Position papers of the 2014 Federated Conference on Computer Science and Information Systems pp. 201–208
DOI: 10.15439/2014F275
ACSIS, Vol. 3

Enhancement of the ValueSec Risk Management Model

Andrzej Bialas
Institute of Innovative Technologies EMAG,
ul. Leopolda 31, 40-189 Katowice, Poland
Email: a.bialas@emag.pl

***Abstract*—The paper concerns the ValueSec methodology and tool which support decisions related to the security measures selection in different application contexts. The ValueSec project, financed by the European Commission Seventh Framework Programme (FP7), considers security measures which properly affect risk, are cost effective, bring benefits and are free of different restrictions (political, social, legal, psychological, etc.). These restrictions, called here qualitative factors (criteria), are hard to identify and assess. The ValueSec methodology is based on three pillars: risk assessment, cost-benefits assessment and qualitative criteria assessment. The paper discusses the project results by identifying their positive and negative features and proposing to enhance the ValueSec methodology. The focus is on one of the possible enhancements, i.e. monitoring factors which influence the measure effectiveness during its operation. The proposed concept shows how the shortage of resources needed for the measure implementation and operation impacts the measure efficiency during the operation.**

I. Introduction

THE paper presents how to enhance the risk management framework elaborated in the ValueSec project, financed by the European Commission Seventh Framework Programme (FP7). The project was performed by 11 partners from Germany, Finland, Norway, Spain, Poland, and Israel, including the Institute of Innovative Technologies EMAG [1]. The results of ValueSec, i.e. the methodology and tools (ValueSec toolset) are dedicated to the security decision makers, policy makers, architects and other stakeholders to support them in strategic decisions concerning the selection of security measures in a certain context of application. Decisions about security measures selections are very complex because each decision requires the trade-off between many factors of diversified nature. Additionally, some of these factors are multi-directional and often opposite to each other.

It was assumed in ValueSec that the selected measures should:

- properly affect the risk,
- be cost-effective,
- take into account non-financial restrictions.

Basically, the main focus area of ValueSec is security. On the other hand, however, the interdisciplinary character of the project lies in economical, political, social, legal, psychological, and other issues (called qualitative factors) which are taken into account here. Their consideration in ValueSec is the basic added value of the project.

The diversified, multidirectional, positive and negative effects form a vector of values related to the security measure. The optimization of this function, from different points of view and decision contexts, is the main objective of the ValueSec project, expressed by its full title "ValueSec – Mastering the Value Function of Security Measures".

Other project aims are:

- to reduce the uncertainty related to the decision context,
- to reduce the fuzziness of the decision process,
- to provide better decisions argumentation for stakeholders, who have diverging priorities, and for citizens, who are usually unable to recognize whether the decisions reflect their interests.

The ValueSec methodology was validated in five application domains [2], called contexts (by running certain scenarios and applying security measures to them, called here use cases):

- public mass event – for the scenario "Valencia's Formula One Race Track" the following are assessed: CCTV, scanners and frequency inhibitors; they are called use cases and are focused on the improved surveillance and detection systems;
- public mass transportation – for the scenario "rolling stock depot security" the following are assessed: the use of a train portal and different access control and face recognition sensors;
- air transportation/airport security – for the scenario "Norwegian airports security" the following are assessed: the implementation of security measures for electronic screening of liquids, aerosols and gels (LAG's) [3],
- communal security planning – for the scenario "Flood protection based on the experience of the German Bundesland Saxony-Anhalt (LSA) during the 2002 and 2013 floods of the Elbe and Mulde

rivers" the following are assessed: the implementation of crisis management software, establishing a standardized secure communication network, and standardization of command & control equipment and management tools & software [4],

- cyber threat – for the scenario "Cyber-security smart grid attack based on the targeted viruses, like Stuxnet" the following are assessed: different security measures applied to different areas/layers like IT infrastructures, IT systems, physical security and procedures.

The paper reviews the ValueSec researches, from ideas to the tool prototype (Section 2). Section 3 discusses how to improve the ValueSec framework, Section 4 and 5 compare the current and the enhanced processes of the security measures selection. Section 5 discusses the implementation of the proposed solutions in the ValueSec toolset. The last section concludes the work and presents some plans for the future in this field.

II. VALUESEC METHODOLOGY AND TOOLSET

The ValueSec methodology does not define a complete risk management framework [5], but its key parts focused on the multidimensional assessment of the security measure before the decision related to its implementation in the considered context is made [1]. The ValueSec methodology, which supports decision makers, can be applied when the decision should be taken with respect to the secured undertaking, event, object or project. This methodology is not used to manage (to monitor, to maintain) the security. It is used rather for one time ventures than for permanent activities.

The general scheme of the ValueSec decision making framework is shown in Fig. 1. In the considered context and scenario the decision maker prepares a set of security measures to assess in this application. Next he/she analyses protected assets or processes, identifies available resources, budget and social values. Each measure is assessed with respect to the risk affected, cost-benefits brought and non-financial restrictions which affect the measure during the operation.

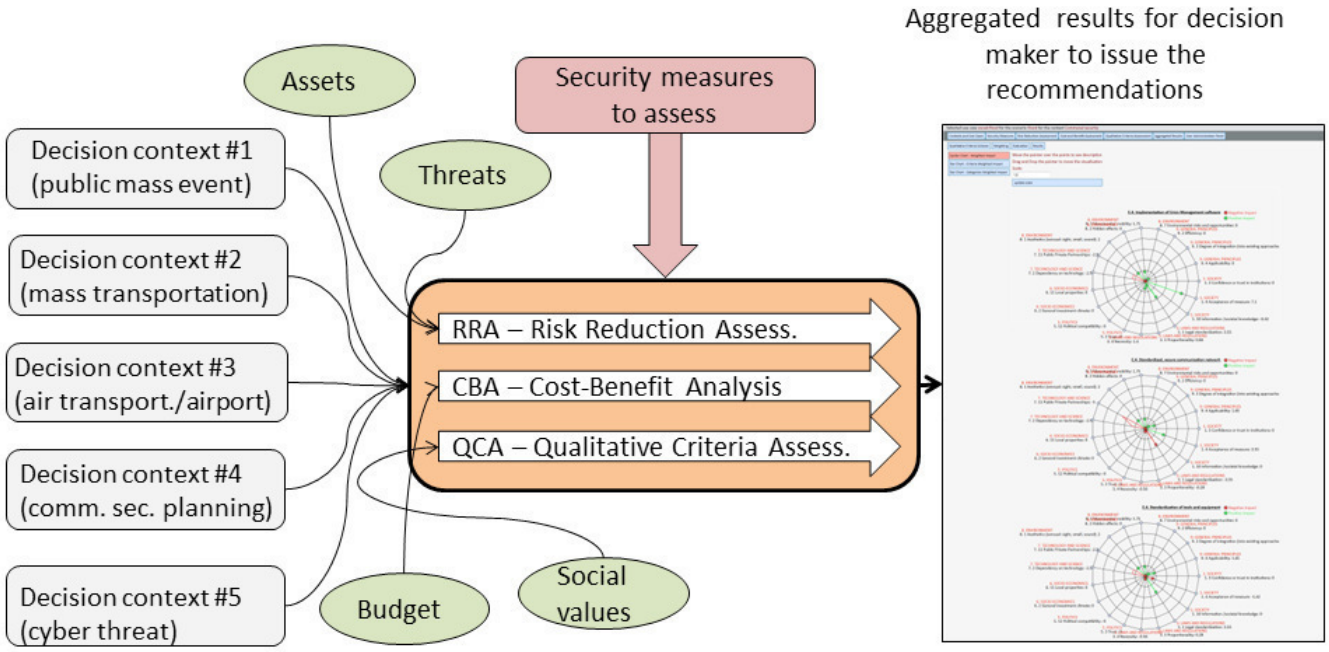

Fig. 1 General scheme of the ValueSec decision framework

The results of the security measure assessment facilitate decision making within different threat and risks, financial, political and social aspects.

As a result, different information related to the assessed measures is obtained. This information needs to be analyzed and synthetized to obtain the aggregated results useful for decision makers to elaborate the final recommendation.

The ValueSec framework is implemented as the ValueSec toolset with tree distinguished pillars:

- Risk Reduction Assessment (RRA) pillar [6],
- Cost-Benefit Analysis (CBA) pillar [7],
- Qualitative Criteria Assessment (QCA) pillar [1].

The RRA pillar is based on four RRA components elaborated by the consortium members and assigned for specific contexts:

- Riger (elaborated by the consortium member ATOS) assigned for the public mass event context; it is an asset-oriented risk analyzer;
- RAS (elaborated by the consortium member TUM) assigned for the public mass transportation and air transportation/airport security contexts; it is a process-oriented risk analyzer and a simulation tool;

- OSCAD (elaborated by the consortium member EMAG) dedicated for communal security planning; it is an asset/process-oriented risk analyzer;
- Lancelot (elaborated by the consortium member WCK) used for cyber threat; it is an asset/process-oriented risk analyzer.

During the framework operations, a given RRA component is used twice:

- to assess existing (inherent) risk,
- to assess the risk after the considered measure implementation.

From all preselected variants of security measures adequately affecting risk, those should be selected, which are cost-benefit effective and are free from non-financial restrictions (with the use of the CBA and the QCA pillar respectively).

For the monetary Cost-Benefit Analysis (CBA) three main categories are distinguished:

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

Each of these main categories is configurable and has its subcategories and sub-subcategories. For example, the category of investment costs has the following subcategories: initial planning, initial procurement process cost, procurement, setup and integration, initial set of spare parts.

The category of operational cost encompasses the subcategories: personnel, basic supplies, customization and adaptation, logistics, quality control, safety and security external services, etc.

Benefit category includes the subcategories: 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, reduction of infrastructure fees, growing business profits, image-related benefits, reduced probability/frequency of threats, etc.

The CBA tool allows to determine the different commonly used key indicators, like: Net Present Value (NPV), Present Value of Benefits/Costs (PVB/PVC), Benefit Cost Ratio (BCR), Internal Rate of Return (IRR), Break even, Pay Back Period years (PBR), etc.

The security measures, properly affecting risk and having acceptable cost-benefit characteristics, are passed for the QCA pillar. This pillar is responsible for the analysis of restrictions with the use of varied factors which are difficult to determine [1]. The following main categories of immaterial parameters of security-related decision making are considered:

- 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.

Each category is configurable and has several subcategories. Some of them – relevant for the given analysis – are selected by the QCA tool user. The tool allows to eliminate the "overlapping" or "doublecounts" items, to identify the interdependencies between subcategories, etc. For each subcategory its positive and negative impact is quantitatively assessed with the use of the predefined utility functions.

The ValueSec toolset offers different kinds of diagrams and tabular data reports as the aggregated results of assessment for each of the considered security measures.

III. Range of the possible enhancements

The ValueSec methodology is based on three independent pillars, which can be iteratively used to elaborate the aggregated results dealing with the assessed security measures in the decision context. The RRA and CBA pillars are used by risk managers but the QCA pillar is the innovative added value of the ValueSec project.

The validation shows that the ValueSec methodology, supported by the toolset, can be useful in five previously mentioned contexts and has considerable potential of applications in other domains. The questions are: Does this framework have only positive features? Can it be improved or extended? How can this be done?

During the elaboration and validation of the ValueSec project results some ideas and concepts were identified.

1. The ValueSec methodology and its supporting toolset provide a lot of diversified information for the decision maker (aggregated results) and, in this sense, support the decision making process.

Please note that the decisions themselves are not supported by any specialized methodology but are elaborated heuristically by people. In this field there is potential to extend the ValueSec methodology by applying commonly used methods, e.g. MCDM/A (Multiple-criteria decision making/analysis). The ValueSec output can be adapted and used as input for the chosen methodology applied to automate the decision process. This is performed to facilitate the work of decision makers.

2. The ValueSec methodology and toolset are focused on the security planning and do not tackle the security measure implementation and use.

The selection of security measures which properly affect risk, are cost-benefits effective and free of restrictions related to the qualitative criteria – does not guarantee a full success. This is due to the fact that these measures can be later improperly implemented, monitored, and the resources for their management can be insufficient. There is a danger that all activities performed according to the ValueSec methodology may be thwarted later, during implementation and operation of the measure. 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.

3. The ValueSec methodology analyses the risk before and after the security measure implementation, but CBA and QCA are performed only in the situation after the measure implementation.

Please note that the risk "before" is related to the existing, previously applied security measures, which also have costs, bring some benefits and have some qualitative restrictions. It would be better to analyze CBA and QCA parameters also before the security measure selection, to obtain a more detailed picture of the current situation. For this reason a differential approach is proposed. The gain related to the security measure selection will be defined more precisely, as a difference between the "before" and "after" situation. It is proposed to invoke the RRA, CBA and QCA components twice to analyze the current situation and the ex-post one.

Moreover, the RRA components should support explicit identification of the benefits related to the measures, which allow to elaborate more valuable input for the CBA analysis.

4. The ValueSec framework, based on rather simple risk model, has restricted possibilities to express more sophisticated relationships between different assets, threats and vulnerabilities, and in results to consider the cascading or escalating effects.

The analysis of this effects is important especially for the critical infrastructures. This limitation of the ValueSec methodology may disturb it dissemination in this domain of application. For this reason the more enhanced RRA components should be implemented and CBA and QCA properly enhanced.

Each of the four identified issues needs further researches to elaborate the useful enhancements of the ValueSec methodology.

In the next two sections one of these four issues will be shortly discussed, i.e. the issue No. 2, related monitoring the efficiency of the implemented security measures.

IV. The Current Security Measures Assessment Process

The current security measure assessment process ought to be shortly presented here.

At the beginning of the process the decision maker selects the context, e.g. "Communal security", the scenario, e.g. "Flood protection" and security measure to analyze, e.g.:

- "Implementation of crisis management software",
- "Establishment of a standardized secure communication network",
- "Standardization of command & control equipment and management tools & software".

Fig. 2 presents the general view of the ValueSec toolset and the three above selected items. Please note all main menu options, which are activated step by step, except "User Administration Panel". This menu option includes general managing functions of the tool.

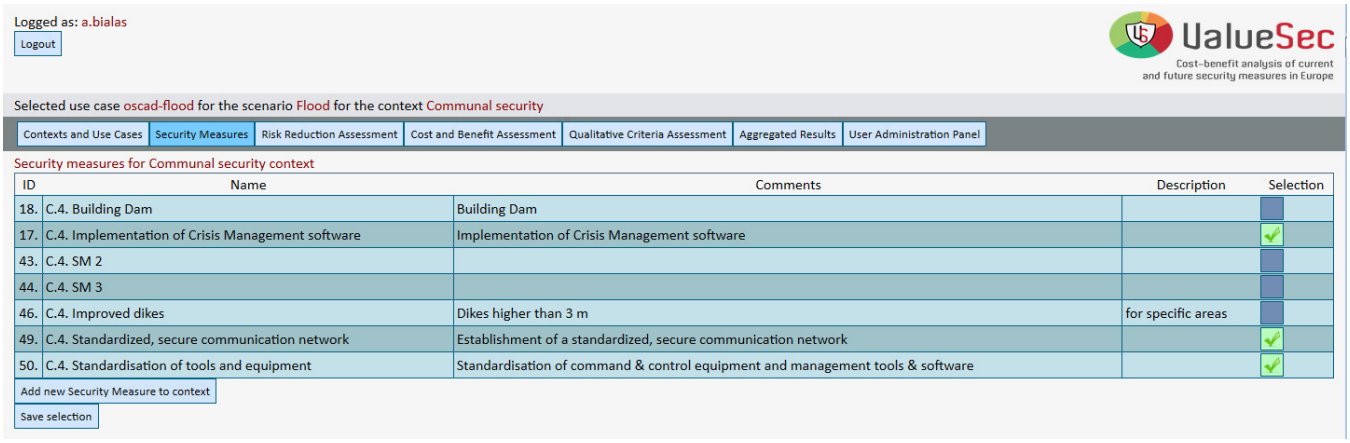

Fig. 2 The ValueSec toolset main menu – selecting security measures for assessment

The ValueSec analyses are performed with use of the components of three pillars (RRA, CBA, QCA). As a result, the decision maker is provided with a huge number of analytical data of different shapes.

The first step of analyses is the assessment how each of the considered security measures affects risk. In the flood protection scenario, the OSCAD software elaborated by EMAG was used [4], [6] as the RRA component. The OSCAD tool allows to analyze risk with respect to processes (e.g. preparedness, reaction, restoration processes) or assets (e.g. people, infrastructure, natural environment). The examples of the considered issues are: loss of lives, injuries, damages of business and technical infrastructure, damages in agriculture and natural environment, etc. The risk assessment is performed twice:

- before the implementation of any measure (inherent risk, current situation),
- when the considered security measure is selected for implementation.

The risk values before and after measure selection are transferred to the main component of the ValueSec toolset, as the key data for the decision maker. This component

calculates the risk reductions caused by any measure and shows them in percentage.

Next the CBA analysis is provided. In the beginning, different analysis parameters are defined (monetary value, time horizon, discount rate, used cost live cycle model, budget limit, investment costs-, future costs- and benefits subcategories). Then the distributions of cost-benefits categories/subcategories in time are produced and different analytical parameters, like NPV, PVB, PVC, BCR are calculated.

The next step is the QCA assessment of the proposed security measures. From the huge number of QCA categories/subcategories the decision maker selects these relevant for the context and scenario, eliminating cases called "overlappings" and "doublecounts", identifying dependencies between the selected items, defining weights and finally performing the evaluation.

For each QCA subcategory item the utility function can be defined, which expresses the item influence (linear or not) in a numerical way. The example of such function for the "Confidence or trust in institution" item, with respect to "Implementation of crisis management software", is shown in Fig. 3. For the five enumerative values placed on the X axis one can assign numbers of the range -10 to 10 in the Y axis.

The user can define the shape of this relationship.

Each pillar component produces its own data set which encompasses the detailed analysis results.

Moreover, the aggregated results in different kinds and shapes are provided to summarize the analysis.

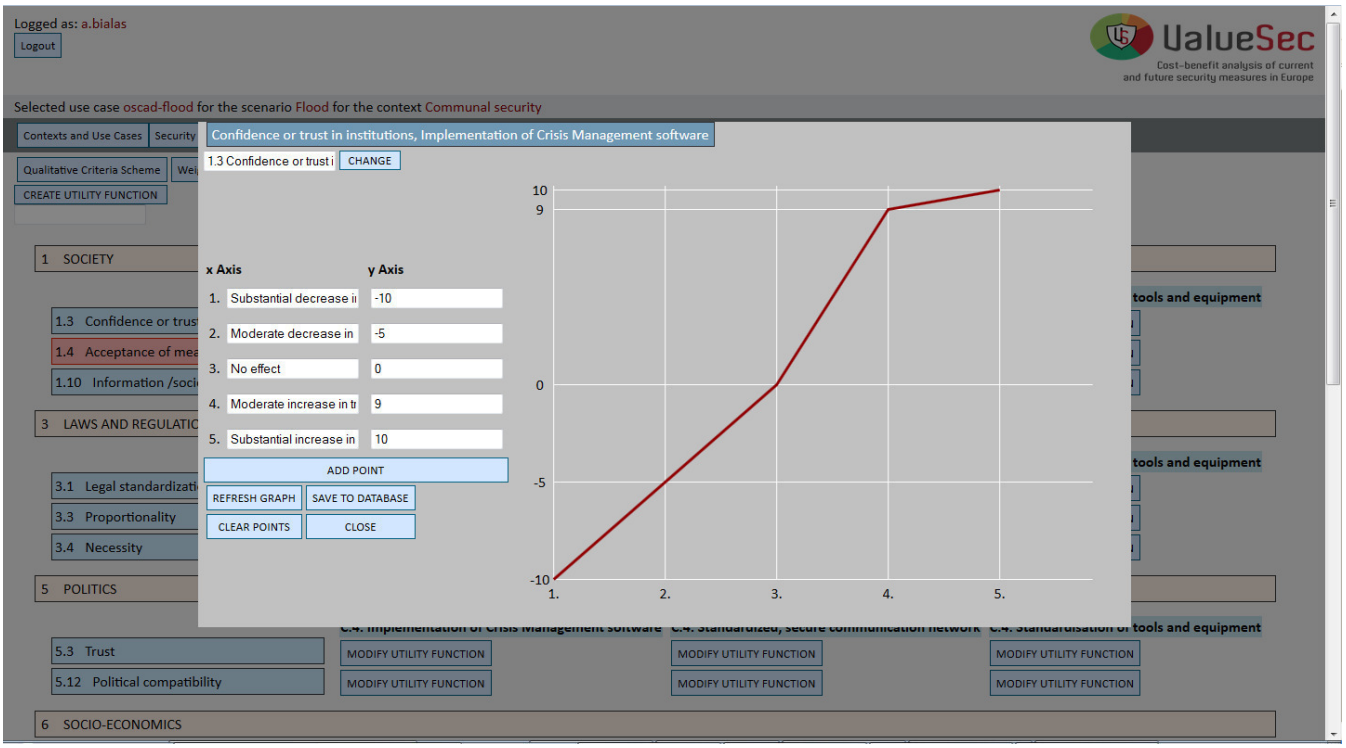

Fig. 3 Defining utility functions which transform analytical enumerative values into numbers expressing negative and positive impacts

Fig. 4 shows an example of data produced for three security measures considered in the scenario dealing with the flood protection. This an example of data called aggregated results.

Please note that the "Standardization of command & control equipment and management tools & software" security measure reduces risk by 10.94 %, has NPV: 750,701.25 Euro, and the middle QCA impact is 0.68. The detailed data interpretation is discussed in the project deliverables [1].

This short description of the ValueSec toolset shows that the decision maker obtains many diversified characteristics (tabular, diagrams) related to the selected measures. This allows to assess how the planned security measure should behave in the considered context.

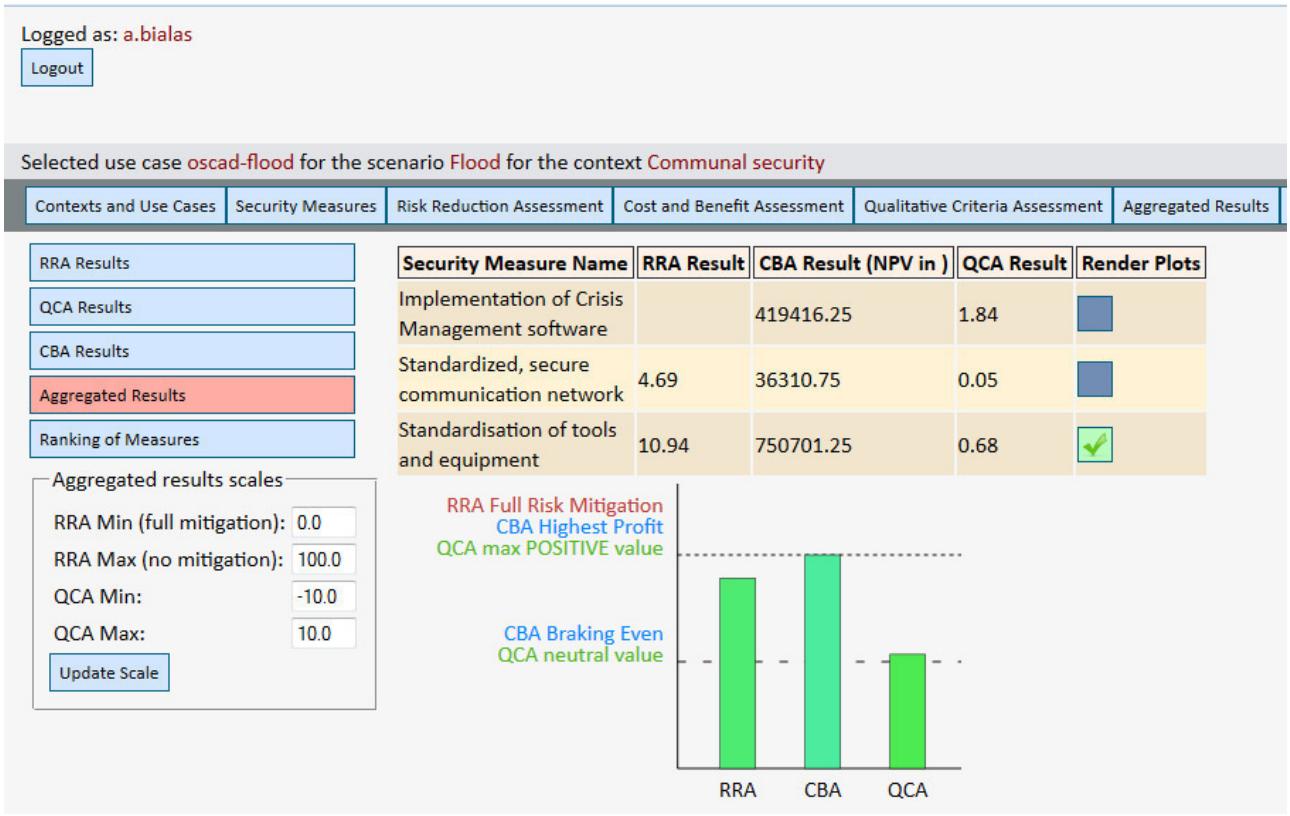

Fig. 4 The ValueSec toolset main menu – selecting security measures for assessment

V. The Enhanced Security Measures Assessment Process

Please note that the presented here considerations end at the security measures selection, i.e. at the security planning. The above analyses do not provide any information or requirements related to the further implementation and maintenance of security measures. Will the properly selected measures be really effective? The stakeholders expect that security measures will not only be properly selected, but also effective when crisis situations occur – they simply expect certain assurance from the security system.

To ensure efficient monitoring of the implemented security measures (section III, issue No. 2), the following solutions can be implemented:

1. Extending the security measure specification by parameters related to the measure implementation and maintenance. Moreover, extending the ValueSec toolset by one menu option representing the security measure sensitivity analysis. The analysis is to show how the shortage of resources impacts the effectiveness of the security measure in the operational environment.
2. Implementing performance indicators which allow to check whether the security measures are effective when critical obstacles occur. The ValueSec toolset menu should be extended again.

To present the proposed solutions, a more precise specification is elaborated. Each security measure (SM) is represented by the `SecurityMeasure` class – a class of the ValueSec ontology. This ontology encompasses the project data and relationships. The `SecurityMeasure` class has many different parameters (ontology properties):

- `SMhasID` – unique identifier assigned to each measure;
- `SMhasName` – name of the measure, e.g. “Building dam” in Fig. 2 (please note: the context identifier “C.4” is not a part of this name but is concatenated to the security measure name);
- `SMhasDescription` – textual, informal description of the measure;
- `SMhasRiskBefore` – inherent risk value (risk before any considered security measure implementation);
- `SMhasRiskAfter` – assessed risk value when the considered security measure is applied;
- `SMhasInvCost` – points at the `InvestmentCost` class individual specifying investment costs (subcategories, their properties and parameters) in the cost-benefit analysis;
- `SMhasOperatCost` – points at the `OperatingCost` class individual specifying operating costs (subcategories, their properties and parameters) in the cost-benefit analysis;

- SMhasFutureBenefit – points at the FutureBenefit class individual specifying future benefits (subcategories, their properties and parameters) considered in the cost-benefits analysis;
- SMhasQCAimpact – points at the QCAimpact class individual specifying overall impacts identified in the QCA analysis (their subcategories, analytical parameters and relations with other items of the model).

Please note that the three complex classes:

- InvestmentCost,
- OperatingCost,
- FutureBenefit,

represent a data model of the CBA component, and the complex class QCAimpact expresses the QCA component.

To assess whether the security measures are properly implemented and maintained, two mechanisms (the tool functionalities) are proposed:

- the simple resource management; each security measure requires minimal resources for its implementation and operation; these resources should be monitored to control residual risk;
- the performance indicators allowing to check if the security measure is effective in a life cycle and/or when critical obstacles occur.

Both these mechanisms go beyond the range of the current ValueSec use because they concern implementation and operation, rather than security planning.

The simple resource management checks if proper resources are applied for the implementation and later for the operation. These resources are identified during the cost-benefit analysis. The investment costs and the operation costs subcategories can be the foundation of the security measure implementation- and operation plans (the risk treatment plans). The resources with respect to time horizons are specified in these plans. For this reason the currently used SecurityMeasure class can be extended by properties dealing with the resources:

- SMhasReqImplemResources – points at the ReqImplemResources class individual, specifying overall resources of different kinds, required for the proper security measure implementation;
- SMhasReqOperResources – points at the ReqOperResources class individual, specifying overall resources of different kinds, required for the proper security measure operation.

Both classes represent the minimal resources which assure proper behavior of the security measure, i.e. allowing to control the risk at the planned level (the residual risk), expressed by the SMhasRiskAfter property of the SecurityMeasure class.

It is assumed that insufficient resources cause that the risk level planned during RRA is not achieved in reality. It means that the insufficient resources increase the planned risk level.

Checking whether current resources are sufficient, and how their insufficiency may increase risk, is called here the Resources-Risk Sensitivity (RRS) analysis. RRS is closely related to CBA (this component provides information about required resources for risk treatment plans) and RRA. Decreased resources of different kinds can be considered as additional "vulnerabilities" which should be considered during risk assessment with use of the RRA component. The RRS component can be based on the modified RRA component. This issue needs further analysis.

The second proposed mechanism concerns the performance indicators which allow to check if the security measure is effective in its life cycle or in individual situations, when critical obstacles occur.

The implementation of performance indicators is rather difficult, especially when the planned security measures are used for a single application, e.g. to secure a specific mass event, organized occasionally. Data types and sources to feed the indicators variables are diverse. Therefore sampling a reasonable data set to derive sensible conclusions for the improvements and corrections requires time and effort. For the permanent operations of the proposed security measures the situation is more favourable. Here it is possible to acquire much information specifying how the security measures behave in a real environment. On this basis the different performance indicators (and statistics) can be defined. These indicators can be used in real time to react to the critical situation and to correct the protection system. Additionally, the indicators can be analyzed periodically to elaborate continual improvement actions. The indicators depend strongly on the domain of their application. The examples of indicators are:

- number of incidents (or losses) of a given type in the specified time period,
- mean time required to manage the incident of a given type,
- number of false alarms.

This mechanism can be supported, e.g. by certain verifications or tests of the implemented security measures, performed outside the ValueSec framework, not discussed in this paper.

To implement these both mechanisms, two main options should be added to the horizontal ValueSec menu shown in Fig. 2:

- Resources-Risk Sensitivity Assessment, encompassing the risk treatment plan elaboration and maintenance, required resources specification, performing the assessment with the use of the RRS component, etc.;
- Performance indicators, including: the indicators related to maintenance, alerting, statistics, etc.

To extend the existing ValueSec toolset prototype, the assumptions and functional project of the software

enhancements should be developed. This undertaking goes beyond this paper. It can be considered by the ValueSec team task and needs proper organization and funds.

VI. Conclusion

The paper concerns improvements of the ValueSec methodology and toolset, based on the experiences gained during the project execution, especially during the validation of the project results. The validation was based on five scenarios in different application domains, called here contexts. The scenarios and their use cases (representative samples of security measures) meet the expectations of broad decision makers' needs.

The paper discusses the ValueSec methodology, presenting the decision framework and its implementation as the software tool prototype.

ValueSec uses the following principles of work. For the given context and with respect to the given scenario, the security measures – candidates for the implementation are selected. Their assessments are performed, based on three pillars:

- RRA pillar, responsible for the assessment how the analysed security measure effectively affects the risk,
- CBA pillar, designed to assess if the security measure candidate is effective with respect to the assumed cost-benefit model criteria,
- QCA pillar, responsible for the identification of any political, social, legal, etc. restrictions, which can decrease the security measure operations in the future, exclude them, or mitigate them before the measure implementation.

Further in the paper, the possible enhancements are discussed, born during validation experiments.

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

- better support of the decision process by means of specialized tools,
- extension of the methodology beyond the planning phase, i.e. to the security measures implementation and operation phases,
- improving the preciseness of the risk assessments,
- introducing more precise risk models, which allow to consider cascading and escalation effects, especially in critical infrastructures.

The discussions of these four issues go beyond a single paper. For this reason, a more detailed discussion is provided only for the second issue.

A solution is proposed which allows to monitor the decreased security measures effectiveness during the operation caused by the shortage of resources. Moreover, performance indicators allowing the corrections in the security system and its continual improvement are discussed. The new RRS component can be considered as the ValueSec fourth pillar. The RRS is an analytic tool used to assess how decreasing resources can reduce the security measures performance. It can be implemented on the basis of the RRA component. The main extension is related to the analyzed vulnerabilities. The new methodology element considers the different shortages of resources as an additional source of vulnerabilities. The RRS component needs validation and experimentations on the real RRA component with the use of, for example, OSCAD, elaborated by EMAG.

Acknowledgment

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

References

[1] *ValueSec web page*: www.valuesec.eu accessed 6 March 2014.

[2] E. Adar, C. Blobner, R. Hutter, K. Pettersen, "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*, Lillehammer, September 17-19, 2012.

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

[4] J. Baginski, "Software support of the risk reduction assessment in the ValueSec project flood use case", in: *New results in dependability and computer system*, W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, J. Kacprzyk, Eds.: *Proceedings of the 8th Int. Conf. on Dependability and Complex Systems DepCos-RELCOMEX*, Brunów, Poland, September 9-23, 2013, *Advances in Intelligent and Soft Computing*, Vol. 224, 2013, Springer-Verlag: Cham, Heidelberg, New York, Dordrecht, London, 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.

[5] *Risk management – Principles and guidelines*, ISO 31000:2009.

[6] A. Białas, "Risk assessment aspects in mastering the value function of security measures", in: *New results in dependability and computer system*, W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, J. Kacprzyk, Eds.: *Proceedings of the 8th Int. Conf. on Dependability and Complex Systems DepCos-RELCOMEX*, Brunów, Poland, September 9-23, 2013, *Advances in Intelligent and Soft Computing*, Vol. 224, 2013, Springer-Verlag: Cham, Heidelberg, New York, Dordrecht, London, 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.

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