist	CI operator	Normal operations; small incidents
3	UNIBO	Evaluator type	Lawyer	Human rights activist	CI operator	Massive cyber terror attack
4	PI	Scenario	Normal day-to-day business	Medium size attacks	Massive cyber terror attack	CI operator view
5	INOV	System operation	O-SOC	N-SOC	E-SOC	CI operator view
6	INOV	System operation	O-SOC	N-SOC	E-SOC	Politician's view

Each analysis of the following session evaluations begins with a table showing the full set of parameters as assumed for the session, and the colour-marked main variable.
All session evaluations in chapters 5.2.1 to 5.2.6 have the same structure in the form of tables. The title of the table can be found in the upper left box of the tables, Additional formal table headers have been omitted deliberately..

[17] External Ethical Advisor

5.2.1 Session1: Evaluator CESS

The purpose of session 1 evaluations was to demonstrate whether and how different evaluator types may assess the ES. Evaluator types were assumed to be
Case1: Researcher, system designer, developer
Case2: CI provider mainly responsible for implementing and operating ES
Case3: Politician responsible for creating the adequate legal and economic environment
It was assumed that the system will operate at full scale at all three levels, and that the system will encounter massive cyber attacks

Major observations of the tool-based evaluations

Session/ Case Parameters	Case 1: Research View	Case 2: CI View	Case 3: Political View
Security Measure	ES at all 3 levels	ES at all 3 levels	ES at all 3 levels
Evaluator Type	System Designer	CI provider (fict.)	Politician (fict.)
Evaluation Objective	Meth/Tool. Demonstration	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.
Scenario/Use Case	Massive Cyber Terror Attack	Massive Cyber Terror Attack	Massive Cyber Terror Attack

The variable parameter is marked.

Analysis

Case1:System Designer View	Positive observations / scores	Negative observations / scores
Summary across all categories	No very significant + and -; very positive societal effects	legal barriers expected
1.Ethical	No discrimination expected Truthfulness of expected effects Protection of personal information	Interference with privacy Trust building measures needed Fear of control of citizens

Case1:System Designer View	**Positive observations / scores**	**Negative observations / scores**
		Missing transparency (of what the system is really doing)
2.Economic	Contribution to economic stability Good cost-benefit Supports cooperation Some market advantage	Economic benefit uncertain Validation necessary Dependence on other sectors & organizations and on technologies
3.Legal	.	Legal conformity unclear Legally just compensation of potential system failures
4.Political	Can supports political CIP strategy Increases political reputation	Unclear political responsibilities Possible negative media reactions May support political opportunism Implies political risks
5.Societal	Direct benefits to society Positive impact on health Improves societal preparedness to cope with risks ES does not create additional risks to society	Some fear of intrusion of technology into society Some reservations concerning technology & processes

Case2: CI Provider View	**Positive observations / scores**	**Negative observations / scores**
Summary across all categories	Substantial economic benefit expected Positive effects on and consideration by society	Some political obstacles expected
1.Ethical	Positive impact on social values No risk of equal treatment and discrimination	Potential of control over citizens

Case2: CI Provider View	**Positive observations / scores**	**Negative observations / scores**
	No danger of confidentiality breaches Good trust in the system Trust: ES provides response to a real threat	
2.Economic	Very high ratings of ES improving • Economic stability • cost-benefit and economic benefit • cooperation • market opportunities	Some risks from dependency on other sectors
3.Legal	Advantage of setting standards	Some difficulties with international compliance
4.Political	Some media support expected Strong improvement of reputation Opportune to political agendas	Shift of responsibilities strongly needed May deviate from political strategies Difficulties in political acceptance May create political risks
5.Societal	Positive to very positive impact in most societal criteria expected (societal benefits, perceived security, health impact, no additional risks	None

Case3: Political View	**Positive observations / scores**	**Negative observations / scores**
Summary across all categories	High positive economic impact Good legal compliance Support political interests Positive societal effect	None
1.Ethical	No discrimination potential	Risks of privacy violations

Case3: Political View	Positive observations / scores	Negative observations / scores
	Good personal information protection True protection against real risks Would become a transparent security measure	
2.Economic	All economic criteria rated high to very high	Except: risk of depending on ...technology (neutral)
3.Legal	Legal national and international conformity given A fair and just system Policy can accomplish to fill legal gaps	None
4.Political	Shift of responsibilities seen very positive Supports political strategy Improves political reputation and acceptance No risk seen at all of opportunistic abuse Positive reactions from NGOs expected	None
5.Societal	Good societal benefits Positive impact on health Improves preparedness of society No additional risks for society Information exploitation no problem	Will not improve security perception Society may object to the introduction

Summary of Comments, Session1
Evaluator: Reinhard Hutter, CESS

Relevant Category or Criterion	Findings	Recommendation from Analyst[18] Blank = None or N/A
General	It becomes obvious in which categories and criteria the 3 different evaluator type assess the system effects different	
Ethical	Ethical evaluation is evaluated by the research oriented evaluator more critical concerning the potential of increased control of citizens, and the transparency of the system. Potential privacy violations is hitting the negative k.o. threshold	
Economic	Economic effects are evaluated very positive in the CI view and the political view; a bit more sceptical by the researcher	
Legal	Similar as with economic evaluation	
Political	Political opportunities are evaluated most positive by the political evaluator	
Societal	Societal impacts are evaluated very positive in the CI view while the political and the researcher vies chow positive as well as few negative effects	
Methodology and tool	The set of criteria is well defined and self-explanatory. The tool is easy to handle. For future use, some more sophisticated functions should be implemented (e.g. concerning criteria independency checking, killer criteria)	Killer criteria can already be applied (not explicitly exercised here, except in Session 1). Other analytical support will require further tool development or use of the ATOS system (see chpt. 4.1).

[18] CESS

5.2.2 Session2 Evaluations

Session2 was evaluated twice, by **KUL and by the EEA** (EXTERNAL Ethical Advisor to ECOSSIAN)

5.2.2.1 Session2a: Evaluator KUL

The purpose of session 2 evaluations was, again, to demonstrate whether and how different evaluator types may assess the ES. Evaluator types were assumed to be
Case1: Lawyer
Case2: Human Rights activist
Case3: CI operator
It was assumed that the system will operate at full scale at all three levels, and that the system will- different from session1 -operate in every-day threat conditions.

Major observations of the tool-based evaluations

Session/ Case Parameter	**Case 1: Lawyer View**	**Case 2: Human Rights View**	**Case 3:CI View**
Security Measure	ES at all 3 levels	ES at all 3 levels	ES at all 3 levels
Evaluator Type (assumed role)	Lawyer	Human Rights activist	CI operator
Evaluation Objective	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.
Scenario/Use Case	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents

The variable parameter is marked.

Analysis

Results of particular relevance are marked

Case1: Lawyer View	Positive observations / scores	Negative observations / scores
Summary across all categories	No significant positive or negative implications	N/A
1.Ethical	Belief in system truthfulness	Integrity and privacy violations, control over citizens expected
2.Economic	Supports economic benefit and cooperation	Influence on economic stability and dependence on technology seen slightly negative
3.Legal	No positive scores	Legal conformity must be proven
4.Political	Very good for political reputation Good political acceptance expected	Political responsibilities are strong obstacle, implying some political risks
5.Societal	Significantly improves preparedness of society at no major risk	Some violations of fundamental rights possible

Case2:Human Rights Activist View	Positive observations / scores	Negative observations / scores
Summary across all categories	No significant positive or negative implications	Some ethical and legal problems expected
1.Ethical	No positive implications expected	Major negative effects concerning • privacy • trust (in the system) • organization integrity and transparency

Case2:Human Rights Activist View	Positive observations / scores	Negative observations / scores
2.Economic	No positive economic impact expected	Dependency on technology may be problematic
3.Legal	No positive legal implications	Legal conformity, Some doubts concerning contractual gaps to be filled
4.Political	Supports political strategy and acceptance	Political responsibility for such system unclear!
5.Societal	Supports preparedness of society	Risk of fundamental rights violation and risks for society seen

Case3: CI Operator View	Positive observations / scores	Negative observations / scores
Summary across all categories	No significant positive or negative implications	
1.Ethical	No problems with privacy truthfulness and transparency expected	Potential of control over citizens
2.Economic	Generally very positive effects expected	...except dependency on technology
3.Legal	No positive ratings	Some problems with legal conformity and contract policies expected
4.Political	Very supportive for political strategy, reputation, acceptance	Political responsibility and risks unclear
5.Societal	Improves preparedness and reduces risks of society	Risk to violate fundamental rights

Summary of Comments, Session2/KUL

Relevant Category or Criterion	Findings	Recommendation from Analyst Blank means None
General	It becomes obvious in which categories and criteria the 3 different evaluator type assess the system effects different	
Ethical	The views on human rights significantly differ (e.g. between the CI operator and the human rights representative	
Economic	Really positive evaluation only by the CI provider	
Legal	Legal problems to be solved is a general an issue All evaluators see the need to clarify political responsibilities	
Political	Significant improvement of political reputation, and compliance with strategy expected	
Societal	High improvement of societal preparedness expected, at the expense risks to violate human rights	
Methodology and tool	The evaluator discusses some deficiencies in the relation of the descriptors ("answers") in the utility functions and the definition of the criteria. Some minor technical bugs still exist (but are of minor relevance for the purpose of these evaluations)	Comments show that for real world evaluations, fine tuning and a common understanding of the criteria definitions and of the utility functions will be a prerequisite. Some technical tool improvements would be suggested

5.2.2.2 Session2b: Evaluator EEA

The purpose of this session 2 evaluations was to receive the feedback from the External Ethical Advisor, in the same settings as assumed for IKUL before.
Case1: Lawyer
Case2: Human Rights activist
Case3: CI operator/Technical View

It was assumed that the system will operate at full scale at all three levels, and that the system will operate –different from session1 -in every-day threat conditions

Major observations of the tool-based evaluations

Session/ Case Parameter	Case 1: Lawyer View	Case 2: Human Rights View	Case 3:Tecnical View
Security Measure	ES at all 3 levels	ES at all 3 levels	ES at all 3 levels
Evaluator Type (assumed role)	Lawyer	Human Rights activist	CI operator
Evaluation Objective	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.
Scenario/Use Case	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents

The variable parameter is marked

AnalysisCase1:Lawyer View	Positive observations / scores	Negative observations / scores
Summary across all categories		Ethical, legal, political reservations/expected negative effects
1.Ethical	Only confidentiality rated slightly positive All other criteria neutral	Privacy, control of citizens and system transparency rated negative
2.Economic	System will support economic stability and economic/market benefits and be cost-effective	System validity and dependence on technology critical
3.Legal	None	All legal implications rated negative (except legal conformity)
4.Political	None	Political risks, Opportunism, NGO reaction

AnalysisCase1:Lawyer View	Positive observations / scores	Negative observations / scores
5.Societal	High direct benefits and improved preparedness of society	Adverse in terms of fundamental rights and technology intrusion

Case2:Human Rights Activist View	Positive observations / scores	Negative observations / scores
Summary across all categories	No positive ratings	Ethical, legal, political and societal reservations/expected negative effects
1.Ethical	No positive ratings	All ethical implications rated negative to very negative
2.Economic	Economic & even environmental benefits;	System validity and dependence on technology critical
3.Legal	None	All legal implications rated negative (except legal conformity)
4.Political	Supports political agendas	Negative media & NGO reactions and other political risks
5.Societal	Preparedness/ awareness of society improves	Adverse in terms of fundamental rights and technology intrusion Negative attitude of society because of expected additional societal risks

Case3:CI Operator/Technical View	Positive observations / scores	Negative observations / scores
Summary across all categories	Moderate/neutral evaluation of ethical and legal implications; positive societal and ethical evaluation	Ethical, legal, political and societal reservations/expected negative effects
1.Ethical	Good compliance with confidentiality and system transparency requirements Some positive effects on society as a whole	No major negative scores
2.Economic	Not evaluated	
3.Legal	None	All legal implications rated negative (except legal conformity and justice)
4.Political	No positive political implications	Political risks, including partnerships
5.Societal	High direct benefits, Improves societal preparedness; positive attitude	No negative scores

Summary of Comments, Session2/EEA

Relevant Category or Criterion	Findings	Recommendation from Analyst
General comments	"When I (EEA) evaluated Ecossian through the lens of a **HR activist**, I adopted the perspective of someone who is afraid of the raising of a "surveillance society" i.e. a society where individuals are routinely monitored for security reasons;	None
	When I (EEA) pretended to be a **lawyer** (I have a background in International and EU law too but I've never practiced as lawyer) my main concern was to assess the compliance of Ecossian with the principle of the rule of law and law certainty. I did also think of the potential (legal) privacy, data"	None

Relevant Category or Criterion	Findings	Recommendation from Analyst
	"As a **CI operator**, I (EEA) pretended to be someone who is fully aware of the potential risks - to the economic well being and stability of a country/society - which may stem from critical infrastructures who are "vulnerable" (because not furthermore protected through Ecossian)"	None
Categories/Criteria	Strong focus on "privacy by design" (PbD) Relative high and numerous socio-political risks and challenges expected from legal and human rights p.o.v., Evaluations from the operator/technical p.o.v., much fewer negative impacts are expected As to the legal conditions, no positive ratings and many negative evaluations of the situation	Will be addressed in great detail in Task 7.3/ D7.10
Methodology and Tool	"In general, I (EEA) found the evaluation test a very useful and informative exercise. For sure, it raises awareness and this is very good (you achieved the goal that is stated in the del). The methodology seems consistent with regard to the tool's goal." Some comments for technical improvement	None

5.2.3 Session3: Evaluator UNIBO

The purpose of this session 3 evaluations was to receive the feedback on system evaluation again from different stakeholder views
Case1: Lawyer
Case2: Human Rights activist
Case3: CI operator
It was assumed that the system will operate at full scale at all three levels, and that the system will operate –different from session2 –under massive Cyber terror threat

Major observations of the tool-based evaluations

Session Parameters	Case 1: Legal View	Case 2: Human Rights View	Case 3: Technical view
Security Measure	ES at all three levels	ES at all three levels	ES at all three levels
Evaluator Type	Lawyer	Human Rights activist	CI operator
Evaluation Objective	Meth/Tool Demonstration	Meth/Tool Demonstration	Meth/Tool Demonstration
Scenario/Use Case	Massive Cyber Terror Attack	Massive Cyber Terror Attack	Massive Cyber Terror Attack

The variable parameter is marked

Analysis

Case1:Lawyer View	Positive observations / scores	Negative observations / scores
Summary across all categories	Very positive evaluation of the legal perspectives	none
1.Ethical	Treatment of confidentiality & integrity issues very positive	Some negative expectations concerning privacy, control of citizens and formation of societal groups (against ES)
2.Economic	Good cost-benefit, general economic and cooperation benefits	Dependency on technology seen critical
3.Legal	Generally (all criteria) positive	None
4.Political	Clear responsibilities Fits political strategy and political acceptance	Some problems with media expected
5.Societal	Very good societal benefits Supports societal preparedness and information	Some reservations concerning fundamental rights and technology intrusion into society

Case1:Lawyer View	Positive observations / scores	Negative observations / scores
	exploitation to society	

Case2:Human Rights Activist View	Positive observations / scores	Negative observations / scores
Summary across all categories	None	Some reservations concerning ethical, legal, political and societal implications
1.Ethical	Positive expectations concerning confidentiality and Trust	Many negative effects in control over citizens, privacy evaluations
2.Economic	Some economic benefits	Deficits in system validation and technology dependency
3.Legal	None	Deficits in legal conformity expected
4.Political	None	Negative expectations concerning media, political acceptance and risks
5.Societal	Good preparedness and exploitation strategy	Fundamental rights and (many) other societal risks

Case3:CI Operator View	Positive observations / scores	Negative observations / scores
Summary across all categories	Similar positive scores as case 1 (legal view); more positive societal effects	None
1.Ethical	Very positive ethical implications (truthfulness; no control over citizens	Only minor concerning confidentiality
2.Economic	Positive in economic effects/market and stability Very good for cooperation	Except dependency on other sectors and on technology

Case3:CI Operator View	Positive observations / scores	Negative observations / scores
3.Legal	Legal criteria evaluated mostly positive	None
4.Political	All "neutral"; some NGO support expected	None
5.Societal	Positive effect for societal benefits, perceived security, preparedness	None

Summary of Comments, Session3

Relevant Category or Criterion	Findings	Recommendation from Analyst
General	Significant differences between the types of evaluators in almost all categories. Differences are explainable from the different perspectives of the evaluators. E.g. on the legal conditions, the human rights view is much more sceptical than the technical and the legal view.	None
Ethical	No further comments received	N/A
Economic	No further comments received	N/A
Legal	No further comments received	N/A
Political	No further comments received	N/A
Societal	No further comments received	N/A
	No further comments received	N/A
Methodology and tool	No further comments received	N/A

5.2.4 Session4: Evaluator PI

The purpose of this session4 evaluations was to receive the feedback from a real CI operator, in our case from the financial sector.
The system should operate at all three levels O-Soc, N-SOC and E-SOC.
The threat level was assumed to vary
Case1: Normal day to day business
Case2: Medium attacks
Case3: Massive Cyber Terror Attack

Major observations of the tool-based evaluations

Session Parameters	Case 1: Normal operation View	Case 2: Medium attack View	Case 3: Massive attack view
Security Measure	ES at all 3 levels	ES at all 3 levels	ES at all 3 levels
Evaluator Type	CI operator	CI operator	CI operator
Evaluation Objective	Meth/Tool Demonstration	Meth/Tool Demonstration	Meth/Tool Demonstration
Scenario/Use Case	Normal day to day business	Medium attacks	Massive Cyber Terror Attack

The variable parameter is marked

Analysis

General remarks: Most of the evaluations are identical across all 3 Cases. I.e. the impacts of the ES are estimated to be relatively independent of the threat level. The exceptions (differences between Cases) are highlighted.

The criteria 2.06 (environment), 4.03 (Media reaction) and 5.05 (health impact) were excluded, assumed not relevant.

Case1/2/3: (no big differences between Cases 1/2/3)	**Positive observations / scores**	**Negative observations / scores**
Summary across all categories	Only positive summary scores Most positive evaluated are political and societal effects	None
1.Ethical	Trust in the system and truthfulness rated very positive. In cases 2 and 3 positive influence on social values expected	Risks concerning control of citizens, building of social groupings and integrity expected. In cases 2 and 3: also privacy violation risks
2.Economic	All economic effects positive to very positive	Except for system validation and dependence on technologies
3.Legal	Legal and international conformity positive. In cases 2 and 3, also the possible contractual solutions rated positive	The problem of fairness in case of system failure is solved insufficiently
4.Political	Compliance with strategy, benefits of partnerships, reputation and NGO reactions rated positive. Political acceptance rises with increasing threat level	Political risks are seen in all 3 cases. In cases 2 an 3 (higher threat levels), the need for changes of responsibilities is considered problematic/unclear
5.Societal	Direct benefits to society, preparedness and risk reduction In cases 2 and 3, perceived security and in case 3 societal attitude become positively obvious	No negative societal impact

Summary of Comments, Session4

Relevant Category or Criterion	Findings	Recommendation from Analyst All: None
General	Remarkably, the CI operator evaluated the political and societal effects very positive, even higher than the economic effects. Most evaluations positive and relative independent of the threat level.	
Ethical	Risk of privacy violation increases in massive threat scenario	
Economic	Generally very positive	
Legal	Regulations/contracts particularly covering massive attack situations needed	
Political	Political acceptance and benefits substantially rise with the threat level	
Societal	Appreciation by society rises with the threat level	
Methodology and tool	None	

5.2.5 Session5: Evaluator INOV

The purpose of this session 2 evaluations was to receive the feedback from a CI operator who views the system characteristics from the different levels of operation:
Case1: O-SOC level
Case2: N-SOC level
Case3: E-SOC level
It was assumed that the system will operate in every-day threat conditions.

Major observations of the tool-based evaluations

Session Parameters	Case 1: O-SOC View	Case 2: N-SOC View	Case 3: E-SOC view
Security Measure	O-SOC	N-SOC	E-SOC
Evaluator Type	CI operator	CI operator	CI operator
Evaluation Objective	Meth/Tool Demonstration	Meth/Tool Demonstration	Meth/Tool Demonstration
Scenario/Use Case	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents

The variable parameter is marked.

Analysis

General remarks: All evaluations are identical across all 3 Cases (one very minor exception). I.e. the impacts of the ES are estimated to be relatively independent of the level at which it operates.

The evaluator reported that he did deliberately not differentiate between the cases as he considers the system to be operating at all levels and evaluation should be the same at all levels

Case1/2/3	Positive observations / scores	Negative observations / scores
Summary across all categories	Average evaluations are positive or slightly positive in all categories Highest scores were given to the societal criteria	None
1.Ethical	Privacy protection and trust and truthfulness were rated high	The potential of confidentiality violations and control of citizens are rated negative
2.Economic	Very high direct economic benefits expected	System Validation processes (upon system

Case1/2/3	Positive observations / scores	Negative observations / scores
	High advantages for cooperation and in the market expected	introduction) are needed Unwanted side effects may occur Dependency on other stakeholders and on technology problematic
3.Legal	Good legal, international and standards conformity	Deficits in just/ fair compensation in case of system failure are still unclear There are gaps in contracts and policies
4.Political	Very good reputation and political acceptance expected Support of NGOs expected	Problems with creating clear partnerships and clear sharing of responsibilities Possible conflicts with national political strategy will include political risks
5.Societal	Medium to high benefits of security and perceived security Positive attitude and better preparedness of society expected	None

Summary of Comments, Session5

Relevant Category or Criterion	Findings	Recommendation from Analyst All: None
General	At average, mainly positive to neutral scores The question was discussed whether ECOSSIAN has a role or not in real disaster situations has been discussed	
Ethical	Positive and negative ethical effects appear balanced	
Economic	High inclination between very positive and very negative impacts	

Relevant Category or Criterion	Findings	Recommendation from Analyst All: None
Legal	High inclination between very positive and very negative impacts	
Political	High inclination between very positive and very negative impacts	
Societal	Generally high positive societal impacts	
Methodology and tool		
	".... these EELPS evaluations are really important for assessing the ECOSSIAN contribution and challenges ahead, as well as to promote continual improvement of cyber security. The ECOSSIAN system is just an instrument. The benefits/risks/costs will depend on the "way that we use it". The ECOSSIAN system was developed with little context being provided regarding actual business, management & operational conditions. That's why I believe that WP7 will be key to the ECOSSIAN systems' success!"	
	The differentiation of the evaluations into different cases of evaluators and threat levels seemed not practicable (only "current" opinion of the evaluator).	
	"The interesting part of these questionnaires is precisely to generate discussions, in order to elicit informal feedback - that complements the formal feedback".	

5.2.6 *Session6: Evaluator INOV*

The purpose of this session 2 evaluations was to receive the feedback from a CI operator who views the system characteristics from the different levels of operation:
Case1: O-SOC level
Case2: N-SOC level
Case3: E-SOC level
It was assumed that the system will operate –compared to Session 5 -under massive Cyber terrorist attack
Major observations of the tool-based evaluations

Session Parameters	**Case 1/2/3**
Security Measure	O-SOC or N-SOC or E-SOC
Evaluator Type	Politician
Evaluation Objective	Meth/Tool Demonstration
Scenario/Use Case	Massive Cyber Terror Attack [19]

The variable parameter is marked.

Analysis

General observation: No differences have been identified between Session5 (CI operator/ normal operation and) Session 6 (Politician/ operation in massive cyber attack).

The evaluators reported that they did not adopt the two different evaluator roles and did not differentiate the valuation between the different threat levels, in session5 and session6, respectively.

Therefore, the evaluations of session 5 and 6 are identical.

[19] compared to Session5

5.3 EELPS Evaluations from the Demonstrations

Closing in on the decisive stage of the ECOSSIAN project, efforts are on-going to prove the concept and the system focus and operational and technical capabilities. In the demonstrations, attacks against three different types of critical infrastructures are simulated in three distinct national cyber security environments. In combining the findings and results of these three national demonstrations, the concluding international demonstration will mark the end of the ECOSSIAN system validation.

Predominantly characterized by the technical nature of the project, the associated evaluation process primarily concentrated on the functional values and benefits of the ECOSSIAN system. However, as discussed in the preceding chapters, ethical, economical, legal, political, and societal issues do have a significant influence and bearing on any security related project. In consequence, the evaluation "pillar" specifically dealing with these EELPS issues has been implemented also in the demonstrations as one of the four evaluation pillars applied.

1. Functional Requirements evaluation
2. Non-functional Requirements evaluation
3. Evaluation of Demonstration Planning and Execution
4. LES Evaluations

The extensive sample evaluations as documented in this deliverable in detail substantiate the validity and essence of the overall EELPS evaluation effort. To complement this effort, each demonstration also included an EELPS questionnaire in order to capture the views from stakeholders present at the respective demonstration with a selection of questions of the LES[20] categories. However, scale and scope of the demonstrations, time available for answering questionnaires and the limited number of respondents and their specific professional background did not yield representative results over the complete range of EELPS issues. For the demonstration questionnaires see D6.4 and for the detailed Evaluation Report & Recommendations see D5.8. Here we give only some typical evaluation samples.

Below Table 14 and Table 15 show the numbers and organization types of respondents and in the different demonstrations, their specific relation to an SOC, and the respective scores given by the participants.

Table 14: Overview of Participants in the ECOSSIAN Demonstrations

Demonstration	ITA[21]	POR	IRL	INT
Government/Administration	4	2		2
System Integration/Engineering Services	2		4	
Public Transport	2	5		
Energy		1	3	2
Gas Utility			2	

[20] Legal, Ethical, Societal

[21] ITA – Italian, POR – Portuguese, IRL – Irish, INT - International

Demonstration	ITA[21]	POR	IRL	INT
Finance/Banking/Insurance	1			
Tele Communications		2		2
Academia/Research		1	1	2
Law Enforcement	1			2
Other		4		9

Table 15: Relationship of above participants with SOCs

Demonstration	ITA	POR	IRL	INT
OSOC	6	2	1	4
NSOC	4	2		2
ESOC				

Table 16: Overview and comparison of cumulated LES scores

	EELPS (LES) **Questions**	**ITA** **08 Nov** **2016**	**POR** **16 Feb** **2017**	**IRL** **01 Mar** **2017**	**INT** **26 Apr** **2017**
	Type of **Critical Infrastructure demonstrated**	**Finance** **Sector**	**Transp.** **Sector**	**Energy** **Sector**	**Non-specific**
	ECOSSIAN complies with existing regulations and the rule of law.	**3,5**	**4,0**	**3,9**	3,6
2	ECOSSIAN is compatible with human rights principles and values such as human dignity, freedom, equality and solidarity.[22]			**3,9**	
3	ECOSSIAN has not the potential to create political risks.	**3,6**	**3.3**	**3,3**	3,5
4	ECOSSIAN has not the potential to increase control over people or society.[23]			**3,2**	3,7

[22] Question asked in the Irish demo only.

[23] Question asked in the Irish demo only.

	EELPS (LES) Questions	ITA 08 Nov 2016	POR 16 Feb 2017	IRL 01 Mar 2017	INT 26 Apr 2017
5	ECOSSIAN fits into related national security strategies.	**4,0**	**4,1**	**3,5**	
6	The ECOSSIAN system does not create major data protection risks.[24]	**3,9**	**3,3**		3,4
7	The ECOSSIAN system creates data protection risks.			**3,3**	
8	ECOSSIAN contributes to or influences positively economic stability.[25]			**3,8**	
9	ECOSSIAN is open and transparent in terms of how it handles security related information.	**4,3**	**3,8**	**3,7**	3,9

Key:
1 – strongly disagree,
2 – disagree,
3 – neither disagree nor agree,
4 – agree,
5 – strongly agree

The statistical results in Table 16 show that responders were positive, individual scores behind ranging mainly between neutral and up to "strongly agree". The scores in the right columns address varying question lines. This is due to the fact that different sets of questions were used in the different sessions. The general score level is comparable to that of the detailed evaluations in chapter 0. There may be the potential of creating more control over people possible (line 4 in Table above). Risks concerning data protection are indicated (Lines 6/7). Most positively evaluated was compliance with existing regulations, line1 (which will be discussed in further detail in D7.10/11), as well as system transparency and handling of security related information (line 9).

From an analytical point of view, there is only limited value to compare the results from the 6 sessions with those from the demonstrations by a number of reasons:

- The main objective of the session evaluations (chapter 0) was to demonstrate the capabilities and to prove the benefits of the EELPS **methodology.**
- The main objective of the EELPS questionnaires (this chapter) and related evaluation during the demonstrations was to receive feedback on an EELPS-related evaluation of the ECOSSIAN **system.**
- The questions to external stakeholders were rather high-level and limited in number while the EELPS tool provides a very detailed scheme of evaluation criteria.
- The evaluation scale, due to the character of the two evaluation types, had to be different: Degree of agreement in the questionnaires (see 5 levels above) vs. a scale between -10 and +10 in the EELPS tool.

[24] Question was slightly different (complementary) in the Irish demo: see next line in table

[25] Question asked in the Irish demo only.

- The demonstration-related evaluations are narrow but rather reality-oriented (concrete scenarios).
- The Session evaluations with the tools span a large range of parameters but were more of a theoretical character.

Nevertheless, both evaluations are cornerstones in approaching the numerous qualitative factors of influence a system such as ECOSSIAN will imply in the socio-political area, and they need to be assessed. One common conclusion, nevertheless, can be drawn: The evaluation of the system in both exercises by external stakeholders – governmental and politically oriented people and by CI stakeholders of the team were very positive at average values level.

Chapter 6 Concluding Summary

6.1 Summary of the Analyses Results

General:
The methodology was considered very important for raising awareness of the different EELPS implications such a complex system like ECOSSIAN will create. Visualizing the results in the graphical displays on a pseudo-quantitative scale substantially eases interpretation and comparisons between different sessions and different cases within a session. For all 6 sessions, all results have been documented and archived, including per session:

- The full configuration of the tool, including selected criteria, weighting schemes and utility functions;
- 1 Numerical summary Tables with weighted and unweighted cumulative scores per category;
- 3 summary bar charts, one per Case, of weighted and unweighted cumultive scores per category;
- 15 bar charts showing the weighted and unweighted scores per criterion (in 5 categories X 3 Cases).

The EELPS evaluation is an important complement to the evaluation of the ECOSSIAN system performance and of its functional and technical characteristics.

Results
No differentiation could be identified for the different cases of topology, i.e. whether the system operated at CI, at national or at EU level. At that point of the project, we do not have sufficient feedback from the different stakeholders for that, in particular not from governmental and EU representatives.
Some of the ethical and societal effects are more dominant in real crises (massive attack) compared to those in a relative benign every-day operation.

Nevertheless, the results show considerable variance, pros and cons, positive and negative ratings of criteria within a category. Results are also supported by the findings from the demonstrations. Some summary result is given here in chapter 5.3; Details can be studied in D5.8.
The results are substantially and systematically varying between the different session. I.e. the different evaluator types see such a system from their individual professional perspective. Some tendency could be read from the detailed results, saying that the views from the legal, the Human Rights and from the Technology perspective tend to evaluate the system more sceptically than do the evaluators in the role of CI operators and political decision makers.
This is not a new phenomenon, particularly not in situations where different stakeholder groups with different basic objectives and agendas (here the private sector, politicians and societal groups) need to come to a joint decision. There are two ways out of this seemingly dilemma in a future evaluation situation when the system will be implemented. For both ways it will be a prerequisite to up-front jointly agree on the catalogue of evaluation categories and criteria, on their definitions and descriptions and on the Utility Functions. The subsequent evaluation steps of selection, weightings and criteria evaluation can be made either (1) separately or (2) jointly. (For more details of the process, see Chapter 4).

1. Separate evaluations: Each "party" performs its own evaluation. The results are mutually presented, discussed and a compromise must be found between the decision makers.

2. Joint evaluations: The evaluations are performed in a joint group of the different stakeholders and this one result is accepted by all.

It is strongly recommended to follow the procedure #2 as it considerably reduces effort and time to come to the compromise. It is also suggested that the steps of defining, selecting, weighting the criteria and the creation of utility function are done by an analytically oriented support group while the final evaluation step is performed by the decision makers or their representatives. This process would further reduce effort for dispute and the risk of producing biased results. It requires, however, a strong and independent moderator who keeps the evaluation community stick to the once agreed methodology framework and rules.

More details can be drawn from the individual session evaluations and discussed further. We want, however to remind that these evaluation exercises were primarily made to demonstrate the methodology and the tools and to draw some conclusions for their future application. It lies beyond the scope of ECOSSIAN to produce a full-scale and scientifically fully grounded socio-political (E-E-L-P-S) assessment of the ECOSSIAN system. This will be possible and reasonable only when the concrete end-users of the system will be finally identified, and when the political and legal framework conditions of the nation(s) involved and of the EU level will be clear. The other way around, the tool has a strong potential of supporting the compromises needed between the parties involved. A framework for developing such a public-privat-partnership (PPP) for a system like ECOSSIAN has been developed and documented in D7.10.

6.2 Conclusions and Recommendations

The deliverable gives a rationale on why a systematic evaluation of the socio-political factors is recommended, we think even required, when it comes to the implementation of a system like ECOSSIAN (ES), by a number of reasons:

- ES has the potential of impacting on societal values and individual rights;
- Its success will depend on broad acceptance by societal groups and by politicians and by CI industries;
- It will need substantially new ways of cooperation among CI sector and between CI providers/operators, state bodies and the EU;
- It needs to be or become compliant to national laws and regulations and to the EU CIP strategic endeavours; it may even need new or modified rules of law;
- It will have a number of economic and political implications that imply still a number of uncertainties.

The proposed EELPS solution is based on state of the art methodology that has been validated in numerous other domains. It has been modified to the needs of justifying security measures in general, and to the expected environment of the future ECOSSIAN introduction and operation.

The applicability and quality of EELPS assessment has been validated by a number of different parameter settings and the results analysed. This includes high positive and negative scoring marks and verbal assessments of the value of such a methodology and the quality of the tool. A selection of EELPS related questions was also used in the ECOSSIAN demonstration and its feedback is analysed in D5.8. The evaluations also demonstrated the flexibility of the method and tool to be adapted to different stakeholder and threat environments that may evolve in the future.

The effort to understand, prepare and handle the EELPS system and tool is limited. But it must be pointed out again, that a full scale evaluation in the process of planning and implementing ECOSSIAN in the real world will require substantial effort in terms of analysing the underlying E-E-L-P-S phenomena and rationalizing the definition and evaluation of the set of criteria.

It is strongly recommended that this methodology becomes an important element of a future process of planning, implementing and operating the ECOSSIAN system. The implementation of the methodology in a tool is available in three different settings:

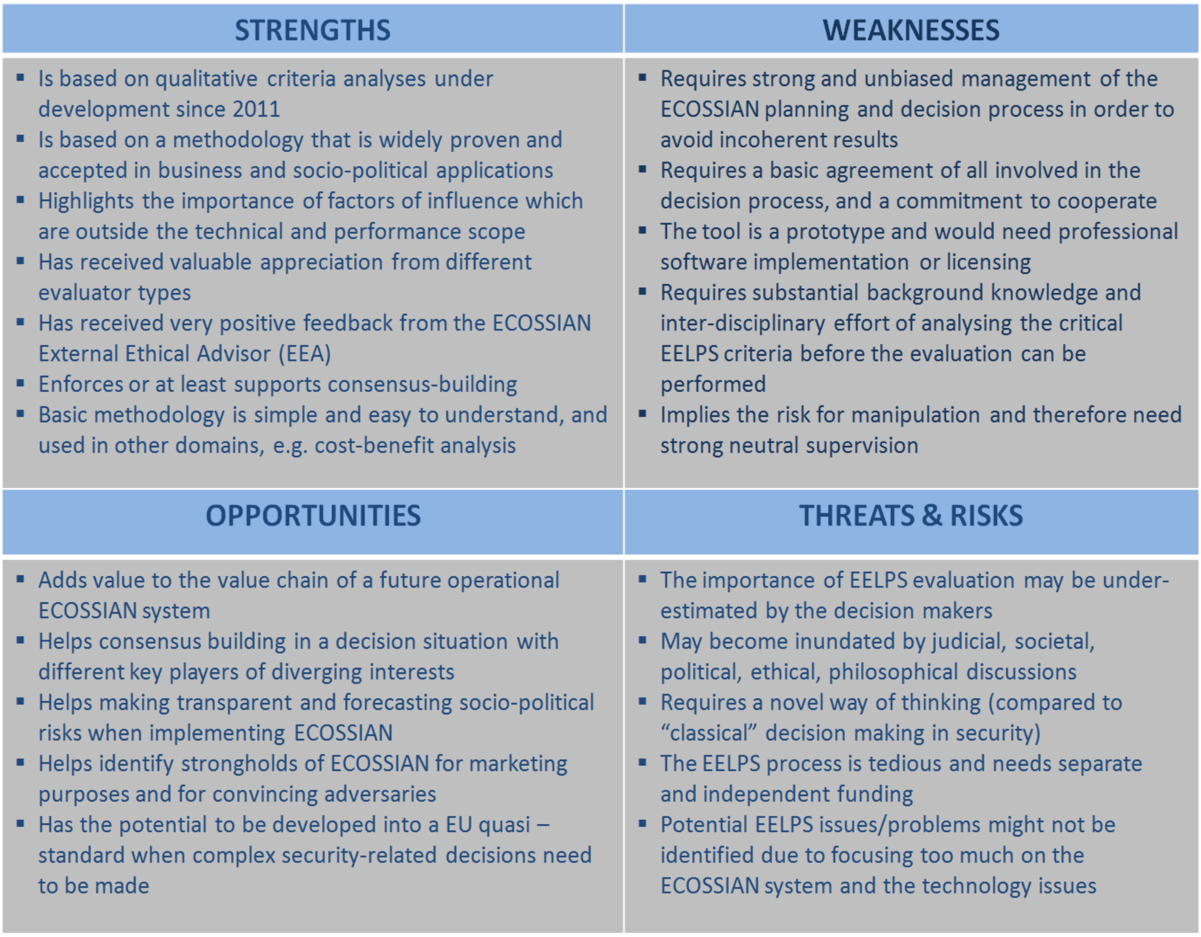
1. The EELPS criteria and tool were developed mainly in ECOSSIAN and in cooperation with the PULSE project (see details in D8.6) and are available as foreground of these projects;
2. The QCA tool developed in ValueSec and improved in CIRAS and operated at ATOS Spain may be used in a more comfortable way. This would require dedicated agreements with the owner ATOS;
3. The MAHP version developed in CIRAS and also operated at ATOS Spain is a methodological variant.

Which version should be used in future planning and decision processes will depend on the timeframe and the partners then involved and on their needs, views and preferences.

6.3 Concluding SWOT

The Table 17 below shows the main findings of the WP7/T7.5/D7.11 work performed in terms of the main **strengths, weaknesses, opportunities** of and **threats** to, the EELPS rationale, approach, tool and its application. The entries should be self-explanatory.

Table 17: SWOT Summary



STRENGTHS	WEAKNESSES
▪ Is based on qualitative criteria analyses under development since 2011 ▪ Is based on a methodology that is widely proven and accepted in business and socio-political applications ▪ Highlights the importance of factors of influence which are outside the technical and performance scope ▪ Has received valuable appreciation from different evaluator types ▪ Has received very positive feedback from the ECOSSIAN External Ethical Advisor (EEA) ▪ Enforces or at least supports consensus-building ▪ Basic methodology is simple and easy to understand, and used in other domains, e.g. cost-benefit analysis	▪ Requires strong and unbiased management of the ECOSSIAN planning and decision process in order to avoid incoherent results ▪ Requires a basic agreement of all involved in the decision process, and a commitment to cooperate ▪ The tool is a prototype and would need professional software implementation or licensing ▪ Requires substantial background knowledge and inter-disciplinary effort of analysing the critical EELPS criteria before the evaluation can be performed ▪ Implies the risk for manipulation and therefore need strong neutral supervision
OPPORTUNITIES	**THREATS & RISKS**
▪ Adds value to the value chain of a future operational ECOSSIAN system ▪ Helps consensus building in a decision situation with different key players of diverging interests ▪ Helps making transparent and forecasting socio-political risks when implementing ECOSSIAN ▪ Helps identify strongholds of ECOSSIAN for marketing purposes and for convincing adversaries ▪ Has the potential to be developed into a EU quasi – standard when complex security-related decisions need to be made	▪ The importance of EELPS evaluation may be under-estimated by the decision makers ▪ May become inundated by judicial, societal, political, ethical, philosophical discussions ▪ Requires a novel way of thinking (compared to “classical” decision making in security) ▪ The EELPS process is tedious and needs separate and independent funding ▪ Potential EELPS issues/problems might not be identified due to focusing too much on the ECOSSIAN system and the technology issues

Chapter 7 List of Terms and Abbreviations

Acronym	Explanation
AHP	Analytical Hierarchical Process
CBA	Cost-Benefit Assessment (or ... Analysis)
CCTV	Close Circuit Television
CIP	Critical Infrastructure Protection
CM	Crisis Management
COTS	Commercial Off The Shelf
CSO	Chief Security Officer
DM	Disaster Management
ECI	European Critical Infrastructure
EEA	External Ethical Advisor
EELPS	Ethical, Economical, Legal, Political, Societal. (Often also summarized under the term →QCA)
EPCIP	European Program for Critical Infrastructure Protection
ES	ECOSSIAN System
LES	Legal, Ethical, Societal (a selection of EELPS questions for the demonstrations)
MAHP	Modified Analytical Hierarchical Process
MCDA	Multi Criteria Decision analysis
MOE	Measure of Effectiveness
MOP	Measure of Performance
NGO	Non-Government Organization
PIA	Privacy Impact Assessment
PPP	Public-Private Partnership
QC	Qualitative Criteria; synonymous for intangible or soft criteria

Acronym	Explanation
QCA	Qualitative Criteria Assessment (see also →QCA)
ROSI	Return On Security Investment
RRA	Risk Reduction Assessment
SCADA	Surveillance, Control and Data Acquisition
SIA	Surveillance Impact Assessment
SLA	Service Level Agreement
SM	Security Measure
SWOT	Strengths, Weaknesses, Opportunities, Threats
UA	Utility Analysis
UAV	Unmanned Aerial Vehicle /also drones
UF	Utility Function

Chapter 8 Bibliography/ References

[1] Saaty, Thomas, Decision making with the analytic hierarchy process. 2008, http://www.colorado.edu/geography/leyk/geog_5113/readings/saaty_2008.pdf

[2] Christof Zangemeister, e.g. (2014):http://books.google.de/books/about/Nutzwertanalyse_in_der_Systemtechnik.html?id=odvxAwAAQBAJ&redir_esc=y

[3] SURPRISE Project, D2.4 – Key factors affecting public acceptance and acceptability of SOST[26], http://surprise-project.eu

[4] ValuSec Project (FP7), D6.2_Tools_and_Data_Setup and 6.3_Experiment_results_conclusions_recommendations, http://www.valuesec.eu

[5] CIRAS Project of DG HOME:

[6] ECOSSIAN project (FP7: http://www.ecossian.eu

[7] CIRAS (CIPS program):http://www.cirasproject.eu

[8] PULSE project (FP7): http://www.pulse-fp7.eu

[9] Samples of rejections or mitigations of security laws by the constitutional court: https://www.tagesschau.de/inland/sicherheitsgesetze108.html or http://www.metronaut.de/2013/01/unstillbarer-hunger-eine-chronik-der-ueberwachungs-und-sicherheitsgesetze

[10]On the role of "societal actors" in H 2020 http://ec.europa.eu/programmes/horizon2020/en/h2020-section/science-and-society

[11]https://www.sicherheitundgesellschaft.uni-freiburg.de/Home-en?set_language=en

[12] http://www.bigs-potsdam.org

[13]expertchoice tools http://expertchoice.com

[14] EPCIP: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm and http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

[15]Project ASSERT (FP7): http://assert-project.eu/wp-content/uploads/2013/04/ASSERT_D1.2_KCL_final.pdf, chpt 5.3

[16] Wright David, and Kush Wadhwa,: A step by-step guide to privacy impact assessment. Empirical research on contextual factors affecting the introduction of PIA frameworks in EU Member States, Poland, April 2012.Available at: http://www.piafproject.eu/ref

[17] Belton & Tewart: Multi Criteria Decision Analysis – an Integrated Approach, Kluwer Academic Publschers, 2002: https://books.google.de/books?hl=de&lr=&id=mxNsRnNkL1AC&oi=fnd&pg=PR11&dq=mcda+multi+criteria+decision+analysis&ots=DKJoKSAzJE&sig=nE1Q9odQ1tihrjLiiEkVlQkbokc#v=onepage&q=mcda%20multi%20criteria%20decision%20analysis&f=false or full copy: http://bookzz.org/s/?q=multiple+criteria+decision+analysis+belton&t=0

[18]http://lexicon.ft.com/Term?term=multiple-criteria-decision-analysis

[19]http://www.victoria.ac.nz/som/researchprojects/publications/Mulit-Criteria_Decision_Analysis.pdf

[26] Surveillance oriented security technologies

[20]ENISA: Introduction to Return on Security Investment, and http://advisera.com/27001academy/free-tools/free-return-security-investment-calculator

[21]Sandro Gaycken, Cyber War-das Wettrüsten hat längst begonnen (the arms race has long started), Goldmann Munich, 2012

[22] D. Wright, 'A framework for the ethical impact assessment of information technology', Ethics and Information Technology, September 2011, Volume 13, Issue 3, pp 199-226.

[23]C. Banville et a., 'A Stakeholder approach to MCDA', Systems Research and Behavioural Science, 1998, vol. 15, 1, 15-32.

[24]G. Munda: Social multi-criteria evaluation: Methodological foundations and operational consequences, European Journal of Operational Research, 158 (2004) 662-677.

[25]F. Rauschmeyer, 'Reflections on ethics and MCA in Environmental Decisions', Journal of Multi-criteria Decision Analysis, vol. 10, 2, 2001, p.65-74.

[26]D. Bouyssou, 'Building criteria: a prerequisite for MCDA', in: *Readings in Multiple Criteria Decision Aid*, C. Bana e Costa (ed.), Springer, Berlin, 1990, p. 58-80.

[27][B.Roy, D. Vanderpooten, "The European School of MCDA: Emergence, Basic Features and Current Works', Journal of Multi-Criteria Decision Analysis, 1996, Vol. 5, 22-38

Chapter 9 Annexes

Annex 1: Categories

Source: [4], ValueSec D5.3 (PU information)

Table 18: Categories

Categ. ID	Name	Helpful question
1.	SOCIETY as a whole	How will the measure impact societal life or societal reaction?
2.	INDIVIDUALS	How will the measure impact on individuals and individual reactions?
3.	LAWS AND REGULATIONS	Is the measure compliant with existing national and international rules of law?
4.	RIGHTS AND ETHICS	Is the measure compliant with or in conflict with fundamental rights?
5.	POLITICS	How does the measure influence the political level or cause specific political reactions?
6.	SOCIO-ECONOMICS	Will the measure influence the economic situation?
7.	TECHNOLOGY AND SCIENCE	How does the measure relate to scientific and technological development?
8.	ENVIRONMENT	Will the measure impact on the environment?
9.	GENERAL PRINCIPLES	Is the measure in line with basic principles of good governance?

Annex 2: Comprehensive Criteria Catalogue

Source: [4], ValueSec D5.3 (PÜ information

Table 19: Qualitative Criteria: Society (groups)

ID	Name	Helpful question	Description & Examples
1.	**SOCIETY as a whole**	**How will the measure[27] impact societal life? What kind of societal reactions will it provoke?**	**A measure may cause positive or negative feelings, attitudes or reactions within society. It may affect specific societal groups in a positive or negative way.**
1.1	Social sorting	Does the measure follow a logics of inclusion/exclusion of societal groups? Does it run the risk of discrimination (race, gender, age, religion, disabled), or does it support socially balanced equality?	Some measures enhance the option for ethnic, ideological etc. profiling, which means a distinction based on ethnicity or other groups which may be used for intelligence purposes,
1.2	Trust in fellow citizens	Does the measure support trust in fellow citizens or does it promote mistrust?	Example: Campaigns promoted by surveillance activities and publicising details do not support trust in fellow citizens.
1.3	Confidence or trust in institutions	Does the measure enhance or reduce further the trust in institutions?	Example: Positive vs. negative discussion about trust in institutions after terror attacks or natural catastrophes
1.4	Acceptance of measure	What is the potential for the measure to be accepted or to produce scepticism or even (counter-) movements ?	The media or organizations often function as "organs" for the public. Would the public accept or reject this measure?
1.5	Preparedness	Does the measure enhance preparedness of society in general?	Example: Preparedness can be enhanced through exercises, information campaigns, scenarios publications etc.
1.6	Engagement of citizen	Does the measure enhance or hamper engagement and commitment of the citizen?	Examples: For larger emergency situations, citizens would have basic supplies and energy in their homes; the measure promote or supports active participation of societal groups in CM
1.7	Control	Are citizens in (better) control of their daily "affairs" or do they lose control through the measure?	Example: With regards to the storage of personal data and data mining the citizens may lose control over their own and personal data.
1.8	Substitution	Is crime or vulnerability relocated,	Example: Data available on the

[27] as discussed under chpt.2.3, the ES is considered a complex security measure

ID	Name	Helpful question	Description & Examples
	effects/ effectiveness	instigated or confined?	internet is prone to identity theft. Will crime/disruption “find” new ways to occur? Smart meters may provide "invitations" to theft of energy
1.9	Securitization	Will the measure motivate to become a new challenge for adversaries, to target e.g. an object, a societal group or a practice. Could this be framed as a (new?) security issue?	Examples: the Islamist terrorist, the right wing terrorist, hacking – all of these were being framed as a “new” security challenge at some point.
1.10	Information /societal knowledge	Do citizens know/ will they be informed about this measure and its consequences?	Most people are not aware about the usage of personal data. Is the available knowledge level in society on the given security measure sufficient?
1.11	Cultural and gender Neutrality	Is cultural and gender neutrality assured or at risk?	Some security technologies allow for discriminatory practices, such as racial profiling (Example: Passenger Name Records) or entail gender-related issues (Example: body scanner).

Table 20: Individual criteria (personal level)

2.	INDIVIDUALS	How will the measure impact on individuals? What reactions of individuals may this cause?	A measure may alter the lives of individuals and may cause different reactions that are important for the success of the measure’s implementation.
2.1	Perceived security	How does the measure influence perceived/ "feeling of" security?	Example: Vigilantism can create higher perceived security – or the opposite.
2.2	Risk appetite	Does the measure nurture or hamper people to take (undue) risks?	Example: Some technologies convey a false impression of being safe and nurture risky behaviour.
2.3	Individual risks and opportunities	Does the measure produce any specific risks for individual citizens?	Example: with regards to the replacement of some analogue security measures through technological procedures, risks are being created for single citizens (e.g. losing access passes or essential information)
2.4	Mental health/ well-being	Does the measure have consequences for individual mental health and well-being?	Example: The visibility of military/arms or massive surveillance may cause severe indispositions in individuals

2.	INDIVIDUALS	How will the measure impact on individuals? What reactions of individuals may this cause?	A measure may alter the lives of individuals and may cause different reactions that are important for the success of the measure's implementation.
2.5	Physical health	Does the measure have consequences for individual physical health?	Example: Screening, X-Rays, microwaves etc. may have (known or unknown?) impacts on the individual health.

Table 21: Criteria on laws & regulations

3.	LAWS AND REGULA-TIONS	Does the measure fit into existing legal frameworks, does it require additional, (potentially) national/ transnational legislation or is it in conflict with the law?	The measure may not be covered by or even in conflict with existing legislation. A sound legal assessment is necessary before implementing the new security measures.
3.1	Legal standardization	Will the implementation of the measure require legal standardization (e.g. across Europe)?	Example: some measures, such as the use of UAVs for civil purposes require new laws or a modification of existing legal frameworks.
3.2	General suspicion	Does the measure contribute to a growing legal/ administrative body against citizen?	Example: Airport screening process or communications data capturing may put every passenger/citizen under general suspicion.
3.3	Proportionality	Is the measure proportional[28] to the aim?	Example: For specific pandemics, does everyone need the vaccine?
3.4	Necessity	Is the measure necessary to reach the aim?	Example: Is high – density CCTV surveillance necessary to master the security challenge in question?
3.5	Suitability	Is the measure suitable to tackle the security challenge?	Are there alternatives that should be considered/analysed because they may answer the problem better?
3.6	Compliance	Does the measure fully comply with existing regulation?	(needs to be defined for the concrete case
3.7	Legal basis	Is the legal basis given or not given?	Example: The collection of data by private companies is not necessarily legitimate, but practiced under the pretence of security requirements.
3.8	International treaties	Does the measure respect international agreements/guidelines/standards?	Examples: Respect of the European Charter of Fundamental rights

[28] General terms like this require further definition when applied in a certain case

3.	LAWS AND REGULA-TIONS	Does the measure fit into existing legal frameworks, does it require additional, (potentially) national/ transnational legislation or is it in conflict with the law?	The measure may not be covered by or even in conflict with existing legislation. A sound legal assessment is necessary before implementing the new security measures.
3.9	Accountability	`Can the involved parties be held accountable for consequences of the measure? Is the accountability clear?	Example: With regards to the civil use of Drones, the legal accountability is unclear.
3.10	Jurisdiction	Is there a clear jurisdiction for the measure?	The jurisdiction is dependent on the measure: Local, International Courts?
3.11	Compensation	Is a compensation program existent for potential damage or loss related to the measure?	Examples: Required acquisition of real estate or infrastructure, secondary effects of measures with radiologic effects etc.
3.12	Professional Requirements	Is specific certified/qualified personnel required to operate the system?	Example: The implementation of drones requires certification of drone pilots. Some measure may require psychological training of operators
3.13	Standards	Does the measure comply with existing standards?	Examples: ISO/IEC 27000 series or 15408 on ICT security.
3.14	Limits	Does (sufficient) regulation of the limits of use/application exist?	Example: Pre-emptive security measures are often perceived/ have the potential to become problematic, exploitable beyond certain limits.

Table 22: Criteria on rights and ethics

4.	RIGHTS AND ETHICS	Is the measure in line/ in conflict with the Charters of Fundamental Rights? May it be subject to any ethical concerns?	Security Measures are in need of a sound ethical assessment and a thorough check of compliance with fundamental rights before implementation.
4.1	Awareness of rights	Does a measure enhance a general awareness for fundamental rights? Are the responsible organizations aware of potential problems?	Example: Some security measures use technologies which obscure the way in which they infringe upon fundamental rights, such as privacy etc.
4.2	Dignity and Integrity	Does the security measure respect human dignity and the integrity of persons?	Example: Full body scanners may be perceived as disrespectful.
4.3	Privacy	Do security measures respect private and family life and protect personal data?	Examples: Security technologies, which create a need to assess procedures and regulations for data

4.	RIGHTS AND ETHICS	Is the measure in line/ in conflict with the Charters of Fundamental Rights? May it be subject to any ethical concerns?	Security Measures are in need of a sound ethical assessment and a thorough check of compliance with fundamental rights before implementation.
			collection and storage.
4.4	Individual Freedom	Do security measures conform with freedoms of religion, thought, expression, information, movement?	Examples: Surveillance or crowd control measures, measures to treat infections may conflict with these rights.
4.5	Non-discrimination and diversity	Is the right to non-discrimination respected?	Example: data mining allows for discriminatory profiling.
4.6	Good planning and administration	Is the security measure based on rational and comprehensible reasoning?	Is the reasoning based on facts, analysis projects and accepted findings?
4.7	Cooperation	Does the measure enhance or hinder cooperation between societal groups?	Example: Excessive surveillance measures are prone to skew the state-citizen-relationship and trust. NGOs may cooperate or protest
4.8	Diversity, equality and value pluralism	Does the security measure respect diversity of cultures, habits, religious principles, etc.?	Is the security measure only useful for a particular group only and/or does it produce negative side-effects for other groups?
4.9	Strength of measure	Is the security measure the "best[29]" possible solution?	E.g. the measure may create new (hidden) vulnerabilities which lead to perpetuating legal challenges. Examples: The screening technology at airports; certain security legislation implying ethical conflict potential.
4.10	Transparency	Is the measure understandable for everyone?	This includes an good understanding of risks and side-effects that might be created. Citizens, for example, often do not know or understand what personal data is being used for.

[29] for a certain measure "best" needs to be defined, e.g. most effective in terms or ???, most cost efficient, most acceptable by society, ...

4.	RIGHTS AND ETHICS	Is the measure in line/ in conflict with the Charters of Fundamental Rights? May it be subject to any ethical concerns?	Security Measures are in need of a sound ethical assessment and a thorough check of compliance with fundamental rights before implementation.
4.11	Innovativeness and constructiveness	Is the measure innovative?[30]	Is the solution an old solution in a new shell, or even destroying other opportunities?
4.12	Professionalism	Is the reasoning and thinking behind the solution clear and accurate?	Were, for example, experts consulted for the design of the solution? Experts from which disciplines?
4.13	Responsiveness and truthfulness	Is the measure directed onwards the original problem or does it side-track or mainly miss the original problem?	Example: The use of drones offer many opportunities for search and rescue missions, but do they actually target the original problem? Regulations may deviate from the original intention.
4.14	Changing values	Is there a potential for a change of societal values?	Many security measures anticipate or foster changing value of privacy.

Table 23: Political criteria

5.	POLITICS	How does the measure influence the political level doctrines? Which political rationales does it follow, what kind of political movements does it enable and does it cause specific political reactions?	Security measures are to a large extent matter of politics. It needs to be assessed what kind of politics and political reactions, consequences etc the measure implies.
5.1	Culture of control	Is the measure perpetuating a "culture of control"?	Cultures of control are traditions and capabilities through which authorities have an overview of/power over people's movements, bodies or actions, e.g. through Surveillance or data capturing technology.
5.2	Integrity	Is the integrity of the decision-maker or party influenced by the measure or is the measure based on integrity of the decision maker	Example: Some measures are implemented mainly to enhance chances personal profile and reputation, e.g. for re-election.
5.3	Trust	Does the measure enhance trust in politics?	Example: Can trust be gained through campaigning and public hearings?
5.4	State-citizen-relationship	Does the measure change the relation to the state?	Example: Certain measures are likely to enhance the feeling of being

[30] This has not so much ethical implication. May be shifted to category 7.

5.	POLITICS	How does the measure influence the political level doctrines? Which political rationales does it follow, what kind of political movements does it enable and does it cause specific political reactions?	Security measures are to a large extent matter of politics. It needs to be assessed what kind of politics and political reactions, consequences etc the measure implies.
			(unduly/excessively) observed by an authority.
5.5	International reputation and foreign affairs	Does the measure influence the international reputation of the country or decision-maker?	Example: Norway's international reputation after 22/7 attacks were influenced by Stoltenberg's speech on openness, but also by tightening its preparedness measures.
5.6	Opposition	Will this measure trigger the opposition to act?	Example: The introduction of the full body scanner has triggered strong political oppositions in some countries.
5.7	Political landscape	Will extremist political parties gain more (or less) power through the implementation of the measure?	Examples: Nationalism/Leftism/other Fundamentalism
5.8	Standardization	Will the measure promote a form of standardization that is desired or undesired?	Example: International procedures on counterterrorism may lead to a form of standardizing specific suspicious populations
5.9	media coverage	How will the media react to the measure?	Controversial measures are likely to trigger negative media response. Negative media coverage can hamper the measure's implementation and success.
5.10	Market-driven politics	Is the measure driven by market-motives?	Evaluation whether the availability or push of technologies by the industry drive the discussion around the measure's implementation.
5.11	Technology: Political impact	Does the measure follow existent politically accepted technology or are new technologies developed? If so, what are the policy risks and benefits?	Example: drones or military appliances have not been developed to be implemented in the civil security sector, but they are implemented and their design is refined for specific purposes.
5.12	Political compatibility	Is the measure compatible with the general security strategy of the government?	Is the measure compatible[31] With specific internal policies (industry policy, economic policy, foreign policy etc.)? With EU strategy? With other international standards &

[31] Some overlaps with criteria in Category 3.

5.	POLITICS	How does the measure influence the political level doctrines? Which political rationales does it follow, what kind of political movements does it enable and does it cause specific political reactions?	Security measures are to a large extent matter of politics. It needs to be assessed what kind of politics and political reactions, consequences etc the measure implies.
			regulations?
5.13	NGO[32] compatibility	How will NGOs in charge of the subject react?	Will there be protests? Will there be support by NGOs?
5.14	Secrecy vs. openness	Are parts about the measure classified/secret or are all positive and negative aspects communicated openly?	Is the implementation known by everyone? Would openness endanger the success of the measure?
5.15	Publicity	Is it possible to utter public criticism about the measure?	Is there a forum to pronounce opinions about the measure?
5.16	Power/ empowerment and participation	Does the measure empower the population? How far is that supportive or counter-productive to the political process?	Evaluation of the different societal groups/ movements and whether they gain power or influence through the measure and whether the measure helps them to act self-determined
5.17	Truthfulness	Does the public know about the motivations that drive the implementation of the measure?	Are motivations communicated openly or are they kept away from the public?
5.18	Visibility	Is the measure visible enough in order to identify it as a security measure?	Example: some surveillance cameras are not (or should not) be) identifiable as such.
5.19	Responsibilities	Is a shift of responsibility needed to implement the measure?	Resilience and preparedness measures may shift responsibility to communities, private enterprises, ...
5.20	Reasoning[33]	Does the measure comply or conflict with the original reasoning that drove its implementation?	Is the measure supported by sound and serious analytical study?
5.21	Sustainability	Is the measure a "quick shot" or can it be expected to stay efficient until a certain time horizon	Evaluate e.g.: Cheap, fast and shot time vs. expensive and sustainable.
5.22	Public-private partnership (PPP)	Does the measure for proper operation, control and effectiveness require PPP arrangements	This is particularly important e.g. in CIP[34] programs

[32] Overlap with 4.8

[33] see also 4.6

[34] See also ECOSSIAN D7.11

Table 24: Socio-economical criteria

6.	SOCIO-ECONOMICS	How will the measure influence the economic situation?	A measure may for example be entangled with private businesses or affect the national economy.
6.1	Consumption (User needs to name the type(s) of consumption in mind)	Does the measure influence consumption behaviour?	Example: Flying is considered safe →more passengers; Waiting lines at airports are considered less comfortable →less passengers
6.2	General investment climate	Does the measure influence the general investment climate?	Due to a specific security measure businesses may feel that their investments are safe.
6.3	Business reputation	Does the measure change reputation of a certain business?	A campaign for avian flu containment may impact positively on the pharmaceutical industry but negatively on tourism industry
6.4	Market & trade relations (Import/Export)	Does the measure impact on the general market or trade relations?	Example: Freezing terrorists assets may impact on trade relations in targeted countries.
6.5	Competition	Is the measure open for competition?	Or does a specific industrial solution dominate the market?
6.6	Production	Does the measure influence production processes?	E.g. could the measure evoke employment risks or even strikes?
6.7	Trade and transportation[35]	Does the measure influence trading and transportation organizations and treaties?	Example: Securing pipelines or shipping routes, directly or by side effects.
6.8	“Insecurity Industry”	Does the measure perpetuate an “insecurity industry”?	Insecurity Industry refers to the production of objects that are sold in the name of security but are in fact adding to a feeling of insecurity, such as emergency food packages; home protection devices.
6.9	Economic stability	Does the measure influence economic stabilities?	Examples: Euro-crisis and financial security; Secures infrastructures
6.10	Potential losses	Does the measure entail potential economic losses? Or does it decrease losses?	Examples: Waiting lines at airports; Reduced revenues of shops in supervised and protected area
6.11	Local properties	Does the measure reduce or increase market values of local properties?	Example: Dams and other infrastructure environment may impact on local property prices.
6.12	Insurability	Are failure or. secondary impacts of the measure	Example: Is there an insurance for the case that screening technology causes health

[35] see also 6.4

6.	SOCIO-ECONOMICS	How will the measure influence the economic situation?	A measure may for example be entangled with private businesses or affect the national economy.
		insured/ insurable?	problems. Are we aware of secondary impacts?

Table 25: Technology and science criteria

7.	TECHNOLOGY AND SCIENCE	How does the measure relate to scientific and technological development? Does it adopt or introduce new standards?	Many security measures are likely to incorporate novel technology. It is important to understand how new this technology is, how it works and what it entails.
7.1	Scientific or technological development	Does the measure need scientific or technological development?	Example: Screening technology, drones, robotics often need specific development for specific purposes.
7.2	Dependency on technology	Is the measure dependent on (a specific) technology? Can the dependency be covered nationally or does it imply foreign support?	Example: drones for Search and Rescue Operations create new dependencies on technologies. Encryption
7.3	Technological standardization	Is the measure based on the idea of (national or international) standards?	Example: Every airport should have similar screening technology (?)
7.4	Scientific soundness	Has the measure a sound scientific base?	Have scientific studies about the measure (from hard sciences and humanities) been tasked or at least been consulted?
7.5	Scientific community	Will the measures be acceptable to the relevant scientific community?	Screening technology may trigger different levels of acceptance in the two scientific communities of engineering and sociology
7.6	Sustainability and risk avoidance	Is the technology used in the measure sustainable?	Example: Screening technology or software security may have a limited lifetime until they can be compromised
7.7	Availability of technology	Is the technology readily available?	Or does it need to be developed? are there development risks?
7.8	Function of technology	What is the degree of functional specificity for the technology of the measure?	Example: Cameras & surveillance may be mainly COTS but may need dedicated protection and command and control /(SCADA technologies
7.9	Usability of technology	Is the technology for the measure immediately usable?	Or is training of staff, change of organizations due to the new technology needed?

7.	TECHNOLOGY AND SCIENCE	How does the measure relate to scientific and technological development? Does it adopt or introduce new standards?	Many security measures are likely to incorporate novel technology. It is important to understand how new this technology is, how it works and what it entails.
7.10	Technical limitations	Is the technological base of the measure sufficient for its purposes?	Or are there any limits to the technology deployed, which may e.g. require further complementary or supportive technologies?
7.11	Public Private Partnerships	Are public private partnerships on technologies needed to develop/implement the measure?	Large-scale CIP technology or specific SLA requirements may need a partnership or dedicated contracting between public and private.

Table 26: Environmental criteria

8.	ENVIRONMENT	How will the measure influence the environment?	A measure may for example reduce natural habitats, endanger species or cause pollution.
8.1	Aesthetics (sensual: sight, smell, sound)	Does the measure have direct impact on aesthetics (e.g. sight, smell or sound) in its environment?	Examples: Impact of dams on the ecological environment.
8.2	Hidden effects	Are there chances of hidden environmental effects?	Example: The impact that nano-technology can have on the environment and/or health.
8.3	Movements/ mobility	Does the measure impact mobility/free movement (of people, cars, etc., from an environmental point of view.)?	Example: Screening technology or massive police controls impact on mobility and free movement of people.
8.4	General built environment	Does the measure impact on the general built environment (esp. living areas, city centres)?	Example: Resilient building infrastructure needs to be planned and constructed, e.g. dams or perimeter installations may have an impact on the built environment.
8.5	Cultural environment	Does the measure impact on specific architecture, memorials, etc.?	Example: Cameras may impact on the way that specific sites in the city are used.
8.6	Natural environment	Does the measure impact on the natural environment (nature and people and people's relation to nature)?	Example: Infrastructure needed for improving may impact on the natural environment.
8.7	Environmental risks and opportunities	What is the balance of environmental risks and opportunities?	E.g. Does a specific technology produce waste, consume assets etc. which need to be traded against the security gain?

Table 27: Criteria of general principles

9.	GENERAL PRINCIPLES	Is the measure in line or in conflict with basic principles and objectives of good governance?	The success of a measure is highly dependent on its compliance with good governance. Should the implementation not be in accordance with such principles, it may in fact be counterproductive.
9.1	Effectiveness	Does the measure work effectively?	How sure can we be that the promised or intended security gain will be achieved?
9.2	Efficiency	Is the measure efficient?	Are resources used optimally to reach the intended goal and effects?
9.3	Degree of integration into existing approaches	Is the measure a specialized solution or does it follow an integrated approach?	Example: Counter-terrorism efforts often follow integrated approaches, including surveillance and counter-radicalization initiative, law enforcement.
9.4	Applicability and spectrum of use	Is the security measure applicable to a broader spectrum of problem areas?	Specific security solutions may only apply to specific targeted groups and not to others of similar requirements
9.5	Flexibility and growth potential	Is the measure very dedicated or can it be upgraded and modified for changing security scenarios	E.g. adaptability to changing threats and vulnerabilities or other "customers"

Annex 3: Tentative Criteria Selection for ECOSSIAN

Legend:

Sources:

VS 1.5= ValueSec Project Criterion # 1.5 of the original List

SP=SURPRISE Project on SOST[36] (http://surprise-project.eu)

PU= PULSE D8.2 V1.0[37]

O=other; own

ASSERT project = http://assert-project.eu

Acronyms:

SM=Security Measure

tbd= to be defined, determined

QCA=qualitative criteria assessment

ECOSSIAN project http://www.ecossian.eu

PULSE project http://www.pulse-fp7.eu

CIRAS project http://www.cirasproject.eu

Categories

S= Societal

E=Ethical incl. psychological

LP=Legal & political

Ec=Economic, technical

Right column: Y= taken, (Y)= taken but deactivated "No" in system; blank: not taken

Table 28: Tentative selection of criteria

	Categ.	Criterion Identifier	Description	Source	Possibly relevant for			Chosen for Test
			Typically in the form of questions		**ECOSSIAN**	**PULSE**	**CIRAS**	
1.	E	Social values	Is there a potential for changing societal values (pos./neg.)	O	?	X		Y
2.	E	Privacy	Do security measures respect private and family life/ ensure physical privacy?	VS4.3	X	X		Y
3.	E	Equality, discrimination	Does the SM support equal treatment or rathe prefer	O		X		Y

[36] SOST= Surveillance Oriented Security Technologies

[37] in particular from Table under 3.5.2; may be further explored

	Categ.	Criterion Identifier	Description	Source	Possibly relevant for			Chosen for Test
			certain groups or individuals	PU				
4.	E	Freedom	Does the SM impact freedom (e.g.of information, communicatin, assembly, travel,...)	PU		?		Y
5.	E	Confidentiality	Does the SM enable/ endanger personal (e.g. medical: consumer) information?	PU	X	X		Y
6.	E	Trust	Does the measure enhance trust in institutions, infrastructure, ...?	VS5.3	X	X		Y
7.	E	Transparence/ privacy	Is the balance of security improvement vs. privacy intrusion fully transparent?	SP	X	X		Y
8.	E	Control of citizens	Will citizens be controlled by the SM?	VS1.7	X	X		Y
9.	E	Organizational/ grouping	Can the measure lead to formation and action of special societal groups and initiatives (positiv and/or negative)?	?	?	X		Y
10.	E	Integrity	Is the integrity of the decision maker on the SM verified?	VS5.2	?			
11.	E	Truthfulness	Is the SM a response to a real risk ore only/partially pretending it? Is it supposed to follow hidden agenda?	?				
12.	E	Transparency/ system	Are the procedures of the SM transparent to society?	PU	?	X		(Y)
13.	E	Controlling by citizens	Will citizens get better (feeling) of being empowered to control)	VS1.7	?	?		
14.	Ec	Economic stability	Does the measure influence economic stabilities?	VS6.9	X			Y
15.	Ec	Compensation of side effects	Can (unwanted) side effects be controlled, tolerated or compensated (e.g. via insurance)	VS3.11	?	?		Y
16.	Ec	Cost-benefit	Is the benefit of the SM vs. cost clear/ transparent?	SP	X	X		Y
17.	Ec	Validation	Does the introduction of the SM foresee measurement of the SM's effectiveness and evaluation on a regular base?	SP	?	X		Y
18.	Ec	Environment	Does the SM have significant	VS8.x	?			Y

	Categ.	Criterion Identifier	Description	Source	Possibly relevant for			Chosen for Test
			(pos./neg.) impact on environmental or other parameters valuable from societal view?[38]					
19.	Ec	Cooperation	Will the SM support or block/hamper cooperation (e.g. ammong peer stakeholders, between nations, with international bodies)	O	X	X		Y
20.	Ec	Market	Does the SM support/increase/decrease market advantage?	VS6.4	X			(Y)
21.	Ec	"foreign" sectors	Will the SM require involvement of "other" sectors (e.g. private security org's., foreign org's)?	SP	X	?		
22.	Ec	Dependency	Is the measure dependent on "foreign technology"; how critical?	VS7.2	?			
23.	LP	Data protection	Does the measure enhance / endanger data protection & information privacy? Are private / personal data accessible and controllable by the individual?	PU	X	X		Y
24.	LP	Legal comformity/compliance	Doe the SM comply with existing regulations and rule of law	VS3.6 & 3.7	X	X		Y
25.	LP	International compliance	Does th measure comply with international guidelines, regulations, treaties etc.?	VS3.8	X	X		Y
26.	LP	Responsibilities	Is a shift of responsibility needed to implement the measure? with pos./neg. effects?[39]	VS5.19	X			Y
27.	LP	Strategy & political relevance	Does the SM fit into related security strategies (if existing); national, EU and other international	VS5.12 PU	X	X		Y
28.	LP	Media reactions	How will the media respond to the SM upon its introduction?	VS5.9	?	?		Y

[38] Environmental impact, depending on the type of SM, may be broken down into many more sub-criteria

[39] linked to the PPP criterion

	Categ.	Criterion Identifier	Description	Source	Possibly relevant for			Chosen for Test
29.	LP	Partnerships	Does the SM imply/ require special partnerships, particularly PPP including NGOs? Are risks of failure or misconduct of these partnerships to be expected?	O	X	X		Y
30.	LP	Reputation	Will the SM improve or reduce political reputation (e.g. locally, nationally, internationally)?	O	X	?		y
31.	LP	Acceptance	What is the potential for the measure to be politically accepted or to produce (counter-) movements/ scepticism?[40]	VS1.4	?	X		Y
32.	LP	Standards	Does the measure comply with standards (if reqested)	VS3.13	?	?		
33.	LP	Opportunism	Is the SM opportune to political agenda(s) & objectives other than strategy (e.g. pol. reputation, imminent elections)		X	?		
34.	LP	NGOs reactions	How will NGOs or other societal groups react?[41]	VS5.13	?	X		(y)
35.	LP	Political risks	Does the SM imply the potential of creating political risks? (specify case)	O	X	?		
36.	S	Fundamental rights	Does a measure respect or endanger fundamental rights, e.g. family life, personal dignity, liberty, health, integrity?[42]	VS4.1 & 4.2 & 4.4 PU	X	X		Y
37.	S	Technology intrusiveness to society	Does the SM support (in the positive sense) or enforce (in the negative sense) intrusion of technology into society / into the private sphere, e.g. dedicated HW/SWinstallations	SP	X	?		Y

[40] maybe redundat to "E"/grouping

[41] possibly linked to environmental criteria

[42] in D8.2, this criterion ins further broken down...(see 3.5.2)

	Categ.	Criterion Identifier	Description	Source	Possibly relevant for			Chosen for Test
38.	S	Culture of control	Does the SM have the potntial to increase contol over people/society[43],[44]	VS5.1	X	X		y
39.	S	Confidence or trust in institutions	Does the measure enhance further the trust in institutions?	VS1.3	X	X		Y
40.	S	Direct benefits to the needs of society	Will people/ society have direct benefits (or detriment) from the SM	SP PU	?	X		Y
41.	S	Perceived security	How does the measure influence societal feeling of security[45]? How will be the perceived effectiveness of the SM?	VS2.1	?	X		Y
42.	S	Health impact	Does/can the SM have (negativ/positive) impct on mental and/or physical health of individuals?	VS2.4 & 2.5		X		y
43.	S	Attitude towards technology	Will society reject / welcome the technology and processes wich would be implemented by the SM?	SP	X	X		Y
44.	S	Preparedness	Does the measure enhance preparedness of society to cope with (new; unexpected) risks?	VS1.5	?	?		(Y)
45.	S	Info./Knowledge	Are or can be citizens informed properly about the SM?	VS1.10	?	?		
46.	S	Risks to society	Beside its primary purpose: Does the measure imply or create additional risks to or additional positive impact on society or individuals? (e.g. social order)	VS2.3 PU		X		
47.	S	Exploitation	Does the SM exploit information (incl. personal info.) to the extent possible and/or necessary?[46]	PU	?	?		
48.								

[43] would be evaluated negative by people; may be evaluated positive by security organizations

[44] redundant to E/control

[45] maybe some overlap to 38

[46] example could be tele-medicine; medical surge capability

This is a tentative set for guiding and animating selection and creation of new Categories and Criteria. The suggested application to the projects as marked in columns 6, 7 and 8 is a recommendation..

Annex 4: Questions to Stakeholders

Questions on ethical, societal, legal, political etc. issues
WP7 /Task7.5 & D7-11 and Task 7.3-D7.10

Questions in this paper are limited to the ethical, societal, political and the PPP etc. aspects of ECOSSIAN . Questions will be manifold as the subject is complex. When talking to "Stakeholders", we need to keep in mind that there will be different types of Stakeholders, and we need to ask the right questions to the right stakeholders. t should be noted, that in the four demonstrationd, different sets of selected questions were finally applied.
Possible categories of stakeholders can come from:

S1: EU representatives (e.g. from DH HOME, ENISA, ERCC, JRC, REA,...)
S2: National CERT and government crisis management authorities
S3: CI providers (managers, CIO, ...)
S4: CI technical experts (control room operators;, security analysts, CSO, SCAADA experts,....)
S5: Societal or societal groups representatives
S6: Scientists and technical experts (Security analysts, software developers

Therefore, the questions are grouped and structured in a table with the relevant stakeholders marked in the right side columns.
Asking the following questions, we should assume that the Stakeholder has before received an exhaustive ECOSSIAN briefing and a WP7 (and T7.3 and T7.5) briefing.
The detail and quality of answers will depend on the number and type of stakeholder we can address.

Table 29: Stakeholder questionnaire

Question Type **(Questions on "intangible" (qualitative) effects:** Many of them may have a positive and/or a negative outcome)		**Stakeholder Category**					
Suppose an ECOSSIAN system to become operational: Which political impacts (positive and negative) do you expect?	Empowerment of governments						
General Questions	**Few examples**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**
Which are the main problems or challenges you would expect when	Sharing of responsibilities	x	x	x			

EU/Nations/CI enterprises need to cooperate in a system like ECOSSIAN in order to improve CIP?							
Which are the main benefits or improvements you would expect when EU/Nations/CI enterprises need to cooperate in a system like ECOSSIAN in order to improve CIP?	Better early warning, sharing of resources	x	x	x		x	
Suppose an ECOSSIAN 3-level system to become operational: Which societal and ethical impacts (positive and negative) would you expect?	Privacy, protection of personal data	x	x	x		x	
Suppose an ECOSSIAN system to become operational: Which legal, regulatory and procedural impacts (positive and negative) do you expect?	Liabilities, need to know	x	x	x			
Suppose an ECOSSIAN system to become operational: Which other topics concerning the societal and political environment, boundary conditions etc. do you consider essential?	Over-regulation of ...	x	x			x	
Do you believe your concerns above have already been properly addressed, discussed, solved?	Own studies	x	x	x		x	
Do you think such a system can/should be introduced in the near future?	5-years timeframe?	x	x	x			
In which scenarios would you expect great benefit of an ECOSSIAN-like system?	Cyber terror; incidental but serious system breakdown,			x	x		x
Would you support (personally, online, ???) a socio-political evaluation of the ECOSSIAN System?		x	x	x	x	x	x
Questions on Ethical issues	**Few examples**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**
Do you expect ethical impact of an ES[47], which ones?	Unequal treatment,	x	x	x		x	x

[47] I use this for "ECOSSIAN System"

Will privacy and protection of personal data be more/ less restricted?	Smart meter data				x		x
Dose such a system have the tendency to "control" citizens?	Profiling of home "behaviour"	x	x			x	x
Could such a system foster trust or mistrust of citizens and societal groups?	Compare e.g. to TTIP					x	x
Questions on Societal issues	**Few examples**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**
Do you think the ES has the potential to impact on fundamental rights?	Freedom of choice of ....(e.g. technology, energy provider, ..)	x				x	x
Does the system have the potential to increase control over people?	Supervising and influencing societal behaviour	x				x	x
Will society get better prepared to cope with security risks?	Including media in the ES loop	x	x			x	
How would you include/ inform society on the introduction of the ES	Media campaign, political action plan, ad. brochures from CIs)						
How could the benefits of an ES be best/successfully communicated to people?	Media campaign	x	x			x	
Questions on legal and political issues; **Detailed questions on PPP see separate section below**	**Few examples**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**
Does sufficient rules of law exist for smooth introduction of ES (national, EU/international?	Existing framework which could be used as role model?	x	x	x			x
How do you see liability regulation in such a system when shared responsibilities are needed in operation?	See also under PPP questions	x	x	x			
Do you expect IPR and business confidentiality problems?	Transparency of information on	x	x	x			

	critical incidents to competitors						
Would an ES contribute to political reputation (national, EU)?	Role model for European cooperation	x	x				
Would you expect NGO activities (protesting; supporting)?	Aversion against "smart technologies" introduction	x	x			x	
Could an ES reduce political security risks of societal and economic impact dimensions	e.g. large scale sabotage, cyber terrorism?	x	x				x
Questions on business and economic issues	**Few examples**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**
Would you expect market advantage with an ES?	"security sells (?)			x			
Would you expect business growth with an ES?	Less competition, better collaboration synergies			x			
Do you expect business risks with a system like ES?	Openness to competitors, ...			x			
• Would such a system block/hamper or support/foster cooperation with peers, competitors?	See the two above	x		x			
Implementation and operation: Would you • support a cost sharing model for procurement and operation, with a framework of cooperative control? • or prefer a government/EU funding with centralized control?	Central EU agency; network of peer volunteers, ...	x	x	x			x
Questions concerning public-private partnerships (PPP) **For Task 7.3/D7.10**	**Few examples**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**

Do you see PPP as a collective need for efficient CIP? • National? • Across Europe?							
Which should be the basic sharing concepts concerning?							
• Investment and financing							
• Joint operation							
• Information sharing (open; classified,...)							
• Sharing of responsibilities and liabilities							
• Sharing of resources (e.g. software, response efforts, ...							
• Joint training, exercising best practices		•	•	•	•	•	•
• Standardization across Europe (which ones?)							
Which are the basic conflict potentials in such CIP-PPP?							
What would be a preferred cooperation regulation? • EU directive & mandatory • framework for voluntary cooperation • ???							
Which are the incentives you would expect for willing to join such PPP?							
Do you know of PPPs which could serve (fully or in parts) as role models for a CIP- PPP							
Which would be the main obstacles against such PPP? e.g. • business autonomy • national sovereignty • heterogeneity between nations •							

How long do you think it will take to implement a working PPP on the basis of a system like ECOSSIAN?							

Annex 5: ECOSSIAN EELPS Evaluation Sessions

Refers to the "setup" step in the XLS Tool "ECOSSIAN EELPS evaluation on V37-Templ.f.sess1-6.xlsm"

Yellow colour marks those parameters that are varied in one session (3 cases per session).

Session 1: Basically different Evaluator Types; Massive threat (Reinhard version: **Moderator: CESS, Reinhard**

Case Parameter	**Case 1: Research View**	**Case 2: CI View**	**Case 3: Political View**
Security Measure	ES at all 3 levels	ES at all 3 levels	ES at all 3 levels
Evaluator Type	System Designer	CI provider (fict.)	Politician (fict.)
Evaluation Objective	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.
Scenario/Use Case	Massive Cyber Terror Attack	Massive Cyber Terror Attack	Massive Cyber Terror Attack

Session 2: Different societal evaluator types; normal operation/small threats

Moderator: KUL, Jessica, and EEA

Case Parameter	**Case 1: Legal View**	**Case 2: Human Rights View**	**Case 3: Technical View**
Security Measure	ES at all 3 levels	ES at all 3 levels	ES at all 3 levels
Evaluator Type	Lawyer	Human Rights activist	CI operator
Evaluation Objective	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.
Scenario/Use Case	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents

Session3: Different societal evaluator types; massive threat

Moderator: UNIBO, Alessandra

Case Parameter	**Case 1: Legal View**	**Case 2: Human Rights View**	**Case 3: Technical View**
Security Measure	ES at all 3 levels	ES at all 3 levels	ES at all 3 levels
Evaluator Type	Lawyer	Human Rights activist	CI operator
Evaluation Objective	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.
Scenario/Use Case	Massive Cyber Terror Attack	Massive Cyber Terror Attack	Massive Cyber Terror Attack

Session 4 FINANCE view: Moderator PI, Massimiliano Aschi?;

Case Parameter	**Case 1: Normal operation View**	**Case 2:Medium attack View**	**Case 3: Massive attack View**
Security Measure	ES at all 3 levels	ES at all 3 levels	ES at all 3 levels
Evaluator Type	CI operator	CI operator	CI operator
Evaluation Objective	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.
Scenario/Use Case	Normal day to day business	Medium attacks	Massive Cyber Terror Attack

Session5: CI operator; different operational levels; small threat

Moderator: INOV, Goncalo

Case Parameter	**Case 1: O-SOC View**	**Case 2:N-SOC View**	**Case 3: E-SOC View**
Security Measure	O-SOC	N-SOC	E-SOC
Evaluator Type	CI operator	CI operator	CI operator
Evaluation Objective	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.
Scenario/Use Case	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents	Normal operation with small cyber security incidents

Session6: Politician; different operational levels; massive threat

Moderator: INOV, Goncalo

Case Parameter	**Case 1: O-SOC View**	**Case 2:N-SOC View**	**Case 3: E-SOC View**
Security Measure	O-SOC	N-SOC	E-SOC
Evaluator Type	Politician	Politician	Politician
Evaluation Objective	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.
Scenario/Use Case	Massive Cyber Terror Attack	Massive Cyber Terror Attack	Massive Cyber Terror Attack