Theoretical and Applied Informatics
ISSN 1896-5334
Vol. 26 (2014), no. 1, 2
pp. 3 - 24

Risk management approach in the ValueSec project[1]

Andrzej BIAŁAS

Institute of Innovative Technologies EMAG
ul. Leopolda 3, Katowice, Poland
andrzej.bialas@ibemag.pl

Abstract: The paper features a comprehensive approach to risk management worked out during the ValueSec project (EU 7th Framework Programme). The motivation for research was presented, along with the course of the research, achieved project results and validation results. The methodology of risk management and a supporting tool were developed as a result of the project. They help decision makers to make complex strategic decisions about security measures. These complex decision-related problems were the reason to launch the research. The elaborated methodology is based on three pillars: assessment of the considered security measure ability to reduce risk, costs and benefits analysis with respect to the security measure application, and analysis of legal, social, cultural, and other restrictions that might impair or even destroy the efficiency of the functioning measures. In the project these restrictions are called qualitative criteria. The main added value of the ValueSec project is the elaboration of a special software module to analyse impacts of qualitative criteria on the considered measure. Based on the methodology, a ValueSec Toolset prototype was developed. The prototype was then validated in the following application domains: mass event, railway transport security, airport and air transport security, protection against flood, and protection of smart grids against cyber-attacks.

Keywords: risk management, security measure, decision support, tool, cost-benefit analysis, soft factors

1. Introduction

The paper concerns the advanced risk management methodology which was a collective result of the ValueSec project – "Mastering the Value Function of Security Measures". The project, completed on January 31, 2014, was financed by the European Commission Seventh Framework Programme (FP7) and was performed by 11 partners from Germany, Norway, Spain, Poland, Finland, and Israel, including the Institute of Innovative Technologies EMAG [1]. The EMAG team, led by the author of this paper, participated in all workpackages, including the selection of a method for implementation, system design, ontology elaboration, system integration and validation. EMAG adapted its own tool OSCAD for the project purpose. The objective

[1] This paper is an extended version of the publication "A comprehensive approach to risk management exemplified by the ValueSec project" presented on the IX International Scientific Conference "Internet in the information society" – IWSI'2014 in Academy of Business in Dąbrowa Górnicza.

of the project was to develop a methodology and tool (called ValueSec Toolset) with a view to support decision makers who have to select certain security measures in a given decision context. The project products support strategic decisions to make them useful for policy makers, security architects and other stakeholders.

Each decision which is to result in selecting a given security measure is a very complex one. During the selection it is vital to take into account many different, often opposite factors. The selected measures should:

- properly affect the risk,
- be cost-effective,
- consider social, political and legal restrictions which are related to the decision making process.

The fact that these restrictions, here called qualitative factors (criteria), are taken into account is the basic added value of the project. The project has an interdisciplinary character – apart from its main area of focus, i.e. security, it concerns economical, political, social, psychological, and other issues.

The project title "Mastering the value function of security measures" identifies its scientific value. The effects of each measure can be both positive and negative and can have different kinds and directions. All together they form a vector of values related to the security measure. They can be considered arguments of the value function of security measures. The optimization of this function from different points of view and decision contexts, and elaboration of the aggregated shape of the value function of the measure are the objectives of the ValueSec project.

Despite balancing (trade-off) a multitude of different and often conflicting framework parameters, decision makers should manage a few other issues.

The considered scenarios are very complex and the decision space is not clearly defined – an uncertainty occurs, especially with respect to time. Besides, the decision rules have to refer to many dimensions (factors). Decisions impact the interests of stakeholders, who have diverging priorities, and citizens, who are sometimes unable to recognize whether the decisions are taken in their interests.

All these issues were dealt with in the ValueSec project, with a view to elaborate the methodology and tool supporting decision makers.

The paper reviews these activities, from ideas to the tool prototype. Sections 2 shows the general concept of the ValueSec decision framework. Section 3 presents implementation of the framework based on three pillars. Next section concerns operations within the framework supported by the ValueSec Toolset. Section 5 is devoted to the validation of the project results. The last section summarizes the whole project and discusses the improvements and applications.

2. ValueSec decision framework

The problem is how to develop the security related framework and tool to support the decision makers in the selection of the right measures in a given context. These

measures should properly affect the risk, bring opportunities, have reasonable costs and be free of different non-financial, "soft" restrictions. This problem is present in many different domains of application.

The researches started in the work package called "Problem Analysis and Requirements". Within this package the researchers identified the decision process and the decision makers' needs. They also defined the cost-benefit-analysis framework for decisions in the security field. The results are publicly available on the project web page [1] as the project public deliverables [2], [3], [4], [5].

The elaborated ValueSec decision framework (Fig. 1) should allow to select security measures, which:

- affect properly the risk,
- have minimal costs and bring maximal benefits,
- have identified restrictions: social, psychological, political, legal, ethical, economical, technical, environmental, etc.

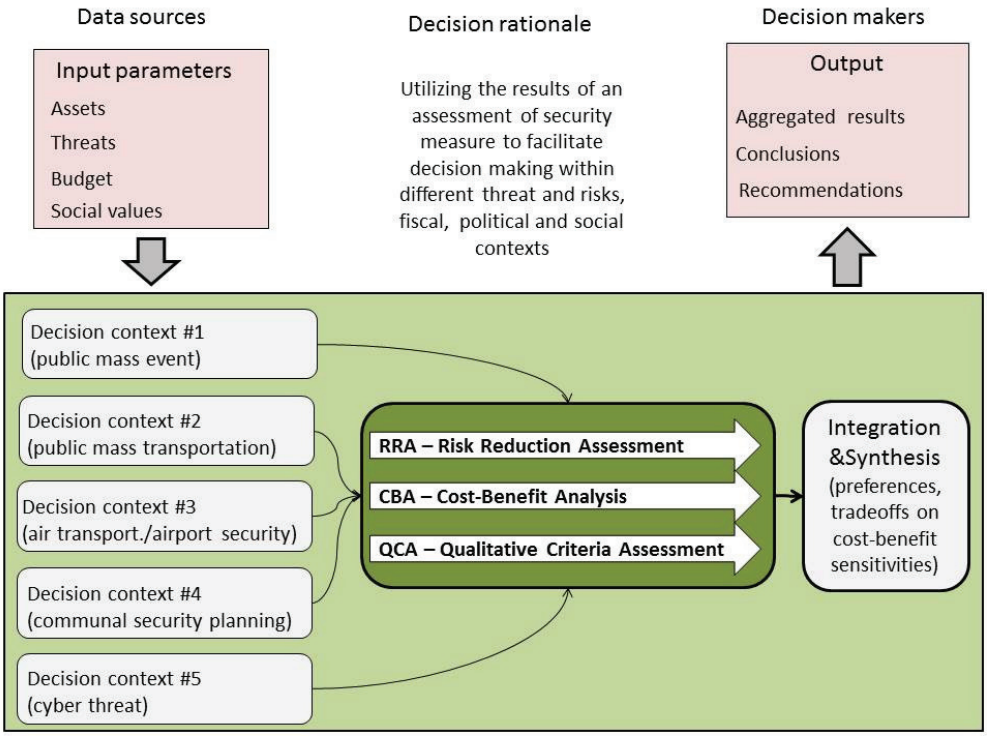


Fig. 1. ValueSec decision framework.

Each requirement is fulfilled by a separate pillar:

- Risk Reduction Assessment (RRA) pillar,

- Cost-Benefit Analysis (CBA) pillar,
- Qualitative Criteria Assessment (QCA) pillar.

Potentially, the elaborated solution has a universal character. It can be used in many application domains but its feasibility and usability should be checked in a broader context.

In the project it was assumed that its results will be validated in five application domains, called contexts [6]:

- public mass event,
- public mass transportation,
- air transportation/airport security,
- communal security planning,
- cyber threat.

Before one decides which security measure to select in a given situation, a huge number of input parameters have to be analyzed: assets, threats, budget, timeframe, organizational, technical and social context, etc.

As a result, a huge number of data characterizing the considered security measure are obtained. To make them useful for decision makers, these results should be further elaborated and presented as the aggregated results allowing for conclusions, recommendations and decision rationale.

3. ValueSec framework implementation

It was assumed in the project that the framework would be implemented in the software tool supporting decision makers. The key parts of the framework are three pillars: RRA, CBA and QCA (Fig. 2).

The project budget/time did not allow to elaborate and implement all these pillars from scratch. For this reason, in the work package "Theories, Methodologies and Tools", an exhaustive review of the existing theories, methods and tools (TMT), related to the project domain was performed [7], [8].

This work resulted in an extensive catalogue of theories, methods and tools, where the TMTs were characterized from the point of view of the project needs, and 29 of them were pointed out as state of the art of the project domain.

The consortium selected 10 risk assessment methods and tools for further analysis. Some methods/tools were selected to use in the framework as RRA candidates. The ultimate selection of the RRA candidates was performed on the Usability assessment criteria basis [9], [10].

No cost-benefit tools satisfying the project needs were identified. Therefore the project partners decided to elaborate the CBA component on the state-of-the-art methods and the partners' own experience.

The QCA idea is the scientific added value of the project. It was decided to perform researches and elaborate the QCA component from scratch on this basis. The

project partners also defined a methodological framework for the assessment of qualitative factors in security decisions [11].

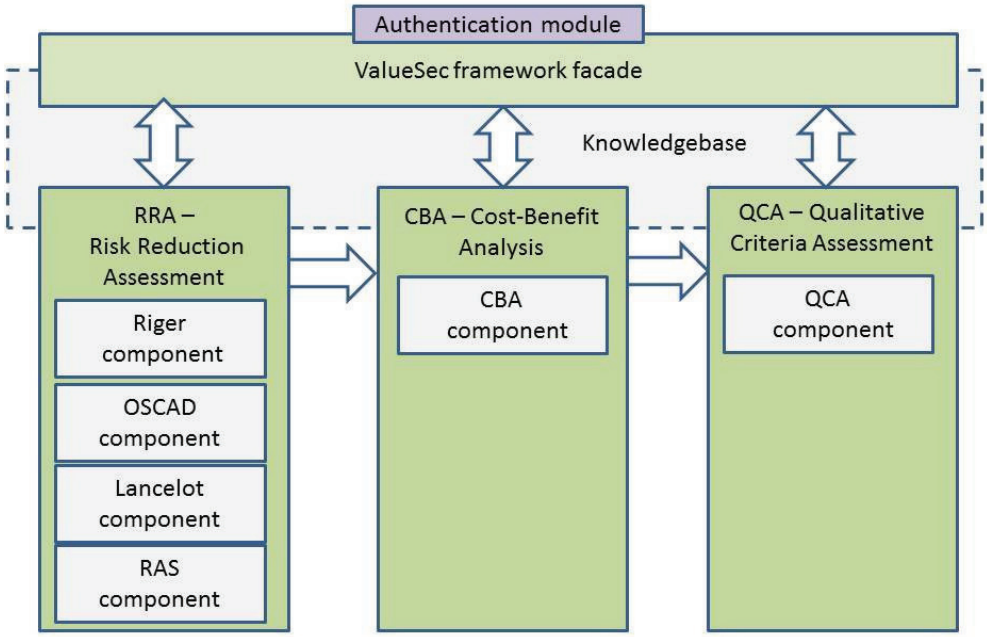


Fig. 2. ValueSec framework based on 3 pillars.

The pillars are integrated by a common façade controlling work flow inside the ValueSec Toolset. Additionally, there are some common components, such as the knowledge base and authentication module.

3.1. RRA pillar

As a result of the conducted assessment of methods and tools, there were four candidates selected for the final implementation of the RRA pillar [1]:

- Riger (elaborated by the consortium member ATOS, Spain) for the public mass event context; asset-oriented risk analyzer;
- RAS (elaborated by the consortium member – Technische Universität München, Germany) for the public mass transportation and air transportation/airport security contexts; process-oriented risk analyzer, simulation tool;
- OSCAD (elaborated by the consortium member – EMAG Institute, Poland) for communal security planning; asset/process-oriented risk analyzer;

- Lancelot (elaborated by the consortium member – WCK, Israel) for cyber threat; process-oriented risk analyzer.

Please note that RRA tools (components) are quantitative risk analyzers assigned to particular project contexts. These tools, except RAS, had been designed for risk management in the IT security domain. For this reason they were adapted for new application domains. As the tools use different risk scales, they were harmonized to obtain comparable results.

During the framework operations a given RRA component is used twice. First, the inherent (existing) risk is assessed, then the risk after the considered security measure implementation. This way the ability of risk mitigation is determined in a simple way, comparing the risk situation "before" and "after".

3.2. CBA pillar

The applied economic models provide the second set of factors considered in the decision making process. From all preselected variants of security measures adequately affecting risk, those should be selected, which are cost-benefit effective and are free from non-economical restrictions. The next step is the CBA analysis process where the monetary approach is used. The key issue is an economic analysis about the cost-efficiency of the applied measures with respect to their costs and benefits [11].

At the beginning of the CBA analysis some framing conditions for decisions are set. They express the external factors and limitations that have an effect on the decision. Such framing conditions can include the following:

- previous decisions implied by a certain security strategy,
- different agreements, e.g. between industries and government on certain security issues,
- threat perception and urgency, e.g. security incidents may trigger urgent needs to initiate some security measures,
- security governance, e.g. the rules of interacting within government and other stakeholders,
- uncertainty and risk attitude of the decision maker.

This analysis encompasses three main categories and their subcategories:

- investment costs,
- future costs,
- future benefits.

Each of these main categories has its subcategories. For example, the category of investment costs has the following subcategories:

- initial planning cost,
- initial procurement process cost,
- procurement,
- setup and integration,

- initial set of spare parts.

Each subcategory can be deeply structured, e.g. initial planning cost has the following sub-subcategories:

- project management,
- market research,
- concept design,
- personnel,
- travels,
- laboratory experiments and tests.

The future benefits can encompass different subcategories, e.g.: reduction of casualties – saved lives, fewer injured people, reduction of damages – property-, infrastructure-, environmental damages, image benefits, etc.

The desired number of subcategories and levels of categorization can be configured. This should satisfy decision makers' needs. At the beginning of the analysis some parameters are declared for the tool:

- time horizon for calculations, e.g. 10 years, based on the security measure functional lifetime, physical lifetime, technological lifetime, economic lifetime, or social lifetime,
- discount rate,
- volume of budget.

The CBA tool allows to calculate the following key indicators [12]:

- Net Present Value NPV; NPV is the difference between the present value of cash inflows and the present value of cash outflows; the security measure is profitable if NPV > 0; the higher the NPV, the better the security measure is according to CBA;
- Present Value of Benefits PVB, Present Value of Costs PVC; Present value of benefits /costs is the estimated current value of a future amount to be received or paid out, discounted at the specified discount rate;
- Benefit Cost Ratio; the benefit-cost ratio (BCR) is a ratio attempting to identify the relationship between the costs and benefits of a proposed security measure / measures. The benefit-cost ratio (BCR) is calculated as the NPV of benefits divided by the NPV of costs where BCR >1 is good;
- Internal Rate of Return IRR (%); the internal rate of return is the discount rate resulting NPV=0. The higher the IRR, the better the security measure is according to CBA;
- Pay Back Period (years); the pay-back period is the length of time required to recover the cost of a security measure; the shorter the pay-back time, the better the security measure is; the costs and benefits are not discounted;
- Discounted Pay Back Period (years); the discounted payback period is the amount of time that it takes to cover the cost of a security measure, by adding positive discounted cash flow coming from the benefits of the

implementation of a security measure; the shorter the pay-back time, the better the security measure is;

- Total costs and benefits; Total costs and benefits are the sum of discounted costs and benefits for the calculation period.

Apart from the above indicators, other diagrams can be presented as the analysis results, like costs and benefits, cash flows, break-even point (BEP). BEP shows when the costs line crosscuts the benefits line (in this point costs and benefits are equal).

3.3. QCA pillar

The Qualitative Criteria Assessment (QCA) pillar is responsible for the analysis of restrictions with the use of varied factors which are difficult to determine [13]. The QCA aims to integrate the different non-tangible decision parameters into an evaluation process. More than a hundred factors in several groups were identified and the character of their influence on the security measure implementation was determined.

Qualitative criteria complete a large part of the decision factors in politics. It is difficult to consider them during the decision process, e.g. “Good-feeling”, implicit policy priorities.

QCA is based on the assessment of a number of immaterial parameters of security-related decision making. These parameters can be assigned to the following groups:

- general principles,
- social parameters (social group level),
- individuals (personal level),
- legal regulations,
- social laws and ethics,
- politics,
- socio-economics,
- technology and science,
- living environment and natural environment.

For example, in the legal regulations group of parameters the following issues are included:

- Will the implementation of the measure lead to legal standardization?
- Growing legal body against citizen and pro surveillance (e.g. screening process puts everyone under general suspicion);
- Is the measure proportional to the aim? How all-encompassing are the effects in relation to its purpose? (e.g. in case of pandemics: Does everyone need the vaccine?).

Each fact is expressed by the configurable “value function”. This way the QCA methodology allows the quantitative assessment of qualitative factors which use these functions.

4. Using the ValueSec Toolset

The detailed presentation of the ValueSec Toolset functionalities and possibilities are beyond the scope of this paper. Only the main steps of analyses related to "Communal security planning" context will be shown (all contexts will be discussed in the next section).

In the chosen context the scenario "Flood protection" was elaborated on the basis of a 2012 flood report obtained from German Bundesland Saxony-Anhalt (LSA). This use case, elaborated by Fraunhofer IFF and EMAG Institute in co-operation with the LSA province representatives, concerns security measures improving the flood preparedness and protection.

The main steps are presented in the following subsections. The entire process is iterative. The user can always go back to an earlier step to make some corrections.

4.1. Selecting security measures

Figure 3 features the "façade" of the ValueSec Toolset. In the beginning, the user selects the context (Communal security), scenario (Flood) and the security measures to assess (Implementation of crisis management software, Establishing a standardized secure communication network, Standardization of command & control equipment and management tools & software).

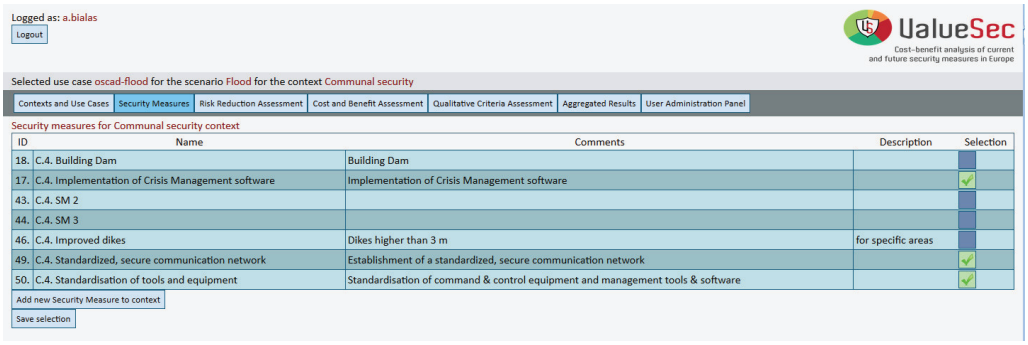


Fig. 3. Selecting security measures for analysis in the ValueSec Toolset.
Source: The ValueSec Toolset (façade) screenshot during validation. Prepared by the author, 2014.

These security measures pass to the RRA component (OSCAD).

4.2. Risk mitigation ability

In the flood protection scenario, the OSCAD software elaborated by EMAG was used. This issue was presented in papers [14], [15] in details.

First, the inherent risk is assessed. Next, the risk is reassessed after the implementation of each of the considered security measures (Fig. 4).

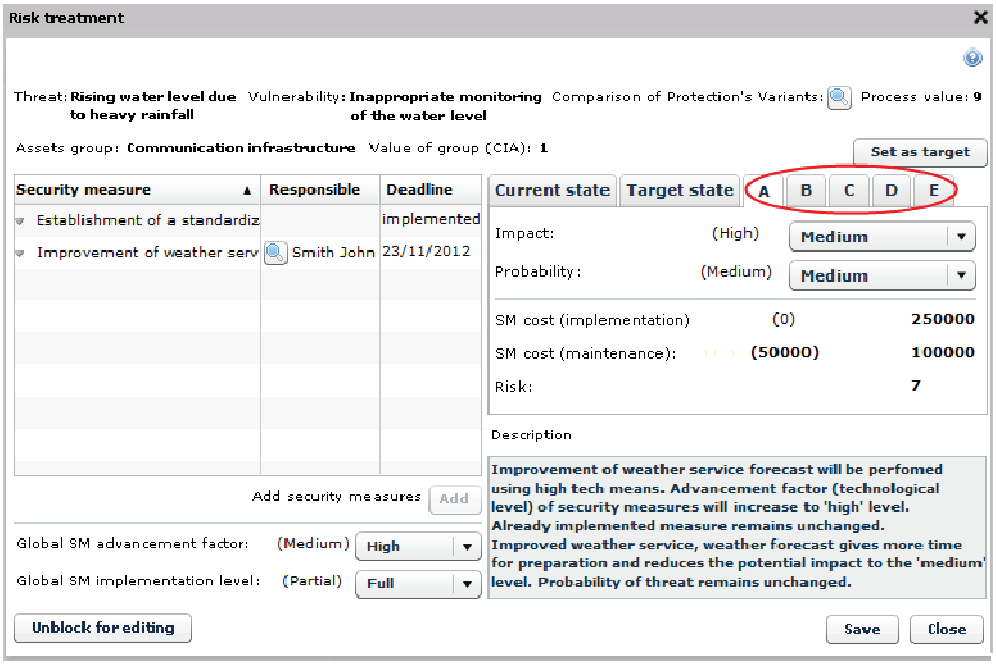


Fig. 4. Risk management window of the OSCAD application.
Source: The OSCAD risk manager screenshot during validation. Prepared by the author, 2014.

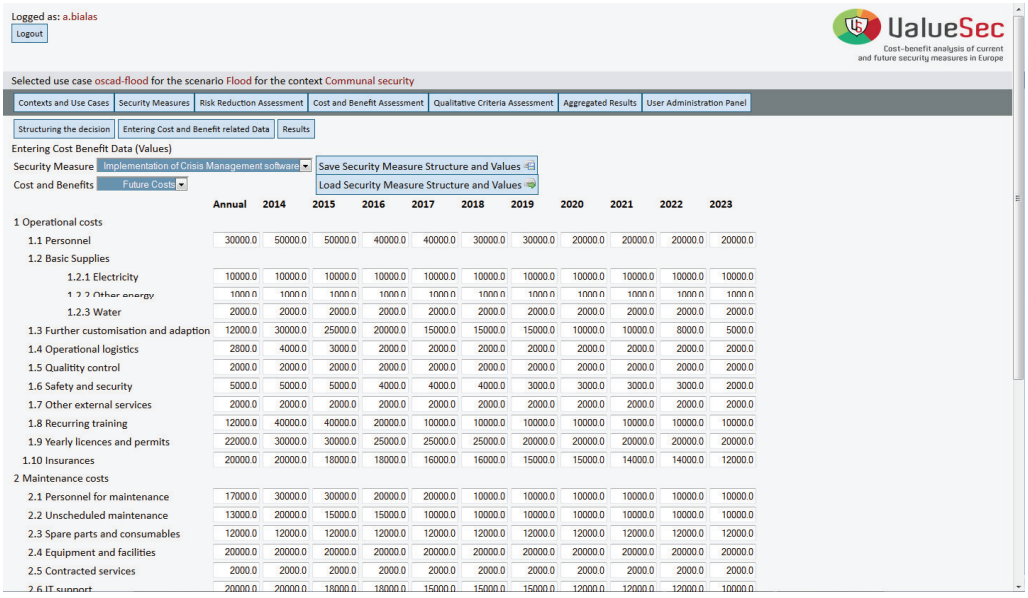
Fig.4 concerns “Communication infrastructure” as a protected asset. For this asset the threat “Rising water level due the heavy rainfall” corresponding to the vulnerability “Inappropriate monitoring of the water level” is considered. To better reduce the risk, the existing measure related to the standardization of communication means, is supplemented by a new one: “Improvement of weather service forecast”. OSCAD allows to consider 5 variants of measures (A-E) before selecting one of them as the target variant for implementation.

During the risk calculation four parameters are taken into consideration: impact, probability, advancement (assurance) of the security measure and its implementation level (planned, under implementation, tested and proven).

The results of the assessment are transferred to the façade of the ValueSec Toolset, allowing to start financial analyses.

4.3. Cost-benefit analysis

Figure 5 presents the structure of "Future costs" related to "the Implementation of crisis management software". Please note the time horizon (2014-2023) for this assessment and costs subcategories.



	Annual	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
1 Operational costs											
1.1 Personnel	30000.0	50000.0	50000.0	40000.0	40000.0	30000.0	30000.0	20000.0	20000.0	20000.0	20000.0
1.2 Basic Supplies											
1.2.1 Electricity	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0
1.2.2 Other energy	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0
1.2.3 Water	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0
1.3 Further customisation and adaption	12000.0	30000.0	25000.0	20000.0	15000.0	15000.0	15000.0	10000.0	10000.0	8000.0	5000.0
1.4 Operational logistics	2800.0	4000.0	3000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0
1.5 Quality control	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0
1.6 Safety and security	5000.0	5000.0	5000.0	4000.0	4000.0	4000.0	3000.0	3000.0	3000.0	3000.0	2000.0
1.7 Other external services	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0
1.8 Recurring training	12000.0	40000.0	40000.0	20000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0
1.9 Yearly licences and permits	22000.0	30000.0	30000.0	25000.0	25000.0	25000.0	20000.0	20000.0	20000.0	20000.0	20000.0
1.10 Insurances	20000.0	20000.0	18000.0	18000.0	16000.0	16000.0	15000.0	15000.0	14000.0	14000.0	12000.0
2 Maintenance costs											
2.1 Personnel for maintenance	17000.0	30000.0	30000.0	20000.0	20000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0
2.2 Unscheduled maintenance	13000.0	20000.0	15000.0	15000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0
2.3 Spare parts and consumables	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0
2.4 Equipment and facilities	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0
2.5 Contracted services	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0
2.6 IT support	20000.0	20000.0	18000.0	18000.0	15000.0	15000.0	15000.0	12000.0	12000.0	12000.0	10000.0

Fig. 5. Costs structure – an example.
Source: The ValueSec Toolset (CBA) screenshot during validation. Prepared by the author, 2014.

Examples of investment costs categories/subcategories are in section 3.2. Benefit categories encompass, for example, the following:

- reduction of casualties: saved lives, reduction of injured people;
- reduction of damages of property, infrastructure, critical infrastructure, and environment;
- reduction of operational costs or resources: personnel, infrastructure, resources, consumables, decreasing of operation time;
- reduction of infrastructure fees;
- growing business profits;
- image-related benefits;
- reduced probability/frequency of threats;
- residual value, etc.

For 2 main costs categories and 1 benefits category the user should iteratively plan values and introduce them into the tool. All these three subsets are configurable for the given application – relevant categories/subcategories are chosen.

Figure 6 summarizes costs and benefits for 2 measures:

- Implementation of crisis management software,
- Establishing a standardized secure communication network.

At this stage of work "Standardization of command & control equipment and management tools & software" was not considered yet.

On the left side each bar represents an investment cost (violet part) and future costs (dark blue). The right part of the bar (blue) represents benefits.

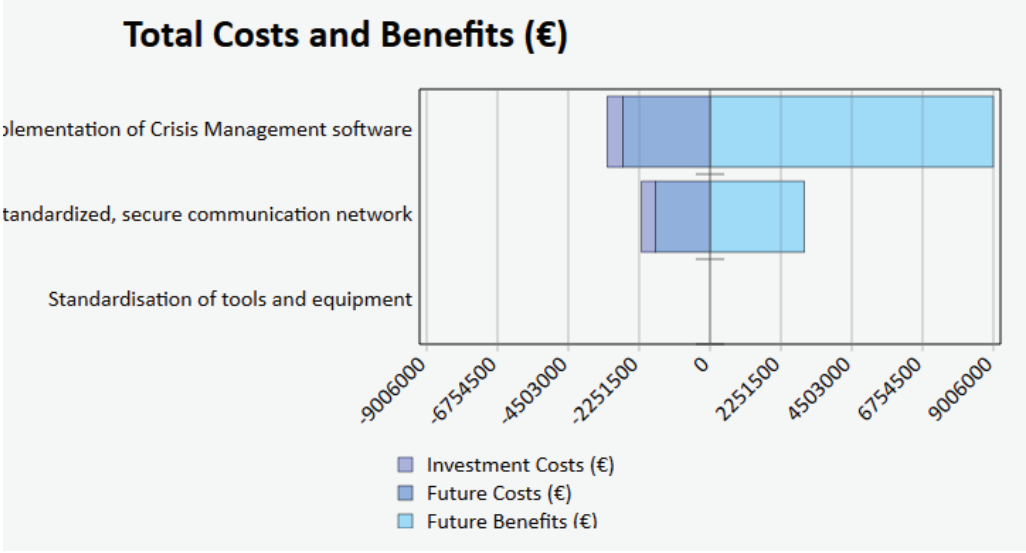


Fig. 6. Cost-benefits summary.
Source: The ValueSec Toolset (CBA) screenshot during validation. Prepared by the author, 2014.

The decision maker can compare benefits with entire costs. The first security measure presented in Fig. 6 costs more but is promising with respect to the expected benefits. Figure 7 shows the break-even diagram (when costs=benefits). For the crisis management software it will be reached near 2020.

Figure 8 summarizes basic cost-benefit indicators for three assessed security measures, i.e.:

- Total investment cost,
- Total future cost,
- Total benefits and,
- Net present value.

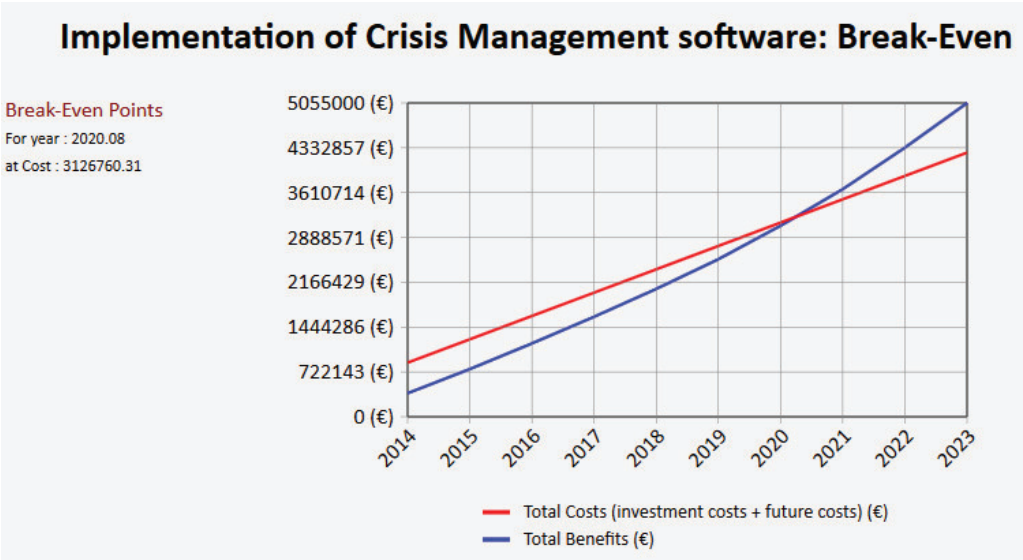


Fig. 7. Break-even chart for the selected measure implementation.
Source: The ValueSec Toolset (CBA) screenshot during validation. Prepared by the author, 2014.

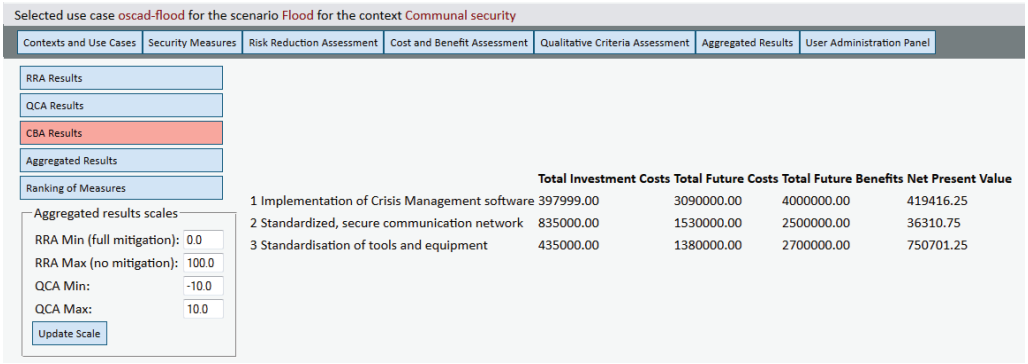


Fig. 8. Cost-benefit summary.
Source: The ValueSec Toolset (CBA) screenshot during validation. Prepared by the author, 2014.

The CBA analysis results can be shown on many other diagrams, which cannot be presented here.

4.4. Qualitative criteria assessment

The third step concerns the QCA assessment. From the huge number of QCA categories/subcategories the user should select these relevant to his/her analytical

work. Some of them can be “overlapping” or “double counts” – these should be eliminated. The following preparation procedure precedes the qualitative criteria assessment procedure:

- Check, eliminate and insert main categories and qualitative criteria (choose from the list of available criteria),
- Eliminate main overlaps and double counts,
- Define interdependencies between issues,
- Visualize interdependencies and overlaps,
- Define killer criteria (they have high importance; surpassing their specific threshold value would automatically render a measure unviable),
- Modify utility functions expressing impact character of the given criterion,
- Assign weights for criteria to be used in further calculation.

This allows to start evaluation of security measures with the use of QCA. The results are presented as various graphical reports for decision makers.

Figure 9 presents, on a spider chart, main categories of qualitative criteria used to evaluate the security measure “Implementation of crisis management software”. Positive (marked green) and negative (marked red) effects are shown.

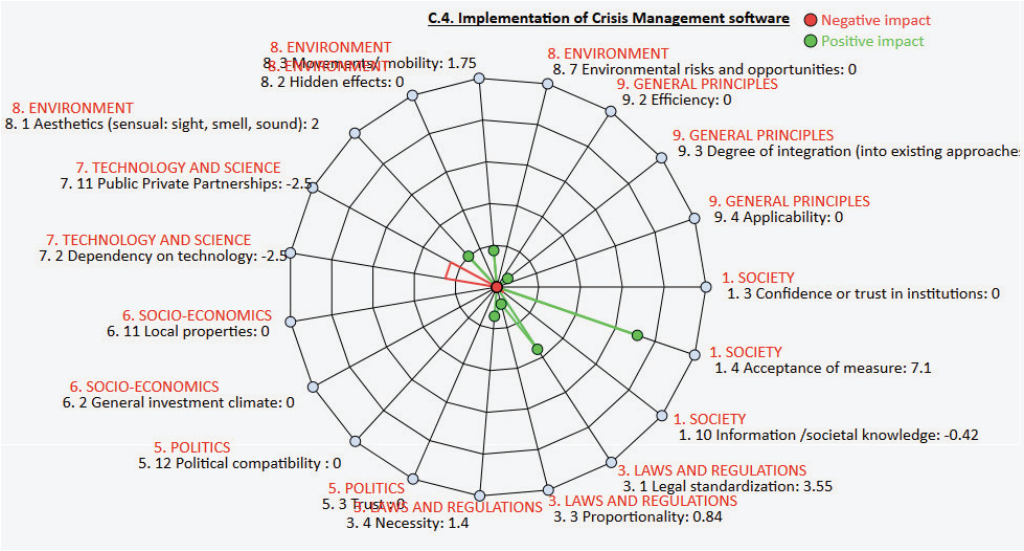


Fig. 9. Spider chart as the QCA output.
Source: The ValueSec Toolset (QCA) screenshot during validation. Prepared by the author, 2014.

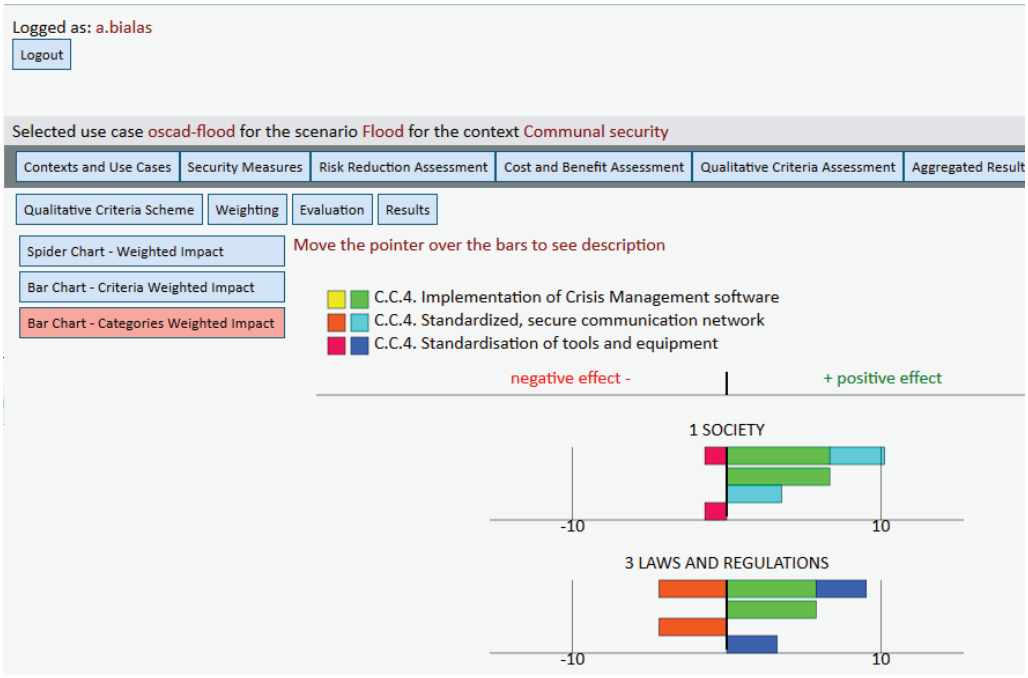


Fig. 10. QCA results presentation on a bar chart.
Source: The ValueSec Toolset (QCA) screenshot during validation. Prepared by the author, 2014.

Figure 10 presents 2 selected categories (Society, Laws and regulations) and their related positive and negative effects.

4.5. Aggregated results for decision makers

All user activities aim at obtaining the aggregated results for each of the assessed security measures. An example of aggregated results presentation diagram is shown in Figure 11. For each of security measure abilities to mitigate risk, CBA- and QCA results are summarized. More details are produced by particular pillars.

The users of the ValueSec Toolset are security experts co-operating with the decision makers (provide input data, make analyses, prepare information for decision makers) and the decision makers themselves (analyze preliminary results, prepare decisions).

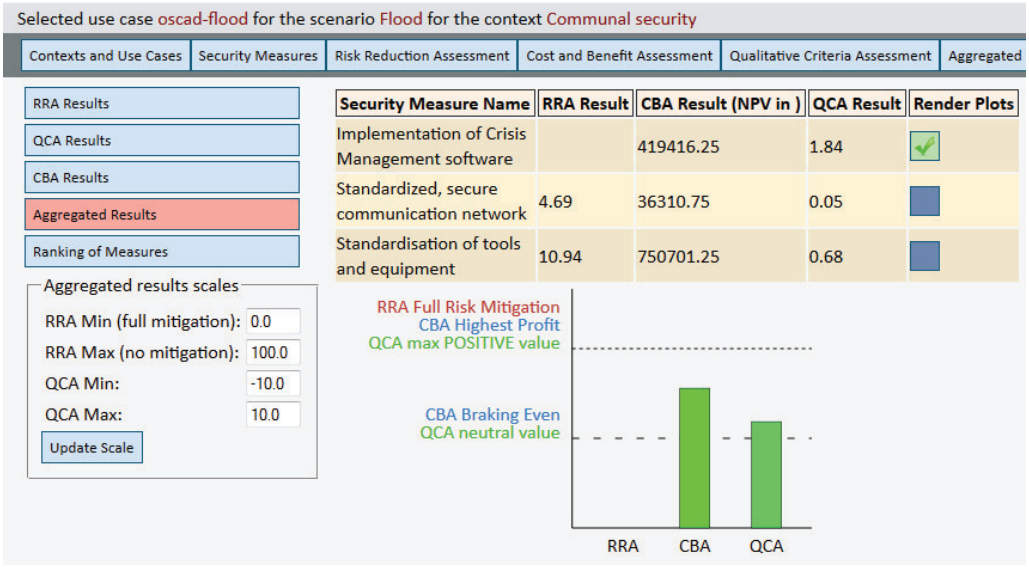


Fig. 11. Aggregated results.
Source: The ValueSec Toolset screenshot during validation. Prepared by the author, 2014.

5. Validation

The methodology and supporting tool were validated in five project contexts. One scenario was selected for a given context while for the given scenario one use case was elaborated, encompassing a subset of security measures.

5.1. "Public mass event" context

The scenario was "Valencia's Formula One Race Track". It is one of the biggest events of its kind in Europe. In 2012 more than 50,000 people participated directly in the event, another 15,000 were in the surroundings, and millions watched the event on mass media. Valencia is an important business and tourist destination. Due to these reasons the event can be an attractive target for terrorists or criminal acts (e.g. a bomb on the paddock). Potential impacts are: loss of lives, injuries, material impacts and loss of image. Political image and local business interests are taken into consideration too.

There are several challenging options to improve the security in such a situation, however the use case was focused on the improved surveillance and detection systems, comparing CCTV, scanners and frequency inhibitors.

5.2. “Public mass transportation” context

The scenario is about the security of a rolling stock depot. High speed trains parked in an open space or the depot are attractive targets for terrorists and criminals. Two main threats are considered.

- intruder can penetrate the area and deposit CBRNE material inside or outside of one or more coaches or a locomotive;
- intruder can get access to the driver’s cockpit and drive the train as a weapon into the near train station.

The following impacts are possible: dead or injured personnel or passengers, destroyed trains, collapsed rails, disturbed traffic in the region, electricity break-down, fire, economic consequences.

The use case takes into consideration a combination of security measures for the protection of the railway site, e.g. a train portal and different access control and face recognition sensors. They can bring preventive and mitigating effects.

5.3. “Air transportation and airport security” context

The scenario concerns the security of Norwegian airports. Current airport restrictions on taking liquids on the board are very inconvenient for passengers and the risk of explosion is likely to be low. European civil aviation is working on the implementation of security measures for electronic screening of liquids, aerosols and gels (LAG’s) [16].

The following impacts are possible: loss of lives, injuries, material impacts and loss of image.

The use case deals with the new generation of LAG scanners. During the use case evaluation, the following factors are analyzed:

- technical challenge of screening liquids – how to choose a right technical solution that fits the requirements (e.g. substances screened, failure rates, passenger throughput rate),
- trade-off between risk reduction and screening properties of the machinery with its costs,
- inconvenience to flight passengers and security operators, security as perceived by the passengers, acceptability.

5.4. “Communal security planning” context

The scenario deals with flood protection and is based on the experience of the German Bundesland Saxony-Anhalt (LSA) during the 2002 and 2013 floods of the Elbe and Mulde rivers. During natural disasters a number of security related decisions are taken on a regional or communal level.

The following impacts are possible: loss of lives, injuries, damages of business and technical infrastructure, damages in agriculture and natural environment.

During the use case, 3 measures are considered, discussed in subsection 4.

5.5. "Cyber threat" context

The scenario deals with an attack on a smart grid attack. Due to its growing dependence on ICT infrastructure, the electricity sector transforms towards smart grid infrastructures. Accidental or intentional ICT-related threats and vulnerabilities impact smart grids as well. The use case concerns the security improvement of energy smart grids against targeted viruses attacks, like Stuxnet.

The following impacts are possible: disturbing or damaging a power supply system.

The smart grid was partitioned into a few layers, such as IT, operational technologies, processes, etc.

During the use case experimentation the connections were identified between different security measures, different areas/layers like IT infrastructures, IT systems, physical security and procedures. Moreover, the decision makers can see how improvement in one area may affect other areas.

6. Conclusions

The paper concerns advanced risk management, especially the security measures selection by policy decision makers. The measures should adequately mitigate risk, be cost-benefit effective and free from different restrictions of poorly identifiable impacts.

The paper discusses the EU FP7 ValueSec project approach and its results. First, the decision framework concept was presented, next its implementation. The elaborated tool was shown on a few examples. The ValueSec project results were validated in 5 applications domains, which where shortly characterized.

ValueSec provides the decision support methodology and tool for policy decision makers with an extended cost-benefit approach. Thanks to these project products the decision makers have better knowledge about many diversified, sometimes implicit factors, and can improve their decision processes in terms of security measures selection. Uncertainty about the decision space is reduced. The decision makers get a common decision picture, as an aggregated result, elaborated by components of three pillars. Both quantitative and qualitative decision factors are considered. This approach increases the transparency of security policy decisions and accountability of the decision makers.

The paper [17] discusses the project results by identifying their positive and negative features and proposing to enhance the ValueSec methodology.

Four possible enhancements are proposed as the fields for further researches:

- better support of the decision process by applying commonly used methods, e.g. MCDM/A (Multiple-criteria decision making/analysis);
- extension of the methodology beyond the planning phase, i.e. to the security measures implementation and operation phases; for this reason it is proposed to conduct a security measures sensitivity analysis against the factors that may decrease the security measure efficiency during the future operation; moreover, performance indicators tracking the effectiveness of the applied measures can be useful; the paper [17] is focused on this issue;
- improving the preciseness of the risk assessments; the gain related to the security measure selection will be defined more precisely, as a difference between the "before" and "after" security measures application; it is proposed to invoke the RRA, CBA and QCA components twice to analyze the current situation and the ex-post one;
- introducing more precise risk models, which allow to consider cascading and escalation effects, especially in critical infrastructures; please note that the ValueSec framework, based on a rather simple risk model, has restricted possibilities to express more sophisticated relationships between different assets, threats and vulnerabilities.

The ValueSec products have huge application potential. Apart from the five application domains discussed during the validation, other domains can be promising. Critical infrastructure protection (CIP) seems to be one of the most important candidates. Some of the ValueSec consortium members (ATOS, CESS and EMAG) have just started a new project CIRAS – Critical Infrastructure Risk Assessment Support (CIPS/ISEC2013 DG HOME) [18]. This project is focused on the adaptation of the ValueSec methodology and tools to the issues of critical infrastructure protection.

Acknowledgement

I wish to thank my colleagues from the ValueSec project team for their co-operation in the course of the project.

References

[1] ValueSec web page: www.valuesec.eu accessed 4 December 2014.

[2] D2.1 *Decision domains concepts and trends*, 2011, http://www.valuesec.eu/content/d21-decision-domains-concepts-and-trends.

[3] D2.2 *Data model and decision model*, 2011, http://www.valuesec.eu/content/d22-data-model-and-decision-model.

[4] D2.3 *Relational concept between security and politico-economic sphere*, 2011, http://www.valuesec.eu/content/d23-relational-concept-between-security-and-politico-economic-sphere.

[5] D2.5 *Report on workshop on user needs and requirements*, 2011, http://www.valuesec.eu/content/d25-report-workshop-user-needs-and-requirements.

[6] Adar E., Blobner C., Hutter R., Pettersen K.: *An extended Cost-Benefit Analysis for evaluating Decisions on Security Measures of Public Decision Makers*. CRITIS 2012, 7th International Conference on Critical Information Infrastructures Security, September 17-19 2012, Lillehammer, Norway.

[7] D3.1 *Framework for the assessment of methods and tools*, 2011, http://www.valuesec.eu/content/d31-framework-assessment-methods-and-tools.

[8] D3.2 *Catalogue of evaluated methodologies and tools available*, 2011, http://www.valuesec.eu/content/d32-catalogue-evaluated-methodologies-and-tools-available.

[9] D4.1 Part 1 *Usability assessment criteria and usability analysis*, 2012, http://www.valuesec.eu/content/d41-part-1-usability-assessment-criteria-and-usability-analysis.

[10] D4.1 Part 2 *Usability assessment criteria and usability analysis*, 2012, http://www.valuesec.eu/content/d41-part-2-usability-assessment-criteria-and-usability-analysis.

[11] Räikkönen M., Rosqvist T., Poussa, L., Jähi M.: *A Framework for Integrating Economic Evaluation and Risk Assessment to Support Policymakers' Security-related Decisions*. PSAM11 & Esrel 2012 Int'l conference proceedings. Scandic Marina Congress Centre, Helsinki, Finland, June 25-29, 2012, USB memory stick, pp. 18-Tu3-2.

[12] Räikkönen M., Kunttu S., Poussa L.: *ValueSec User guide – the CBA excel demo*, 2013.

[13] D3.3 *Evaluation of methods and tools, and the required improvements*, 2012, http://www.valuesec.eu/content/d33-evaluation-methods-and-tools-and-required-improvements.

[14] Białas A.: *Risk assessment aspects in mastering the value function of security measures*. In: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J (Eds.): New results in dependability and computer systems. Proc. of the 8th Int. Conf. on Dependability and Complex Systems DepCos-RELCOMEX, Sept. 9-23, 2013, Brunów, Poland, Advances in Intelligent and Soft Computing, Vol. 224, 2013, Springer-Verlag: Cham, Heidelberg, New York, Dordrecht, London, ISBN 978-3-319-00944-5, pp. 25-39. http://link.springer.com/chapter/10.1007%2F978-3-319-00945-2_3#page-1 DOI: 10.1007/978-3-319-00945-2_3.

[15] Baginski J.: *Software support of the risk reduction assessment in the ValueSec project flood use case*. In: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J (Eds.): New results in dependability and computer systems. Proceedings of the 8th Int. Conf. on Dependability and Complex Systems DepCos-RELCOMEX, September 9-23, 2013, Brunów, Poland, Advances in Intelligent and Soft Computing, Vol. 224, 2013, Springer-Verlag: Cham, Heidelberg, New York, Dordrecht, London, ISBN 978-3-319-00944-5, pp. 11-24.

http://link.springer.com/chapter/10.1007%2F978-3-319-00945-2_2#page-1 DOI: 10.1007/978-3-319-00945-2_2.

[16] Bjorheim Abrahamsen E., Aven T., Pettersen K., Rosqvist T.: *A framework for selection of strategy for management of security measures*. PSAM11 & Esrel 2012 Int'l conference proceedings. Scandic Marina Congress Centre, Helsinki, Finland, June 25-29, 2012, USB memory stick, pp. 18-Tu2-4.

[17] Białas A.: *Enhancement of the ValueSec Risk Management Model*. Annals of Computer Science and Information Systems, Volume 3, Position Papers of the 2014 Federated Conference on Computer Science and Information Systems, DOI: http://dx.doi.org/10.15439/978-83-60810-60-6 pp. 201–208.

[18] CIRAS web page: http://www.cirasproject.eu/ accessed 4 December 2014.

Podejście do zarządzania ryzykiem w projekcie ValueSec

Streszczenie

Artykuł przedstawia kompleksowe podejście do zagadnienia zarządzania ryzykiem wypracowane w ramach projektu ValueSec zrealizowanego w Siódmym Programie Badań krajów Unii Europejskiej.

Zaprezentowano motywację do podjęcia badań, ich przebieg, osiągnięte wyniki oraz proces walidacji rozwiązań. Metodykę zarządzania ryzykiem i narzędzie wspomagające opracowano z myślą o decydentach podejmujących złożone, strategiczne decyzje odnośnie wyboru zabezpieczeń. Ich złożone problemy decyzyjne były motywacją do realizacji badań. Metodyka opiera się na trzech filarach (Fig. 1): oszacowaniu zdolności rozważanego zabezpieczenia do redukowania ryzyka, analizie kosztów i korzyści związanych z jego zastosowaniem oraz analizie ograniczeń prawnych, społecznych kulturowych, itp., które mogłyby zniweczyć efektywność funkcjonowania zabezpieczenia. Ograniczenia te jako kryteria jakościowe zaimplementowano w narzędziu informatycznym (Fig. 2), które należy uznać za główną wartość dodaną projektu Valuesec. Na podstawie metodyki opracowano prototyp narzędzia zwanego ValueSec Toolset, który poddano walidacji w następujących dziedzinach zastosowań: impreza masowa, bezpieczeństwo transportu szynowego, bezpieczeństwo lotniska i transportu lotniczego, ochrona przed powodzią oraz ochrona energetycznych sieci typu „smart grid" przed atakami cybernetycznymi.

Proces walidacji rozpoczyna się od wyboru dziedziny i scenariusza zastosowań oraz zabezpieczeń, które będą poddawane analizie (Fig. 3). Najpierw prowadzona jest ocena ryzyka, jakie występuje bez rozważanego zabezpieczenia, następnie oceniane jest ryzyko po zastosowaniu rozważanego zabezpieczenia (Fig. 4). Ryzyko powinno być poniżej progu akceptowalności. Następnym krokiem jest analiza kosztów-korzyści (CBA) dla zabezpieczenia, które odpowiednio zmniejsza ryzyko. Narzędzie CBA należy odpowiednio przygotować do prowadzenia analiz, w tym zdefiniować strukturę kosztów (Fig. 5) i korzyści. W wyniku przeprowadzonej analizy decydent otrzymuje pełny obraz na temat kosztów i korzyści dotyczących danego zabezpieczenia (np.: Fig. 6 – Fig. 8). Ostatnim krokiem procesu oceny zabezpieczeń jest uruchomienie narzędzia do ocen jakościowych (QCA). Przykłady raportów graficznych będących wynikiem oceny typu QCA pokazano na Fig. 9 – Fig. 10, zaś przykład graficznego raportu zbiorczego – na Fig. 11.