

UNIVERSITY OF TARTU  
Institute of Computer Science  
Software Engineering Curriculum

**Oleksandr Cherednychenko**

**Designing Visually Effective and Intuitive Model-  
ling Notations for Security Risk Management**

**Master's Thesis (30 ECTS)**

Supervisor: Raimundas Matulevičius, PhD

Tartu 2018

# **Designing Visually Effective and Intuitive Modelling Notations for Security Risk Management**

## **Abstract:**

Security risk management is a set of activities, aimed at identifying and mitigating security risks starting from the early stages of software development. A set of security risk-oriented modelling languages could be used by both end users and security analysts to perform modelling activities. However, existing languages lack semantical transparency, which results in additional grasping barriers and steepness of learning curve. Moreover, presently available modelling languages were developed with no explicit design rationale in mind and perform poorly in terms of effectiveness and intuitiveness. Since the vital characteristic of modelling language is cognitive effectiveness, this research is focused on improving visual perception of the available security risk-oriented modelling languages (Secure BPMN, Secure Tropos, Misuse Cases, Mal-activity Diagrams). This goal is fulfilled by proposing a set of icons, which could be incorporated into existing modelling languages. Unified set of icons would enhance the recognizability of domain-specific concepts, outlined in Information Systems Security Risk Management Domain Model, as well as reduce the learning curve and improve the overall cognitive efficiency of available notations. Proposed icon set is composed based on the outcomes of several empirical studies, performed in 3 distinct locations, belonging to various geographical areas and exhibiting a variety of cultural backgrounds. Improved cognitive effectiveness of notations, augmented with proposed icon set, is validated by the conducted evaluation study, which demonstrated increased level of comprehension as compared with existing notations.

## **Keywords:**

Security Risk Management, ISSRM, visual notation, semantic efficiency, icon set, perception.

**CERCS:** T120 Systems engineering, computer technology

## **Visuaalselt efektiivsete ja intuiitivsete modelleerimisteadete disainimine turvariski juhtimiseks**

### **Lühikokkuvõte:**

Turvariski juhtimine on toimingute kogum, mille eesmärk on tuvastada ja vähendada turvariske tarkvaraarenduse varastest etappidest alates. Modelleerimisel võivad nii lõppkasutajad kui ka turvaanalüütikud kasutada turvariskidele orienteeritud modelleerimiskeeli. Siiski puudub olemasolevatel kehtel semantiline läbipaistvus, mis tekitab õppimiskõverale täiendavaid takistavaid barjääre ja äkilisust. Veelgi enam, praegu saadaolevad modelleerimiskeeled töötati välja ilma mingit kindlat disaini arvestamata ja nende intuiitivsus on vilets. Kuna modelleerimiskeele oluline tunnusjoon on kognitiivne efektiivsus, keskendub see uuring saadaval olevate turvariskidele orienteeritud modelleerimiskeelte (Secure BPMN, Secure Tropos, Misuse Cases, Mal-activity Diagrams) mõistmise parandamisele. Sellel eesmärgil pakutakse ikoonide komplekti, mille võiks integreerida olemasolevatesse modelleerimiskeeltesse. Ikonide ühtlustatud komplekt suurendaks domeenikohaste kontseptide äratuntavust, mis on toodud infosüsteemide turvariskide juhtimise domeenimudelis, lühendaks õppimiskõverat ning parandaks olemasolevate teadete üldist intuiitivsust. Soovitatav ikoonide komplekt on koostatud mitme empiirilise uuringu põhjal, mis on tehtud kolmes kohas, mis asuvad eri geograafilistes piirkondades ja esindavad erinevaid kultuurilisi taustu. Teadete parandatud kognitiivset efektiivsust, täiendatuna soovitatud ikoonide komplektiga, on kontrollitud hindamisuringuga, mis näitas olemasolevate teadetega võrreldes paremat mõistmistaset.

### **Võtmesõnad:**

Turvariski juhtimine, ISSRM, visuaalne teavitamine, semantiline tõhusus, ikoonide komplekt, arusaamine.

**CERCS:** T120 Süsteemitehnoloogia, arvutitehnoloogia

## Acknowledgements

Foremost, I would like to express my gratitude to my supervisor Assoc. Prof. Raimundas Matulevičius for his extensive guidance, enthusiasm, continuous support and warm encouragement. It has been a pleasure to have been his student.

My sincere thanks for the help with empirical studies goes to Assist. Prof. Ognjen Ridić (International University of Sarajevo), Assist. Prof. Kanita Karađuzović – Hadžiabdić (International University of Sarajevo), Assoc. Prof. Semen Tseitlin (Dnipro National University of Railway Transport), Prof. Vladislav Skalozub (Dnipro National University of Railway Transport), Mr. Fedor Voloshin (Ukrainian Railways Information Technology Bureau) and Mr. Sergii Chepizhko (Ukrainian Railways Information Technology Bureau). Without their kind assistance this work could not have been successfully conducted. I would also like to thank the survey participants for their time and contribution.

I thank my friends both in Ukraine and Estonia for all the positive emotions we shared together, the stimulating discussions we had and those moments of synergy we experienced.

Last but not least, I would like to thank my family for everlastingly supporting me throughout my life path and all the years of study. This accomplishment would not have been possible without you.

## Table of Contents

1	Introduction .....	13
1.1	Research Questions .....	14
1.2	Contribution.....	14
1.3	Roadmap.....	15
1.4	Research Methodology .....	15
2	Background .....	18
2.1	Information System Security Risk Management.....	18
2.2	Security Risk Management-Oriented Modelling Languages .....	19
2.3	Rationale for Framework Selection.....	19
2.4	Physics of Notation Overview .....	20
2.5	Summary .....	22
3	Related Work .....	23
3.1	Semantical Analysis of BPMN.....	23
3.2	Semantical Analysis of UML .....	24
3.3	Semantical Analysis of i* .....	25
3.4	Semantical Analysis of Misuse Cases .....	26
3.5	Gaps Overview .....	26
3.6	Summary .....	27
4	Language Analysis .....	28
4.1	Principle of Semiotic Clarity .....	28
4.2	Principle of Perceptual Discriminability .....	29
4.3	Principle of Semantic Transparency.....	31
4.4	Principle of Complexity Management .....	32
4.5	Principle of Cognitive Integration .....	32
4.6	Principle of Visual Expressiveness .....	32
4.7	Principle of Dual Coding.....	33
4.8	Principle of Graphic Economy .....	34
4.9	Principle of Cognitive Fit .....	34
4.10	Redesign Ideas .....	35
4.11	Summary .....	35
5	Evaluation Survey .....	36
5.1.1	Audience .....	36
5.1.2	Design .....	36
5.1.3	Process .....	37

5.2	Analysis .....	37
5.3	Threats to Validity .....	40
5.4	Results Comparison.....	40
5.5	Summary .....	41
6	Symbolization Survey .....	43
6.1.1	Audience .....	43
6.1.2	Design .....	43
6.1.3	Process .....	43
6.2	Analysis .....	43
6.3	Threats to Validity.....	44
6.4	Summary .....	45
7	Symbol Identification Survey .....	46
7.1.1	Audience .....	46
7.1.2	Design .....	46
7.1.3	Process .....	46
7.2	Analysis .....	46
7.3	Threats to Validity.....	48
7.4	Summary .....	48
8	Validation Survey.....	50
8.1	Proposed Notations.....	50
8.1.1	Audience .....	50
8.1.2	Design .....	50
8.1.3	Process .....	51
8.2	Analysis .....	51
8.3	Threats to Validity.....	54
8.4	Summary .....	55
9	Conclusion .....	57
9.1	Summary .....	57
9.2	Answers to Research Questions .....	57
9.3	Limitations.....	58
9.4	Future Work .....	58
10	References .....	59
	Appendix .....	62
I.	Notation Overview .....	62
II.	Secure BPMN – Physics of Notation Summary.....	64

III.	UML – Physics of Notation Summary .....	65
IV.	i* - Physics of Notation Summary .....	66
V.	Analysis of Secure BPMN .....	67
	Principle of Semiotic Clarity .....	67
	Principle of Perceptual Discriminability .....	69
	Principle of Semantic Transparency .....	70
	Principle of Complexity Management .....	72
	Principle of Cognitive Integration.....	72
	Principle of Visual Expressiveness .....	73
	Principle of Dual Coding .....	74
	Principle of Graphic Economy.....	74
	Principle of Cognitive Fit.....	75
	Conclusion .....	75
VI.	Analysis of Secure Tropos .....	76
	Principle of Semiotic Clarity.....	76
	Principle of Perceptual Discriminability .....	79
	Principle of Semantic Transparency .....	79
	Principle of Complexity Management .....	81
	Principle of Cognitive Integration.....	82
	Principle of Visual Expressiveness .....	82
	Principle of Dual Coding .....	83
	Principle of Graphic Economy.....	84
	Principle of Cognitive Fit.....	84
VII.	Analysis of Misuse Cases.....	84
	Principle of Semiotic Clarity.....	85
	Principle of Perceptual Discriminability .....	86
	Principle of Semantic Transparency .....	87
	Principle of Complexity Management .....	89
	Principle of Cognitive Integration.....	89
	Principle of Visual Expressiveness .....	89
	Principle of Dual Coding .....	90
	Principle of Graphic Economy.....	91
	Principle of Cognitive Fit.....	91
VIII.	Analysis of Mal-activity Diagrams.....	92
	Principle of Semiotic Clarity.....	92

Principle of Perceptual Discriminability .....	93
Principle of Semantic Transparency .....	94
Principle of Complexity Management .....	95
Principle of Cognitive Integration.....	96
Principle of Visual Expressiveness .....	96
Principle of Dual Coding .....	97
Principle of Graphic Economy .....	97
Principle of Cognitive Fit.....	97
IX. Questionnaire for Evaluation Survey .....	99
X. Evaluation Survey – Results Analysis.....	102
XI. Evaluation Survey – Results of Model Matching .....	104
XII. Questionnaire for Symbolization Survey .....	105
XIII. Symbolization Survey – Obtained Symbols .....	109
XIV. Symbolization Survey – Symbol Analysis .....	114
XV. Questionnaire for Symbol Identification Survey.....	127
XVI. Symbol Identification Survey – Results Analysis .....	129
XVII. Questionnaire for Validation Survey .....	131
XVIII. Validation Survey – Results Analysis.....	138
XIX. Validation Survey – Results of Model Matching .....	156
XX. Icons Details .....	158
License .....	159



## List of Abbreviations

List of abbreviations, used in this paper, could be found below.

ISSRM	Information System Security Risk Management
SRM	Security Risk Management
BPMN	Business Process Model and Notation
UML	Unified Modelling Language
PoN	Physics of Notation Framework
SEQUAL	Semantic Quality Framework
CDs	Cognitive Dimensions Framework
CASE	Computer-Aided Software Engineering
NA	Not Applicable

## List of Tables

Table 1. PoN analysis metrics .....	28
Table 2. Comparative semiotic clarity .....	29
Table 3. Visual variable properties .....	30
Table 4. Semantic transparency characteristics .....	31
Table 5. Visual variables.....	33
Table 6. Hybrid symbols overview .....	33
Table 7. Evaluation survey outcomes .....	37
Table 8. Evaluation survey statistics.....	39
Table 9. Popularity of languages.....	39
Table 10. Evaluation survey - aggregation over concepts .....	39
Table 11. Evaluation survey - aggregation over languages .....	40
Table 12. Identified symbols.....	47
Table 13. Icon origins .....	48
Table 14. Validation survey structure .....	51
Table 15. Validation survey – evaluation of individual symbols .....	52
Table 16. Validation survey – aggregation over concepts .....	52
Table 17. Notational comparison – aggregation over concepts .....	53
Table 18. Notational comparison – aggregation over languages .....	54
Table 19. Icons for refinement.....	55
Table 20. Mean hit rate by concepts .....	55
Table 21. Mean hit rate by languages .....	56
Table 22. Symbol set of ISSRM-extended BPMN .....	67
Table 23. Semantical transparency of extended BPMN symbol set .....	70
Table 24. Visual variables of BPMN, partially adopted from (Moody, 2009a) .....	73
Table 25. Security-extended BPMN analysis .....	76
Table 26. Symbol set of ISSRM-extended Secure Tropos .....	77
Table 27. Semantic transparency of extended Secure Tropos symbol set .....	80
Table 28. Visual variables of Secure Tropos, adopted from (Moody, 2009a).....	82
Table 29. Symbol set of ISSRM-extended Misuse Cases.....	85
Table 30. Semantic transparency of the extended Misuse Cases notation.....	88
Table 31. Visual variables of extended Misuse Cases, partially adopted from (Moody, 2009a).....	90
Table 32. ISSRM-extended symbol set of Mal-activity Diagrams.....	92
Table 33. Semantic transparency of the extended Mal-activity Diagrams notation .....	94

Table 34. Visual variables of extended Mal-activity Diagrams, adopted from (Moody, 2009a).....96

## List of Figures

Figure 1. Research Methodology .....	17
Figure 2. Comparison of security risk-oriented modelling languages, adopted from (Matulevičius, 2017) .....	29
Figure 3. Comparison of asset-related concepts, adopted from (Matulevičius, 2017) .....	62
Figure 4. Comparison of risk-related concepts, adopted from (Matulevičius, 2017) .....	63
Figure 5. Comparison of risk treatment-related concepts, adopted from (Matulevičius, 2017) .....	63

## 1 Introduction

With the Fourth Industrial Revolution inevitably advancing on all fronts, humanity is currently standing on the verge of the new industrial era. Since information technologies are progressively disrupting existing business processes, it could be said that success of the enterprise steadily becomes inseparable from the flawless operation of complex technological systems. As the importance of IT demonstrates escalating growth, integrity and security of information systems are crucial for any business that aspires to be even remotely successful.

As it was recently demonstrated by the recent Equifax breach, one cybersecurity incident could effectively destroy a major domain-dominating corporation (Fein, 2017). Thus, the importance of addressing security is essentially a question of corporate life and death. While there are various approaches to address security, it is more effective to do so in initial stage, by construction, than by the fact (Dubois, Heymans, Mayer, & Matulevičius, 2010).

Requirements Engineering field, focused on formalizing specifications for software systems, offers several modelling languages, namely Secure BPMN, Secure Tropos, Misuse Cases and Mal-activity Diagrams, specifically extended to deal with security risk management. However, despite the theoretical availability of tools for addressing security at construction stage, this approach is still not widespread in the industry. Let us look at the possible reasons for unpopularity of security risk management.

Successful management of security risks heavily depends on the fruitful interaction between interested parties, namely business stakeholders and security/requirements analysts. Security-extended modelling languages are intended to serve as a means of communication, with visual diagrams conveying meaning to individuals with both technical and non-technical backgrounds. Thus, intuitiveness of selected modelling language is of paramount importance. While security/requirements analysts are expected to be proficient users of security-extended modelling languages, same could not be said about the business users. Considering the fact that existing modelling languages were not designed with human perception in mind and do not offer explicit design rationale, it could be said that currently available modelling languages do not facilitate intuitive interaction, but rather hinder it. Since this outcome is far from desired, it seems rational to develop refined modelling notations, which are expected to be semantically transparent and easy to grasp for all parties, involved in the dealing with security risks at early stages of software development.

As it was already mentioned, Requirements Engineering field currently offers several modelling languages. With the development of ISSRM (Dubois et al., 2010) and subsequent extension-related papers (Chowdhury, Matulevičius, Sindre, & Karpati, 2012), (Altuhhova, Matulevičius, & Ahmed, 2013), (Matulevičius, Mouratidis, Mayer, Dubois, & Heymans, 2012) and (Soomro & Ahmed, 2012), available languages have been modified to support security risk management concepts, forming an interconnected modelling approach. However, papers introducing language extensions do not provide justification on selected representations of ISSRM concepts, further contributing to difficulties with perception of concepts. Thus, it was decided that focus should be placed on designing a set of icons which would depict ISSRM concepts in a clear and understandable way. Proposed set of icons could be later included into all 4 extended modelling notations, significantly contributing to the ease of perception and facilitating practice of managing security risks on the early stages of software development.

Since resulting notations should be immediately understandable for the participants of modelling activities, it was decided to utilize so-called “crowdsourced design” instead of delegating design of icons solely to the relevant experts. “Crowd” here is referring to the community of professionals, who are likely to participate in security risk management activities or have already taken part in managing risks.

## 1.1 Research Questions

Ergo, the main research question of this study could be formulated as:

**MRQ.** *How to improve visual effectiveness and intuitiveness of modelling notations for security risk management?*

The main research question could be further decomposed into 4 core questions, which are as follows:

**RQ1.** *What is the state of the art in the domains of security risk-oriented modelling languages and visual notation analysis?*

The initial question aims to explore the domain of security risk-oriented languages and identify relevant notations. Additionally, it is also important to overview the trends in notation analysis and identify the framework that would be suitable for analysis. Overall, this research question is investigating background which is to serve as foundation for notational improvements.

**RQ2.** *How are current security risk-oriented modelling notations evaluated?*

Second research question deals with the evaluation of existing notations, which is to be performed to understand the necessity of notation improvement. Evaluation is performed both in theory (notational analysis of conformance to PoN principles) and in practice (empirical studies). Issues, identified as a result of evaluation, are to be tackled further in this research.

**RQ3.** *What visual icons could be introduced into available security risk-oriented modelling notations?*

Following research question covers the process of obtaining semantically transparent icons, which could be potentially introduced into the redesigned notations. Resulting icons should be semantically transparent for both experts and novice users. Efficiency of redesigned notations, enhanced with resulting iconset, is also to be validated empirically.

**RQ4.** *How could the effectiveness of security risk-oriented modelling notations be evaluated?*

Final question targets the efficiency of modelling notations, enhanced with proposed iconset. Original notations and notations, augmented with icons, are to be compared so that efficiency could be measured. As a result, the impact of introducing crowdsourced icons could be evaluated.

## 1.2 Contribution

Based on several empirical studies, performed in various European regions, this paper aims to develop a set of icons, depicting security risk management-related concepts. Proposed iconset, verified with validation survey, could be introduced into 4 security modelling languages (Secure Tropos, Secure BPMN, Misuse Cases and Mal-activity Diagrams) and is intended to enhance currently existing notational symbols. Implementation of unified icon-

set throughout all languages, supporting ISSRM, should improve the semantical transparency of these languages and contribute to the further acceptance of good practices of managing security risks during the early stages of software development. Wide acceptance of early security risk management approach is expected to ensure increased resilience to cybersecurity incidents.

### **1.3 Roadmap**

Let us look at the structure of this paper chapter-wise.

Chapter 2 covers the background of the performed research and includes overview of Security Risk Management, brief description of Physics of Notation framework and existing approaches in the domain of visual notation construction. Chapter 3 includes an overview of existing papers, covering the topic of analysing semantic transparency of various modelling languages via the Physics of Notation framework. Chapter 4 includes the comprehensive analysis of security risk-oriented modelling languages according to PoN principles. In Chapter 5, the first evaluation survey is described in detail. Chapter 6 covers information on the symbolization survey, executed to obtain initial iconset from a crowdsourcing experiment. In Chapter 7 selection of resulting icons from proposed iconset is performed. Chapter 8 covers a validation of improvements in visual effectiveness for notations, augmented with proposed icon set. Finally, Chapter 9 is providing overall summarization of concluded work, as well as drawing broad outline of future activities to be performed. Chapter 10 includes a comprehensive list of references.

### **1.4 Research Methodology**

This subchapter is dedicated to the research methodology and includes the detailed description of methodology which is to be used throughout the paper.

Considering the specifics and magnitude of research questions, it was decided to define a research method as triangulation (Jick, 1979), combining qualitative and quantitative research methods into a unified approach. Overall research methodology is designed according to what could be called a de-facto standard procedure for the visual notation analysis and, with minor variations, is described in a number of highly relevant research papers - namely (Caire, Genon, Heymans, & Moody, 2013), (El Kouhen, Gherbi, Dumoulin, & Khendek, 2015), (Leitner, Schefer-Wenzl, Rinderle-Ma, & Strembeck, 2013) and (Genon, 2016). It should also be noted that out of abovementioned papers, work by Genon (2016) provides the most comprehensive and up-to-date description of visual notation research method and thus should be selected as a primary reference source. However, particularities of Security Risk Management process stipulate that a number of distinctions should be introduced to the research methodology, offered in (Genon, 2016). Hereafter these distinctions are described in detail.

First, it should be noted that unlike the abovementioned papers, which concentrate on the various security-extended modeling languages (Secure BPMN, Secure Tropos, Mal-activity Diagrams and Misuse Cases), this paper focuses on a set of icons, which could later be incorporated in the security-extended languages. Since the anticipated outcome includes development of an iconset for ISSRM risk-based concepts, there should also be iconset aggregation, not required in (Genon, 2016). Furthermore, it should be mentioned that Genon (2016) had access to a revised version of modeling language (i\*), refined by (Moody, Heymans, & Matulevičius, 2010). As for the Security Risk Management-related notations, this paper pioneers the visual notation research. Thus, analysis of existing notations from the

PoN standpoint should be performed prior to the subsequent experiment studies. Furthermore, since enhancing notation with icons is one of the approaches to improve notation, as defined in PoN (Semantic Transparency principle), resulting iconset would be incorporated into the refined notations and compared against the existing versions. Based on the above-mentioned aspects, it was decided to augment the approach of Genon (2016) with several additional ideas, taken from papers by El Kouhen et al. (2015), Leitner et al. (2013) and Caire et al. (2013), and obtain a revised version of the methodology, tailored to the goals and intentions of this paper.

Research questions, presented in Subchapter 1.1, are to be followed via the developed research methodology, which is described below. Overview of the research methodology is represented on Figure 1.

- 1. Background Overview.** Initial step includes brief review of ISSRM domain model. This is followed by a review of available security-oriented modelling languages. Finally, description of existing visual analysis frameworks is also provided and complemented with rationale for framework selection. This step is aimed to provide context for the research as well as to justify the choice of analytical framework.  
*Input:* ISSRM domain model, visual notation analysis frameworks  
*Process:* Overview  
*Output:* Synthesized background data, details on framework choice
- 2. Related Work Overview.** The second step contains overview of papers, describing efforts to evaluate and improve security-oriented modelling notations. Papers are ranging from overviews of various modelling notations to the descriptions of improvement efforts, achieved via language redesign. Based on the overview, effective improvement and analysis techniques could be identified and afterwards applied on subsequent research stages.  
*Input:* Available research on security-oriented modelling languages  
*Process:* Overview  
*Output:* State of the art in security modelling domain, information on visual notation analysis trends, available techniques of obtaining iconic symbols
- 3. Language Analysis.** Subsequent step covers thorough analysis of existing security-extended modeling languages from the PoN perspective. Performed analysis is expected to provide materials and guidelines for modification of available notations, so that four notations in question would adhere to the 9 principles of PoN. Furthermore, this step is included to provide a background on the extensive usage of icons, which are to be designed and refined in the subsequent steps.  
*Input:* Available notations of 4 SRM-extended modeling languages – BPMN, Secure Tropos, Misuse Cases, Mal-activity Diagrams  
*Process:* Analysis  
*Output:* Redesign recommendations for the abovementioned languages
- 4. Evaluation Survey.** This fourth experiment focuses on obtaining users' opinion regarding best representation of ISSRM concepts as presented in four security-extended languages – Secure BPMN, Secure Tropos, Misuse Cases and Mal-activity Diagrams. Participants would be offered 13 questions with representations of security concepts from all 4 above mentioned languages, and they are expected to select the most representative depiction for each of 13 concepts.  
*Input:* Representations of 13 ISSRM concepts from 4 extended modeling languages



*Process:* Survey

*Output:* Evaluation of ISSRM concept representation, perception feedback

- 5. Symbolization Survey.** During this stage, target audience participates in the symbolization experiment. Participants are asked to sketch representations of 13 ISSRM-related concepts, so that resulting icons would be clear and understandable. It should also be noted that symbolization is to be performed by participants with hands-on experience in security modeling, being a part of the professional community.

*Input:* ISSRM domain model concepts

*Process:* Survey

*Output:* Candidate iconset

- 6. Symbol Identification Survey.** Symbol Identification experiment aims to provide information on which icons out of a candidate set (combination of prototype and stereotype sets) should be selected for incorporation into the revised notation. Overall idea of the experiment is somewhat similar to the initial evaluation experiment, since participants would be offered 5 icons for each of 13 ISSRM concepts and would be required to choose one, the most representative, which could be a candidate to be included in icon-enhanced notations.

*Input:* Candidate iconset

*Process:* Survey

*Output:* Resulting iconset

- 7. Validation Survey.** This experiment deals with perception metrics, namely hit rate and semantic transparency coefficient. Hit rate here refers to the ability of symbols to be recognized without errors. As for the transparency, it is focused on immediateness of symbol cognition and is describes the connection between design and symbol definition.

*Input:* Icon-enhanced notations, existing notations

*Process:* Survey

*Output:* Perception metrics (hit rate and semantic transparency coefficient)

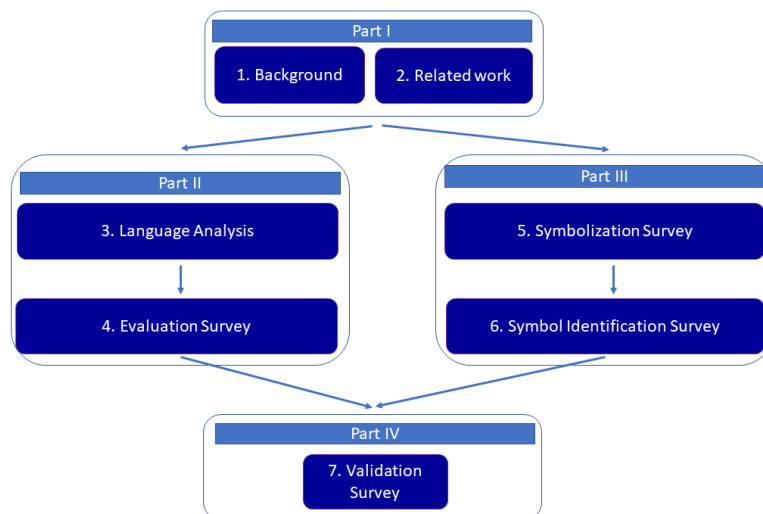


Figure 1. Research Methodology

## 2 Background

This chapter covers the background of performed research and includes the motivation behind the analysis framework selection, overview of Security Risk Management and brief description of SRM-extended modelling languages. The chapter is intended to provide an answer to the first part of the initial research question, which is as follows:

*RQ1. What is the state of the art in the domains of security risk-oriented modelling languages and visual notation analysis?*

### 2.1 Information System Security Risk Management

The present-day reality of information systems could be characterised as being overflooded with various security-related risks. The numerosity of risks places constraints on the possible risk treatments, invoking the need for enterprises to manage potential treats in a cost-effective manner, with a possibility to contrast mitigation activities against costs of potential breaches. Since available security-extended languages, namely Secure Tropos, Mal-activity Diagrams, Misuse Cases and Secure BPMN lacked dedicated risk-oriented tools, it was decided by Dubois et al. (2010) to develop a set of concepts, specifically oriented towards dealing with risk representation on the early stages of information systems development. Authors acknowledge that while one valid course of action would be to design a brand-new modeling language with a pre-built support of security risk management concepts, it might not be optimal due to the substantial number of languages already available, as well as author's adherence to evolutionary and not revolutionary approaches. Thus, ISSRM domain model is intended to cover key risk-oriented concepts and is designed to be used as a basis to extend existing modeling languages. After being extended with SRM concepts, languages are expected to be fully complaint with the proposed domain model and could be used for the risk representation purposes in software development process.

Let us now look at the domain model structure, as specified in (Dubois et al., 2010). Overall, ISSRM domain model consists of three categories, namely asset-related concepts, risk-related concepts and risk treatment-related concepts.

Asset-related concepts are illustrating resources, crucial for the business model of enterprise to succeed, and are comprised of business asset, information system asset and security criterion. While business asset is quite self-explanatory, information system asset requires additional clarification and is defined as a resource, directly related to information technology, such as CRM system or intranet portal. As for the security criterion, is a characteristics of business asset's security needs, with possible options including integrity and confidentiality.

Risk-related concepts are the most numerous category, incorporating risk, impact, event, vulnerability, threat, threat agent and attack method. Threat agent is a person that intends to abuse the information system asset. Method of abuse, employed by threat agent, is called attack method. A combination of attack method and treat agent is defined as threat. A vulnerability is a potential security weakness, that could be exploited. Mix of threat and vulnerability constitute an event. Impact is the potential outcomes of the threat being executed. Risk, in its turn, is a combination of threat with one or several vulnerabilities, resulting in a negative impact and mistreatment of assets.

Finally, risk treatment-related concepts include risk treatment, security requirement and control. Risk treatment is an approach regarding how to deal with the recognized risks, and it could be expressed in terms of avoiding, reducing, transferring and retaining. Security requirements are employed to minimize identified risks. As for the control, it is defined as a practical realization of security requirement, aimed at diminishing potential risks.

It should also be noted that Mayer, Heymans, & Matulevicius (2007) specify a dedicated six-step risk management process, which is to be utilized at the early stages of information system development.

## **2.2 Security Risk Management-Oriented Modelling Languages**

As it was mentioned above, ISSRM model was designed with the emphasis on security-related modelling language extension. While language-extending activities were out of the scope in (Dubois et al., 2010), several papers covering the specifics of ISSRM extension have emerged in years after the work by Dubois et al. (2010) had been published. As of 2017, all major security-oriented modeling languages were extended and adjusted to support the ISSRM concepts, with Chowdhury et al. (2012) extending Mal-activity Diagrams, Al-tuhhova et al. (2013) dealing with Secure BPMN, Matulevicius et al. (2012) adjusting the Secure Tropos and Soomro & Ahmed (2012) refining Misuse Cases.

The detailed description of the language extensions is out of this paper's scope. Overview of notations, utilized in ISSRM-extended modelling languages, could be found in Appendix I.

## **2.3 Rationale for Framework Selection**

Currently, visual notation researchers are offered a choice of three established frameworks, namely Cognitive Dimensions (T. R. G. Green & Petre, 1996), SEQUAL (Krogstie, Sindre, & Jørgensen, 2006) and Physics of Notation (Moody, 2009a). Prior to conducting the subsequent work, it is of paramount importance to analyze the advantages and shortcomings of the abovementioned frameworks in order to identify the most appropriate one. Needless to say, the suboptimal choice would significantly hamper the expected contribution and outcomes of this paper.

It could be said that the most well-established out of the frameworks under review is Cognitive Dimensions. Published by T. R. Green (1989) in what could be considered a classic paper, CDs was envisioned as a practical tool, suitable for solving real-world problems (T. R. Green, Blandford, Church, Roast, & Clarke, 2006) and providing a broad-brush assistance in making design decisions (Dagit et al., 2006). While the initial version of the framework was developed with the idea of being suitable for information-based artifacts irregardless of domain, subsequent paper by T. R. G. Green & Petre (1996) was tailored to be utilized specifically in conjunction with visual notation artifacts. However, in what could be considered a concluding paper (T. R. Green et al., 2006), authors acknowledge that CDs still lacks a well-established procedure or methodology. Since the absence of methodology leads to the problems with comprehension and vague dimensions (T. R. Green et al., 2006), authors propose two approaches that could address the underdevelopment of methodology, but do not provide selection guidelines. Additionally, T. R. Green et al. (2006) acknowledge that they are aware of the existing list of dimensions being vague and overlapping. While it is stated that improvements are being explored (T. R. Green et al., 2006), no practical information on the improvements is provided. Furthermore, in the paper, devoted to CDs evaluation, D. Moody (2009b) indicates that according to Gregor's taxonomy (Gregor, 2006), CDs could be considered a Type I theory, and thus should be treated as a prescientific theory, suitable for analyzing and describing but not appropriate as evaluation criteria or design guidelines (Moody, 2009b). Overall, it could be said that while CDs framework has been widely accepted by visual language researchers (Blackwell, 2006), a number of identified issues prevents it from being an effective tool for designing visually effective modelling notations.

SEQUAL, in its turn, is a framework, based on semiotic principles and tailored to evaluating conceptual models (Krogstie et al., 2006). It could be said that SEQUAL suffers from the similar limitations as CDs, namely high-level generic nature and lack of empirical research, related to the visual notations domain (Granada, Vara, Brambilla, Bollati, & Marcos, 2017). Furthermore, it should be noted that in a paper by D. Moody (2009a), CDs framework is considered as closest theory, resembling visual notation theory, while information regarding SEQUAL is not presented at all. Thus, it could be said that SEQUAL framework is not directly related to the visual notations domain and could not be considered as a better alternative to CDs.

Finally, Physics of Notations was developed by D. Moody (2009a) as a direct successor to CDs, evolving a scientific theory from Gregor's Type I (CDs) to Type IV (PoN). Thus, Physics of Notation was designed as a superior version of CDs, tailored to be applied in the visual notations domain. While PoN possesses certain problems, specifically lack of established design process (da Silva Teixeira et al., 2016) and lack of empirical grounding (Van Der Linden & Hadar, 2015), it is widely accepted by researchers and is extensively utilized for visual notation analysis. Considering the abovementioned aspects and limitations, it could be said that Physics of Notation is the most sophisticated framework, currently available to a notations researcher, and therefore should be used in this research. The following subsection will give a high-level overview of main PoN principles.

## **2.4 Physics of Notation Overview**

As mentioned above, Physics of Notation is a theory for designing and evaluation visual notations. It was proposed by Moody, (2009a) and focuses on the visual notation effectiveness, which is frequently neglected in the Software Engineering-related researches (Moody, 2009a). PoN is based on the renowned work by Bertin (1983) and constitutes a prescriptive theory for visual notations, consisting of nine principles. It should be mentioned that principles are extracted from theoretical and practical studies and offer approaches to both analyse existing notations and design brand-new ones.

According to the principle of semiotic clarity, a one-to-one correspondence between symbols and their respective concepts is expected. Unlike natural languages, having accumulated synonyms and homonyms as a result of language evolution over the years, visual notation languages should showcase explicitness and preciseness. When one-on-one correspondence is not the case, several issues, including symbol redundancy, symbol overload, symbol excess and symbol deficit could occur.

Principle of Perceptual Discriminability implies that it should be possible to easily discriminate between the symbols, with visual distance being a metrics of discriminability. Out of available visual variables, shape is a key characteristic (Moody, 2009a), and a diverse range of shapes is to be used to model effective notations. As a means to improve visual distance, it is possible to utilize redundant coding and use a number of visual variables to clearly distinguish the concepts (Lohse, 1997). If visual elements have a unique value for at least one variable, they tend to have a perceptual pop out effect. Thus, for the notation to become effective, each symbol is expected to have a unique value on at least one visual variable and be easily distinguishable.

Third principle of Sematic Transparency suggests using visual representations with inbuilt meaning, so that the essence could be obtained by perception. Overall, transparency ranges on a scale from inferring immediate meaning to inferring a false (perverse) explanation, with the latter option to be avoided. Since icons, unlike symbolic signs, reduce the learning

curve and improve visual appearance, they are recommended to be utilized instead of abstract symbols for the modelling purposes. It should also be mentioned that transparency could be applied not only to the representation of concepts, but to the depiction of relationships between concepts as well.

Complexity Management principle refers to the ability of notation to depict information without overwhelming human perception. Complexity of diagrams could be measured as a number of elements, represented on a diagram, and it is of paramount importance to have a complexity within the limits. Two types of limits, namely perceptual and cognitive, are invoked by human perception constraints and should be not breached. When cognitive limits are exceeded, cognitive overload occurs. Perceptual breach, in its turn, leads to the inability to discriminate diagrams elements, caused by the overwhelming diagram size.

Principle of Cognitive Integration is relevant for the situations when several diagrams are representing a single information system. For the mutli-diagrams to be efficient, two features, namely conceptual integration and perceptual integration, are to be supported. Conceptual integration could be supported by a summary diagram, providing an overall picture of the system. Contextual information could also be included in each of sub diagrams, showing their relationships and place in the system. Perceptual integration, in its turn, is to be supported by positioning data, with wayfinding technique being universal for any physical space and including four stages of orientation, route choice, route monitoring and destination recognition being supported by identification, level numbering, navigational cues and navigational map.

Sixth principle of Visual Expressiveness encourages to apply the complete set of visual variables, ranging from position to shape. While the majority of visual notation are encompassing only one variable – shape, it recommended to draw inspiration from cartography and utilize an extensive set of visual variables. While colour is one of the most effective variables, which could be used to dramatically improve discriminability, it is recommended to limit its usage to redundant coding due to the possible loss of information (black-and-white printers, colour blindness).

Principle of Dual Coding offers a redefined approach to the usage of text in visual languages. According to (Moody, 2009a), text encoding is most effective when employed in a supportive role, complementing graphical symbols and not substituting them. As already mentioned, text should not be used as a sole means of symbol discriminability. However, text is immensely helpful when utilized as supportive coding, aimed at supporting and clarifying conveyed meaning.

Eighth principle of Graphic Economy specifies that the amount of chosen graphical symbols is expected to be cognitively manageable, and cognitive overload should be avoided. Graphic complexity is especially relevant for the novice users, since they have to maintain the meaning of symbols in their memory until they reach proficiency. There are three established techniques for dealing with graphical overcomplexity: reduce semantic complexity, increase symbol deficit and increase visual expressiveness (Moody, 2009a).

The final principle of Cognitive Fit encourages to use different dialects of visual languages for different target groups and various tasks. While the majority of Software Engineering notations operate single visual representation for all purposes (Moody, 2009a), this approach might not always be optimal. At least two reasons, namely difference between novices and experts and variety of representational mediums encourage designers to produce language dialects, tailored according to the specifics of situation.

## 2.5 Summary

In this chapter, Security Risk Management-oriented modelling languages were reviewed to provide answers to the formulated research sub questions, which are:

***RQ1.1. What is the Information System Security Risk Management domain model?***

ISSRM domain model is introduced by Dubois et al. (2010) and includes a set of concepts, specifically oriented towards dealing with risk representation on the early stages of IS development.

***RQ1.2. What security risk-oriented modelling languages are currently available?***

Secure BPMN, Secure Tropos, Misuse Cases and Mal-activity Diagrams were introduced in papers by Altuhhova et al. (2013), Matulevicius et al. (2012), Soomro & Ahmed (2012), and Chowdhury et al. (2012).

***RQ1.3. What frameworks for the visual notation analysis are currently available?***

Visual notation researchers could choose between Cognitive Dimensions (T. R. G. Green & Petre, 1996), SEQUAL (Krogstie et al., 2006) and Physics of Notation (Moody, 2009a). It should also be noted that while having some limitations, Physics of Notation currently the is the most sophisticated visual analysis framework, widely adopted in the academia.

### 3 Related Work

This chapter includes an overview of available papers, covering the topic of analysing modelling language semantics via the available visual notation-oriented frameworks, and completes the answer to the following research question:

***RQ1.** What is the state of the art in the domains of security risk-oriented modelling languages and visual notation analysis?*

#### 3.1 Semantical Analysis of BPMN

It should be noted that visual notation of BPMN was thoroughly analysed in the paper by Genon, Heymans, and Amyot (2010). Authors start from providing a reasoning behind the selection of analysis framework, motivating their choice between Physics of Notation and SEQUAL. This is followed by a brief overview of Physics of Notation components, namely 9 principles which are to be used for evaluation and improving a visual notation. Subsequently, Genon et al. (2010) provide a detailed analysis of BPMN 2.0 according to 9 principles. Proposed analysis is also complimented with suggestions of visual symbols, which would potentially be a better alternative to existing ones in terms of cognitive effectiveness. However, authors acknowledge that proposed graphical elements are given only for illustrative purposes, are not validated with potential BPMN users, and no effort to provide a comprehensive redefined notation for BPMN 2.0 is made. Thus, the paper is intended to raise awareness and pave the way for discussion among BPMN community, not to act like a redesign guide.

Brief overview of 5 BPMN security extensions could be found in (Maines, Zhou, Tang, & Shi, 2017). While the primarily contribution of the paper is introduction of security-related modelling language extension framework, aspects of notational compliance with PoN principles are also covered. Maines, Zhou, Tang, & Shi (2017) evaluate extensions based on number of PoN principles, which are fulfilled by the extensions. It should be noted that while all the reviewed extensions incorporate iconic symbols, they are able to satisfy only two to four of PoN principles, with one notation even failing to be perceptually discriminable. Thus, it could be concluded that sole presence of icons does not correspond to notational success, and poor design choices can render even iconic-based notation into a poorly perceptible one. Another issue, found in one of the five notations is perverse icon design, making utilization of icons harmful for effective cognition. While Moody (2009a) states that there should be a balance in adhering to the principles since conforming to one may cause a negative effect on the other, certain crucial principles have a priority to be satisfied. Overall, it could be concluded that performed analysis indicates that icons are a powerful tool which is to be handled with consideration, as poor design choices and perverse icons could make a negative impact on the perception, hampering it instead of facilitating.

As for the empirically-based analysis, it is represented in the paper by Leitner et al. (2013). Abovementioned work should also be noted for its focus on cognitive analysis of security concepts, despite those concepts being not identical to ISSRM-specified ones. Since the authors, motivated by unavailability of existing security-related icons, limit the scope to the development of visual elements and not to the analysis of existing graphical symbols, existence of Physics of Notation framework is acknowledged, but its 9 principles are not taken into consideration. Leitner et al. (2013) propose to obtain graphical symbols via a series of experiments, starting from production of drawings. In the first experiment, 43 students of Business Informatics were employed in drawing the best symbol to represent a name and the definition of security concept. As an outcome, researchers were provided with 473 draw-

ings. Subsequently, judges ranking method was applied to those 473 drawings, and stereotypical images of 11 concepts were obtained. Finally, stereotypical images were validated in a series of semi-structured interviews with 6 experts from security, process modeling and visualization domains. As a result, authors suggest that after a minor refinement, resulting set of stereotypical images is suitable to be a basis for icons, which could form a foundation of security-oriented extension to BPMN and/or UML. It should also be mentioned that even though experts agreed on stereotype symbol set's suitability for integration, they also highlighted several symbols which are to be redesigned to avoid redundancy. The summary of BPMN analysis, based on (Genon et al., 2010), could be seen in Appendix II.

### **3.2 Semantical Analysis of UML**

Thorough theoretical analysis of UML visual syntax and its cognitive effectiveness is presented in (Moody & van Hillegersberg, 2008). This paper's approach could be compared to the viewpoint of Genon et al. (2010), with the idea of language being analysed via a set of framework's principles. However, one significant difference of the work by D. Moody and van Hillegersberg (2008) is a selection of framework for analysis, since authors use initial version of Physics of Notation, described in (Moody, 2008). Initial version of the frameworks deviates from defined by Moody (2009a) in the number of principles, with initial 5 principles being extended to 9 in subsequent work. Thus, paper by Moody & van Hillegersberg (2008) is based on the outdated framework and does not provide a complete evaluation of language. Furthermore, it should also be mentioned that even though authors complement evaluation of UML according to each of 5 principles with improvement recommendations, those recommendations are more of the theoretical nature and only a handful of redesigned graphical constructs is offered. Additionally, no end user evaluation is performed, and analysis is based solely on the input by experts. So, paper by D. Moody and van Hillegersberg (2008) aims at initiating the discussion about ways to improve cognitive perception of UML, and is the first step to make UML semantically transparent. Furthermore, it should also be noted that this discussion should be especially promising in the light of creating UML 3.0, with version 2.5 being up-to-date as of now.

Another study, tackling the empirical research on UML perception, is the work by El Kouhen, Gherbi, Dumoulin, and Khendek (2015). Authors decided to start the research with a brief overview of 9 principles, encompassing the Physics of Notation, and evaluation of UML in terms of adherence to the principles. Subsequently, paper describes 3 experiments, which were performed to test the hypothesis of crowd-sourced notation design being superior to expert-developed notation in terms of semantic transparency. Since the aim of the research is to test not the visual notation itself but rather approaches to redesigning notations (specifically, end-user involvement), only several elements of UML were utilized, and the majority of performed empirical experiments, namely Experiments 1, 2, 3, and 4 were reused from (Caire et al., 2013). The key difference in paper by El Kouhen et al. (2015) is the presence of comparison between crowdsourced notation and notation, produced by the experts (in accordance with Physics of Notation principles). Let us now look at the performed sequence of experiments. During the first symbolization experiment, naïve participants produced graphical representations of UML concepts. This experiment was followed by analysis via the judges ranking method, with set of stereotype symbols outlined as a result. Following prototyping experiment was characterized by selection of best representation from stereotype sets by another group of naïve users (undergraduate computer science students with various backgrounds). Final experiment, crucial for semantic transparency, included another group of naïve users, who were asked to infer the meaning of 3 sets of symbols from their visual representation. Among those 3 sets one was crowdsourced (created by naïve



users in Experiments 1-3), and two were designed by experts (standard UML notation; notation, based on Physics of Notation principles).

As a result, the initial hypothesis was confirmed. Crowdsourced set of graphical symbols is more semantically transparent than design, made by experts, and outperforms classical UML notation by 300%. It should also be noted that cultural bias, resulting in differences in perception between individuals with various cultural backgrounds, is overcome by employing naïve users from several distinctive geographical regions. The overview of UML adherence to PoN guidelines, based on (Moody & van Hillegersberg, 2008), could be seen in Appendix III.

### 3.3 Semantical Analysis of i\*

Visual notations in the field of requirements engineering were analysed in the paper by D. L. Moody, Heymans, and Matulevičius (2010). Similar to the majority of abovementioned researches, authors utilize Physics of Notation framework to analyse the current version of i\* visual notation. However, apart from the focus on i\* notation, main difference between (Genon et al., 2010) and (Moody & van Hillegersberg, 2008) is in the systematic and detailed analysis of i\* according to each of the 9 principles, with analysis being complemented by detailed improvement recommendations, which could in fact serve as a guide to redesign i\* notation. Furthermore, most of improvements are also including suggestions of visual symbols, which could contribute to the i\* being cognitively effective. However, while suggested symbols were designed based on Physics of Notation principles and are expected to be visually efficient, empirical studies were not performed, meaning that proposed graphical elements were not validated by end users. Thus, while the paper's primary aims are highlighting importance of visual notation's cognitive effectiveness and suggesting ways to improve i\* notation, presence of detailed improvement suggestions and high concentration of graphical constructs allow it to serve not only as awareness call, but as a first of its kind redesign guide to i\* visual notation.

In what could be considered a follow-up paper, Caire et al. (2013) utilize graphical constructs, proposed in (Moody et al., 2010) and perform several empirical studies, aimed at comparing notation, designed by experts, with notation produced by community (naïve users). Undergraduate students in Economics and Management were employed as target audience (community) in performed experiments. First experiment, focused on symbolisation, empowered participants to generate symbols for i\* concepts. Follow-up stereotype-based experiment included identification of stereotype symbol set, obtained after applying judges' ranking method to the symbols, produced on Stage 1. Subsequently, prototyping experiment was performed by naïve participants, different from Experiment 1 audience, and best drawings for each of 9 i\* concepts were selected from the initial Stage 1 symbols. Afterwards, 65 naïve participants were offered to rate 4 sets of symbols (Standard i\*, Physics of Notation-based i\*, developed by Caire et al. (2013), stereotype i\* (most common symbols by naïve users), prototype i\* (best symbols by naïve users, as judged by other naïve users)). These 4 sets of symbols were evaluated in terms of hit rate and semantic transparency, and obtained results were slightly unexpected by authors. It was proven that graphical sets, generated by naïve users, outperform concepts, created by experts, with semantic transparency being more than 5 times higher. As for the application of Physics of Notation, it has been proven effective, with the hit rate of Physics of Notation-based symbols being twice as higher than for classical i\* notation. Furthermore, the most remarkable outcome is the superiority of prototype symbol set, meaning that most frequently occurring constructs, drawn by naïve users, are superior to the stereotype set, consisting of symbols selected by naïve

users as best. Finally, Caire et al. (2013) performed recognition experiment, where the ability of yet another naïve users to learn and remember symbols from 4 sets has been evaluated. Results of recognition experiment were in line with previous findings, validating the idea that design rationale has significant influence on the recognition error rates. Ergo, the paper is focused on redefining approaches to designing cognitively effective notations, verifying the superiority of crowd-designed notations over expert-produced design. The summary of i\* analysis according to the PoN principles, based on (Moody et al., 2010), could be seen in Appendix IV.

### **3.4 Semantical Analysis of Misuse Cases**

Visual notation of Misuse Cases, derived from UML's Use Cases, is analyzed in the paper by Saleh & El-Attar (2015). As in the previously reviewed papers, authors analyze existing Misuse case notation, proposed in (Sindre & Opdahl, 2005) from the perspective of compliance with 9 Physics of Notation principles. For the evaluation purposes, PoN was chosen over CDs due to a number of limitations of the latter, with lack of evaluation metrics being one of the most crucial CDs shortfalls. The detailed evaluation, topped with a number of specific improvement suggestions, is followed by a description of new notation design, aimed at mitigating the identified issues and discrepancies within the notation and balancing between complexity and improved visual perception. Proposed notation is also empirically evaluated through two surveys. First survey is focused on the semantic transparency, and was distributed in a form of questionnaire, delivered via email. Authors received 55 results (out of 111 invitations), including response from the creator of original Misuse Cases. Based on the responses, Saleh & El-Attar concluded that symbols from revised notation were strongly preferred over the original ones, with misuse case symbol being the only exception. Since the semantic transparency survey covered only individual symbols, not touching the diagrams, a diagram-oriented experiment was also performed across the audience of undergraduate software engineering students. Students were provided with diagrams in both original and refined notation and were asked to fill in the questionnaire. Two variables, namely response time and number of committed errors, were considered as evaluation metrics, and experiment outcomes show that redesigned notation indeed could be read and perceived in a more rapid manner. As for the reading errors, experiment result has not proved the hypothesis that new notation is less error-prone. Furthermore, it should be also noted that in addition to diagram-based questions, students were asked free-from feedback on positive and negative sides of refined notations, and extensive utilization of colour, allowing symbols to be more distinct, was named as a main contributor to positive perception of new notations.

Overall, it could be said that the paper by Saleh & El-Attar (2015) targets notational issues of Misuse Cases, identified with the assistance of PoN analysis, and proposes a redefined notation design, heavily utilizing colour and iconic symbols. Empirical studies have validated the improved semantical transparency and proved that new notation has improved response time.

### **3.5 Gaps Overview**

The most significant gap, related to the analysis of modelling notations for Security Risk Management, is the lack of papers, explicitly targeting the abovementioned domain. Furthermore, a combination of omissions could also be found in papers, relating to the adjacent domains, and since those issues are in fact applicable to the notation-related aspect of all modelling languages, irrelevant of specific domain, they are intended to be addressed in this paper as well.

Firstly, it should be mentioned that clear majority of reviewed papers are focused on either evaluation of existing notation constructs or on development of new graphical concepts set. It could be argued that in the paper by Leitner et al. (2013) it is impossible to perform analysis since initially there is no notation to analyse. However, this is not applicable for other cases due to the presence of initial notations. Furthermore, if to get back to the defined scope there already are several notations developed for security-extended modelling languages. Thus, in this paper it would be crucial to perform analysis of existing visual constructs prior to designing a set of new graphical symbols.

Subsequently, several frameworks could be used for analysing effectiveness of the visual notations, namely Physics of Notation and SEQUAL. Since Physics of Notation is clearly a superior framework, being tailored for analysing visual notations, it is also chosen to be used in this research for analysis.

Moreover, reviewed papers offer miscellaneous approaches to the process of visual notation design. They could be conceptually divided into two categories: expert-based and crowd-based (crowdsourced). Since studies by Caire et al. (2013) and El Kouhen et al. (2015) establish crowdsourced design approach as vastly superior, it seems reasonable that this research is to utilize crowdsourced approach as well.

Finally, the significance of cultural differences in the perception of graphical symbols is explicitly mentioned in (Moody et al., 2010). To diminish cultural factor and ensure uniform perception of visual constructs throughout distinct cultures, it is of paramount importance to perform empirical studies across culturally diverse audience, originating from various regions.

### **3.6 Summary**

In this chapter, existing papers on the analysis of semantic transparency were studied to provide an answer to the following sub question:

***RQ1.4.** What approach is efficient for designing improved visual notation?*

Physics of Notation theory, proposed by Moody (2009a), is specifically suited for the process of refining modeling notations and is superior to other available analysis frameworks. It should be also said that performed overview revealed a couple of requirements, needed for the approach to be effective. First, it would be crucial to perform analysis of existing visual constructs prior to designing a set of new graphical symbols. Furthermore, notation should be designed via crowdsourcing, not designed by experts. Finally, it is of paramount importance to perform empirical studies among culturally diverse audience, originating from various regions.

## 4 Language Analysis

Analysis of 4 ISSRM-extended modelling languages is performed to partially answer the following research question:

**RQ2.** *How are current security risk-oriented modelling notations evaluated?*

Since there are no studies, researching the adherence of 4 extended modelling languages to Physics of Notations are currently available, it was decided to perform a systematic analysis, based on nine PoN principles (Moody, 2009a). Since in the paper by Moody (2009a) analysis metrics are not explicitly defined, prior to conducting the analysis it was decided to extract metrics from the paper contents. Resulting metrics, which were used for the analysis, are represented in the Table 1.

Table 1. PoN analysis metrics

PoN Principle	Metrics	Measure
Semiotic Clarity	Categories of: symbol redundancy, symbol overload, symbol excess, symbol deficit, unique symbols, combined symbols, not represented symbols, symbols with one-to-one-correspondence.	Number of symbols falling under each category
Perceptual Discriminability	Visual variables: size, colour, shape, brightness, texture	Overview of utilization for each variable
Semantic Transparency	Categories of: immediate symbols, opaque symbols, perverse symbols, iconic symbol, symbolic symbols	Percentage of symbols falling under each category
Complexity Management	Elements on the diagram	Number of elements
Cognitive Integration	Cognitive integration principles	Adherence to principles
Visual Expressiveness	Visual expressiveness, visual freedom; Visual variables: horizontal position, vertical position, size, colour, texture, shape, brightness, orientation	Expressiveness degree, freedom degree; utilization of visual variables
Dual Coding	Hybrid symbols	Number of symbols
Graphic Economy	Best practices	Adherence to best practices
Cognitive Fit	Best practices	Adherence to best practices

### 4.1 Principle of Semiotic Clarity

According to the theory of symbols, defined by Goodman (1968), for a notation to satisfy the requirements of notational system there should be a 1:1 correspondence between symbols and the relevant concepts. Thus, prior to performing the analysis it is essential to define both the symbol set and concept set as used in ISSRM-extended modelling languages. As for the concept set, definition is relatively straightforward, and 13 ISSRM concepts covered in (Dubois et al., 2010) could be characterized as language concepts. Symbol sets for the extended modeling notations could be found in pioneering papers by Altuhhova et al. (2013), Matulevicius et al. (2012), Soomro & Ahmed (2012) and Chowdhury et al. (2012). Based on the provided symbols, analysis of the extended modelling languages could be performed from the Semiotic Clarity perspective. For the purposes of analysis, four anomalies, as defined in (Moody, 2009a), are to be considered: symbol redundancy, symbol overload, symbol excess and symbol deficit. These anomalies could be defined as follows:

- symbol redundancy: 1 construct – several symbols;
- symbol overload: 1 symbol – several constructs;
- symbol excess: 1 symbol – no constructs;
- symbol deficit: 1 construct – no symbols.

Outcomes of the semiotic clarity analysis, adopted from (Matulevičius, 2017) are represented in Figure 2.

Semiotic clarity	BPMN	Secure Tropos	Misuse cases	Mal-activity diagrams
One-to-one correspondence	<i>Threat agent</i>	<i>Threat agent</i>	<i>Security criterion, Impact, Vulnerability, Threat agent</i>	<i>Impact, Threat agent, Control</i>
Redundancy	<i>Assets</i>	<i>Event</i>	<i>Assets</i>	<i>Assets, Attack method</i>
Overload	<i>Assets</i>	<i>Assets</i>	<i>Assets</i>	<i>Assets</i>
Incompleteness	<i>Security criterion, Risk, Impact, Event, Vulnerability, Threat, Risk treatment and Control</i>	<i>Risk, Impact, Vulnerability, Threat, Risk treatment, and Control</i>	<i>Risk, Event, Threat, Risk treatment, and Control</i>	<i>Security criterion, Risk, Event, Vulnerability, Threat, and Risk treatment</i>
Under-definition (excess)	<i>Assets, Attack method, and Security requirements</i>	<i>Assets, Security criterion, Attack method, and Security requirements</i>	<i>Assets, Attack method, and Security requirements</i>	<i>Assets, and Security requirements</i>

Figure 2. Comparison of security risk-oriented modelling languages, adopted from (Matulevičius, 2017)

Since the detailed analysis in terms of semiotic clarity is already performed in (Matulevičius, 2017), this work offers a comparative overview according to the semiotic clarity anomalies. The overview is shown in Table 2.

Table 2. Comparative semiotic clarity

Language	Unique Symbols	Combined Symbols	Not represented	One-to-one correspondence	Redundancy	Overload	Deficit	Excess
BPMN	8	3	2	1	1	1	8	3
Secure Tropos	9	1	2	1	1	1	6	4
Misuse Cases	8	3	2	4	1	1	5	3
Mal-activity Diagrams	7	2	3	3	2	1	6	2

As indicated in the table above, the overall number of symbols with one-on-one correspondence is relatively low, with the highest percentage of all represented symbols being 36% for Misuse Cases. At the same time, deficit could be characterized as the biggest issue, with over 70% (8 out of 11) symbols suffering from it. Excess is also notable, with number of affected symbols varying from 2 to 4 among 10-11 symbols in total. Finally, overload and redundancy could be called non-significant as only 1 to 2 symbols across all the notations are targeted by these anomalies.

Overall, the situation with the semiotic clarity across extended modelling languages yields no revelations, as those languages were not tailored to be applied in security risk modelling domain (Matulevičius, 2017). It should also be noted that further refinement along the Physics of Notations guidelines may reduce the number of clarity anomalies.

## 4.2 Principle of Perceptual Discriminability

Perceptual discriminability could be broadly defined as simplicity and accuracy for the graphical symbols to be discriminated between one another (Moody, 2009a). As such, discriminability is determined by visual distance between symbols, characterized as a number of differentiating visual variables and number of perceptible steps. Overall, perceptual discriminability is a crucial characteristic, as according to Winn it determines the speed and

accuracy of symbol recognition (as cited in Moody et al., 2010). Since perceptual discriminability is directly connected to visual variables, defined by Bertin (1983), it was decided to analyze the utilization of five key planar variables (shape, colour, brightness, size, texture) across the four ISSRM-extended notations. The results of analysis are represented in Table 3.

Table 3. Visual variable properties

Language	Shape	Colour	Brightness	Size	Texture
BPMN	Several concepts are represented with identical shapes, existing range of shapes is not sufficient for reliable discrimination	For a number of concepts colour serves as the only means of discrimination, 3 ISSRM concepts groups are represented with corresponding colours – sufficient visual popout	Not utilized	Sufficient, several “add-on” symbols which are to be applied on top are noticeably smaller	Limited, only two border styles (single and bold) are employed
Secure Tropos	Suboptimal, range of shapes is extensive but distinction within several concept groups is complicated due to similar shape appearance	Ineffective, variety of colours is overwhelming, certain concepts are depicted with multicolored concepts which makes the appearance overly patchy, colour scheme is not appealing	Not utilized	Rather effective, initiation of actions is depicted via spatial enclosure and size variations.	Underused, single border style is exploited
Misuse Cases	Only three shapes are used across the notation, distinction is hampered by the shape similarity	Not utilized	Three shades of grey are exploited, utilized shades are hardly discriminable between each other, visual popout is non-existent	Not utilized, elements are of single size	Underused, single border style
Mal-activity Diagrams	Only two shapes are exploited, shape-based distinction can't be performed.	Not utilized	Shades of single grey colour are utilized, differentiation between colours is hindered by similar appearance, no visual pop-out	Efficient, visual discrimination is facilitated via spatial enclosure and size variations.	Underused, single border style

As it could be seen on the table above, extended modeling languages employ visual variables in a suboptimal manner. Colour, that according to Winn is one of the most cognitively effective variables (as cited in Moody, 2009a), is used inefficiently in two out of four reviewed notations. While Secure Tropos possesses relatively minor issue of overwhelming color variety, extended BPMN notation violates PoN principle of robust design, as colour should be utilized only for redundant coding and not as a sole basis for symbol differentiation (Moody, 2009a). As for the two remaining languages, namely Mal-activity Diagrams and Misuse Cases, they do not exploit colour at all and replace it with brightness. Despite several advantages, including printer friendliness, this design choice radically declines visual popout and could be perceived as ineffective. At the same time, proposed in (Altuhhova et al., 2013) usage of colour to mark 3 distinctive groups of ISSRM concepts is an sample of good design, with the similar approach in ArchiMate being described as “an example of graphic excellence” (Moody, 2009a).

Shape, as a primary basis for object identification (Moody, 2009a), is also not used effectively across the notations. Secure Tropos is the only language with a sufficient range of shapes, while span of shapes for all other languages is quite limited. Problem is especially evidential in case of Mal-activity Diagrams, as only two shapes are exploited across the whole notation of 10 (3 are not represented) ISSRM concepts, depicted in (Matulevičius, 2017). According to (Moody, 2009a), discriminability could be achieved via the utilization

of non-resembling shapes from different shape families. It could be clearly seen that this is not the case for extended SRM notations, as existing range of shapes is sufficient only in one (Secure Tropos) of four analyzed notations. While this situation most probably stems from the legacy of non-extended modeling languages, resulting notations do not ensure easy detection of concepts and thus are far from the visual excellence, characterized by Moody (2009a) as utilization of clearly discriminable shapes from various shape families.

Texture here is another example of underused variable, with 1-2 visual options being employed in SRM-extended modeling languages. While texture would not provide sufficient visual popout if used as standalone, it could complement one of main visual variables, be it shape or colour. However, this is not the case as only BPMN exploits two different border styles, while three other notations are content with a single option.

Finally, it could be concluded that while number of used visual variables is expected to ensure sufficient discriminability between symbols, number of poor design choices hamper the visual distance between symbols and affect discriminability in a negative way.

### 4.3 Principle of Semantic Transparency

Semantic transparency characterizes how well the meaning of the symbol can be deduced from its visual appearance. Semantic transparency, defining how well the symbol provide cues to its denotation, could be described by one of three states (Moody, 2009a), which are semantically immediate, semantically opaque or semantically perverse. Overview of notations in terms of the symbol transparency could be seen in Table 4.

Table 4. Semantic transparency characteristics

Language	Total unique symbols	Immediate Symbols	Opaque Symbols	Perverse Symbols	Iconic elements	Symbolic elements
BPMN	8	3/8 37.5%	4/8 50%	1/8 12.5%	4/8 50%	4/8 50%
Secure Tropos	9	0/9 0%	9/9 100%	0/9 0%	0/9 0%	9/9 100%
Misuse Cases	8	2/8 25%	6/8 75%	0/8 0%	2/8 25%	6/8 75%
Mal-activity Diagrams	7	0/7 0%	7/7 100%	0/7 0%	0/7 0%	7/7 100%

As depicted on the table above, overall situation with intuitiveness has space for improvement. First, it should be noted that semantically perverse symbols, which are to be avoided, are not an issue since only BPMN (one out of four languages) has one perverse symbol.

At the same time, iconic symbols, that according to Pierce resemble the concepts they depict (as cited in Moody, 2009a), are underrepresented and included only in two notations out of four total. Since there exists a direct connection between iconic and semantically immediate symbols, lack of icons directly leads to the reduction of immediate symbols, leading to the situations when majority of symbols are semantically opaque. As stated in (Moody, 2009a), utilization of icons could improve the perceptual resemblance, while at the same time making the notation more accessible and appealing to the novice users. Unfortunately, over half of symbols (100% for Secure Tropos and Mal-activity Diagrams) are represented with abstract shapes, providing novice users with absolutely no clue about their meaning and increasing the learning curve as no visual aid to remember the symbol meanings is provided.

It could be concluded that in order to achieve semantic transparency and increase the number of semantically immediate symbols, replacement of abstract shapes with meaningful icons should be performed. As indicated by Saleh & El-Attar (2015), icons are also effective when they not replace but complement existing abstract shapes, increasing overall semantic transparency.

#### **4.4 Principle of Complexity Management**

Complexity management is defined as the ability of visual notation to depict information while not overflowing human mind (Moody, 2009a). While complexity here sounds somewhat broad, it could be further defined as number of elements on a diagram. As such, complexity impacts key metrics, which are perceptual limits and cognitive limits. According to (Moody, 2009a), the most effective way to represent complex situations and diagrams is to allow diagrams to be divided into cognitively manageable chunks. De Marco states that it could be achieved by recursive decomposition, so that diagram elements would be defined by complete diagrams at the next level of abstraction (as cited in Moody, 2009a).

While several complexity management issues were identified in the analysis of non-extended modelling languages, same evaluation could not be applied to the extended versions as in the relevant works by Altuhhova et al. (2013), Matulevicius et al. (2012), Chowdhury et al. (2012), Soomro & Ahmed (2012) and Matulevičius (2017) diagrams are not partitioned and a single unified diagram is utilized. Thus, it could be said that extended versions of the SRM-oriented modelling languages include one single diagram. While the decomposition, made on hierarchical basis, might indeed be beneficial in terms of effective complexity management, lack of related research means that proposing decomposition strategies is out of scope for this work. Overall, it could be concluded that on the current stage evaluation of complexity management strategies is non-viable due to the limited body of available diagrams and lack of complexity-oriented research.

#### **4.5 Principle of Cognitive Integration**

Cognitive integration should be applied when system is represented by more than one diagram. The idea is that since relevant information is spread across a number of diagrams, diagram readers often struggle with keeping the current position and comprehending the complete picture (Siau, 2004). For the multiple diagrams to be cognitively effective, they are to include integration mechanisms, supporting both conceptual integration and perceptual integration (Hahn & Kim, 1999).

As it was already mentioned in the subchapter on Complexity Management (4.4), due to the absence of diagram variety it is reasonable to believe that ISSRM-extended modelling languages currently support only single unified diagram. Thus, analysis of cognitive integration could not be performed as it can only be applicable when multiple diagrams are used to represent the system (Moody, 2009a).

#### **4.6 Principle of Visual Expressiveness**

Visual expressiveness could be defined as a number of visual variables, used in a notation and evaluating overall exploitation of available design space (Moody, 2009a). Based on the visual expressiveness metrics, visual variables of the notation could be divided between two subsets, which are information-carrying variables and free variables.

According to the distribution between visual expressiveness and degrees of visual freedom, notations could range from nonvisual (expressiveness = 0, 8 degrees of freedom) to visually saturated (expressiveness = 8, 0 degrees of freedom). Table 5. characterizes the visual variables as employed in extended modelling languages. Information regarding capacity of visual variables is adopted from (Moody, 2009a), while the overall representation is taken from (Genon et al., 2010).



Table 5. Visual variables

Visual Variable	Capacity	BPMN	Secure Tropos	Misuse Cases	Mal-activity Diagrams
Horizontal position (x)	10-15	Enclosure	Enclosure	Enclosure	Enclosure
Vertical position (y)	10-15	Enclosure	Enclosure	Enclosure	Enclosure
Size	20	2	2	2	2
Colour	7-10	8	11	Not utilized	Not utilized
Texture	2-5	2	1	1	1
Shape	Unlimited	7	7	3	3
Brightness	6-7	Not utilized	Not utilized	3	3
Orientation	4	Not utilized	Not utilized	Not utilized	Not utilized

As it is shown in the table above, all the extended notations have visual expressiveness of 6, and are characterized by 2 degrees of visual freedom. While it could be said that 6 visual variables should in theory be enough to ensure the effective discriminability of notations, suboptimal design choices have negative effect on the discriminability, which is further reduced by a limited range of values for majority of visual variables.

Colour, as one of most cognitively effective variables, is underused in half of languages, as Misuse Cases and Mal-activity Diagrams exploit brightness instead. Furthermore, Secure Tropos has a colour overload, as it utilizes 11 colour options while colour has the maximum capacity of 10. Thus, only one of four notations utilizes full range of colour while remaining within capacity. As for the shape, employing unlimited capacity, it should be said that both Misuse Cases and Mal-activity Diagrams do not exploit full range as only 3 possible shape options are operated across the notations. BPMN and Secure Tropos, in their turn, include 7 possible shapes. However, while this number should be sufficient to ensure effective discrimination between symbols, this is not the case since utilized shapes are from similar shape families. Texture variable is also clearly underused, as only one modelling language has two possible options, with remaining three languages are using only one texture available. While texture could not be called a primary variable, it could be utilized as an additional one, further aiding the discriminability. Finally, despite the big potential of size with a capacity of 20, just two possible options are exploited across all the reviewed languages. Similarly to the texture, size is not a primary distinction variable but could be helpful in assisting role.

#### 4.7 Principle of Dual Coding

Dual coding theory (Paivio as cited by Moody, 2009a) states that text and graphics together transmit information better than either one of them by itself. Text encoding is especially efficient not when it replaces graphics but rather when it complements visual representations. It should also be said that there are several ways to encapsulate textual information, namely annotations and hybrid symbols (Moody, 2009a). Overview of the situation with hybrid symbols could be seen in Table 6.

Table 6. Hybrid symbols overview

Language	Total symbols	Hybrid Symbols	
BPMN	8	0/8	0%
Secure Tropos	9	0/9	0%
Misuse Cases	8	3/8	37.5%
Mal-activity Diagrams	7	0/7	0%

As it could be seen from the table above, only one extended modelling language, namely Misuse Cases, employs hybrid symbols. All the other ones don't make use of this technique. Moody (2009a) indicates that dual coding does not affect discriminability. However, supplementary text encoding assists interpretations by offering clues to the meaning of symbols

and improves retention through interlinked visual and verbal encoding. (Moody 2009a). Since both interpretation and retention are important for the notation to be attractive to novice users, it might be justified to convert non-hybrid symbols into hybrid ones. However, it should be noted that not only hybrid symbols, but also iconic ones provide clues to the symbol meanings. Thus, transformation of iconic symbols into hybrid ones would not be that much viable.

#### **4.8 Principle of Graphic Economy**

Graphic complexity is overall characterized by a number of graphical symbols in the notation, which could be also called size of visual vocabulary. Graphic complexity is especially problematic for novice users, as they need to keep the meanings of symbols in their working memory. As it was shown by empiric studies, graphic complexity has a significant negative effect on novice users (Nordbotten & Crosby, 1999). Moody (2009a) offers three approaches to reduce graphic complexity, which are: reduce semantic complexity, increase symbol deficit and increase visual expressiveness. While in the paper by Moody (2009a) it is indicated that limit of human ability to discriminate between perceptually distinct alternatives, introduced by Miller, is six symbols, it is also said that the limit applies only when single visual variable is used (as cited in Moody, 2009a). As it was noted in the subchapter 4.6, all of the ISSRM-extended modelling languages employ 6 visual variables and thus do not pose challenges to the human cognition. Furthermore, proposed alterations of existing notations, which are to include introduction of semantically immediate icons, are expected to embrace visual popout and additionally improve symbol discriminability.

#### **4.9 Principle of Cognitive Fit**

Cognitive fit theory states that non-resembling representations of information are acceptable for various tasks as well as audiences. In connection with visual notation design, cognitive fit implies that for different audiences (especially for experts and novices) development of different subdialects might be required to facilitate complete understanding of visual representation. Additionally, it might be required to develop a variety of dialects for different representational mediums, including black-and-white printer and hand-drawn sketches (Moody, 2009a).

First, it should be noted that all four extended modelling languages are visually monolingual, proposing one all-rounder visual dialect for all possible utilizations. However, these single dialects do not account for differences between novice and experienced users. Furthermore, current versions of extended notations have a high degree of similarity with non-extended ones, so that minimal number of brand new symbols has been introduced. While this similarity is beneficial for the experienced users who have knowledge of non-extended Secure Tropos, BPMN, and UML, it is not so helpful for novices and only increases the learning curve. Since domain of SRM places heavy emphasis on fruitful collaboration between business novice users and industry professionals, needs of naïve users should be given more priority.

As for the representation mediums, only two out of four languages, namely Mal-activity Diagrams and Misuse Cases, could be represented in black-and-white format without information loss. This is achieved via redundant coding and exploitation of brightness (visual variable) instead of colour. At the same time, underutilization of colour, which is one of the most effective visual variables, could not be called an optimal design choice, especially for notations comprising over 10 symbols. Current extended BPMN notation prevents diagrams from being utilized in non-colour version, since colour is exploited not for redundant coding but rather as sole basis of discrimination between certain symbols. While Secure Tropos

does not solely rely on colour for symbol discrimination, colour coding is also important due to the high degree of similarity between symbol shapes. As for the symbol sketching, situation is somewhat identical since only two notations (Mal-activity Diagrams and Misuse Cases) are straightforward enough to be drawn by hand. Complicated shapes and colour varieties of both Secure Tropos and BPMN would be too big a challenge for limited drawing abilities of software engineers.

Finally, adherence to cultural differences could not be evaluated since the majority of symbols across ISSRM-extended modelling languages are abstract shapes and not icons. However, cultural aspects should be taken into consideration during the development of proposed icons, as reliance on culture-specific associations, commonly utilized to increase semantic transparency, is a potential problem (Moody et al., 2010).

#### 4.10 Redesign Ideas

Based on the performed analysis of 4 security-extended modeling languages, certain patterns could be spotted. Several issues, common for all notations, could be described as incorrect (limited or non-redundant) usage of colours and lack of visually immediate symbols. Since icons could be used as both additional visual variable and as a replacement for opaque symbols, it could be concluded that implementation of icons would improve visual effectiveness. However, it should also be remembered that 4 security-extended languages for the purposes of Security Risk Management are to be considered as not standalone but rather as multiple perspectives of secure software system model (Matulevičius, 2017). Considering the fact that 4 abovementioned languages were specifically extended to support ISSRM concepts, it seems logical to conclude that set of icons, depicting those concepts, should be unified in 4 languages as well. Apart from increasing visual efficiency and intuitiveness, unified set of icons would also streamline transformation between various modeling perspectives and respectively, modeling languages. However, it becomes unclear on the proper procedure for such a set of icons. Based on approaches, outlined in (Genon, 2016), (Caire et al., 2013), (El Kouhen et al., 2015) and (Leitner et al., 2013), it could be concluded that notation crowdsourcing has proven itself to be a reliable and efficient approach. Crowdsourcing here denotes the practice of requesting potential and actual users of anticipated notations to design symbols by themselves, according to their preferences. Since this paper tackles the similar issue, it was decided to use crowdsourcing as a tool to obtain potential set of icons for ISSRM concepts. Following chapter covers the process of obtaining user sketches as well as performing initial evaluation.

#### 4.11 Summary

Four ISSRM-extended modelling languages were analysed for their adherence to PoN principles to answer the sub question:

***RQ2.1.** Do available security risk-oriented modelling languages comply with PoN principles?*

Performed theoretical analysis has revealed a number of inconsistencies with 9 PoN Principles. Incorrect (limited or non-redundant) usage of colours and lack of visually immediate symbols are issues, common for all 4 notations. As icons could be used as both additional visual variable and as a replacement for opaque symbols, augmentation of existing notations with icons would have a positive effect on intuitiveness and visual effectiveness.

## 5 Evaluation Survey

In this chapter initial evaluation survey, which is performed to obtain information on naïve user's perception of existing visual notations, is covered in detail. Evaluation survey is performed to conclude an answer to the following research question:

*RQ2. How are current security risk-oriented modelling notations evaluated?*

### 5.1.1 Audience

Due to the similarities with anticipated potential users of improved ISSRM notations (business background, no previous knowledge of Security Risk Modeling domain), business students were selected as a primary audience for the evaluation experiment. Taking into consideration cognitive fit requirement (suitability of proposed iconset for users with varied cultural backgrounds), experiment was performed in Bosnia and Herzegovina, with business majors from International University of Sarajevo constituting the survey audience. 53 participants from both undergraduate and graduate programs of business domain (37 bachelor students, 14 master students, 2 doctoral students) have filled in the designed questionnaire. Additionally, 6 faculty members also provided their answers, bringing the total count to 59. As for the gender distribution, survey audience was comprised of 22 females and 37 males. All participants possessed certain degree of business information technology knowledge while being previously not exposed to requirements engineering or security modelling. It should be said that skillset of participants is of crucial importance, since they are supposed to possess perception perspective, similar to that of naïve business users.

### 5.1.2 Design

First of all, it should be noted that not all concepts have a visual depiction in all security-extended languages. For the purposes of consistence, missing visual symbols for Control (2 symbols) and Risk Treatment (3 symbols) were designed based on the conventions of the languages and best practices of PoN. Thus, at least 3 variants of representations are available for each ISSRM concept and participants have several options to choose from.

Students would be requested to fill in a designed questionnaire, containing visual depictions (3 to 4) of ISSRM concepts from four security-extended modelling languages (Secure BPMN, Secure Tropos, Misuse Cases, Mal-activity Diagrams), as well as to recognize above mentioned concepts on 4 diagrams (one for each language). Additionally, questionnaire included 3 free-form questions so that participants could express their opinion regarding the overall representation of ISSRM concept groups.

Questionnaire was designed in a printable black-and-white version and was comprised of 12 one-sided pages, covering the total of 26 questions, divided into 3 parts. First 5 questions were intended to collect background data, while subsequent 16 are to capture the particularities of ISSRM concept perception across four modelling languages. Finally, last 5 questions were designed to test symbol recognition on the diagrams and collect survey feedback. It should also be mentioned that none of the questions was mandatory, and in order to accommodate possible selection issues NA options were also provided for every question from 2<sup>nd</sup> part.

Students were expected to read the definition of the concept, look at the available representations and select the most appealing one by putting X or V in the selection box below the relevant image. Estimated time of completion is 20 minutes. Detailed questionnaire design could be found in Appendix IX.

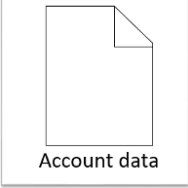
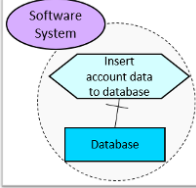
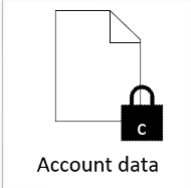
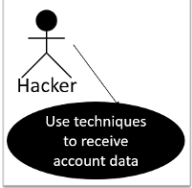
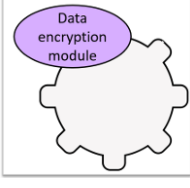
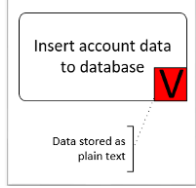
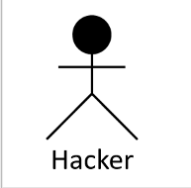
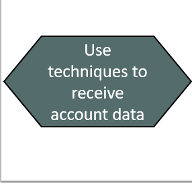

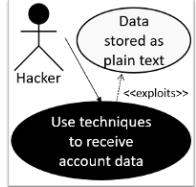
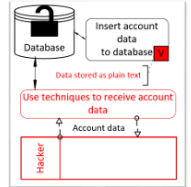
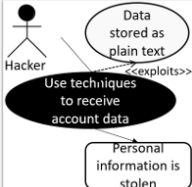


### 5.1.3 Process

Considering the specifics of the Bosnian study process, paper questionnaires were distributed to the students during their classes. Students were afterwards requested to fill in the questionnaire and bring back in one week. Afterwards, papers were manually collected from students and further analysed. It should also be noted that while analysis of web-based questionnaire would be less time-consuming, it was decided that since there was a significant risk of survey having unacceptably low completion rate, paper questionnaire was designed and distributed.

## 5.2 Analysis

59 filled questionnaires were collected from the survey participants. The statistics of performed survey could be seen in the Table 7. Details on pivot tables, utilized for analysis, could be found in Appendix X. As a result, for each ISSRM symbol participants identified one visually appealing symbol from 3-4 options, taken from notations of 4 extended modelling languages. It should be also noted that this chapter provides analysis only of the first two evaluation survey parts. As for the third part, covering symbol recognition in models, it is further analysed in the Chapter 8 as it's intended to provide initial data for the comparison of current modelling notations with icon-enhanced ones.

Table 7. Evaluation survey outcomes

 Account data		 Account data	
Business Asset   46% 27/59	IS Asset   49% 29/59	Criterion   64% 38/59	Threat   49% 29/59
			
Control   56% 33/59	Vulnerability   37% 22/59	Threat Agent   49% 29/59	Attack Method   30% 18/59
			
Impact   47% 28/59	Security Event   34% 20/59	Risk   32% 19/59	Risk   32% 19/59
			
Risk treatment   42% 25/59	Security Requirement   59% 35/59		

Since theoretical analysis of 4 SRM-extended visual notations has been already performed in Section 4, it would now be interesting to compare PoN-based analysis with empirical results.

While certain PoN principles could not be utilized due to their applicability to models rather than standalone symbols, principles of Perceptual Discriminability and Semantic Transparency could be further explored and compared. Overall, it should be said that outcomes of the Evaluation survey correspond to the theoretical analysis. As it could be seen in the Table 7, vast majority of chosen symbols incorporate icons and are semantically immediate. While utilization of colour could not be evaluated due to the survey questionnaire being distributed in black-and-white version, other visual variables as well as semantic transparency characteristics could be easily assessed. Out of symbols for 12 ISSRM concepts (Risk Treatment is not represented in any of 4 languages), only 4 chosen symbols are not comprised of icons (33%). Considering that symbols for three of the concepts (Control, Vulnerability, and Attack Method) do not provide iconic-based options, it could be said that only for 1 concept out of 12 abstract-shaped symbols was chosen over iconic one. This situation occurred with Information System symbol and could be at least partially attributed to the ambiguous appearance of database icon in BPMN, which was seemingly unrecognized by the survey audience. Overall, it should be said that whenever possible, in all cases but one survey audience clearly preferred symbols comprised of icons. This is the case even for situations when corresponding abstract symbols were less visually overloading, as the visual representation of Risk. While symbol form Secure Tropos notation looks less crowded, it was rejected in favour of icon-based representations. At the same time example of Risk illustrates difficulties in choosing between iconic symbols, as drawings from both BPMN and Misuse Cases obtained identical amount of support.

As for the descriptive statistics, only three symbols (Criterion, Security Requirement and Control) have approval of more than half of survey audience, while six more symbols acquired support in the range of 40%-50%. Finally, four last concepts are characterized by quite low level of consensus, between 30% and 40%. Concepts could be characterized not only by support, but also by number of NA answers, indicating difficulties with the selection of visual representation. Only two of all concepts, namely Vulnerability and Security Event, have a high rate of NA (above 10%), with all the others keeping the figure in the range of 5%-10%.

It is also possible to draw direct connections between semantic transparency, as outlined in Table 4, and popularity of languages among participants based on the origins of chosen symbols. As it could be seen, BPMN and Misuse Cases are leaders among symbol occurrences while at the same time being only two languages with iconic symbols already incorporated. While Secure Tropos currently has no symbols, selection of symbols from its notation could be explained by a wide range of shapes as compared to counterparts. As for the Mal-activity Diagrams, it's result is no clearly representing symbols and no icons. Details on pivot table analysis for all 13 concepts could be found in Appendix X.

Table 8. Evaluation survey statistics

ISSRM Concept	Top-scoring symbol	Not Applicable
Business Asset	46%   27/59	8%   5/59
IS Asset	49%   29/59	7%   4/59
Criterion	64%   38/59	7%   4/59
Threat	49%   29/59	7%   4/59
Vulnerability	37%   22/59	14%   8/59
Threat Agent	49%   29/59	8%   5/59
Attack method	31%   18/59	10%   6/59
Impact	47%   28/59	5%   3/59
Security Event	34%   20/59	15%   9/59
Risk	32%   19/59	8%   5/59
Risk treatment	42%   25/59	5%   3/59
Security Requirement	59%   35/59	8%   5/59
Control	56%   33/59	10%   6/59

Table 9. Popularity of languages

Modeling language	Occurrences	Iconic elements	Symbolic elements
BPMN	5	4/8   50%	4/8   50%
Secure Tropos	2	0/9   0%	9/9   100%
Misuse Cases	5	2/8   25%	6/8   75%
Mal-activity Diagrams	0	0/7   0%	7/7   100%
Custom designed	2	NA	NA

As mentioned in subchapter 5.1.2, the questionnaire included two parts, regarding evaluation of individual concepts and diagram concept matching. The detailed results of model perception and concept-matching are represented in Appendix XI.

The results were analysed according to two metrics, taken from the paper by Caire et al. (2013) - hit rate (percentage of correct symbols for model-matching) and semantic transparency coefficient (which is describing connection between symbol design and symbol definition). Authors also highlight that according to the ISO 9168 standard, symbol comprehensibility threshold is set at 67% hit rate. Aggregated data on the ISSRM concepts could be found in Table 10. As it could be seen from the table below, none of the represented concepts has actually achieved the sufficient hit rate level. Thus, it could be said that existing modelling notations are not especially intuitive, and business users require extensive training before they could correctly perceive information, depicted on the SRM-related diagrams.

Table 10. Evaluation survey - aggregation over concepts

Concepts	Mean (hit rate)	Mean (semant. transp. coefficient)	Occurrences
Attack Method	29.66%	0.19	4
Business Asset	28.39%	0.17	4
Control	20.34%	0.07	1
Impact	29.66%	0.19	2
Information System Asset	28.81%	0.18	4
Security Criterion	23.73%	0.12	3
Security Requirement	25.85%	0.14	4
Threat	20.34%	0.09	1
Threat Agent	41.53%	0.32	4
Vulnerability	29.38%	0.19	3

Based on the data, shown in table, it is seen that mean hit rate for individual concepts varies dramatically, from 20% for Threat and Control to 41% for Threat Agent. However, this difference should be attributed not only to the visual depiction of the symbols, but to the overall perception of ISSRM concepts by the target audience as well.

Finally, data on the performance of notations is shown in Table 11. It could be concluded that while BPMN could be called a most well-percieved notation, there is no clear leader and all four notations are below established comprehensibility threshold. Thus, improvement of four notations is clearly needed.

Table 11. Evaluation survey - aggregation over languages

Languages	Mean (hit rate)	SD (hit rate)	Mean (semant. transp. coeff.)	SD (semant. transp. coeff)
BPMN	33.41%	10.30	0.22	0.12
Mal-activity Diagrams	27.60%	9.11	0.16	0.11
Misuse Cases	29.03%	6.75	0.19	0.08
Secure Tropos	27.12%	8.74	0.17	0.10

### 5.3 Threats to Validity

It might be the case that survey design is not quite optimal, and users could have been confused with the presence of NA option since they were instructed to choose the clearest representation among proposed symbols.

As the survey was performed in the end of December, it is possible that participants were overloaded with other academic obligations and have not allocated sufficient time for the symbol selection process.

Considering that no reward was available, and participants were motivated only by their good will and the authority of Associate Professor who assisted with distribution of questionnaires among his students and chair colleagues, some participants might have just selected random symbols and did not effectively participate. It should be also noted that several questionnaires with identical answers for all questions were found on the data preparation stage. As a mitigation strategy, those answers were converted into NA.

An issue also might arise from the visual appearance of questionnaire, which was distributed to students in black-and-white version. While significant discriminability of symbols was ensured by visual variables of brightness, texture, shape, and size, colour was excluded from the symbol recognition process.

Unfamiliarity of target audience with security risk modelling and modelling languages in general was established based on the study program, with modeling-related courses being absent from the curriculum. At the same time, this might not be the case especially for certain master students since master's program could be described as MBA-like, open for students with a variety of pervious professional experience. Same could also be applicable to faculty stuff, since their knowledge of modelling notations was not explicitly evaluated. While to best knowledge previous exposure to modelling could be characterized as minimal, possibility of certain survey participants having substantial modeling experience could not be completely ruled out.

Since all survey participants are from the same university, similar cultural background may have influenced the final choice of symbols. This was partially mitigated by the fact that survey was performed in the internationally-oriented university, with students and faculty coming from different cultures and having experience of intercultural interaction.

### 5.4 Results Comparison

Based on the analysis, perfomed in Subchapter 5.2, it could be said that theoretical findings, presented in Chapter 4, were confirmed by the results of empirical research. As stated in



Chapter 4, performed analysis has revealed that existing ISSRM-extended modelling notations do not satisfy the majority of PoN principles. While several PoN principles, including Graphic Economy and Complexity Management, could not be evaluated due to their orientation on models' level rather than on individual symbols, remaining ones could be further explored.

Following the principle of Perceptual Discriminability, it could be said that existing notations are characterized by a high degree of symbol similarity, especially evidential in Misuse Cases and Mal-activity Diagrams. Similarity between representations of different concepts, combined with underrepresentation of other visual variables, means that users of the notation have hard time telling the symbols apart. While the introduction of icons is not the only possible way of improving discriminability, augmentation of existing symbols with icons should improve visual pop-out and contribute to symbol distinctiveness.

Semantic transparency analysis has revealed a high share of abstract shapes and opaque symbols across the four notations. Secure Tropos, employing only abstract shapes, performs especially bad in terms of transparency. While outcomes of survey indicate that symbols for two concepts, originating from Secure Tropos, were preferred over other 3 notations, all possible options for Attack Method did not include icon-based symbol. As for the second symbol (Information System Asset), its choice was likely driven by the semantic perverseness of the symbol from BPMN. Thus, two notations (Mal-activity Diagrams and Secure Tropos), that were least popular among survey participants, are also characterized by 0 semantically immediate symbols. So, it could be concluded that naïve users prefer notations with high degree of semantic transparency, and its improvement could be achieved via introducing immediate (and not perverse) icons.

Visual Expressiveness, in its turn, could not be fully evaluated through the performed empirical study since survey questionnaire was provided to participants in black-and-white form. Thus colour, being one of most effective visual variables, was unavailable for symbol representation, and it could be assumed that symbol distinction was performed only with shape and brightness. As already mentioned, results of the theoretical analysis revealed that existing range of shapes is limited and based on the empirical study it could be said that end users overall prefer iconic-based immediate symbols over abstract ones.

According to the Cognitive Fit principle, modelling language could be utilized on various representation mediums and exploited by users with different backgrounds and knowledge levels. While suitability to various mediums was not tested by users, graphic complexity of chosen symbols allows to assume that they would be unsuitable for hand drawing. As for the background and knowledge level, iconic symbols should be universally understandable and accessible for novice and experienced users alike.

Overall, it could be said that theoretical findings were reinforced by the empirical study results. Introduction of iconic symbols should contribute to the compliance of modeling languages with PoN principles.

## 5.5 Summary

This survey was performed to acquire insights on the naïve user's comprehension of currently existing SRM-extended notations and to answer the sub question, which is as follows:

**RQ2.2.** *How are available security risk-oriented modelling languages perceived by end users?*

Overall, it could be said that business (naïve) users prefer semantically immediate symbols, comprised of iconic elements. Extended BPMN and extended Misuse Cases are perception

leaders (highest number of symbol occurrences), while at the same time being only two languages with iconic symbols incorporated. As for the model perception, measured via hit rate (percentage of correct answers), it varies from 20% to 41%. So, it could be said that end-users without previous knowledge of SRM notations are not able to perform visual recognition on the sufficient level.

## 6 Symbolization Survey

This chapter includes information on the key experiment, required to design the candidate icon set, and is intended to answer the following research question:

*RQ3. What visual icons could be introduced into available security risk-oriented modelling notations?*

### 6.1.1 Audience

In compliance with the cognitive fit requirement, it was decided to perform the symbolization survey in the Baltics region, namely in Estonia. Considering the specifics of Security Risk Management notations, effectively preventing unexperienced user from designing the visually effective iconic symbols due to the initial steep learning curve, it was decided to combine conventional experts design with crowdsourcing technique, described in (Caire et al., 2013), and have symbols created by crowdsourcing from a group of notation experts. Thus, a questionnaire was designed and sent to security experts, skilled in secure system modelling and dealing with security modeling languages as a part of their everyday work duties while at the same time having no prior experience of notation design. As for the demographics, all survey participants possess graduate degree in Computer Science or Software Engineering (8 Masters, 3 PhD) and are in the age range between 26 and 37.

### 6.1.2 Design

Overall design of the questionnaire is adapted from the corresponding questionnaire, provided in (Genon, 2016). Since the experiment would require participants to draw the perspective icons by hand, it was decided to go with a paper-based questionnaire. Detailed questionnaire design could be found in Appendix XII.

Overall, the proposed questionnaire consists of 2 parts, with first one being focused on demographics information and containing questions regarding gender, age, geographic region and educational level. As for the second part, it consists of 13 pages, one for each ISSRM concept. The typical page includes ISSRM concept definition, real-world concept example, concept keywords, participant instructions, square area for concept drawing and finally, the difficulty rating. Page appearance is similar for all concepts, with the only difference being content in definition, example and keywords. It should be also noted that while overall survey page layout was adapted from (Genon, 2016), it also includes several refinements, namely presence of real-world example and keywords. This alteration is meant to simplify the design process for participants.

### 6.1.3 Process

Overall symbolization process is meant to be started with reading the concept definition, followed by getting acquainted with example and keywords. Afterwards, participants are to provide a concept drawing in the dedicated square area. Finally, complexity of concept depicted is to be rated at the table below on the grade from 1 (very easy) to 5 (very difficult).

## 6.2 Analysis

As a result of symbolization experiment, 11 completed questionnaires were obtained. Thus, each of 13 ISSRM concepts could potentially be depicted by one of 11 produced drawings, with an overall size of potential iconset being 143 symbols. Icons, obtained from survey participants, could be found in Appendix XIII.

According to the proposed research methodology, depicted on Figure 1, symbolization survey is envisioned to provide material for subsequent works, and initial iconset is to be further analysed via the dedicated Symbol Identification survey. Since it seems suboptimal to provide participants with 11 icons to choose from, it was decided to perform a combined stereotyping/prototyping analysis and identify stereotypes (symbols that are most widespread among proposed concept depictions) as well as prototypes (symbols that carry most immediate depictions of certain concept). For the purposes of analysis, it was defined that symbol should be labelled as stereotype based on the degree of stereotypy measure, as introduced in (Howell & Fuchs, 1968). It was also decided that 18% (2/11) would be a minimal support threshold. Combination of stereotype and prototype symbols should comprise proposed candidate iconset, which is to consist of 5 candidate symbols for each concept. Detailed data on the symbol analysis and selection reasoning could be found in Appendix XIV.

As for the overall candidate iconset creation methodology, it could be described as follows. Initially, one stereotype icon for each ISSRM concept was identified whenever possible, as for the stereotype to be present icon needed to have degree of stereotypy of at least 18% (2/11). It was impossible to highlight stereotypes for two concepts, namely Attack Method and Security Requirement.

Subsequent step was focused on the selection of prototypes, which were identified according to the perception of the author and were based on his subjective evaluation of semantical clarity and immediateness. In case total count of candidate symbols for a given concept was less than 5, additional icons, inspired by available stereotype symbols, were designed by the author of this paper so that total number of possible icons for each ISSRM concepts would be 5.

It should also be mentioned that while selection of prototype symbols for each concept was performed solely on the basis of degree of stereotypy measure, stereotypes were chosen in a subjective manner and according to the author's best knowledge. However, established associative templates and semiotic patterns have clearly impacted the result. While it could be said that author has been exposed to various cultural setting and possesses considerable international communication experience, selection of stereotypes still was somewhat influenced by the particularities of cultural background. Thus, in order to ensure widespread immediateness and preserve symbol appropriateness throughout various cultures, it is of paramount importance to perform iconset selection and validation survey in distinct geographical locations, characterized by a variety of settings.

### **6.3 Threats to Validity**

Utilized degree of stereotypy measure was calculated based on results of symbol clustering, performed by the author according to the similarities in visual appearance of symbols. However, there is a chance of certain key symbol features being omitted due to the specifics of clustering process and potential difficulties of SRM experts to express ideas, caused by the lack of drawing fluency.

It might be the case that certain participants were not especially enthusiastic about redesigning the modelling notation as they were quite satisfied with the existing one. So, absence of NA option and questionnaire design, forcing experts to produce their version of symbols, might have pressured the participants into submitting suboptimal drawings, which under different circumstances they would characterize as not acceptable.

With the participants being domain experts, it is reasonable to suggest that a fair share of target audience guessed the intended result of the experiment, meaning that produced answers would also reflect their attitude towards presumable goal of the survey. Additionally,

survey audience might have felt the pressure of evaluation, and interpret the questionnaire in the way that they are asked not only to answer the questions but also to solve the survey goal, enforcing additional constraints and affecting the survey results.

Since all survey participants share similar cultural background, this fact might have influenced their choice of symbols, which would be not so comprehensible by the representatives of other cultures. Additionally, all survey participants possess postgraduate education (Master's or PhD degrees). As comprehension of symbols depends on cultural background and educational level, there is a possibility that produced symbols are somewhat biased and would not be so favorably received by different audiences.

## **6.4 Summary**

This chapter covers the details of symbolization survey and provides an answer to the sub question, which is:

***RQ3.1.** Where could potential iconic symbols be sourced from?*

Since literature review indicated the superiority of crowd-sourced notations, it was decided to exploit the SRM experts for design-related purposes. As a result, 143 symbols (11 participants \* 13 concepts) were obtained and could be characterized as an initial iconset, which is to be refined and narrowed down in the subsequent surveys.

## 7 Symbol Identification Survey

This chapter describes the process of identifying the most suitable symbols to be included in the respective SRM modeling notations and answers the following research question:

*RQ3. What visual icons could be introduced into available security risk-oriented modelling notations?*

### 7.1.1 Audience

As per the cognitive fit requirement, symbol identification element was performed in yet another geographical region – Eastern Europe, with the survey participants originating from Ukraine. Since symbols, which are to be included in the perspective SRM notations, are to be perceived by both experienced and novice users, it was decided to distribute the survey among the professional community. Thus, employees of state-owned IT company, focused on the development and maintenance of railway management systems, were chosen to be the target audience due to the fact that despite certain familiarity with conventional modelling notations (including those of UML and BPMN), Security Risk Modeling techniques are currently not utilized in the work process.

### 7.1.2 Design

Considering the benefits, provided by web-based questionnaire, it was decided to exploit the features of open-source LimeSurvey software and deploy the survey web application to a dedicated server, provided by DigitalOcean hosting service. The overall survey design follows the previously described pattern and consists of two parts, namely Background and Symbol selection. Background part includes questions on age, gender, educational level and prior modelling language knowledge. Symbol selection, in its turn, could be further divided in three sections, covering three groups of ISSRM domain model (Dubois et al., 2010). Each section starts from the definition, which is followed by the descriptions of relevant concepts, provided along with the relevant symbol set. So, participants are offered the selection of 5 symbols for each concept and are requested to choose the best-of-breed. Concepts in each of the 3 sections are concluded with a free-text question, where participants are encouraged to provide unstructured feedback and suggestions. Detailed questionnaire design could be found in Appendix XV.

It should also be mentioned that to ensure full comprehension, survey and instructions were provided to participants in Russian language, with definitions of SRM concepts were taken from the paper by (Dubois et al., 2010) and translated.

### 7.1.3 Process
















Since the symbol identification survey was designed with LimeSurvey and made available in the Internet, process of distribution and obtaining results was rather streamlined. Survey link was sent to perspective participants via corporate email (following the management consent), and filled responses were collected by the backend of LimeSurvey instance, deployed to the cloud server. Afterwards, obtained responses were downloaded from the server and further analysed.

## 7.2 Analysis

As a result, 39 answers from survey participants were collected through online surveying software.

The outcomes of performed survey could be seen in Table 12. Participants selected the most visually appealing symbol out of 5 options, provided for each of 13 ISSRM concepts. Analysis details could be found in Appendix XVI.

Table 12. Identified symbols

											
Business Asset Prototype	33% 13/39	IS Asset Stereotype	41% 16/39	Criterion Stereotype	28% 11/39	Threat Prototype	41% 16/39	Threat Suggestion, based on prototype	41% 16/39	Vulnerability Stereotype	33% 13/39
											
Threat Agent <sup>2</sup> Refined prototype	41% 16/39	Attack Method <sup>3</sup> Suggestion, based on prototype	51% 20/39	Impact Suggestion, based on prototype	28% 11/39	Security Event <sup>4</sup> Suggestion, based on prototype	36% 14/39	Security Event Prototype	36% 14/39	Risk Stereotype	49% 19/39
											
Risk treatment <sup>5</sup> Stereotype	33% 13/39	Security Requirement <sup>6</sup> Prototype	41% 16/39	Control <sup>7</sup> Stereotype	31% 12/39						

First of all, it could be seen in the table above that each of two concepts (Threat and Security Event) are represented by two symbols with identical support. Considering that proposed icon set should include unique icons for 13 ISSRM concepts, it was decided to choose optimal symbols (highlighted in green) based on symbol interconnection. Since “hacker in hood” icon was selected as the clearest representation of Threat Agent, similar icon of hacker with laptop added should serve as icon for Threat. Similar approach could be applied in case of Security Event, where link between Impact and Security Event means that icon with key and keyhole is preferable.

<sup>1</sup> Derived from “Hacker” by Peter van Driel from [www.iconfinder.com](http://www.iconfinder.com) and “Skull and Crossbones” by Andrew Cameron from the Noun Project

<sup>2</sup> Derived from “Hacker” by Peter van Driel from [www.iconfinder.com](http://www.iconfinder.com)

<sup>3</sup> Derived from “Skull and Crossbones” by Andrew Cameron from the Noun Project

<sup>4</sup> “Key in keyhole” by flaticon from [www.freepik.com](http://www.freepik.com)

<sup>5</sup> “Shield” by Marek Polakovic from the Noun Project

<sup>6</sup> Derived from “Checklist” by Aaron K. Kim from the Noun Project and “Shield” by Marek Polakovic from the Noun Project

<sup>7</sup> “Shield” by To Uen from the Noun Project

Additionally, it should be noted that two of icons in Table 12, namely Risk and Vulnerability, have almost identical appearance as they differ only in shape. Thus, to ensure compliance with perceptual discriminability principle (Chapter 4.2), it could be recommended to complement one of these icons with additional visual variables and components.

Origins of the resulting iconset could be found in Table 13. Detailed process of obtaining iconic symbols is described in Chapter 6. As it could be seen from the table, the most common source of inspiration for icons were stereotypes.

Table 13. Icon origins

Symbol Category	Occurrences
Stereotype	6
Prototype	4
Refined prototype	1
Suggestion, based on prototype	4

As outlined in Section 4.9, one of the reasons for designing additional notation dialects might be suitability for manual drawing. Indeed, specifics of SRM process mean that modelling is quite often performed on the traditional mediums, be it paper or whiteboard. Since this scenario does not include utilization of CASE tools, proposed modelling notations (and icons as their component) should be suitable for hand-drawing. Thus, it was decided to analyse resulting icons for their suitability to be hand-drawn. Time constraints and limited drawing skills of software engineers mean that proposed icons should be comprised of easy-to-draw constructs (basic and easily decomposable shapes) while providing sufficient level of discriminability. Considering the visual appearance of icons, it could be said that the icons are fully suitable to be drawn by hand as they are comprised of decomposable and easy-to-reproduce elements.

### 7.3 Threats to Validity

As the survey was performed in the end of December, it is possible that participants were overloaded with the preparations to winter holidays and have not allocated sufficient time for the survey completion process, reducing the quality of answers.

Considering that no reward was available, and participants were motivated only by their good will and the informal request of manager, some participants might have used random basis for the symbol selection process, making their participation virtually ineffective. In order to mitigate this issue, obtained results were analysed for the presence of unusual patterns and outliers.

Since the target audience presumably has very limited experience with modelling languages and is not exposed to modern modelling approaches, it might be the case that intuitive and visual effectiveness of models are not their perceived characteristics.

Since all survey participants share corporate culture and the substantial share of them are alumni of the same university, similar cultural background may have influenced the final choice of symbols.

### 7.4 Summary

This chapter covered the process of identifying the most suitable symbols out of available icon set and answered the sub question, which is as follows:

**RQ3.2.** *Which iconic symbols are preferred by end users?*



End-users favour icons that are semantically transparent and easily distinguishable. Out of all symbol categories, presented in candidate set, stereotypes (symbol that is most widespread among proposed concept depictions) were the most popular. This further reinforces the idea of notation crowdsourcing being superior to other approaches, as the initial selection of stereotypes was performed by distinct audience in another geographical location. Resulting iconset, depicting 13 ISSRM concepts, is to be evaluated in the final, validation survey. Furthermore, based on the concept of Rich Pictures, covered in (Lewis, 1992), it was also decided to produce a stand-alone rich-picture like notation and compare its performance with that of existing SRM extended notations as well as icon-augmented ones.

## 8 Validation Survey

In this chapter Validation survey is described in detail to answer the following research question:

*RQ4. How could the effectiveness of security risk-oriented modelling notations be evaluated?*

### 8.1 Proposed Notations

This survey is aimed to provide a comparison of 4 existing SRM notations versus their icon-enhanced rivals. Revised notations are created based on the icon set, outlined in the Subchapter 7.2, so that existing symbols of all 4 extended notations, taken from the relevant papers, were augmented with introduced icons. As a material for comparison, it was decided to utilize user registration models, adopted from (Matulevičius, 2014). Since the 4 original models were already exploited in the Symbolization survey and could be found in Appendix IX, Validation survey would include only 4 revised models, made with the addition of introduced icons. Additionally, these 4 models were also complemented with a rich-picture like model, comprised solely of iconic symbols and called “Security Ideogram”. Thus, 4 ISSRM notations were contrasted with 4 icon-augmented ones and with dedicated pictogram-based notation so that survey participants could evaluate the effect of icon utilization.

#### 8.1.1 Audience

Validation survey was performed among University of Tartu students, taking the Security Risk Modelling-oriented graduate course. All the participants are majoring in the field of Information Technology, with study programs including Software Engineering (1), Computer Science (2), Informatics (1) and Cyber Security (12). It should also be noted that since the course is highly specialized, students have already been exposed to the domain of Security Risk Modelling or/and have interest in the field. As for the experience with 4 extended modelling notations, participants are expected to possess basic notational knowledge, obtained through several relevant lectures. Thus, survey audience falls under the category of “security experts”, who would potentially use modelling languages to model information systems.

Since extended modelling languages are planned to be utilized by two categories of end users, namely experts and naïve users, survey was also performed within the beginner user audience, comprised of students from Dnipro National University of Railway Transport (Dnipro, Ukraine). The total number of participants is 23, and they are comprised of 6 BSc students, 4 PhD students and 13 MSc students, majoring in Computer Engineering (6), Cyber Security (3) and Software Engineering (14). It should also be noted that all survey participants have the understanding of information technologies and general-purpose modelling languages but have never been exposed to security risk-modelling extensions or ISSRM domain model concepts.

#### 8.1.2 Design

First of all, it should be said that Validation survey is comprised of 47 questions and includes 5 main sections. Detailed survey structure could be found in Table 14.

Table 14. Validation survey structure

Section	Contents
Background	6 questions on participants gender, age, education, study program and knowledge of modelling notations.
BPMN Model	Participants are provided with a BPMN model, designed with utilization of introduced iconset, and textual description of the modelled system. Afterwards, they are requested to match diagram concepts with their names.
BPMN Concepts	Participants are offered 6 BPMN symbols, modelled in two versions – original notation and notation, complemented with icons, and are asked to choose the preferred version.
Secure Tropos Model	Participants are provided with a Secure Tropos model, designed with the utilization of introduced iconset, and textual description of the modelled system. Afterwards, they are requested to match diagram concepts with their names.
Secure Tropos Concepts	Participants are offered 8 Secure Tropos symbols, modelled in two versions – original notation and notation, complemented with icons, and are asked to choose the preferred version.
Misuse Cases Model	Participants are provided with a Misuse Cases model, designed with the utilization of introduced iconset, and textual description of the modelled system. Afterwards, they are requested to match diagram concepts with their names.
Misuse Cases Concepts	Participants are offered 8 Misuse Cases symbols, modelled in two versions – original notation and notation, complemented with icons, and are asked to choose the preferred version.
Mal-activity Diagrams Model	Participants are provided with a Mal-activity Diagrams model, designed with the utilization of introduced iconset, and textual description of the modelled system. Afterwards, they are requested to match diagram concepts with their names.
Mal-activity Diagrams Concepts	Participants are offered 7 Mal-activity Diagrams symbols, modelled in two versions – original notation and notation, complemented with icons, and are asked to choose the preferred version.
Security Ideograms Model	Participants are provided with a Security Ideograms model, designed based on the introduced iconset, and textual description of the modelled system. Afterwards, they are requested to match diagram concepts with their names.
Review	In the final sections, participants are asked to review their answers and to provide overall survey feedback via the open text question.

It should be also mentioned that diagram, utilized for the purposes of matching described concepts with their names and providing data for the validation metrics, is similar for all 5 notations (4 extended languages and Security Ideograms) and originates from (Matulevičius, 2014).

Questionnaire for the survey was designed with the open-source LimeSurvey software and is distributed to the participants in a digital form. LimeSurvey instance was deployed on the cloud server, provided by DigitalOcean. Detailed questionnaire design could be found in Appendix XVII.

### 8.1.3 Process

Survey was introduced to the participants during relevant university classes. Participants were provided with URL link and were given one week to complete the survey. Afterwards, results were downloaded and analysed.

## 8.2 Analysis

This subsection includes results of Validation survey answers provided by both audiences, experts and naïve users. Analysis details could be found in Appendix XVIII.

As mentioned in subsection 8.1.2, Validation survey is comprised of two types of assignments, namely models and individual symbols. Since the analysis approaches to the results of those assignments differ, they are represented in separate tables. The results of individual symbol evaluation could be found in Table 15.

Table 15. Validation survey – evaluation of individual symbols

Language	Concept	Novice users				Expert users			
		new	old	total	support	new	old	total	support
BPMN	Business Asset	22	1	23	95.65%	13	3	16	81.25%
	Information System Asset	17	6	23	73.91%	14	2	16	87.50%
	Vulnerability	15	8	23	65.22%	4	12	16	25.00%
	Attack Method	17	6	23	73.91%	8	8	16	50.00%
	Security Requirement	17	6	23	73.91%	12	4	16	75.00%
	Threat Agent	20	3	23	86.96%	13	3	16	81.25%
Secure Tropos	Business Asset	19	4	23	82.61%	15	1	16	93.75%
	Information System Asset	18	5	23	78.26%	16	0	16	100.00%
	Threat	18	5	23	78.26%	14	2	16	87.50%
	Vulnerability	22	1	23	95.65%	14	2	16	87.50%
	Attack Method	20	3	23	86.96%	12	4	16	75.00%
	Security Requirement	19	4	23	82.61%	15	1	16	93.75%
	Criterion	20	3	23	86.96%	14	2	16	87.50%
	Threat Agent	20	3	23	86.96%	14	2	16	87.50%
Mal-activity Diagrams	Business Asset	18	5	23	78.26%	12	4	16	75.00%
	Information System Asset	18	5	23	78.26%	13	3	16	81.25%
	Impact	19	4	23	82.61%	15	1	16	93.75%
	Attack Method	17	6	23	73.91%	12	4	16	75.00%
	Security Requirement	17	6	23	73.91%	16	0	16	100.00%
	Control	18	5	23	78.26%	15	1	16	93.75%
	Threat Agent	19	4	23	82.61%	16	0	16	100.00%
Misuse Cases	Business Asset	12	11	23	52.17%	11	5	16	68.75%
	Information System Asset	21	2	23	91.30%	14	2	16	87.50%
	Impact	19	4	23	82.61%	16	0	16	100.00%
	Vulnerability	19	4	23	82.61%	16	0	16	100.00%
	Attack Method	16	7	23	69.57%	10	6	16	62.50%
	Security Requirement	9	14	23	39.13%	13	3	16	81.25%
	Criterion	19	4	23	82.61%	13	3	16	81.25%
	Threat Agent	16	7	23	69.57%	13	3	16	81.25%

As it could be seen on the table above, the level of support for the new symbols (augmented with designed icons) is overwhelming, and it could be said that survey participants clearly prefer the icon-enriched notations over the traditional ones. However, certain individual symbols are not well-perceived by the novice and expert users audiences (highlighted with red in the table above). This is the case for BPMN notation, where redesigned symbol, depicting Vulnerability are deemed inferior to previous designs. Similar situation is observed also with Misuse Cases, where support for Security Requirement is also quite low. In order to provide a comprehensive picture of the expert users' evaluation, mean support for each of 10 concepts was also calculated and could be found in Table 16.

Table 16. Validation survey – aggregation over concepts

Concepts	Novice users		Expert users	
	Occurrences	Mean (support)	Occurrences	Mean (support)
Attack Method	4	76.09%	4	65.63%
Business Asset	4	77.17%	4	79.69%
Control	1	78.26%	1	93.75%
Criterion	2	84.78%	2	84.38%
Impact	2	82.61%	2	96.88%
Information System Asset	4	80.43%	4	89.06%
Security Requirement	4	67.39%	4	87.50%
Threat	1	78.26%	1	87.50%
Threat Agent	4	81.52%	4	87.50%
Vulnerability	3	81.16%	3	70.83%

Based on the numbers, shown in Table 15 and Table 16, it could be said that certain individual symbols, having support of less than 50% is indeed not the best candidates and should be further investigated before they could potentially be introduced into respective notations. The detailed results of model-matching (by expert users) could be found in Appendix XVIII.

At the same time, aggregated support figures, shown in Table 16, indicate that overall support for introduced icons is quite high, especially among the naïve users. Expert users are

also quite enthusiastic about the potential of freshly designed icons, as the lowest mean support (for Attack Method) is nevertheless on the 65% level.

As for the evaluation of model-matching survey component, it was decided to adapt overall approach of Caire et al. (2013) and apply the measures of hit rate (percentage of correct symbols) and semantic transparency coefficient (describes connection between design and symbol definition). It is also noted in (Caire et al., 2013) that effective notational symbols should respect the ISO 9186 comprehensibility threshold which is 67% hit rate. Overview of mean hit rate and semantic transparency, grouped by ISSRM concepts, could be found in Table 17.

Table 17. Notational comparison – aggregation over concepts

Concept	Icon-enriched notations						Existing notations		
	Novice users			Expert users			Novice users		
	Occurrences	Mean (hit rate)	Mean (semant. transp. coefficient)	Occurrences	Mean (hit rate)	Mean (semant. transp. coefficient)	Occurrences	Mean (hit rate)	Mean (semant. transp. coefficient)
Attack Method	4	82.61 %	0.80	4	98.44%	0.98	4	29.66 %	0.19
Business Asset	4	40.22 %	0.31	4	87.50%	0.85	4	28.39 %	0.17
Control	1	65.22 %	0.59	1	81.25%	0.78	1	20.34 %	0.07
Criterion	3	39.13 %	0.30	3	75.00%	0.71	3	23.73 %	0.12
Impact	2	65.22 %	0.60	2	100.00 %	1.00	2	29.66 %	0.19
Information System Asset	4	43.48 %	0.35	4	90.63%	0.89	4	28.81 %	0.18
Security Requirement	4	59.78 %	0.54	4	89.06%	0.87	4	25.85 %	0.14
Threat	1	52.17 %	0.45	1	87.50%	0.86	1	20.34 %	0.09
Threat Agent	4	78.26 %	0.75	4	98.44%	0.98	4	41.53 %	0.32
Vulnerability	3	56.52 %	0.50	3	93.75%	0.93	3	29.38 %	0.19

It could be seen that the lowest mean hit rate for answers by expert users is 75%, which is still within the ISO threshold. Icons seem to considerably change the hit rate for novice users, since 4 concepts out of icon-enriched notations have reached the required hit rate threshold while numbers for existing versions of notations are significantly below required 67%.

However, it should also be noticed that according to detailed model-matching figures, represented in Appendix XVIII, expert users were unable to correctly distinguish Criterion symbol in extended BPMN notation, as it's hit rate (62%) is slightly below established ISO threshold. Thus, it could be concluded that icon for Criterion should receive additional attention before it would be fully suitable for implementation.

Finally, descriptive statistics for the modelling languages (answers by expert users) could be seen in Table 18.

Table 18. Notational comparison – aggregation over languages

Languages	Icon-enriched notations								Existing notations			
	Novice users				Expert users				Novice users			
	Mean (hit rate)	SD (hit rate)	Mean (semant. transp. coefficient)	SD (semant. transp. coefficient)	Mean (hit rate)	SD (hit rate)	Mean (semant. transp. coefficient)	SD (semant. transp. coefficient)	Mean (hit rate)	SD (hit rate)	Mean (semant. transp. Coefficient)	SD (semant. transp. Coefficient)
BPMN	55.28 %	20.50	0.48	0.24	89.29 %	5	0.88	0.15	33.41 %	10.30	0.22	0.12
Mal-activity Diagrams	67.08 %	18.76	0.62	0.22	91.96 %	3	0.91	0.12	27.60 %	9.11	0.16	0.11
Mis-use Cases	59.78 %	15.89	0.54	0.18	91.41 %	2	0.90	0.10	29.03 %	6.75	0.19	0.08
Secure Tropos	52.17 %	17.85	0.45	0.20	91.41 %	1	0.90	0.07	27.12 %	8.74	0.17	0.10
Ideograms	57.83 %	14.93	0.53	0.17	90.00 %	4	0.89	0.14	NA	NA	NA	NA

As for the overall perceptiveness of modeling language, which could be described through hit rate and semantic transparency coefficient, figures in the Table 18 show that notations, augmented with proposed iconset, are quite efficient in conveying meanings of concepts. At the same time, the table above indicates that the idea of Ideogram notation, based strictly on introduced icons, is not that efficient and its performance is on the level with traditional notations, complemented with iconset. However, similar performance could be also attributed to the fact that survey participants were already familiar with traditional notations, which was not the case with Ideograms.

### 8.3 Threats to Validity

It should be taken into the account that survey conclusion could also be impacted by the selection of metrics. While hit rate and semantical transparency coefficient have been approved in (Caire et al., 2013), measure of support was not previously utilized in the provided manner.

While survey was proposed for all the students (total of 67), taking security risk modelling-related class at the University of Tartu, only 16 of them decided to complete the survey which was advertised as one of the tools to further improve modelling skills. So, it could be assumed that only the motivated students, interested in the domain, decided to answer all the questions and provide materials for analysis. Motivation and dedication towards survey most likely is also projected on the content of the course as well, which means that students from the survey audience could be considered more skilful in SRM modelling. Additionally, it should be said that the majority of participants are enrolled into the Cybersecurity curriculum, further reinforcing the motivation to contribute to the survey. Thus, it is reasonable to conclude that high numbers for hit rate and semantic transparency coefficient are at least partially caused by student's knowledge of notation elements (concepts of four languages were introduced to the audience during several preceding lectures) and could not be attributed solely to the visual effectiveness of symbols, augmented with introduced iconset.

It is also possible to suppose that through the provided questions survey participants were able to deduce the survey aims and answered accordingly. Having just recently learned four modelling notations, representatives of target audience definitely should not be very thrilled

with the perspective to relearn the meanings of additional symbols, which were to be introduced as a direct result of the survey.

## 8.4 Summary

**RQ4.2** *Should designed iconic symbols be refined prior to the implementation into the subsequent versions of security-risk oriented notations?*

Results of validation survey provided a comprehensive picture on the perception of proposed iconset by target audience. Since symbols are validated once they comply with set thresholds, design of several proposed symbols should be altered before they could be introduced to the modeling notations. Vulnerability icon, as currently available in Secure BPMN, was clearly preferred by the participants over the redesigned version. According to the hit rate, icon for Criterion (in Secure BPMN as well) should also be modernized as it has scored below the defined threshold. Details on symbols which might be refined could be found in Table 19.

Table 19. Icons for refinement

Symbol	Language	Metrics	Audience	Issue
Vulnerability	BPMN	Support	Expert users	Quite low (25%), majority of participants prefer previous version
Security Requirement	Misuse Cases	Support	Novice users	Quite low (39%), majority of participants prefer previous version
Criterion	BPMN	Hit rate	Expert users	Less than ISO threshold

**RQ4.1** *Are security risk-oriented notations, augmented with iconic symbols, more effective?*

Finally, it is now interesting to look at the performance of hit rate (key metrics) in the three distinct datasets (existing notations, novice users; icon-enriched notations, novice users; icon-enriched notations, expert users). Numbers, aggregated by language concepts, could be found in Table 20.

Table 20. Mean hit rate by concepts

Concepts	Mean (hit rate)		
	Existing notations	Icon-enriched notation	
	Novice users	Novice users	Expert users
Attack method	29.66%	82.61%	98.44%
Business Asset	28.39%	40.22%	87.50%
Control	20.34%	65.22%	81.25%
Impact	29.66%	65.22%	100.00%
Information System Asset	28.81%	43.48%	90.63%
Criterion	23.73%	39.13%	75.00%
Security Requirement	25.85%	59.78%	89.06%
Threat	20.34%	52.17%	87.50%
Threat Agent	41.53%	78.26%	98.44%
Vulnerability	29.38%	56.52%	93.75%

On the table above, it could be clearly seen that icon-enriched notations are superior to traditional ones, and addition of icons allows to achieve significant raise in hit rate. While traditional notations require steep learning curve, as evidenced by mean hit rate not raising above 41%, icon-enriched notations at least partially allow unexperienced users to grasp the security-related concepts from the first glance, as four concepts already have hit rate higher than ISO threshold.

Mean hit rates, aggregated by modelling languages, could be found in Table 21.

Table 21. Mean hit rate by languages

Languages	Mean (hit rate)		
	Existing notations	Icon-enriched notations	
	novice users	novice users	expert users
BPMN	33.41%	55.28%	89.29%
Mal-activity Diagrams	27.60%	67.08%	91.96%
Misuse Cases	29.03%	59.78%	91.41%
Secure Tropos	27.12%	52.17%	91.41%
Ideograms	Not applicable	57.83%	90.00%

As it could be perceived from the table above, overall hit rate for the languages within participant groups stays overall on the same level, with insignificant fluctuations. The only deviation is Mal-activity Diagrams, having mean support equal to ISO minimum in icon-enriched version. It should also be noted that Ideogram (icon-based) notation does not actually stand out, as it has hit rate similar to other notations. Thus, it could be said that design of separate icon-based notation is not justifiable in terms of increasing hit rate and improving perception.

Performed empirical experiment has shown that notational symbols, augmented with icons, are clearly preferred by end users over previous depictions and could indeed increase the cognitive effectiveness.



## 9 Conclusion

Finally, the last chapter is providing overall summarization of concluded work, as well as drawing broad outline of future tasks to be conducted.

### 9.1 Summary

Overview of Security Risk Management domain has identified the lack of design rationale behind available SRM-extended modelling notations. Results of analysis, performed according to the Physics of Notations theory, were reinforced by the outcomes of empirical survey and have shown the actual intuitiveness and inefficiency of current modelling notations. Following the established process of “notational crowdsourcing”, a set of semantically transparent icon designs has been obtained from the community of security modelling experts. Survey among potential end users allowed to choose best-of-breed icon for each of 13 ISSRM concepts. Proposed icon set was evaluated with a concluding survey and acquired results have shown the superiority of icon-augmented notations over the traditional ones. While the introduction of semantically transparent icons is not the only possible approach to improve the effectiveness of modelling notations, obtained quantitative data indicate that it’s an effective way to increase hit rate, overall intuitiveness and reduce learning curve.

### 9.2 Answers to Research Questions

*MRQ. How to improve visual effectiveness and intuitiveness of modelling notations for security risk management?*

One empirically proven approach to further improve the effectiveness and intuitiveness of SRM-oriented notations is to augment existing concept symbols with semantically transparent icons. However, this is not the only possible approach, and additional improvements could be made by fully aligning the notations with PoN principles, proposed by Moody (2009a).

*RQ1. What is the state of the art in the domains of security risk-oriented modelling languages and visual notation analysis?*

Available security-risk oriented modelling languages are derived from the traditional modelling languages and are constructed by extending general-purpose modelling languages to support a set of concepts, described in ISSRM domain model (Dubois et al., 2010). The established standard in visual notation analysis is the Physics of Notation theory, described in a seminal paper by Moody (2009a). Proposed analytical approach is specifically tailored for notational assessment and refinement and has been widely used by the researchers (Granada et al., 2017).

*RQ2. How are current security risk-oriented modelling notations evaluated?*

According to the empirical research, existing notations are rather poorly perceived by the end users without previous exposure to SRM-related notations. Performed PoN analysis has also revealed issues with cognitive efficiency from the theoretical perspective.

*RQ3. What visual icons could be introduced into available security risk-oriented modelling notations?*

Perspective icons could be obtained through a well-established crowdsourcing process, described in (Leitner et al., 2013) and (El Kouhen et al., 2015). Unlike in the traditional notation design process, candidate icons are to be drawn by the potential notation end users.

**RQ4.** *How could the effectiveness of security risk-oriented modelling notations be evaluated?*

Effectiveness could be measured with the help of metrics, introduced in (Caire et al., 2013), namely hit rate and semantic transparency coefficient. While those metrics are calculated for each component (concept) separately, aggregated numbers could provide an overall notational characteristic.

Executed experiments indicate that notations, complemented with icons, are favoured by end users and, as evidenced by increase in hit rate and semantic transparency coefficient, could increase the overall cognitive effectiveness of ISSRM-extended notations.

### **9.3 Limitations**

First of all, it should be said that perception of visual symbols is heavily dependent on cultural background. While surveys were performed in different countries (Ukraine, Bosnia and Herzegovina and Estonia), characterized by distinct cultures, traditions and historical circumstances, all three countries nevertheless have strong ties with pan-European identity. Thus, it could be concluded that observed connection between raise in hit rate and introduction of icons may not be applicable in worldwide context.

Design of surveys (especially of Validation survey) was done in a way that participants were shown individual symbols (along with their titles) prior to being asked to identify the same symbols on the provided models. So, it could be assumed that success in matching elements of models (symbols) with their titles could be partially attributed to the fact that survey participants were using visual resemblance with previously seen individual symbols and not just visual appearance of diagrams.

Moreover, it should be also noted that based on the design of questionnaires, participants could have understood the purpose of performed surveys. This might especially be the case for Validation survey, as students, having relatively recently learned the ISSRM-extended notation, could have had limited motivation to identify icon-enriched notations as superior since that would result in extensive re-learning.

### **9.4 Future Work**

While as noted in subchapter 8.4, several symbols might need additional refinement and consideration, proposed unified set of icons could overall be utilized in the subsequent update of SRM-related notations and is suggested to be introduced in the refined versions of Secure BPMN, Secure Tropos, Mal-activity Diagrams and Misuse Cases.

Since as of now SRM-extended modelling notations are not supported by CASE tools, it is also proposed to design a universal security risk modelling-related tool with support of both available SRM notations and icons from proposed iconset.

Finally, it should also be noted that proposed introduction of semantically transparent icons is only one of possible approaches to improve the cognitive efficiency of modelling notations. Since the implementation of proposed iconset covers limited number of PoN principles, additional improvements of notational intuitiveness and visual effectiveness could be achieved via ensuring complete compliance to the Physics of Notation guidelines.

## 10 References

- Altuhhova, O., Matulevičius, R., & Ahmed, N. (2013). An extension of business process model and notation for security risk management. *International Journal of Information System Modeling and Design (IJISMD)*, 4(4), 93–113.
- Bertin, J. (1983). Semiology of graphics: diagrams, networks, maps.
- Blackwell, A. F. (2006). Ten years of cognitive dimensions in visual languages and computing: Guest Editor's introduction to special issue. *Journal of Visual Languages & Computing*, 17(4), 285–287.
- Caire, P., Genon, N., Heymans, P., & Moody, D. L. (2013). Visual notation design 2.0: Towards user comprehensible requirements engineering notations. In *Requirements Engineering Conference (RE), 2013 21st IEEE International* (pp. 115–124). IEEE.
- Chowdhury, M., Matulevičius, R., Sindre, G., & Karpati, P. (2012). Aligning mal-activity diagrams and security risk management for security requirements definitions. *Requirements Engineering: Foundation for Software Quality*, 132–139.
- da Silva Teixeira, M. das G., Quirino, G. K., Gailly, F., de Almeida Falbo, R., Guizzardi, G., & Barcellos, M. P. (2016). PoN-S: A Systematic Approach for Applying the Physics of Notation (PoN) (pp. 432–447). Presented at the International Workshop on Business Process Modeling, Development and Support, Springer.
- Dagit, J., Lawrance, J., Neumann, C., Burnett, M., Metoyer, R., & Adams, S. (2006). Using cognitive dimensions: advice from the trenches. *Journal of Visual Languages & Computing*, 17(4), 302–327.
- Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A Systematic Approach to Define the Domain of Information System Security Risk Management. In S. Nurcan, C. Salinesi, C. Souveyet, & J. Ralyté (Eds.), *Intentional Perspectives on Information Systems Engineering* (pp. 289–306). Berlin, Heidelberg: Springer Berlin Heidelberg. [https://doi.org/10.1007/978-3-642-12544-7\\_16](https://doi.org/10.1007/978-3-642-12544-7_16)
- El Kouhen, A., Gherbi, A., Dumoulin, C., & Khendek, F. (2015). On the semantic transparency of visual notations: experiments with UML. In *International SDL Forum* (pp. 122–137). Springer.
- Fein, R. (2017, October 20). Equifax deserves the corporate death penalty. Retrieved from <https://www.wired.com>
- Genon, N. (2016). *Unlocking Diagram Understanding: Empowering End-Users for Semantically Transparent Visual Symbols* (PhD Thesis). Université de Namur, Press universitaire de Namur.
- Genon, N., Heymans, P., & Amyot, D. (2010). Analysing the cognitive effectiveness of the BPMN 2.0 visual notation. In *International Conference on Software Language Engineering* (pp. 377–396). Springer. Retrieved from [https://link.springer.com/chapter/10.1007/978-3-642-19440-5\\_25](https://link.springer.com/chapter/10.1007/978-3-642-19440-5_25)
- Goodman, N. (1968). *Languages of art: An approach to a theory of symbols*. Hackett publishing.
- Granada, D., Vara, J. M., Brambilla, M., Bollati, V., & Marcos, E. (2017). Analysing the cognitive effectiveness of the webml visual notation. *Software & Systems Modeling*, 16(1), 195–227.
- Green, T. R. (1989). Cognitive dimensions of notations. *People and Computers V*, 443–460.
- Green, T. R., Blandford, A. E., Church, L., Roast, C. R., & Clarke, S. (2006). Cognitive dimensions: Achievements, new directions, and open questions. *Journal of Visual Languages & Computing*, 17(4), 328–365.

- Green, T. R. G., & Petre, M. (1996). Usability analysis of visual programming environments: a ‘cognitive dimensions’ framework. *Journal of Visual Languages & Computing*, 7(2), 131–174.
- Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, 611–642.
- Hahn, J., & Kim, J. (1999). Why are some diagrams easier to work with? Effects of diagrammatic representation on the cognitive intergration process of systems analysis and design. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 6(3), 181–213.
- Howell, W. C., & Fuchs, A. H. (1968). Population stereotypy in code design. *Organizational Behavior and Human Performance*, 3(3), 310–339.
- Jick, T. D. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative Science Quarterly*, 24(4), 602–611.
- Krogstie, J., Sindre, G., & Jørgensen, H. (2006). Process models representing knowledge for action: a revised quality framework. *European Journal of Information Systems*, 15(1), 91–102.
- Leitner, M., Schefer-Wenzl, S., Rinderle-Ma, S., & Strembeck, M. (2013). An Experimental Study on the Design and Modeling of Security Concepts in Business Processes. In *PoEM* (pp. 236–250). Springer.
- Lewis, P. (1992). Rich picture building in the soft systems methodology. *European Journal of Information Systems*, 1(5), 351–360.
- Lohse, G. L. (1997). The role of working memory on graphical information processing. *Behaviour & Information Technology*, 16(6), 297–308.
- Maines, C. L., Zhou, B., Tang, S., & Shi, Q. (2017). Towards a Framework for the Extension and Visualisation of Cyber Security Requirements in Modelling Languages (pp. 71–76). Presented at the Developments in eSystems Engineering (DeSE), 2017 10th International Conference on, IEEE.
- Matulevičius, R. (2014). Model comprehension and stakeholder appropriateness of security risk-oriented modelling languages. In *Enterprise, Business-Process and Information Systems Modeling* (pp. 332–347). Springer.
- Matulevičius, R. (2017). *Fundamentals of Secure System Modelling*. Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-319-61717-6>
- Matulevičius, R., Mouratidis, H., Mayer, N., Dubois, E., & Heymans, P. (2012). Syntactic and semantic extensions to secure tropos to support security risk management. *J. UCS*, 18(6), 816–844.
- Mayer, N., Heymans, P., & Matulevičius, R. (2007). Design of a Modelling Language for Information System Security Risk Management. (pp. 121–132). Presented at the RCIS.
- Moody, D. (2008). Evidence-based Notation Design: Towards a Scientific Basis for Constructing Visual Notations in Software Engineering. (under review).
- Moody, D. (2009a). The “physics” of notations: toward a scientific basis for constructing visual notations in software engineering. *IEEE Transactions on Software Engineering*, 35(6), 756–779.
- Moody, D. (2009b). Theory development in visual language research: Beyond the cognitive dimensions of notations (pp. 151–154). Presented at the Visual Languages and Human-Centric Computing, 2009. VL/HCC 2009. IEEE Symposium on, IEEE.
- Moody, D., Heymans, P., & Matulevičius, R. (2010). Visual syntax does matter: improving the cognitive effectiveness of the i\* visual notation. *Requirements Engineering*, 15(2), 141–175. <https://doi.org/10.1007/s00766-010-0100-1>

- Moody, D., & van Hillegerberg, J. (2008). Evaluating the visual syntax of UML: An analysis of the cognitive effectiveness of the UML family of diagrams. In *International Conference on Software Language Engineering* (pp. 16–34). Springer.
- Nordbotten, J. C., & Crosby, M. E. (1999). The effect of graphic style on data model interpretation. *Information Systems Journal*, 9(2), 139–155.
- Saleh, F., & El-Attar, M. (2015). A scientific evaluation of the misuse case diagrams visual syntax. *Information and Software Technology*, 66, 73–96.
- Siau, K. (2004). Informational and computational equivalence in comparing information modeling methods. *Journal of Database Management*, 15(1), 73.
- Sindre, G., & Opdahl, A. L. (2005). Eliciting security requirements with misuse cases. *Requirements Engineering*, 10(1), 34–44.
- Soomro, I., & Ahmed, N. (2012). Towards Security Risk-Oriented Misuse Cases. In *Business Process Management Workshops* (pp. 689–700).
- Van Der Linden, D., & Hadar, I. (2015). Cognitive effectiveness of conceptual modeling languages: Examining professional modelers (pp. 9–12). Presented at the Empirical Requirements Engineering (EmpiRE), 2015 IEEE Fifth International Workshop on, IEEE.

# Appendix

## I. Notation Overview

While detailed description of extension process is out of scope of this paper, comparison of extended modeling languages, adopted from (Matulevičius, 2017), could be found below. Figure 3 represents the comparison of asset-related concepts. Figure 4 shows the comparative table of risk-related concepts. Finally, Figure 5 depicts the contrast between the representation of risk treatment-related concepts.





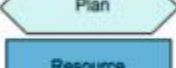
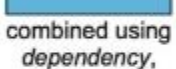

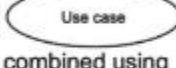



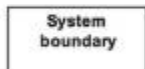





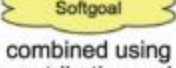
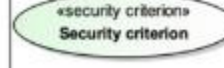
ISSRM	BPMN	Secure Tropos	Misuse cases	Mal-activity diagrams
<b>Assets</b>	  Event Gateway combined using <i>Sequence flows</i>	 Actor  Hardgoal  Plan  Resource combined using <i>dependency, contribution, means-ends, and decomposition links</i>	 Actor  Use case combined using <i>communication, extends, includes links</i>	 Decision  <b>Activity</b> combined using <i>control flow links</i>
<b>Business asset</b>	 Data object	combined using <i>dependency, contribution, means-ends, and decomposition links</i>	 System boundary	 Swimlane
<b>IS asset</b>	 Pool  Data Store			
<b>Security criterion</b>	 c i a added to the <i>Business asset</i> constructs, such as <i>Task</i> or <i>Data object</i>	 Security constraint  Softgoal combined using <i>contribution and security constraint decomposition links</i>	 «security criterion» Security criterion	-

Figure 3. Comparison of asset-related concepts, adopted from (Matulevičius, 2017)






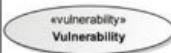











ISSRM	BPMN	Secure Tropos	Misuse cases	Mal-activity diagrams
Risk	Combination of <i>Event</i> and <i>Impact</i>	Combination of <i>Event</i> and <i>Impact</i>	Combination of <i>Event</i> and <i>Impact</i>	Combination of <i>Event</i> and <i>Impact</i>
Impact		impacts →		<b>Mal-activity</b> contained in the <i>mal-swimlane</i> that expresses <i>attack method</i>
Event	Combination of <i>Vulnerability</i> , and <i>Threat</i>	 or combination of <i>Vulnerability</i> , and <i>Threat</i>	Combination of <i>Vulnerability</i> and <i>Threat</i>	Combination of <i>Threat</i> and <i>Vulnerability</i> , if it is implicitly defined
Vulnerability	 added to the <i>IS asset</i> constructs, such as <i>Task</i> or <i>Data store</i>	 added to the <i>IS asset</i> construct such as <i>Goal</i> , <i>Task</i> , or <i>Resource</i>		-
Threat	Combination of <i>Attack method</i> and <i>Threat agent</i>	 	Combination of <i>Attack method</i> and <i>Threat agent</i>	Combination of <i>Attack method</i> and <i>Threat agent</i>
Attack method	  Event Gateway combined using <i>Sequence flows</i>	 potentially combined with other <i>Tasks</i> using <i>decomposition links</i>	 potentially combined with other <i>misuse cases</i> using <i>includes</i> and <i>extends</i> links	As method: <b>Mal-activity</b> combined using <i>control flow links</i> As means 
Threat agent				

Figure 4. Comparison of risk-related concepts, adopted from (Matulevičius, 2017)

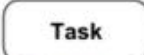



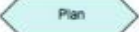


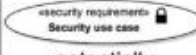
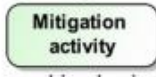

ISSRM	BPMN	Secure Tropos	Misuse cases	Mal-activity diagrams
Risk treatment	-	-	-	-
Security requirement	  Event Gateway combined using <i>Sequence flows</i>	     combined using <i>dependency, contribution, means-ends, and decomposition links</i>	 potentially combined using <i>extends, includes</i> links	 combined using <i>control flow links</i>
Control	-	-	-	

Figure 5. Comparison of risk treatment-related concepts, adopted from (Matulevičius, 2017)

## II. Secure BPMN – Physics of Notation Summary

According to Genon et al. (2010).

PoN Principle	Description
Semiotic clarity	23.6 % symbol deficit, 5.4% symbol overload, 0.5% symbol excess, 0.5% symbol redundancy. While symbol overload and excess could be overlooked, symbol deficit should be dealt with.
Perceptual discriminability	Discriminability should be increased by the usage of shape categories. Extensive utilization of colour should also be introduced.
Semantic transparency	Symbol shapes are not semantically transparent and have no rationale behind the shape selection, existing BPMN icons are semantically opaque and should be replaced.
Complexity management	Existing modularization mechanisms are sufficient.
Cognitive integration	No technique is offered to reinforce integration. Integrations could be improved by introducing diagram level numbering, signposting and navigation maps.
Visual expressiveness	While visual variables are chosen appropriately, colour is underused.
Dual coding	While no issue is noted, text could be further used to facilitate dual coding and decrease the overall number of employed symbols.
Graphic economy	Models currently have a graphic complexity of 171. This is way over the limit, especially for novice users, and should be improved by utilizing dual coding.
Cognitive fit	While the most common symbols are basic shapes, well-suited for representation in different media, no differentiation between notations for novices and experts is offered. So, it might be beneficial to introduce separate language dialects.



### III. UML – Physics of Notation Summary

According to Moody & van Hillegersberg (2008).

PoN Principle	Description
Semiotic clarity	Levels of symbol redundancy, overload, and symbol excess are unacceptably high and should be reduced. Unnecessary symbols should be excluded, existing symbols should be further differentiated between each other, symbol should act as a sole representative of a concept.
Perceptual discriminability	Current symbols are not especially discriminable, only one visual variable (shape) is used for differentiating, selected shapes are similar and often confused. Symbols should have a unique value on at least one visual variable, shapes for various constructs should be easily distinguishable.
Semantic transparency /Perceptual immediacy	UML heavily relies on abstract shapes which do not convey meaning, out of all diagram types icons currently are allowed to be used only in Use Case Diagrams. Perceptually direct shapes instead of simple ones should be used where possible, usage of icons should be extended. Since spatial relationships are more transparent for end-users than arrow-based they should be extensively utilized as well.
Visual expressiveness	Only two visual variables (shape and value) are used in the majority of diagrams, colour is specifically avoided. Since colour is cognitively efficient, it should be introduced and employed across the diagrams. Encoding should be graphical rather than textual, as the cognitive effectiveness of the text is lower.
Graphic economy/ Graphic parsimony	Graphic complexity is overwhelming and should be reduced. Number of constructs in each diagram type is to be shortened, while number of visual variables to differentiate between symbols should be increased.

## IV. i\* - Physics of Notation Summary

According to Moody et al. (2010).

PoN Principle	Description
Semiotic clarity	Symbol redundancy and overload are present, with symbol overload being a particularly significant issue. Redundancy should be solved by ensuring that each concept is denoted by a sole symbol, additional visual variables should be used.
Perceptual discriminability	Shape similarity between symbols is indicated and should be removed. Since relationships are differentiated primarily by the means of text, and their representation is not discriminable, text should be replaced by visual symbols.
Semantic transparency	Semantic transparency is heavily underused, most symbols are represented by abstract shapes. Transparent notation symbols and icons should be utilized to improve the level of transparency.
Complexity management	Overcomplexity of diagrams is a serious issue, effective complexity management mechanisms are missing. Decomposition of all constructs and diagram partitioning should be introduced, recursive decomposition capability should be present as well.
Cognitive integration	Not quite a problem since only two diagrams are available, could be problematic once complexity management is introduced. Diagram names should be replaced with more specific ones, diagram types should be linked, it would be beneficial to introduce contextual and overview diagram (map).
Visual expressiveness	Three visual variables are utilized, overall expressiveness is sufficient. However, colour should be used more effectively, and additional visual variables could be introduced to increase distinguishability.
Dual coding	No use of dual coding, graphics either text. Relationships should be labelled; supportive definitions and textual annotations should be introduced.
Graphic economy	Graphic complexity is currently overwhelming, especially for a novice user. Number of constructs should be decreased; different diagram types could also reduce the graphic complexity of each type. Certain symbols could be shown in form, other than graphical, and usage of multiple variables would also expand the differentiating ability.
Cognitive fit	Single visual dialect is currently available. Several dialects should be introduced based on the knowledge level (expert vs novice), cultural background and representation medium (simplified for hand sketching and enriched).


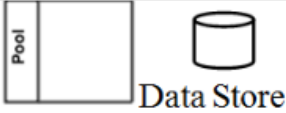




## V. Analysis of Secure BPMN

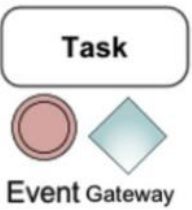
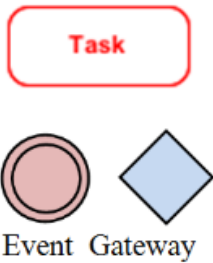
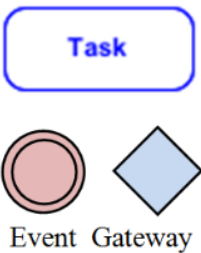
First of all, it should be noted that a thorough analysis of non-extended BPMN from the PoN viewpoint was done in (Genon et al., 2010) and is summarized in Appendix II. Thus, analysis of traditional BPMN is out of scope and is not performed. This chapter is focused solely on the analysis of security-extended BPMN, encompassing the ISSRM concepts as proposed in (Altuhhova et al., 2013).

### Principle of Semiotic Clarity

According to the theory of symbols, defined by Goodman (1968), for a notation to satisfy the requirements of notational system, there should be a 1:1 correspondence between symbols and the relevant concepts. Thus, prior to performing the analysis it is essential to define the symbol set and concept set as used in ISSRM-extended BPMN. As for the concept set, definition is relatively straightforward, and 13 ISSRM concepts covered in (Dubois et al., 2010) could be characterized as language concepts. To distinguish the symbol set, it should be taken into consideration that symbols for certain concepts are composite and not unique across the symbol set. Thus, it is possible to identify a list of symbols along with their category, which is to be defined as unique, combined or not represented. Symbol set of extended BPMN is depicted in Table 22.

Table 22. Symbol set of ISSRM-extended BPMN

ISSRM	BPMN	Symbol Category
Business Asset	 Data Object	Unique
IS Asset	 Data Store	Unique
Threat agent		Unique
Impact		Unique
Security criterion		Unique
Vulnerability		Unique

Assets		Unique
Attack method		Unique
Security requirement		Unique
Risk	Combination of <i>Event</i> and <i>Impact</i>	Combined
Event	Combination of <i>Vulnerability</i> and <i>Treat</i>	Combined
Threat	Combination of <i>Attack method</i> and <i>Threat agent</i>	Combined
Risk treatment	-	Not represented
Control	-	Not represented

Based on the provided symbols list, analysis of the extended BPMN notation could be performed from the Semiotic Clarity perspective. For the purposes of analysis, four anomalies, as defined in (Moody, 2009a), are to be considered: symbol redundancy, symbol overload, symbol excess and symbol deficit. These anomalies could be defined as follows.

- Symbol redundancy: 1 construct – several symbols.
- Symbol overload: 1 symbol – several constructs.
- Symbol excess: 1 symbol – no constructs.
- Symbol deficit: 1 construct – no symbols.

Following the provided definitions, it is now possible to quantify the cases of anomalies. Information System Asset is a clear occurrence of symbol redundancy, as one construct could be represented by two symbols. As for the symbol overload, this seems to be the incident of Information System Asset-Threat Agent, as two concepts are represented by a similar symbol of pool with difference only in colour appearance. Same situation could be observed with Assets – Attack Method – Security Requirement, as they are as well represented by a combination of three similar BPMN symbols (task, event and gateway) with only colour of task symbol ensuring the differentiation. Symbol deficit clearly occurs with

Risk Treatment and Control, since there are no corresponding symbols in extension, provided by Altuhhova et al. (2013). Additionally, three other concepts, namely Risk, Event and Threat, suffer from symbol deficit as they are represented not by a dedicated symbol, but rather by amalgamation of existing ones, used on their own to denote other concepts. Furthermore, as defined by (Matulevičius, 2017), three other concepts (Security Criterion, Impact and Vulnerability) are affected by symbol deficit since not all aspects of those ISSRM concepts could be represented with proposed symbols. Finally, three concepts – Assets, Attack Method and Security Requirements – exhibit symbol excess as they are represented by a combination of three BPMN symbols (task, event and gateway) which on their own do not depict any of ISSRM concepts. Based on the abovementioned clarity-related issues, relevant modifications to problematic symbols should be introduced on the notational level.

### **Principle of Perceptual Discriminability**

Perceptual discriminability is defined as both the simplicity and the accuracy with which the graphical symbols could be told apart (Moody, 2009a). As such, discriminability is determined by visual distance between symbols, which could be characterized as a number of visual variables on which they differentiate and number of perceptible steps. Thus, prior to performing the analysis, it would be required to define a set of visual variables, currently used in ISSRM-extended BPMN notation. Based on the symbol set overview, presented in Table 22, it is possible to deduce that four visual variables, namely colour, shape, size and texture (appearance of borders) are currently employed for the discriminability purposes. While 4 visual variables should be sufficient to ensuring distinguishable symbol appearance, this not the case due to the particularities of variable application in the notation design.

The prime visual variable, shape, is presently applied in a suboptimal manner. While selection of shapes allows distinction between representations of Business Assets and Information System Asset, same could not be said about other symbols. Information System Asset and Threat are represented by an identical shape, based on the pool symbol of non-extended BPMN, and could be differentiated only by colour. Same occurs in the group of three concepts (Assets, Attack Method, Security Requirement), which are represented by a combination of similar shapes, derived from BPMN symbols of task, event and gateway. Following the abovementioned pattern, these symbols could be represented only by colour. Finally, Impact and Security Criterion are represented by a similar shape of lock with differences in lock shackle appearance, denoting a degree of similarity as well as ensuring differentiation from other concepts.

As for the usage of colour, it should be said that colour could be used to improve discriminability between symbols but should not serve as only means of discrimination. However, Altuhhova et al. (2013) propose colour coding to distinguish between various groups of ISSRM constructs (asset-related, risk related and risk treatment related). This approach results in situation when two groups of concepts (Information System Asset – Threat Agent and Assets – Attack Method – Security Requirement) could be distinguished only by colour, which is not acceptable. While Altuhhova et al. (2013) acknowledge familiarity with PoN principles and suggest that alternative notation could be designed for black/white printing purposes, colour as single means of discrimination is not a good practice due to several other reasons, including colour blindness, and should be complimented by additional visual variable. Colour is especially effective for redundant coding, allowing easy discrimination and high degree of visual pop-out. However, in the proposed BPMN notation colour is used as a distinguishable variable and it's redundant coding potential is not exploited. Thus, it

should be said that abovementioned symbols require the addition of extra visual variable, such as shape (iconic) or texture, for the discriminability purposes.

Due to the specifics of notation size is not extensively utilized. However, it seems quite in place for distinction of what could be called “add-on concepts”, as symbols for Vulnerability, Impact and Security Criterion are to be applied on top of other symbols and are noticeably smaller.






Finally, usage of texture (border appearance) is limited, and only two solid styles of border line (single solid and double solid) are utilized across the symbol set. Since in comparison with traditional BPMN texture seems underexploited, it might be a good idea to expand the texture appearance options and use texture to ensure effective distinction between the symbols, currently discriminated only by colour. Finally, It could be concluded that while number of used visual variables is expected to ensure sufficient discriminability between symbols, number of poor design choices hamper the visual distance between symbols and affect discriminability in a negative way.


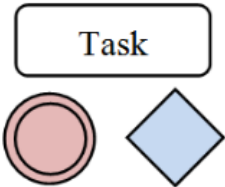
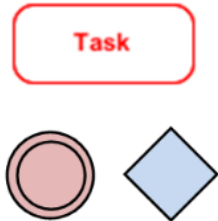
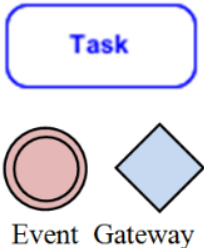
### Principle of Semantic Transparency

Semantic transparency is to be defined as how well could the meaning of the symbol be deduced from its visual appearance. Semantic transparency, defining how well the symbols provide cues to their meaning, could be described by one of three states (Moody, 2009a), which are *semantically immediate*, *semantically opaque* or *semantically perverse*.

So, semantic transparency is to be determined for each symbol. Transparency characteristics of extended BPMN symbol set (only unique category) are covered in the Table 23.

Table 23. Semantical transparency of extended BPMN symbol set

ISSRM	BPMN	Semantic Transparency	Sign type
Business Asset	 Data Object	Perverse	Iconic
IS Asset	 Data Store	Opaque/ Immediate	Symbolic/ Iconic
Threat agent		Opaque	Symbolic
Impact		Immediate	Iconic
Security criterion		Immediate	Iconic

Vulnerability		Opaque	Symbolic
Assets		Opaque	Symbolic
Attack method		Opaque	Symbolic
Security requirement	 Event Gateway	Opaque	Symbolic

Based on the guidelines, provided in (Moody, 2009a), it could be said that semantically pervasive symbols should be redesigned, and semantical immediateness is to be embraced whenever possible. As for the semantically immediate symbols, one way to achieve immediateness is to implement icons instead of abstract symbolic signs. Icons are utilized in extended BPMN notation, and all semantically immediate symbols (Impact, Security Criterion and partially Information System Asset), as defined in Table 23, are in fact icons. However, usage of icons is not so straightforward, as shown in the situation with Business Asset and previously described in (Genon et al., 2010). While data object symbol is an icon, its visual appearance resembles stick-it note and bears no association with Business Asset whatsoever. Since semantically perverse symbols are confusing the notation end users, best practice is to have them redesigned.

As for the opaque symbols, a clear pattern of them being symbolic signs is also visible. Overall, usage of semantically opaque symbols is permissible. However, it should be noted that replacement of abstract shapes by icons is makes the diagrams friendlier to novices. Additionally, it should be mentioned that icons are encouraged to be used along the other visual variables to ensure redundant coding and improve symbol discriminability. Taking into consideration the results of discriminability analysis, performed in subchapter 0, augmentation of existing symbols by introduced icons would ensure effective redundant coding and improve the visual pop-out. Thus, it is recommended to augment the symbolic appearance of Information System Asset (pool sign), Threat Agent, Assets, Attack method and Security requirement with semantically immediate icons.

Finally, Vulnerability symbol is also semantically opaque and should be refined. Even though, as defined in (Matulevičius, 2017), Vulnerability concept in BPMN serves in a limited role of Vulnerability point, it's current shape is that of square. Thus, it is recommended to replace the square with a circle, which is expected to be semantically immediate representation of vulnerability point.

### **Principle of Complexity Management**

Complexity management is defined as ability of a visual notation to depict information while not overflowing human mind (Moody, 2009a). While complexity here sounds somewhat vague, it could be further defined as number of elements on a diagram. As such, complexity impacts key metrics, which are as perceptual limits and cognitive limits.

While complexity is a diagram-level issue, possible improvements are to be performed on the notation level. It should also be mentioned that effective techniques include modularization and hierarchical organization (Moody, 2009a). Since ISSRM-extended BPMN on the notational level is similar to the non-extended version, it seems justified to start the analysis from stating information, adopted from the paper by Genon et al. (2010).

So, BPMN 2.0 provides several mechanisms to deal with the complexity of diagrams, including viewpoints, Link Events and Sub Processes. Viewpoints provide modelling along 4 different viewpoints that correspond to the 4 different types of diagrams. Link Events combined with Sub Processes enable vertical decomposition of diagrams in two levels: high-level view (collapsed sub process) and a fine-grained one (expanded sub process). Structuring, which could be achieved by Sub processes, allows the system to be represented with different detalization levels. However, as noted by Genon et al. (2010), different levels should be represented in independent diagrams instead of expanding into parent diagrams.

While all the above-mentioned information is applicable to extended BPMN, there are also certain extension-specific features. As proposed by Altuhhova et al. (2013), three groups of ISSRM concepts are colour coded and differentiated between each other. Thus, diagram levels could be organized not only on the basis of detalization levels, but derived from distinct groups of ISSRM concepts.

### **Principle of Cognitive Integration**

Cognitive integration should be applied when system is represented by more than one diagram. The idea is that since relevant information is spread across a number of diagrams, diagram readers often struggle with keeping the current position and comprehending the complete picture. For the multiple diagrams to be cognitively effective, they are to include integration mechanisms (Moody, 2009a), which are conceptual integration and perceptual integration. As it was already mentioned in the Complexity Management principle, BPMN notation supports multiple diagrams. However, as pointed out by Genon et al. (2010), no technique is available to reinforce perceptual or conceptual integration. Out of a pool of mechanisms, including diagram level numbering, signposting, navigational maps, none are currently implemented. As suggested by Genon et al. (2010), navigational map could be created on the basis of Link Events and Sub Processes. As for the contextualization, it is partially achieved by the integration of expanded Sub Processes into parent Activities. Since extended BPMN in terms of cognitive integration is similar to non-extended one, proposed changes could also be considered and implemented.



## Principle of Visual Expressiveness

Visual expressiveness could be defined as a number of visual variables, used in a notation and evaluating overall exploitation of available design space (Moody, 2009a). Based on the visual expressiveness metrics, visual variables of the notation could be divided between two subsets, which are information-carrying variables, and free variables.

According to the distribution between visual expressiveness and degrees of visual freedom, notations could range from nonvisual (expressiveness = 0, 8 degrees of freedom) to visually saturated (expressiveness = 8, 0 degrees of freedom). The Table 24 summarizes information on power (highest measurement level that could be encoded), capacity (number of possible values for each variable) and values as employed in extended BPMN. Information regarding power and capacity of visual variables is adopted from (Moody, 2009a), while the overall representation style is taken from (Genon et al., 2010).

Table 24. Visual variables of BPMN, partially adopted from (Moody, 2009a)

Visual Variable	Power	Capacity	Extended BPMN values
Horizontal position (x)	Interval	10-15	Enclosure
Vertical position (y)	Interval	10-15	Enclosure
Size	Interval	20	Normal (symbolic representation), small (iconic representation)
Colour	Nominal	7-10	Black, red, yellow, grey, blue, dark red, pink, azure.
Texture	Nominal	2-5	single solid, double solid
Shape	Nominal	Unlimited	circle, roundangle, diamond, rectangle, various icon shapes
Brightness	Ordinal	6-7	Not utilized
Orientation	Nominal	4	Not utilized

As it could be seen from the Table 24, ISSRM-extended BPMN has a visual expressiveness of 6 and is characterized by 2 degrees of visual freedom. However, it should be mentioned that while visually 6-dimensional notation of extended BPMN is considered to be sufficient for the discriminability purposes (Moody, 2009a), poor design choices have a negative impact on the pairwise visual variation across visual vocabulary, as described in subchapter 0.

As for the overall overview of exploited visual variables, it is provided as follows. Both horizontal and vertical positions could be utilized to depict intervals. However, similar to the situation with non-extended BPMN (Genon et al., 2010), both variables are employed only to denote enclosure (location of symbol inside of another one) and are not fully exploited.

Usage of size in extended BPMN could be characterized as a step forward, comparing with the non-extended version, and is closely connected to the positioning (enclosures). Since iconic representations are expected to be contained in another symbols, their representation in size differ, allowing end users to discriminate between symbols with added easiness.

It could be said that visual variable of texture is somewhat underused, since out of 5 possible perceptible steps only two are currently incorporated.

As for the colour, it's usage in extended BPMN notation violates the best practices and should be refined. Currently 9 colours could be present on the diagram, meaning that 9 out of 10 perceptible steps are in place. However, while colour is one of the most cognitively effective of all visual variables (Moody, 2009a), it's usage should follow the robust design guidelines. According to the robust design principles, outlined by D. Moody (2009a), colour could be used only for redundant coding. As it was already mentioned in subchapter 0, this

is not the case for the notation, proposed by Altuhhova et al. (2013), and colour is currently used as a sole basis of differentiation between a number of symbols. Such utilization of colour clearly violates the robust design principles and should be optimized by adding supplemental visual variable like texture or icon-based shape.

Considering the variable of shape, it should first be noted that it's the only variable featuring unlimited capacity. As for the utilization of shapes in extended BPMN notation, it could be said that a combination of abstract shapes with iconic ones should provide sufficient discrimination capabilities. However, as already mentioned, the majority of existing shapes, adopted from non-extended BPMN, suffer from being semantically opaque, with even one case of semantically preserve shape. So, as outlined in subchapter 0 and covered in (Genon et al., 2010), existing abstract shapes should be replaced or augmented by their semantically immediate counterparts.

Finally, extended BPMN notations makes no use of two remaining visual variables – Brightness and Orientation. While no specific details are provided, it should be noted that instead of potentially overloading available variables, it is possible to employ those currently not utilized for obtaining potential benefits from dual coding and increasing visual expressiveness.

### **Principle of Dual Coding**

According to the dual coding theory, text and graphics in combination convey information better than either one of them by itself. There are several ways to encapsulate textual information, namely annotations and hybrid symbols (Moody, 2009a). In the current version of notation, dual coding is used to denote four concepts – Vulnerability, Security Criterion, Business Asset and Information System Asset. Starting from Vulnerability depiction, it could be said that available symbol is not especially informative. While it was already proposed to alter shape of the Vulnerability and introduce a circle instead (as more semantically immediate visualisation of Vulnerability point), increased visual perceptibility could also be achieved by refining a hybrid symbol and complementing existing graphical symbol with textual information. Similar pattern could also be applied to the Security Criterion, since current version with just first letter inside the lock shape seems to be incomplete. It could be assumed that addition of complete Security Criterion option name, such as “Confidence” for “C” letter, would include the discriminability as well as recognition of the symbol. Considering the consistence and shape similarity, it is also suggested to transform Impact symbol into a hybrid one, so that the appearance of all lock-shaped symbols would be kept in line.

As for the other two concepts, namely Information System Asset and Business Asset, they offer the example of effective dual coding usage. Thus, only possible upgrade would be the replacement of Business Asset icon with a more semantically immediate one.

Finally, it should be noted that for the remaining symbols (Threat Agent, Assets, Attack Method, Security Requirements), it has already been proposed to complement colour coding by introduction of additional icons. Since two visual variables (colour and shape) are sufficient for the easy differentiation between symbols, additional colour coding would be excessive.

### **Principle of Graphic Economy**

Graphic complexity is overall characterized by a amount of graphical symbols in the notation, which could be also called size of visual vocabulary. As denoted in Table 22, extended BPMN employs 14 symbols, and is therefore overwhelming. D. Moody (2009a) offers three

approaches to reduce visual vocabulary, which are reduce semantic complexity, increase symbol deficit and increase visual expressiveness.

Symbol deficit is already present in the notation, so it won't be helpful in reducing the complexity. Reduction of semantic complexity is the most straightforward approach, aimed at analyzing the unnecessary symbols and excluding them from the notation. However, the overall number of symbols is specified by ISSRM domain model, and can't really be reduced. Thus, the only applicable approach is related to the improvement of visual expressiveness by increasing the visual distance between symbols. It should be noted that analysis of previous Physics of Notation principles already included practical recommendations, such as implementation of dual coding and immediately perceptive icons. So, it could be concluded that refined notation would already be characterized by increased visual expressiveness, and no additional steps are required for improving it. Finally, it should also be mentioned that one additional approach to reduce semantic complexity is to implement additional language dialect. This suggestion is further covered in the subsequent subchapter.

### **Principle of Cognitive Fit**

Cognitive fit theory states that non-resembling representations of information are acceptable for various tasks as well as audiences. In connection with visual notation design, cognitive fit implies that for different audiences (especially for experts and novices) development of different subdialects might be required to facilitate complete understanding of visual representation. Additionally, it might be required to develop a variety of dialects for different representational mediums, so that black-and-white printer, unable to transmit colours, would not make a notation undistinguishable (Moody, 2009a). Extended version of BPMN, developed by Altuhhova et al. (2013), would indeed require separate dialect for various mediums since discrimination between several concepts was based solely on colour. However, changes proposed in this chapter ensure that colour coding would be complemented by icons and therefore reduced to redundant coding. Thus, proposed changes are expected to eliminate the problem, resulting in one dialect being sufficient and discriminable across all mediums.

As for the expert-novice difference, there indeed might be a need for the separate notations for pro users and beginners. This need is further reinforced by the fact that size of visual vocabulary is excessive for beginner users, and separate dialect offers a convenient way of dictionary optimization. However, the obstacle for such a separation would be a need to divide symbols between essential and occasionally-used symbol sets. Since this separation have not yet been performed and is out of scope for this paper, separate dialects for experts and novices currently could not be defined. Thus, the only available strategy to mitigate issues with perception among novice users is extensive introduction of visually expressive and semantically immediate symbols.

### **Conclusion**

The concentrated results of preformed analysis could be found in Table 25.

Table 25. Security-extended BPMN analysis

Principle	Results
Semiotic clarity	Occurrences of symbol excess, symbol deficit, symbol redundancy and symbol overload. Cases of symbol redundancy and symbol overload have priority to be dealt with.
Perceptual Discriminability	Shapes and colours are used suboptimally, distinction between symbols is complicated. Colour coding should be complemented by additional visual variable such as iconic shapes or texture.
Semantic Transparency	Majority of symbols are semantically opaque due to them being abstract shapes, should be augmented by icons. One iconic symbol is semantically perverse which is not acceptable.
Complexity Management	Several mechanisms to deal with complexity are inherited from non-extended BPMN, they could be complemented by diagram structuring.
Cognitive Integration	No technique is currently available to reinforce perceptual or conceptual integration. One mitigating approach would entitle the creation of navigational map on the basis of Link Events and Sub Processes.
Visual Expressiveness	Notation has a visual expressiveness of 6 and is characterized by 2 degrees of visual freedom. However, poor design choices have a negative impact on the pairwise visual variation across visual vocabulary
Dual Coding	While hybrid symbols are already introduced, their appearance should be refined. Furthermore, several non-hybrid symbols should be transformed into hybrid ones.
Graphic Economy	Existing notation employs 14 symbols and is therefore overwhelming. Applicable approach to reduce complexity of visual vocabulary is related to the improvement of visual expressiveness by increasing the visual distance between symbols.
Cognitive Fit	While specifics of currently used dialect render it inoperable in case of non-colour representation, proposed changes mitigate the problem and eliminate the need for specific dialect. As for the expert-novice difference, it is considered that extensive introduction of visually expressive symbols should reduce learning challenges for novice users and would not require dedicated dialect.



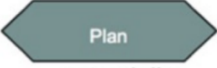
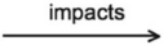



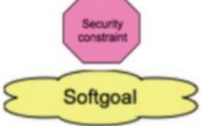
## VI. Analysis of Secure Tropos

The analysis of extended Secure Tropos is performed according to the notation, presented in (Matulevicius et al., 2012). Since authors also provided the evaluation, according to the semiotic clarity principle, their findings would serve as a basis for the corresponding principle overview. Additionally, it should also be mentioned that unlike the majority of ISSRM-extended notation, adherence of  $i^*$  notation, exploited in Secure Tropos, is already reviewed in (Moody et al., 2010). Thus, this analysis is built upon the results, stemming from the two abovementioned papers.

### Principle of Semiotic Clarity

According to the theory of symbols, defined by Goodman (1968), for a notation to satisfy the requirements of notational system, there should be a 1:1 correspondence between symbols and the relevant concepts. Thus, prior to performing the analysis it is essential to define the symbol set and concept set as used in ISSRM-extended Secure Tropos. As for the concept set, definition is relatively straightforward, and 13 ISSRM concepts covered in (Matulevicius et al., 2012) could be characterized as language concepts. To distinguish the symbol set, it should be taken into consideration that symbols for certain concepts are composite and not unique across the symbol set. Thus, it is possible to identify a list of symbols along with their category, which is to be defined as unique, combined or not represented. Symbol set of extended Secure Tropos is depicted in Table 26.

Table 26. Symbol set of ISSRM-extended Secure Tropos

ISSRM	Secure Tropos	Symbol Category
Threat agent		Unique
Vulnerability		Unique
Attack method		Unique
Impact		Unique
Event	 or combination of <i>Vulnerability, and Threat</i>	Unique
Business Asset		Unique
IS Asset		Unique
Security criterion		Unique

Security requirement		Unique
Threat		Unique
Risk	Combination of Event and Impact	Combined
Risk treatment	-	Not represented
Control	-	Not represented

Based on the provided symbols list, analysis of the extended Secure Troops notation could be performed from the Semiotic Clarity perspective. For the purposes of analysis, four anomalies, as defined in (Moody, 2009a), are to be considered: symbol redundancy, symbol overload, symbol excess and symbol deficit. These anomalies could be defined as follows.

- Symbol redundancy: 1 construct – several symbols.
- Symbol overload: 1 symbol – several constructs.
- Symbol excess: 1 symbol – no constructs.
- Symbol deficit: 1 construct – no symbols.

Following the provided definitions, it is now possible to quantify the cases of anomalies. Information System Asset is a clear occurrence of symbol redundancy, as one construct could be represented by two symbols. As for the symbol overload, this seems to be the incident of Information System Asset-Threat Agent, as two concepts are represented by a similar symbol of pool with difference only in colour appearance. Same situation could be observed with Assets – Attack Method – Security Requirement, as they are as well represented by a combination of three similar BPMN symbols (task, event and gateway) with only colour of task symbol ensuring the differentiation. Symbol deficit clearly occurs with Risk Treatment and Control, since there are no corresponding symbols in extension, provided by Altuhhova et al. (2013). Additionally, three other concepts, namely Risk, Event and Threat, suffer from symbol deficit as they are represented not by a dedicated symbol, but rather by amalgamation of existing ones, used on their own to denote other concepts. Furthermore, as defined by (Matulevičius, 2017), three other concepts (Security Criterion, Impact and Vulnerability) are affected by symbol deficit since not all aspects of those ISSRM concepts could be represented with proposed symbols. Finally, three concepts – Assets, Attack Method and Security Requirements – exhibit symbol excess as they are represented by a combination of three BPMN symbols (task, event and gateway) which on their own do not depict any of ISSRM concepts. Based on the abovementioned clarity-related issues, relevant modifications to problematic symbols should be introduced on the notational level.

## Principle of Perceptual Discriminability

Perceptual discriminability is defined as both the simplicity and the accuracy with which the graphical symbols could be told apart (Moody, 2009a). As such, discriminability is determined by visual distance between symbols, which could be characterized as a number of visual variables on which they differentiate and number of perceptible steps. Thus, prior to performing the analysis, it would be required to define a set of visual variables, currently used in ISSRM-extended BPMN notation. Based on the symbol set overview, presented in Table 26, it is possible to deduce that three visual variables, namely shape, size and colour are currently employed for the discriminability purposes. While 3 visual variables should be overall sufficient to ensuring distinguishable symbol appearance, this not the case due to the particularities of variable application in the notation design.

The prime visual variable, shape, is currently used not in the most optimal manner. While exploited range of shapes is quite varied and includes among other pentagon, hexagon and octagon, shape-based distinction within concept groups is quite complicated. This is especially the case with assets (both IS Asset and Business Asset), as they could be represented by almost identical rectangles of hardgoal and resource. Same should be also said about the Threat, depicted by a combination of goal and plan. Since hardgoal and goal are different only in coloring, represented by shades of same colour, differentiation becomes tangled. Overall, shape issues are especially noticeable within Attack method, Threat, Security Requirement, Business Asset and Information Asset, with the other concepts being distinct in shape.

As for the usage of colour, it should be said that coloring principles are directly transferred from the non-extended Secure Tropos could be characterized as suboptimal. Considering the fact that colors in  $i^*$  are used ineffectively (Moody et al., 2010), same could be said about the ISSRM-extended Secure Tropos. While the color palette is extensive and varies from black to purple, the overall impression is that colours are chosen on a chaotic basis and do not embrace similarities between three major groups of ISSRM concepts. Furthermore, certain concepts, including Threat and Security Criterion, are depicted with a combination of different-colored elements, further reducing the intuitiveness of notation. Overall, a combination of different concepts has an unnecessary patchy appearance, not assisting easy discrimination and effectively eliminating the visual popout. Since the current colour palette is unnecessary multicolored, it should be further altered. The modifications should be based on the proposal of Altuhhova et al. (2013), so that concepts, belonging to the same ISSRM categories, would be painted correspondingly.

While due to the specifics of notation size is not extensively used, it's utilization is rather effective as the activity initiation of Actor/Threat Agent is represented via spatial enclosure.


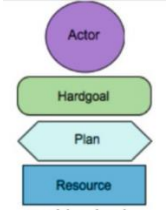







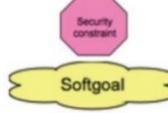
Finally, it could be concluded that while number of used visual variables is expected to ensure sufficient discriminability between symbols, number of poor design choices hamper the visual distance between symbols and affect discriminability in a negative way.

## Principle of Semantic Transparency


Semantic transparency is to be defined as how well the meaning of the symbol could be deduced from its visual appearance. Semantic transparency, defining how well the symbols provide cues to their meaning, could be described by one of three states (Moody, 2009a), which are *semantically immediate*, *semantically opaque* or *semantically perverse*.

So, semantic transparency is to be determined for each symbol. Transparency characteristics of extended BPMN symbol set (only unique category) are covered in the Table 27.

Table 27. Semantic transparency of extended Secure Tropos symbol set

ISSRM	Secure Tropos	Semantic Transparency	Sign type
Business Asset		Opaque	Symbolic
IS Asset		Opaque	Symbolic
Threat agent		Opaque	Symbolic
Impact		Opaque	Symbolic
Event		Opaque	Symbolic
Threat		Opaque	Symbolic
Attack method		Opaque	Symbolic
Threat Agent		Opaque	Symbolic
Vulnerability		Opaque	Symbolic
Security criterion		Opaque	Symbolic



Security requirement		Opaque	Symbolic
----------------------	---	--------	----------

Based on the guidelines, provided in (Moody, 2009a), it could be said that semantically pervasive symbols should be redesigned, and semantical immediateness is to be embraced whenever possible. As for the semantically immediate symbols, one way to achieve immediateness is to implement icons instead of abstract symbolic signs.

Since extended Secure Tropos notation is solely comprised of abstract geometric shapes, it could be said that all the symbols are opaque, and none is semantically immediate. While it's not mandatory to replace opaque symbols with the immediate ones, introduction of immediate symbols (icons) would improve the visual efficiency and reduce the steepness of learning curve.

Additionally, it should be mentioned that icons are encouraged to be used along the other visual variables to ensure redundant coding and improve symbol discriminability. Taking into consideration the results of discriminability analysis, replacement of existing symbols with introduced icons would ensure effective redundant coding and improve the visual pop-out.

### Principle of Complexity Management

Complexity management is defined as ability of a visual notation to depict information while not overflowing human mind (Moody, 2009a). While complexity here sounds somewhat vague, it could be further defined as number of elements on a diagram. As such, complexity impacts key metrics, which are as perceptual limits and cognitive limits.

While complexity is a diagram-level issue, possible improvements are to be performed on the notation level. It should also be mentioned that effective techniques include modularization and hierarchical organization (Moody, 2009a). Since ISSRM-extended Secure Tropos on the notational level is similar to non-extended  $i^*$  notation, it seems justified to start the analysis from stating information, adopted from the paper by (Moody et al., 2010).

As outlined by (Moody et al., 2010), lack of complexity management mechanisms prevents  $i^*$  from being adapted in complex real-world projects. Authors also propose to introduce recursive (element to diagram) decomposition, which is intended to solve the complexity issue.

While all the above-mentioned information is applicable to extended Secure Tropos, there are also certain extension-specific features. As proposed by Altuhhova et al. (2013), three groups of ISSRM concepts are colour coded and differentiated between each other. Thus, diagram levels could be organized not only on the basis of detalization levels but derived from distinct groups of ISSRM concepts.

## Principle of Cognitive Integration

Cognitive integration should be applied when system is represented by more than one diagram. The idea is that since relevant information is spread across a number of diagrams, diagram readers often struggle with keeping the current position and comprehending the complete picture. For the multiple diagrams to be cognitively effective, they are to include integration mechanisms (Moody, 2009a), which are conceptual integration and perceptual integration. As it was already mentioned in the Complexity Management principle,  $i^*$  notation supports multiple diagrams.

However, (Moody et al., 2010) point out that since only two diagrams are currently available in the  $i^*$ , cognitive integration is not an issue. At the same time, introduction of the additional diagrams would cause a need for effective complexity management mechanism.

As for the ISSRM-extended Secure Tropos, it should be mentioned that both (Matulevičius et al., 2012) and (Matulevičius, 2017) provide examples of only one, unified diagram style, thus minimizing the problem of cognitive integration.

## Principle of Visual Expressiveness

Visual expressiveness could be defined as a number of visual variables, used in a notation and evaluating overall exploitation of available design space (Moody, 2009a). Based on the visual expressiveness metrics, visual variables of the notation could be divided between two subsets, which are information-carrying variables, and free variables.

According to the distribution between visual expressiveness and degrees of visual freedom, notations could range from nonvisual (expressiveness = 0, 8 degrees of freedom) to visually saturated (expressiveness = 8, 0 degrees of freedom). Table 28 summarizes information on power (highest measurement level that could be encoded), capacity (number of possible values for each variable) and values as employed in extended Secure Tropos. Information regarding power and capacity of visual variables is adopted from (Moody, 2009a), while the overall representation style is taken from (Genon et al., 2010).

Table 28. Visual variables of Secure Tropos, adopted from (Moody, 2009a)

Visual Variable	Power	Capacity	Extended SecureTropos values
Horizontal position (x)	Interval	10-15	Enclosure
Vertical position (y)	Interval	10-15	Enclosure
Size	Interval	20	Normal, large (enclosure)
Colour	Nominal	7-10	Purple, green, light blue, blue, pink, yellow, orange, black, dark green, sage, purple
Texture	Nominal	2-5	Single solid
Shape	Nominal	Unlimited	Circle, rounded rectangle, hexagon, rectangle, octagon, cloud, pentagon
Brightness	Ordinal	6-7	Not utilized
Orientation	Nominal	4	Not utilized

As it could be seen from the Table 24, ISSRM-extended Secure Tropos has a visual expressiveness of 6 and is characterized by 2 degrees of visual freedom. However, it should be mentioned that while visually 6-dimensional notation of extended BPMN is considered to be sufficient for the discriminability purposes (Moody, 2009a), poor design choices have a negative impact on the pairwise visual variation across visual vocabulary.

As for the overall overview of exploited visual variables, it is provided as follows. Both horizontal and vertical positions could be utilized to depict intervals. However, similar to

the situation with non-extended  $i^*$ , both variables are employed only to denote enclosure (location of symbol inside of another one) and are not fully exploited.

Usage of size in extended Secure Tropos is currently identical to that of non-extended version, with only Actor/Attacker element being significantly larger as to depict the power of activity initiation. All the other symbols are currently being of the similar size, non-discriminable on its basis.

Visual variable of texture is somewhat underused, since out of 5 possible perceptible steps only one is currently incorporated. It could be recommended to further exploit the texture, and it could be effective to complement colour-based coding by introducing several types of symbol border shapes.

As for the colour, it's usage in extended Secure Tropos notation violates the best practices and should be refined. Currently 11 colours could be present on the diagram, meaning that perceptible steps are overloaded, since colour variable has a maximum capacity of 10. Since colour is one of the most cognitively effective of all visual variables (Moody, 2009a), it's usage should follow the robust design guidelines. According to the robust design principles, outlined by D. Moody (2009a), colour could be used only for redundant coding, and it's capacity should not exceed that of 10. While redundant coding is ensured by the variety of symbol shapes, colour palette currently leads to cognitive overload. Thus, it is recommended to reduce the overall number of exploited colours. Additionally, colour coding should follow the proposition of (Altuhhova et al., 2013), so that elements, belonging to the distinct groups of ISSRM concepts, would be painted accordingly.

Considering the variable of shape, it should first be noted that it's the only variable featuring unlimited capacity. As for the utilization of shapes in extended Secure Tropos notation, it could be said that utilized range of shapes provides sufficient discrimination capabilities. However, all of the existing shapes, adopted from non-extended BPMN, suffer from being semantically opaque. So existing abstract shapes should be replaced or augmented by their semantically immediate counterparts, obtained via the implementation of icons.

Finally, extended Secure Tropos notation makes no use of two remaining visual variables – Brightness and Orientation. While no specific details are provided, it should be noted that instead of potentially overloading available variables, it is possible to employ those currently not utilized for obtaining potential benefits from dual coding and increasing visual expressiveness.

### **Principle of Dual Coding**

Dual coding theory indicates that text and graphics together transmit information better than either one of them by itself. There are several ways to encapsulate textual information, namely annotations and hybrid symbols. (Moody, 2009a).

Currently, extended Mal-activity Diagrams notation has no hybrid symbols, reducing the notational intuitiveness and increasing steepness of learning curve. While dual coding is a powerful approach, enabling increase in visual perceptibility, it could be said that refinement of colour coding and intuitive iconic symbols would increase the visual popout while at the same time reducing overall notation complexity. Thus, transformation of non-hybrid symbols into hybrid ones is not justified, and it is recommended only to implement notation modifications, proposed in previous subchapters.

## **Principle of Graphic Economy**

Graphic complexity is overall characterized by an amount of graphical symbols in the notation, which could be also called size of visual vocabulary. As denoted in Table 28Table 22, extended Secure Tropos employs 12 symbols, and is therefore overwhelming. (Moody, 2009a) offers three approaches to reduce visual vocabulary, which are reduce semantic complexity, increase symbol deficit and increase visual expressiveness.

Symbol deficit is already present in the notation, so it won't be helpful in reducing the complexity. Reduction of semantic complexity is the most straightforward approach, aimed at analyzing the unnecessary symbols and excluding them from the notation. However, the overall number of symbols is specified by ISSRM domain model, and can't really be reduced. Thus, the only applicable approach is related to the improvement of visual expressiveness by increasing the visual distance between symbols. It should be noted that analysis of previous Physics of Notation principles already included practical recommendations, such as implementation of dual coding and immediately perceptive icons. So, it could be concluded that refined notation would already be characterized by increased visual expressiveness, and no additional steps are required for improving it. Finally, it should also be mentioned that one additional approach to reduce semantic complexity is to implement additional language dialect. This suggestion is further covered in the subsequent subchapter.

## **Principle of Cognitive Fit**

Cognitive fit theory states that non-resembling representations of information are acceptable for various tasks as well as audiences. In connection with visual notation design, cognitive fit implies that for different audiences (especially for experts and novices) development of different subdialects might be required to facilitate complete understanding of visual representation. Additionally, it might be required to develop a variety of dialects for different representational mediums, so that black-and-white printer, unable to transmit colours, would not make a notation undistinguishable (Moody, 2009a). Extended version of Secure Tropos would indeed require separate dialect for various mediums since discrimination between several concepts is heavily based on colour differences as corresponding shapes are rather similar. However, changes proposed in this chapter ensure that colour range would be scaled down, shapes would be refined, and icons are to be introduced. Thus, proposed changes are expected to eliminate the problem, resulting in one dialect being sufficient and discriminable across all mediums.

As for the expert-novice difference, there indeed might be a need for the separate notations for pro users and beginners. This need is further reinforced by the fact that size of visual vocabulary is excessive for beginner users, and separate dialect offers a convenient way of dictionary optimization. However, the obstacle for such a separation would be a need to divide symbols between essential and occasionally-used symbol sets. Since this separation have not yet been performed and is out of scope for this paper, separate dialects for experts and novices currently could not be defined. Thus, the only available strategy to mitigate issues with perception among novice users is extensive introduction of visually expressive and semantically immediate symbols.

## **VII. Analysis of Misuse Cases**

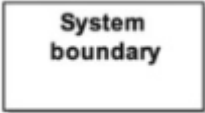
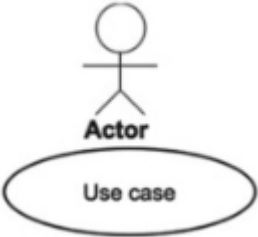
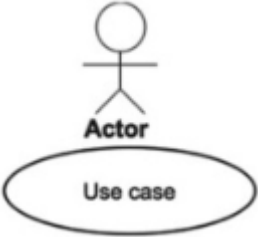
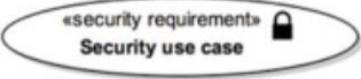

First, it should be noted that details regarding the extended Misuse Case notation were taken from (Soomro & Ahmed, 2012) and (Matulevičius, 2017). Since Misuse cases are derived from Use cases, constituting one of UML diagram types, analysis of UML from the PoN viewpoint, as described in (Moody & van Hilleberg, 2008), provides several valuable

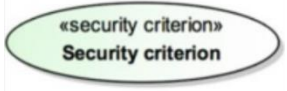


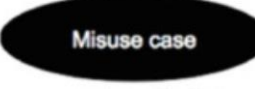
notation insights. Furthermore, it should be noted that Saleh & El-Attar (2015) perform an analysis, dedicated specifically to the Misuse Cases notation. Since the paper by Saleh & El-Attar (2015) thoroughly investigates non-extended Misuse Cases notation and provides a number of suggested improvements, it serves as a source of valuable insights and overall inspiration. This research, in its turn, concentrates on the analysis of extended Misuse Cases notation, as introduced in (Soomro & Ahmed, 2012).

### Principle of Semiotic Clarity

Before performing the analysis, it's crucial to define both symbol set and concept set, employed in ISSRM-extended Misuse Cases. Concept set could be defined as 13 ISSRM concepts, outlined in the paper by Dubois et al. (2010). As for the symbol set, it could be characterized based on the suggestion by Soomro & Ahmed (2012). However, it's important to remember that symbols set could be divided into three unequal parts, which are unique symbols, combined or not represented ones. Out of three categories, only unique symbols should be referred to as symbol set. Obtained set of symbols for extended Misuse Case notation is present in Table 29.

Table 29. Symbol set of ISSRM-extended Misuse Cases

ISSRM	BPMN	Symbol Category
IS Asset		Unique
Business Asset		Unique
Assets		Unique
Security requirement		Unique
Threat agent		Unique

Security criterion		Unique
Impact		Unique
Vulnerability		Unique
Attack method		Unique
Risk	Combination of <i>Event</i> and <i>Impact</i>	Combined
Event	Combination of <i>Vulnerability</i> and <i>Treat</i>	Combined
Threat	Combination of <i>Attack method</i> and <i>Threat agent</i>	Combined
Risk treatment	-	Not represented
Control	-	Not represented

Based on the provided list of symbols, it is now possible to perform the analysis from the Semiotic Clarity perspective, in regard to four metrics – symbol redundancy, symbol overload, symbol excess and symbol deficit.

As for the symbol redundancy, Assets is a clear case since single construct could be presented by several symbols (Matulevičius, 2017). Additionally, Assets are also an example of overload, since same combination of constructs could represent different ISSRM concepts (Matulevičius, 2017). Symbol deficit is evidential in the situation with Risk Treatment and Control as none of those concepts has a symbolic representation. Furthermore, Event, Risk and Threat are also cases of symbol deficit, as they are represented by a combination of available symbols rather than by dedicate ones. Finally, it should be noted that Assets, Business Asset and Security Requirements both suffer from the symbol excess. As for the Assets and Business Asset, this is caused by the oval symbol, serving as a depiction for use case in non-extended Use Case notation. However, unlike the Use Cases, ISSRM-extended Misuse Case notation does not include use case symbol, meaning symbol excess. Finally, Security Requirement is affected by symbol excess as it includes a closed lock symbol, having no ISSRM correspondence o its own.

### Principle of Perceptual Discriminability

Perceptual discriminability is defined as simplicity and the accuracy with which the graphical symbols could be separated between each other (Moody, 2009a). Based on the overview of symbols, presented in the Table 29, it could be seen that two out visual variables, namely shape and colour, are utilized across the notation. While two variables are not sufficient to discriminate between such a broad range of symbols, distinction is further hampered by suboptimal design choices, such as exploitation of only three shape types, including stick

figure. It could be deduced that symbols, chosen by Soomro & Ahmed (2012), are derived from non-extended Misuse Case notation, based on the original Use Case version. However, growth of concept set made the notation complicated for perception, and opportunity to trace origins and draw from Use Case knowledge should not be prioritized over discriminability. Furthermore, novice users are expected to comprise a significant share of potential user audience. Since novices would have no prior experience with UML and, respectively, Use Cases, strict resemblance to Use Case notation is not mandatory.

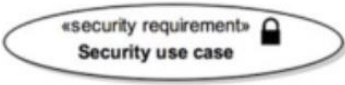
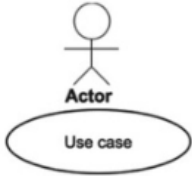
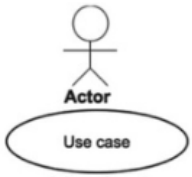
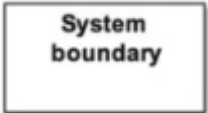

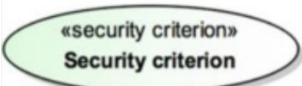

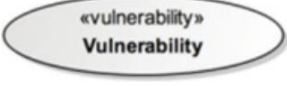

As for the discriminability between symbols, it should be noted that its unacceptably low and should be further improved. Information Asset symbol is the only one with the distinct shape, ensuring sufficient visual popout. Symbols, representing Asset, Business Asset and Threat agent are similar, with stick figure being different only for Threat agent. While it should be acknowledged that chosen design approach allows Threat agent to be differentiated on different representation mediums (including black-and white copies), usage of colour is not recommended as a single discriminative variable. Furthermore, colored (darkened) part of stick figure covers only part of its appearance (head), further reducing the popout. Following the analysis of shape, it should also be mentioned that Assets, Business Asset, Security requirement, Security Criterion, Impact, Vulnerability and Attack method all share the same abstract shape of oval, and with the single exception of Security Requirement, could be recognized only by colour and textual information (as hybrid symbols). Additionally, utilized colours (for Security Criterion, Impact and Vulnerability) are not visually appearing and could be described as various shades of gray. While authors (Soomro & Ahmed, 2012) clearly had black-and white printer friendliness in mind, obtained result is far from perfect. It should also be mentioned that in the case of abovementioned concepts, colour is employed as a single visual variable and only means of discrimination. According to the PoN principles (Moody, 2009a), this is not acceptable.

Overall colour and shape decisions, made by authors, are puzzling if to consider a Security Requirement symbol, comprised of shape and iconic symbol. Unlike colour, iconic symbols are a superior choice as only means of distinction and should be used in a more extensive manner. Furthermore, it should be also mentioned that a number of symbols (Security Requirement, Security Criterion, Impact, Vulnerability) are in fact hybrid symbols, combining graphics and text annotation. However, while dual coding of information has shown itself highly efficient (Moody, 2009a), textual information should not be used on its own and could be used as a replacement of visual variables only as a last resort. Thus, since symbols of the current symbol set could not be effectively distinguished, it is recommended to expand the range of employed visual variables (extra colours, additional shapes) as well as icons. Overall, It could be concluded that symbols of the current symbol set could not be effectively distinguished.

### **Principle of Semantic Transparency**

From the semantic transparency point of view, symbols could be characterized as either semantically immediate, semantically opaque or semantically perverse (Moody, 2009a). Transparency characteristics of extended BPMN symbol set (only unique category) are covered in the Table 30.

Table 30. Semantic transparency of the extended Misuse Cases notation

ISSRM	BPMN	Semantic Transparency	Sign type
Security requirement		Immediate	Iconic
Business Asset		Opaque	Symbolic
Assets		Opaque	Symbolic
IS Asset		Opaque	Symbolic
Threat agent		Immediate	Iconic
Security criterion		Opaque	Symbolic
Impact		Opaque	Symbolic
Vulnerability		Opaque	Symbolic
Attack method		Opaque	Symbolic

First of all, it should be noted that no semantically pervasive symbols could be found. However, only one symbol out of entire itemset is semantically immediate, with all others being semantically opaque. While semantically opaque symbols are acceptable (D. Moody, 2009a), one way to improve the visual intuitiveness of a notation is to transform opaque items to semantically immediate ones. As demonstrated by (A scientific evaluation of the



misuse case diagrams visual syntax), one effective approach is to complement abstract shapes with color coding and, more importantly, iconic symbols. Apart from iconic symbols allowing colour to be exploited for redundant coding, icons are also instrumental in making the symbols more discriminable as well as reducing the learning curve. Currently, only one icon (closed lock) is included in the extended Misuse Case notation, and more should be introduced to transform the opaque symbols into semantically immediate ones.

Apart from abstract geometric shapes (oval and rectangle), humanlike stick figure is also to be considered a part of notation. While this stick figure, denoting User/Misuser, could be characterized as semantically immediate in case of Use Case and non-extended Misuse Case notations, same could hardly be said for the ISSRM-extended notation. Thus, it is recommended to refine the existing “black thoughts” depiction of Threat agent concept and make it more semantically transparent. Overall, it could be said that since the majority of existing icons are semantically opaque, it is recommended to complement existing symbols with semantically immediate icons to improve the semantic transparency of notation. Introduction of colour coding and iconic symbols is proposed as a means to increase semantic transparency and visual popout.

### **Principle of Complexity Management**

While complexity here sounds relatively vague, it could be further defined as number of elements on a diagram. Complexity impacts key metrics, which are perceptual limits and cognitive limits. While complexity is a diagram-level issue, possible improvements are to be performed on the notation level. It should also be mentioned that effective techniques include modularization and hierarchical organization (Moody, 2009a)

Similar to non-extended Misuse Cases (Saleh & El-Attar, 2015), extended notation currently provides no complexity management mechanisms, and diagrams have to be shown as single monoliths. Since extended Misuse Cases represent single layer of abstraction, with no further potential for decomposition and refinement, implementation of complexity management technique is not an option. Furthermore, it should also be noted that proposed notation improvements should further improve the ability to discriminate between symbols.

### **Principle of Cognitive Integration**

Cognitive integration could be applicable when system is represented by multiple diagrams. Since extended Misuse Case diagrams, similarly to non-extended (Saleh & El-Attar, 2015), offer single monolithic diagrams, this principle could not be applied for analysis.

### **Principle of Visual Expressiveness**

Visual expressiveness could be defined as a amount of visual variables, utilized in a notation and measuring overall usage of design space (Moody, 2009a). Based on the visual expressiveness metrics, visual variables of the notation could be divided between two subsets, namely information-carrying variables and free variables.

The Table 31 summarizes information on power (highest measurement level that could be encoded), capacity (number of possible values for each variable) and values as employed in extended Misuse Cases. Information regarding power and capacity of visual variables is adopted from (Moody, 2009a), while the overall representation style is taken from (Genon et al., 2010).

Table 31. Visual variables of extended Misuse Cases, partially adopted from (Moody, 2009a)

Visual Variable	Power	Capacity	Extended Misuse Cases values
Horizontal position (x)	Interval	10-15	Enclosure
Vertical position (y)	Interval	10-15	Enclosure
Size	Interval	20	Normal, large
Colour	Nominal	7-10	Black, light grey, grey, white
Texture	Nominal	2-5	Single solid
Shape	Nominal	Unlimited	Oval, rectangle, stickman figure
Brightness	Ordinal	6-7	Not utilized
Orientation	Nominal	4	Not utilized

As it could be understood from the Table 31, ISSRM-extended Misuse Case notation is characterized by visual expressiveness of 6, so that degree of visual freedom is 2. As noted by (Moody, 2009a), utilization of 6 visual variables is considered to be sufficient for the discrimination purposes. However, it should be mentioned that visual notation of extended Misuse Cases is far from being expressive due to the limited choice of options for the above mentioned visual variables. Colour and shape are among the underused, since only 3 colours and two possible shapes are employed throughout the notation. Thus, it is recommended to expand the colour range, as well as selection of shapes in order to make the notation more visually effective. However, it should be recollected that colour could be used only for redundant coding.

Two other variables – Size and Texture, are exploited but could be represented by only a restricted values, specifically single solid texture and normal/large sizes. This design choice renders symbols not expressive and thus, not distinguishable, as visual distance is ensured only by two variables (Colour and Shape), with Size and Texture being practically useless. So, it is suggested to exploit Size and Texture up to their potential, introducing various textures as well as sizes. It should be noted that in regard to the Size, representation of Information System Asset offers an exception, as corresponding symbol differs in size from the all the other. However, since it's used only for the depiction of sole concept and has 2 options with capacity of 20, it's hardly a positive example.

Both horizontal and vertical positions could be utilized to depict intervals. However, similar to the situation with non-extended BPMN (Genon et al., 2010), both variables are employed only to denote enclosure (location of symbol inside of another one) and are not fully exploited.

Finally, it should be said that Misuse Case notation makes no use of two remaining visual variables – Brightness and Orientation. While no specific details are provided, it should be noted that instead of potentially overloading available variables, it is possible to employ those currently not utilized for obtaining potential benefits from dual coding and increasing visual expressiveness.

### Principle of Dual Coding

Dual coding theory states that text and graphics together transmit information better than either one of them by itself. There are several ways to encapsulate textual information, namely annotations and hybrid symbols. (Moody, 2009a).

Current version of extended Misuse Case notation has four hybrid symbols, namely Security Requirement, Security Criterion, Impact and Vulnerability. In these symbols textual information expands the abstract shapes and improves discriminability. Security requirement

symbol differs from all the rest, as it features not only text annotation, but also an icon. All the remaining notation items are not hybrid. While dual coding is a powerful approach, enabling increase in visual perceptibility, it could be said that four abovementioned symbols could not be discriminated easily as their visual appearance is quite similar and text annotations do not provide significant visual popout. As proposed in the Chapter 0, existing abstract shapes should be complimented by iconic symbols, and colour should be utilized for redundant coding. Thus, available hybrid symbols should be further refined and augmented by icons and colour coding.

As for the rest of the symbols, currently not bearing textual information, it could be said that addition of icons and colour coding would make them sufficiently discriminable. Thus, transformation of non-hybrid symbols into hybrid ones is not justified.

### **Principle of Graphic Economy**

As for the graphic complexity, it is overall characterized by a number of graphical symbols in the notation, also called size of visual vocabulary. As denoted in Table 29, extended Secure Tropos notation utilizes 12 symbols. (Moody, 2009a) indicates that upper limit of graphic complexity could be defined at 6. To mitigate the negative impact on cognition, several guidelines are offered in a paper by (Moody, 2009a). They are: to reduce semantic complexity, increase symbol deficit and increase visual expressiveness. Since symbol deficit is already introduced, and semantic complexity is optimized, the most effective way to ensure manageable cognitive load is to increase visual effectiveness. As already mentioned, proposed alterations of existing notation, including the refinement of colours and introduction of semantically immediate icons to augment the abstract shapes, are expected to embrace visual popout and improve symbol discriminability.

### **Principle of Cognitive Fit**

According to the principal of cognitive fit, different representations of information are acceptable for various assignments and audiences (Moody, 2009a). Regarding visual notation design, cognitive fit means that different audiences (especially experts and novices) and different representation mediums (colourized and black-and-white versions) require tailored visual dialects. As for the demands of various representation mediums, it could be said that current notation is

well-rounded and could be used in both black-and-white and coloured versions. This is achieved by the utilization of grey-black colour palette, as well as hybrid symbols with textual descriptions. While selected palette has certain benefits, it is ineffective in terms of visual popout and visual distance. Thus, it is recommended to expand the choice of colour and extend the palette. It should be mentioned that proposed abolition of grey-black colour choice would not result in symbols being indiscriminable, since colour would be used only for redundant coding and sufficient visual distance would be enforced by iconic symbols. So, there is no need to introduce several dialects for various mediums. Considering notation complexity and accessibility to beginners, it could be said that ISSRM-extended Misuse Case notation originates from the Use Cases, which are characterized as being accessible to non-technical stakeholders (Saleh & El-Attar, 2015). While extended notation has an increased visual vocabulary and is not accessible for novice users, proposed changes and implementation of semantically immediate icons should ensure that symbols are visually expressive and learning curve is low. Thus, it is unjustified to develop separate dialects based on user's knowledge level.






## VIII. Analysis of Mal-activity Diagrams







As with Misuse Cases, Mal-activity Diagrams also originate from a subset of UML (Activity Diagrams) and share many efficient as well as inefficient design choices with general UML notation. Since PoN analysis of UML was already performed in (Moody & van Hillegersberg, 2008) and is out of the cope for this paper. Subsequent subchapter focuses on the notational aspect of security-extended Mal-activity Diagrams, as presented in (Chowdhury et al., 2012).

### Principle of Semiotic Clarity

Before performing the analysis, it's crucial to define both symbol set and concept set, employed in extended Mal-activity Diagrams notation. Concept set could be defined as 13 ISSRM concepts, outlined in the paper by Dubois et al. (2010). As for the symbol set, it could be characterized based on the paper by Chowdhury et al. (2012). However, it's important to remember that symbols set could be divided into three unequal parts, which are unique symbols, combined or not represented ones. Out of three categories, only unique symbols should be referred to as symbol set. Obtained set of symbols for extended Mal-activity Diagrams notation is present in Table 32.

Table 32. ISSRM-extended symbol set of Mal-activity Diagrams

ISSRM	BPMN	Symbol Category
IS Asset		Unique
Security requirement		Unique
Threat agent		Unique
Control		Unique
Impact		Unique

Attack method	<p>As method:</p>  <p>combined using <i>control flow</i> links</p> <p>As means</p> 	Combined
Business Asset	 <p>Decision</p>  <p>Activity</p>	Combined
Assets	 <p>Decision</p>  <p>Activity</p>	Combined
Risk	Combination of Event and Impact	Combined
Event	Combination of Threat and Vulnerability	Combined
Threat	Combination of Attack method and Threat Agent	Combined
Security criterion	-	Not represented
Vulnerability	-	Not represented
Risk treatment	-	Not represented

Provided list of symbols could now be utilized as a basis for Semiotic Clarity analysis, which is to be performed with 4 metrics of symbol redundancy, symbol overload, symbol excess and symbol deficit in mind. As for the symbol redundancy, Assets and Attack Method are the cases, as single construct could be presented by several symbols (Matulevičius, 2017). Additionally, Assets are also an example of overload due to the fact that same combination of constructs could represent different ISSRM concepts (Matulevičius, 2017). Symbol deficit is evidential in the situation with Security criterion, Vulnerability and Risk treatment as none of those concepts has a symbolic representation. Furthermore, Risk, Event and Treat are also cases of symbol deficit, as they are represented by a combination of available symbols rather than by dedicate ones. Finally, it should be noted that Assets and Security Requirements both suffer from the symbol excess. This is caused by the nature of combined symbols, as individually diamond-shaped symbol has no semantic meaning and no ISSRM correspondence.

### Principle of Perceptual Discriminability

Perceptual discriminability is defined as simplicity and the accuracy with which the graphical symbols could be separated between each other (Moody, 2009a). Based on the overview of symbols, presented in Table 32, it could be seen that two visual variables, namely shape and brightness, are utilized across the notation. While two variables are not sufficient to discriminate between a range of symbols, distinction is further hampered by suboptimal

design choices, such as exploitation of only three shape types. It could be deduced that symbols, chosen by Chowdhury et al. (2012), are derived from non-extended Mal-activity Diagrams notation, based on the original Activity Diagrams version. However, growth of concept set made the notation complicated for perception, and opportunity to trace origins and draw from Use Case knowledge should not be prioritized over discriminability. Furthermore, novice users are expected to comprise a significant share of potential user audience. Since novices would have no prior experience with UML and, respectively, Activity Diagrams, strict resemblance to Activity Diagrams notation is not a benefit. As for the discriminability between symbols, it should be noted that its quite low and should be further improved. While symbol groups, represented by diamonds, rounded rectangles and rectangles could be relatively easily discriminated based on substantial differences in size, colour and shape, same could not be said about symbols inside groups. Differentiation between Information System Asset, Threat Agent and Control is quite complicated, since visual representation of all this symbol is actually an identical rectangle-shaped figure, providing no visual differentiation markers. As for the group comprising Business Asset, Impact, Attack Method and Security Requirement, situation with discriminability is slightly better, with difference in brightness levels ensuring visual popout.

While it should be acknowledged that chosen design approach allows abovementioned symbols to be differentiated on different representation mediums (including black-and white copies), usage of colour is not recommended as a single discriminative variable.


While notation authors clearly had black-and white printer friendliness in mind, obtained result is far from perfect. It should also be mentioned that in the case of abovementioned concepts, colour is employed as a single visual variable and only means of discrimination. According to the PoN principles (Moody, 2009a), this is not acceptable.







Overall, it should be concluded that since symbols of the current symbol set could not be effectively distinguished, it is recommended to expand the range of employed visual variables (extra brightness levels, utilization of colours, additional shapes) as well as icons. It could be concluded that since symbols of the current symbol set could not be effectively distinguished.

### Principle of Semantic Transparency

From the semantic transparency point of view, symbols could be characterized as either semantically immediate, semantically opaque or semantically perverse (Moody, 2009a). Transparency characteristics of extended Mal-activity Diagrams symbol set are covered in Table 33.

Table 33. Semantic transparency of the extended Mal-activity Diagrams notation

ISSRM	BPMN	Symbol Category	Semantic Transparency
IS Asset		Symbolic	Opaque

Security requirement		Symbolic	Opaque
Threat agent		Symbolic	Opaque
Control		Symbolic	Opaque
Impact		Symbolic	Opaque
Business Asset		Symbolic	Opaque
Assets		Symbolic	Opaque

As could be seen from the table above, no semantically perverse symbols could be found. However, sole dependency on the symbolic elements means that current version of ISSRM-extended notation is semantically opaque, with no symbols being immediate. While according to (Moody, 2009a) opaque symbols are acceptable for the notation, one obvious way to improve the intuitiveness is to introduce semantically immediate, iconic-based ones. As shown in the (Saleh & El-Attar, 2015), one possible approach would be to introduce colour encoding and iconic symbols. In addition to iconic symbols taking main burden of sense-bearing, leaving colour only for redundant coding purpose, icons would also be immensely helpful to increase discriminability and reduce the learning curve. While current notation employs only abstract geometric shapes, a number of icons should be introduced to facilitate the process of semantic immediateness transformation.

Overall, it could be said that since current symbols are semantically opaque, it is recommended to complement existing symbols with semantically immediate icons to improve the semantic transparency of notation. Introduction of colour coding and iconic symbols is proposed as a means to increase semantic transparency and visual popout.

### **Principle of Complexity Management**

While complexity could be used in quite a broad meaning, it could be further described as a number of elements on the diagram. Complexity could be measured by two key metrics,

which are perceptual limits and cognitive limits. While complexity is a diagram-level issue, possible modifications could be also performed on a notation level. It should be also noted that according to the paper by (Moody, 2009a), efficient techniques include modularization and hierarchical organization. Similar to pre-ISSRM Mal-activity Diagrams, extended notation offers no complexity management mechanisms, meaning that diagrams are to be represented as single monoliths. As extended Mal-activity Diagrams represent single layer of abstraction, no further potential for decomposition or refinement is present. Thus, implementation of complexity management instruments is not an option. Furthermore, it should also be noted that proposed notation alterations should further improve the ability to discriminate between symbols, further reducing the need for decomposition.

### Principle of Cognitive Integration

Cognitive integration could be applicable when system is represented by multiple diagrams. Since extended Mal-activity Diagrams, similarly to non-extended UML, offer single monolithic diagrams, this principle could not be applied for analysis.

### Principle of Visual Expressiveness

Visual expressiveness could be defined as a amount of visual variables, utilized in a notation and measuring overall usage of design space (Moody, 2009a). Based on the visual expressiveness metrics, visual variables of the notation could be divided between two subsets, namely information-carrying variables and free variables.

The Table 34 summarizes information on power (highest measurement level that could be encoded), capacity (number of possible values for each variable) and values as employed in extended Mal-activity Diagrams. Information regarding power and capacity of visual variables is adopted from (Moody, 2009a), while the overall representation style is taken from (Genon et al., 2010).

Table 34. Visual variables of extended Mal-activity Diagrams, adopted from (Moody, 2009a)

Visual Variable	Power	Capacity	Mal-activity diagram values
Horizontal position (x)	Interval	10-15	Enclosure
Vertical position (y)	Interval	10-15	Enclosure
Size	Interval	20	Normal, large-scale
Brightness	Ordinal	6-7	Light, medium, dark
Texture	Nominal	2-5	Single solid
Shape	Nominal	Unlimited	Diamond, rectangle, rounded rectangle
Orientation	Nominal	4	Not utilized
Colour	Nominal	7-10	Not utilized

As it could be understood from the Table 34, ISSRM-extended Mal-activity Diagrams notation is characterized by visual expressiveness of 6, so that degree of visual freedom is 2. As noted by (Moody, 2009a), utilization of 6 visual variables is considered to be sufficient for the discrimination purposes. However, it should be mentioned that visual notation of extended Mal-activity Diagrams is far from being expressive due to the limited choice of options for the above mentioned visual variables. Brightness and shape are among the underused, since only 3 levels of brightness and three possible shapes are employed throughout the notation. Furthermore, despite being one of most effective visual variables colour is not exploited at all. Thus, in order to make the notation more visually effective it is recommended to expand the selection of shapes as well as introduce extensive colour coding. However, it should be recollected that colour could be used only for redundant coding.



Two other variables – Size and Texture, are exploited but could be represented by only a restricted values, specifically single solid texture and normal/full scale sizes. This design choice renders symbols not expressive and thus, not distinguishable, as visual distance is ensured only by two variables (Brightness and Shape), with Size and Texture being reduced to second-tier roles. So, it is suggested to exploit Size and Texture up to their potential, introducing various textures as well as sizes.

As for both horizontal and vertical positions could be utilized to depict intervals. However, similar to the situation with non-extended BPMN (Genon et al., 2010), both variables are employed only to denote enclosure (location of symbol inside of another one) and are not fully exploited.

### **Principle of Dual Coding**

Dual coding theory states that text and graphics together transmit information better than either one of them by itself. There are several ways to encapsulate textual information, namely annotations and hybrid symbols. (Moody, 2009a).

Currently, extended Mal-activity Diagrams notation has no hybrid symbols, reducing the notational intuitiveness and increasing steepness of learning curve. While dual coding is a powerful approach, enabling increase in visual perceptibility, it could be said that addition of colour coding and intuitive iconic symbols would increase the visual popout while at the same time reducing overall notation complexity. Thus, transformation of non-hybrid symbols into hybrid ones is not justified, and it is recommended only to implement notation modifications, proposed in previous chapters.

### **Principle of Graphic Economy**

As for the graphic complexity, it is overall characterized by a number of graphical symbols in the notation, also called size of visual vocabulary. As denoted in Table 33, extended Mal-activity Diagrams notation utilizes 7 symbols. (Moody, 2009a) indicates that upper limit of graphic complexity could be defined at 6. To mitigate the negative impact on cognition, several guidelines are offered in ((Moody, 2009a). They include reduction of semantic complexity, increase of symbol deficit and increase of visual expressiveness. Since symbol deficit is already introduced, and semantic complexity is optimized, the most effective way to ensure manageable cognitive load is to increase visual effectiveness. As already mentioned, proposed alterations of existing notation, including the addition of colours and introducing semantically immediate icons to augment the abstract shapes, are expected to embrace visual popout and improve symbol discriminability.

### **Principle of Cognitive Fit**

According to the principal of cognitive fit, different representations of information are acceptable for various assignments and audiences (Moody, 2009a). Regarding visual notation design, cognitive fit means that different audiences (especially experts and novices) and different representation mediums (colourized and black-and-white versions) require tailored visual dialects. As for the demands of various representation mediums, it could be said that current notation is well-rounded and could be used on various representation mediums. This is achieved primarily by the utilization of grey-black brightness levels. While selected palette has certain benefits, it is ineffective in terms of visual popout and visual distance. Thus, it is recommended to introduce the utilization of colour and extend the overall palette. It should be mentioned that proposed abolition of grey-black colour scheme would not result in symbols being indiscriminable, since colour would be used only for redundant coding and sufficient visual distance would be enforced by iconic symbols. So, there is no need to

introduce several dialects for various mediums. Considering notation complexity and accessibility to beginners, it could be said that ISSRM-extended Mal-activity Diagrams notation originates from the Activity Diagrams, which on certain level are similar to widely accepted block diagrams. While extended notation has an increased visual vocabulary and is not accessible for novice users, proposed changes and implementation of semantically immediate icons should ensure that symbols are visually expressive and learning curve is low. Thus, it is unjustified to develop separate dialects based on user's knowledge level.

# IX. Questionnaire for Evaluation Survey

**What educational level are you currently obtaining? (please select applicable)**

Bachelor (1 <sup>st</sup> cycle)	<input type="checkbox"/>
Master (2 <sup>nd</sup> cycle)	<input type="checkbox"/>
PhD (3 <sup>rd</sup> cycle)	<input type="checkbox"/>
Other (please specify)	<input type="text"/>

**What is your gender ?**

Male  Female

**What is your age ?**

->

**In what geographic region are you currently located? (please select applicable)**

Balkans	<input type="checkbox"/>
Eastern Europe	<input type="checkbox"/>
Baltics	<input type="checkbox"/>
Other (please specify)	<input type="text"/>

**Please rate your computer skills (select one applicable option out of 5 for each sub question)**

	Poor	Fair	Average	Good	Excellent
How would you rate your familiarity with <b>Computer Concepts</b> (PC components, operating system basics) ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
How would you rate your familiarity with <b>Word Processing</b> (composing, editing, formatting) ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
How would you rate your familiarity with <b>Internet</b> (navigating webpages, performing search, emailing) ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Asset-related concepts present things that have value to the organization and that need to be protected.

**Business asset** is an asset that has value to the organizations and needs to be protected (e.g., capabilities, employees)

				No answer
--	--	--	--	-----------

What is the clearest representation of business asset ?

**Information system (IS) asset** is component or part of the information system(s), supporting business assets.

				No answer
--	--	--	--	-----------

What is the clearest representation of information system asset ?

**Security criterion** is a property or constraint on business assets characterizing their needs for security. It is expressed in terms of confidentiality, integrity, and availability.

			No answer
--	--	--	-----------

What is the clearest representation of security criterion?

If you have ideas on improving the representations of Asset-related concepts, please write them below.

->

Risk-related concepts present how risk itself is defined.

**Threat** is the potential attack targeting IS assets that may lead to harm (e.g., a hacker using social engineering to obtain confidential account data).

				No answer
--	--	--	--	-----------

What is the clearest representation of threat?

**Vulnerability** is a characteristic of an information system asset that can be a weakness or a flaw in terms of security.

			No answer
--	--	--	-----------

What is the clearest representation of vulnerability?

**Threat agent** is an entity that can potentially cause harm to assets of the information system (e.g., a hacker with strong skills).

				No answer
--	--	--	--	-----------

What is the clearest representation of threat agent?

**Attack** method is a means by which a threat agent carries out a threat (e.g., system intrusion).

				No answer
--	--	--	--	-----------

What is the clearest representation of attack method?

**Impact** is the potential negative consequence of a risk that may harm assets of a system when a threat is accomplished (e.g., password discovery).

			No answer
--	--	--	-----------

What is the clearest representation of impact?

**Security event** is a combination of threat and a vulnerability (e.g., a hacker using social engineering because of lack of awareness).

			No answer
--	--	--	-----------

What is the clearest representation of security event?

**Risk** is the combination of a threat with one or more vulnerabilities leading to negative impacts harming one assets.

What is the clearest representation of risk?

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No answer
--------------------------	--------------------------	--------------------------	--------------------------	-----------

If you have ideas on improving the representations of Risk-related concepts, please write them below.

->

7

Risk treatment-related concepts are defined and implemented to reduce the risks.

**Risk treatment** is the decision of how to treat the identified risks (avoid, reduce, transfer or retain).

What is the clearest representation of risk treatment?

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No answer
--------------------------	--------------------------	--------------------------	--------------------------	-----------

**Security requirement** is a condition that is defined to reduce the risks (e.g., backup copies of information and software shall be taken and tested regularly).

What is the clearest representation of security requirement?

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No answer
--------------------------	--------------------------	--------------------------	--------------------------	-----------

**Control** is the implementation of security requirements (e.g., firewall, building guard).

What is the clearest representation of control?

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No answer
--------------------------	--------------------------	--------------------------	--------------------------	-----------

If you have ideas on improving the representations of Risk treatment-related concepts, please write them below.

->

8

Please match numbers of concepts (from 1 to 7), depicted in the BPMN model below, with their names.

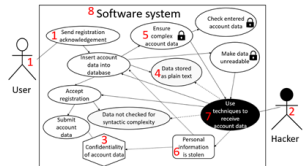
	1	2	3	4	5	6	7
Business asset	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information system asset	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security criterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerability	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Attack method	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Threat agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security requirement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please match numbers of concepts (from 1 to 7), depicted in the Secure Tropos model below, with their names.

	1	2	3	4	5	6	7	8
Business asset	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information system asset	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security criterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Threat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Attack method	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerability	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Threat agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security requirement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

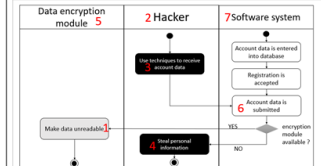
10

Please match numbers of concepts (from 1 to 8), depicted in the **Malactivity** model below, with their names.



	1	2	3	4	5	6	7	8
Business asset	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information system asset	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security criterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Impact	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Attack method	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerability	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Threat agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security requirement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please match numbers of concepts (from 1 to 7), depicted in the **Misuse** model below, with their names.



	1	2	3	4	5	6	7
Business asset	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information system asset	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Impact	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Attack method	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Threat agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security requirement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## X. Evaluation Survey – Results Analysis

<table border="1"> <thead> <tr> <th>Labels</th> <th># Business Asset</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>27</td> </tr> <tr> <td>2</td> <td>12</td> </tr> <tr> <td>3</td> <td>8</td> </tr> <tr> <td>4</td> <td>7</td> </tr> <tr> <td>NA</td> <td>5</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Business Asset	1	27	2	12	3	8	4	7	NA	5	<b>Total</b>	<b>59</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># IS Asset</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>13</td> </tr> <tr> <td>2</td> <td>29</td> </tr> <tr> <td>3</td> <td>9</td> </tr> <tr> <td>4</td> <td>4</td> </tr> <tr> <td>NA</td> <td>4</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# IS Asset	1	13	2	29	3	9	4	4	NA	4	<b>Total</b>	<b>59</b>
Labels	# Business Asset																												
1	27																												
2	12																												
3	8																												
4	7																												
NA	5																												
<b>Total</b>	<b>59</b>																												
Labels	# IS Asset																												
1	13																												
2	29																												
3	9																												
4	4																												
NA	4																												
<b>Total</b>	<b>59</b>																												
<table border="1"> <thead> <tr> <th>Labels</th> <th># Criterion</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>38</td> </tr> <tr> <td>2</td> <td>13</td> </tr> <tr> <td>3</td> <td>4</td> </tr> <tr> <td>NA</td> <td>4</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Criterion	1	38	2	13	3	4	NA	4	<b>Total</b>	<b>59</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># Threat</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>13</td> </tr> <tr> <td>2</td> <td>4</td> </tr> <tr> <td>3</td> <td>29</td> </tr> <tr> <td>4</td> <td>9</td> </tr> <tr> <td>NA</td> <td>4</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Threat	1	13	2	4	3	29	4	9	NA	4	<b>Total</b>	<b>59</b>		
Labels	# Criterion																												
1	38																												
2	13																												
3	4																												
NA	4																												
<b>Total</b>	<b>59</b>																												
Labels	# Threat																												
1	13																												
2	4																												
3	29																												
4	9																												
NA	4																												
<b>Total</b>	<b>59</b>																												
<table border="1"> <thead> <tr> <th>Labels</th> <th># Vulnerability</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>22</td> </tr> <tr> <td>2</td> <td>16</td> </tr> <tr> <td>3</td> <td>13</td> </tr> <tr> <td>NA</td> <td>8</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Vulnerability	1	22	2	16	3	13	NA	8	<b>Total</b>	<b>59</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># Treat Agent</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>2</td> </tr> <tr> <td>2</td> <td>20</td> </tr> <tr> <td>3</td> <td>29</td> </tr> <tr> <td>4</td> <td>3</td> </tr> <tr> <td>NA</td> <td>5</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Treat Agent	1	2	2	20	3	29	4	3	NA	5	<b>Total</b>	<b>59</b>		
Labels	# Vulnerability																												
1	22																												
2	16																												
3	13																												
NA	8																												
<b>Total</b>	<b>59</b>																												
Labels	# Treat Agent																												
1	2																												
2	20																												
3	29																												
4	3																												
NA	5																												
<b>Total</b>	<b>59</b>																												
<table border="1"> <thead> <tr> <th>Labels</th> <th># Attack Method</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>6</td> </tr> <tr> <td>2</td> <td>18</td> </tr> <tr> <td>3</td> <td>15</td> </tr> <tr> <td>4</td> <td>14</td> </tr> <tr> <td>NA</td> <td>6</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Attack Method	1	6	2	18	3	15	4	14	NA	6	<b>Total</b>	<b>59</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># Impact</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>28</td> </tr> <tr> <td>2</td> <td>21</td> </tr> <tr> <td>3</td> <td>7</td> </tr> <tr> <td>NA</td> <td>3</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Impact	1	28	2	21	3	7	NA	3	<b>Total</b>	<b>59</b>		
Labels	# Attack Method																												
1	6																												
2	18																												
3	15																												
4	14																												
NA	6																												
<b>Total</b>	<b>59</b>																												
Labels	# Impact																												
1	28																												
2	21																												
3	7																												
NA	3																												
<b>Total</b>	<b>59</b>																												
<table border="1"> <thead> <tr> <th>Labels</th> <th># Security Event</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>16</td> </tr> <tr> <td>2</td> <td>14</td> </tr> <tr> <td>3</td> <td>20</td> </tr> <tr> <td>NA</td> <td>9</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Security Event	1	16	2	14	3	20	NA	9	<b>Total</b>	<b>59</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># Risk</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>19</td> </tr> <tr> <td>2</td> <td>16</td> </tr> <tr> <td>3</td> <td>19</td> </tr> <tr> <td>NA</td> <td>5</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Risk	1	19	2	16	3	19	NA	5	<b>Total</b>	<b>59</b>				
Labels	# Security Event																												
1	16																												
2	14																												
3	20																												
NA	9																												
<b>Total</b>	<b>59</b>																												
Labels	# Risk																												
1	19																												
2	16																												
3	19																												
NA	5																												
<b>Total</b>	<b>59</b>																												
<table border="1"> <thead> <tr> <th>Labels</th> <th># Risk Treatment</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>14</td> </tr> <tr> <td>2</td> <td>17</td> </tr> <tr> <td>3</td> <td>25</td> </tr> <tr> <td>NA</td> <td>3</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Risk Treatment	1	14	2	17	3	25	NA	3	<b>Total</b>	<b>59</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># Security Requirement</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>3</td> </tr> <tr> <td>2</td> <td>13</td> </tr> <tr> <td>3</td> <td>35</td> </tr> <tr> <td>4</td> <td>3</td> </tr> <tr> <td>NA</td> <td>5</td> </tr> <tr> <td><b>Total</b></td> <td><b>59</b></td> </tr> </tbody> </table>	Labels	# Security Requirement	1	3	2	13	3	35	4	3	NA	5	<b>Total</b>	<b>59</b>		
Labels	# Risk Treatment																												
1	14																												
2	17																												
3	25																												
NA	3																												
<b>Total</b>	<b>59</b>																												
Labels	# Security Requirement																												
1	3																												
2	13																												
3	35																												
4	3																												
NA	5																												
<b>Total</b>	<b>59</b>																												

Labels	# Control
1	33
2	15
3	5
NA	6
<b>Total</b>	<b>59</b>

## XI. Evaluation Survey – Results of Model Matching

Language	Concept	correct	incorrect	NA	total	hit rate	semant. transp. coefficient
BPMN	Business Asset	11	40	8	59	18.64	0.05
BPMN	Information System Asset	27	25	7	59	45.76	0.37
BPMN	Security Criterion	17	33	9	59	28.81	0.17
BPMN	Vulnerability	17	32	10	59	28.81	0.17
BPMN	Attack method	23	28	8	59	38.98	0.29
BPMN	Threat Agent	27	27	5	59	45.76	0.37
BPMN	Security Requirement	16	35	8	59	27.12	0.15
SecureTropos	Business Asset	25	27	7	59	42.37	0.34
SecureTropos	Information System Asset	17	36	6	59	28.81	0.19
SecureTropos	Security Criterion	11	39	9	59	18.64	0.07
SecureTropos	Threat	12	39	8	59	20.34	0.09
SecureTropos	Attack method	11	34	14	59	18.64	0.07
SecureTropos	Vulnerability	18	32	9	59	30.51	0.21
SecureTropos	Threat Agent	21	29	9	59	35.59	0.26
SecureTropos	Security Requirement	13	38	8	59	22.03	0.11
MisUse	Business Asset	19	35	5	59	32.20	0.23
MisUse	Information System Asset	14	38	7	59	23.73	0.13
MisUse	Security Criterion	14	36	9	59	23.73	0.13
MisUse	Impact	15	36	8	59	25.42	0.15
MisUse	Attack method	15	34	10	59	25.42	0.15
MisUse	Vulnerability	17	34	8	59	28.81	0.19
MisUse	Threat Agent	26	26	7	59	44.07	0.36
MisUse	Security Requirement	17	33	9	59	28.81	0.19
Mal-Activity	Business Asset	12	37	10	59	20.34	0.07
Mal-Activity	Information System Asset	10	37	12	59	16.95	0.03
Mal-Activity	Impact	20	29	10	59	33.90	0.23
Mal-Activity	Attack method	21	29	9	59	35.59	0.25
Mal-Activity	Threat Agent	24	26	9	59	40.68	0.31
Mal-Activity	Security Requirement	15	32	12	59	25.42	0.13
Mal-Activity	Control	12	37	10	59	20.34	0.07



## XII. Questionnaire for Symbolization Survey

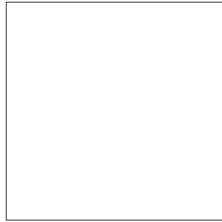
<p><b>What educational level are you currently obtaining? (please select applicable)</b></p> <p>Bachelor (1<sup>st</sup> cycle) <input type="checkbox"/></p> <p>Master (2<sup>nd</sup> cycle) <input type="checkbox"/></p> <p>PhD (3<sup>rd</sup> cycle) <input type="checkbox"/></p> <p>Other (please specify) <input style="width: 80%;" type="text"/></p> <hr/> <p><b>What is your gender ?</b></p> <p>Male <input type="checkbox"/> Female <input type="checkbox"/></p> <hr/> <p><b>What is your age ?</b></p> <p>-&gt; <input style="width: 80%;" type="text"/></p> <hr/> <p><b>In what geographic region are you currently located? (please select applicable)</b></p> <p>Balkans <input type="checkbox"/></p> <p>Eastern Europe <input type="checkbox"/></p> <p>Baltics <input type="checkbox"/></p> <p>Other (please specify) <input style="width: 80%;" type="text"/></p> <hr/> <p><b>Where do you keep passwords to your social media accounts ? (please select applicable)</b></p> <p>In memory <input type="checkbox"/></p> <p>On paper <input type="checkbox"/></p> <p>In dedicated software (password manager) <input type="checkbox"/></p> <p>Other (please specify) <input style="width: 80%;" type="text"/></p> <p style="text-align: right;">2</p>	<p><b>Definition</b> <b>Business asset</b> – resource that has business value for the enterprise</p> <p><b>Example</b> Facebook account data</p> <p><b>Keywords</b> possession, resource, business, importance, profit</p> <hr/> <p>1. Please <u>read</u> the description of concept. Afterwards, <u>sketch</u> an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.</p> <div style="border: 1px solid black; width: 100%; height: 100%; margin: 10px 0;"></div> <p>2. Please <u>rate</u> the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.</p> <table border="1" style="width: 100%; text-align: center; border-collapse: collapse;"> <tr> <td style="width: 20%;">1 Very easy</td> <td style="width: 20%;">2 Easy</td> <td style="width: 20%;">3 Neither easy nor difficult</td> <td style="width: 20%;">4 Difficult</td> <td style="width: 20%;">5 Very difficult</td> </tr> <tr> <td style="height: 20px;"></td> <td></td> <td></td> <td></td> <td></td> </tr> </table> <p style="text-align: right;">3</p>	1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult															
1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult																	
<p><b>Concept</b> <b>Information System asset</b> - company's resource, directly related to information technology</p> <p><b>Example</b> Facebook database</p> <p><b>Keywords</b> technology, digital, system, importance, value</p> <hr/> <p>1. Please <u>read</u> the description of concept. Afterwards, <u>sketch</u> an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.</p> <div style="border: 1px solid black; width: 100%; height: 100%; margin: 10px 0;"></div> <p>2. Please <u>rate</u> the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.</p> <table border="1" style="width: 100%; text-align: center; border-collapse: collapse;"> <tr> <td style="width: 20%;">1 Very easy</td> <td style="width: 20%;">2 Easy</td> <td style="width: 20%;">3 Neither easy nor difficult</td> <td style="width: 20%;">4 Difficult</td> <td style="width: 20%;">5 Very difficult</td> </tr> <tr> <td style="height: 20px;"></td> <td></td> <td></td> <td></td> <td></td> </tr> </table> <p style="text-align: right;">4</p>	1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult						<p><b>Definition</b> <b>Security criterion</b> – specification of business asset's security needs</p> <p><b>Example</b> Confidentiality of account data</p> <p><b>Keywords</b> security, need, description, details</p> <hr/> <p>1. Please <u>read</u> the description of concept. Afterwards, <u>sketch</u> an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.</p> <div style="border: 1px solid black; width: 100%; height: 100%; margin: 10px 0;"></div> <p>2. Please <u>rate</u> the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.</p> <table border="1" style="width: 100%; text-align: center; border-collapse: collapse;"> <tr> <td style="width: 20%;">1 Very easy</td> <td style="width: 20%;">2 Easy</td> <td style="width: 20%;">3 Neither easy nor difficult</td> <td style="width: 20%;">4 Difficult</td> <td style="width: 20%;">5 Very difficult</td> </tr> <tr> <td style="height: 20px;"></td> <td></td> <td></td> <td></td> <td></td> </tr> </table> <p style="text-align: right;">5</p>	1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult					
1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult																	
1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult																	

**Definition** **Threat agent** - person that intends to abuse the information system asset

**Example** Hacker who wants to get account data

**Keywords** expert, hack, break into, exploit

1. Please read the description of concept. Afterwards, sketch an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.



2. Please rate the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.

1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult

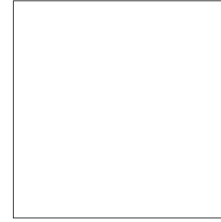
6

**Definition** **Attack method** - method of abusing the IS asset as used by threat agent

**Example** Social engineering

**Keywords** Break into, system, approach, technique, way, hacker

1. Please read the description of concept. Afterwards, sketch an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.



2. Please rate the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.

1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult

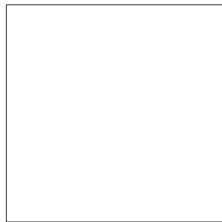
7

**Definition** **Threat** - combination of treat agent and attack method

**Example** Hacker using social engineering to find out account data

**Keywords** danger, opportunity, system, break into

1. Please read the description of concept. Afterwards, sketch an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.



2. Please rate the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.

1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult

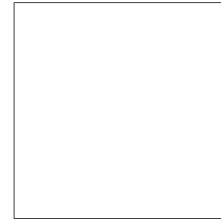
8

**Definition** **Vulnerability** - potential security weakness, that could be exploited

**Example** Account data stored as plain text

**Keywords** weak spot, flaw, security

1. Please read the description of concept. Afterwards, sketch an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.



2. Please rate the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.

1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult

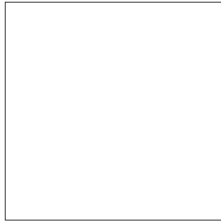
9

**Definition** **Event** – combination of threat and vulnerability

**Example** Hacker uses social engineering to get account data by tricking account owner to reveal answer to security question

**Keywords** problem, issue

1. Please read the description of concept. Afterwards, sketch an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.



2. Please rate the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.

1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult

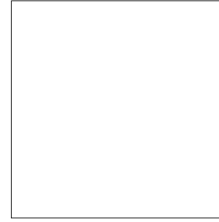
10

**Definition** **Impact** - potential negative outcomes of the accomplished threat

**Example** Account data is revealed and stolen

**Keywords** consequence, effect

1. Please read the description of concept. Afterwards, sketch an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.



2. Please rate the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.

1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult

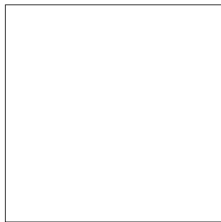
11

**Definition** **Risk** - combination of threat with one or several vulnerabilities, resulting in negative impact and harm to assets

**Example** Hacker uses social engineering to steal account data by tricking account owner to reveal answer to security question

**Keywords** trouble, possibility, fear

1. Please read the description of concept. Afterwards, sketch an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.



2. Please rate the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.

1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult

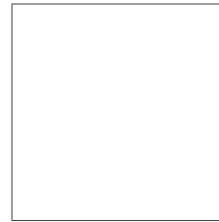
12

**Definition** **Risk treatment** – strategy of dealing with identified risks

**Example** Prevent account details from being easily accessible

**Keywords** risk, minimize, idea, decision

1. Please read the description of concept. Afterwards, sketch an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.



2. Please rate the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.

1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult

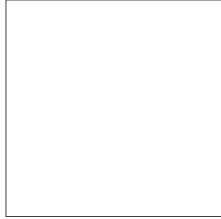
13

**Definition** **Security requirement**- activity which could be performed to minimize identified risks.

**Example** Implement two-factor authentication

**Keywords** action, risk, minimize

1. Please *read* the description of concept. Afterwards, *sketch* an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.



2. Please *rate* the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.

1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult

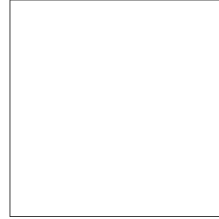
14

**Definition** **Control**- practical realization of security requirement, aimed at minimizing potential risks.

**Example** Two-factor authentication

**Keywords** system, technology, risk, minimize

1. Please *read* the description of concept. Afterwards, *sketch* an icon, which in your opinion would be a clear representation of concept, in the square below. Try to capture the essence and don't focus too much on the quality of the icon.



2. Please *rate* the how difficult it was to sketch the concept. Mark by placing X or V on the scale below.

1 Very easy	2 Easy	3 Neither easy nor difficult	4 Difficult	5 Very difficult

15

### XIII. Symbolization Survey – Obtained Symbols

#### Business Asset

BA

Add this icon to any resource construct in any modelling language

Facebook account data

#### Information System Asset

Facebook database

IA

DB symbol

System symbol

the quality of the icon.

2 options

#### Security Criterion

lock →

Confidentiality of account

on.

Or the 'secure' symbol can be 'inside' of asset.

This icon is for security criterion

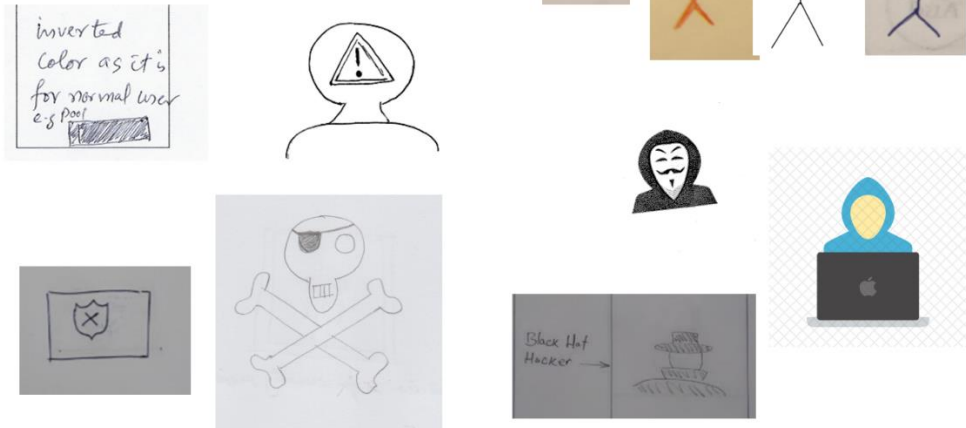
Example: L C A

security access Layers

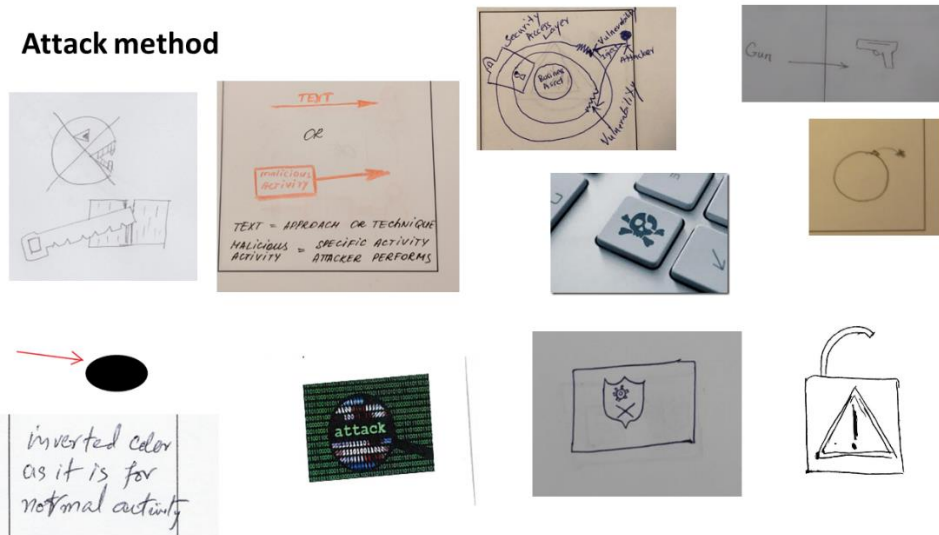
Business Asset

ACCOUNT DATA

### Threat agent



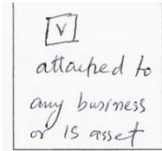
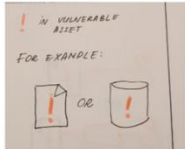
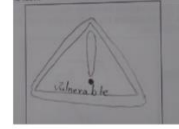
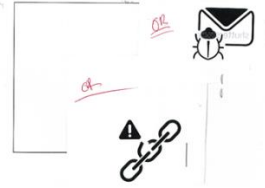
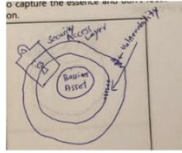
### Attack method



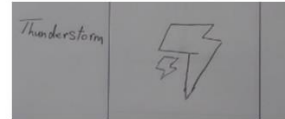
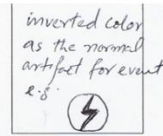
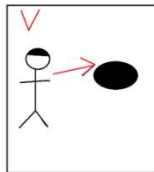
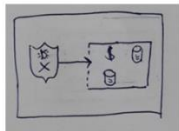
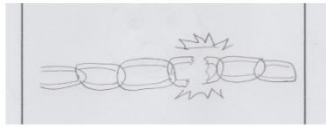
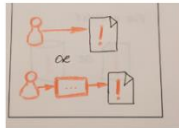
### Threat



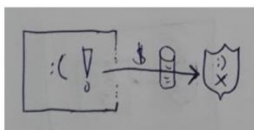
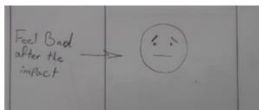
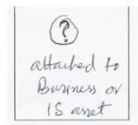
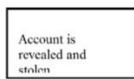
## Vulnerability



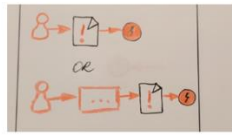
## Event



## Impact

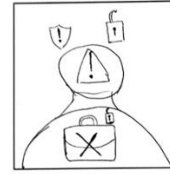
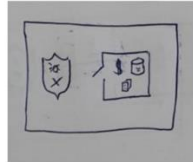
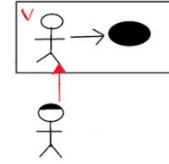
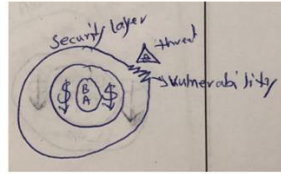


## Risk



to use icon =  
 aggregation of  
 its element  
 (head of...  
 arrow method  
 (value of  
 method))

that's a whole  
 scenario  
 Enclose it in  
 a box (double dotted  
 border line)



OR simply



## Risk treatment

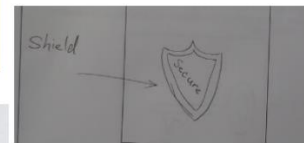
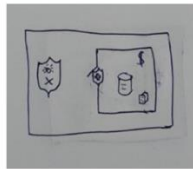


I would  
 combine it  
 Security Requirement.

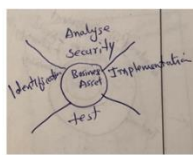
FOR EXAMPLE:  
 TEXT = DESCRIPTION OF  
 RISK TREATMENT  
 (ACTIVITY/METHOD)



OR better:



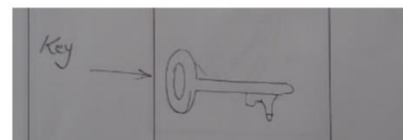
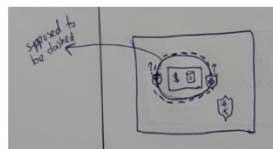
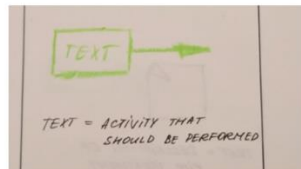
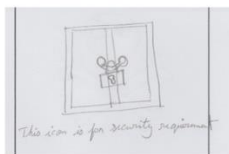
## Security requirement



Definition: Security requirement - activity which  
 should be performed to minimize  
 identified risks.  
 Example: Implement two factor authentication (MFA) for all  
 Remote access, risk, mitigation (140)

As context  
 Security  
 Requirement.

Security  
 requirement






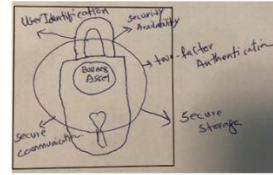
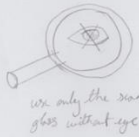
# Control

C

Double border  
line with normal  
activity

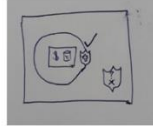


we only see search  
glass without eye





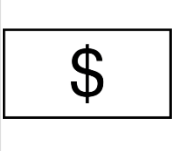







C: TEXT






iC' file context  
TEXT = DESCRIPTION OF REALIZATION  
OF SECURITY REQUIREMENTS

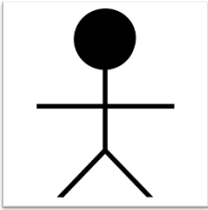






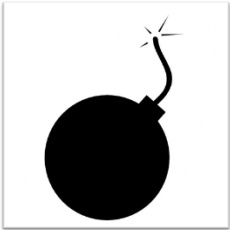




**XIV. Symbolization Survey – Symbol Analysis**





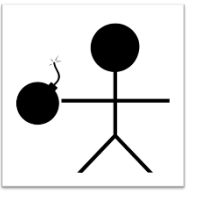
ISSRM Concept	Sketch	Degree of stereotypy	Justification	Category
Business Asset		27% 3/11	Vertical rectangle with distinct corner resembles business document, with lines reminding of lines of text.	Stereotype
		9% 1/11	Combination of vertical rectangles as a stack of business documents.	Prototype
		9% 1/11	Dollar sign is suggested as part of Business Asset symbol with the support of 4/11	Prototype
		9% 1/11	Briefcase symbolize business and relevant assets as kept inside	Prototype
		9% 1/11	Banknote is an obvious choice since it depicts revenue, obtained from assets.	Prototype




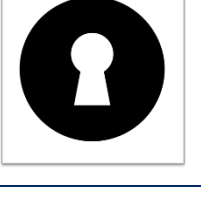
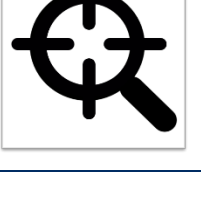
ISSRM Concept	Sketch	Degree of stereotypy	Justification	Category
Information System Asset		36% 4/11	Distinct cylindrical shape is an established depiction of databases, crucial for business.	Stereotype
		27% 3/11	Monitor as common representation of computer.	Prototype
		9% 1/11	Like Business Asset depiction, binary code as a visual representation of digital technologies	Prototype
		NA	As desktops are widely replaced by laptops, this symbol might be a more immediate representation for business users	Suggestion, based on prototype
		NA	Combination of binary code as a distinctive mark of digital technology with roundel, currently used in SRM-extended BPMN	Suggestion, based on prototype

ISSRM Concept	Sketch	Degree of stereotypy	Justification	Category
Security criterion		45% 5/11	Lock symbol indicates security needs as lock is a universal depiction of security – utmost need of assets.	Stereotype
		18% 2/11	Similar to the previous one however letter “C” streamlines symbol recognition as it is the first letter of concept name.	Prototype
		9% 1/11	Shield with tick resembles high-level security needs which imply that assets are intended to stay safe.	Prototype
		9% 1/11	Since opened lock could be perceived as general depiction of breached security, security, lock is meant to serve as a visualization of risk importance.	Prototype
		NA	Lock symbol, indicating security needs, is surrounded by gears – symbol of settings.	Suggestion, based on prototype




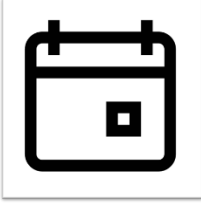

ISSRM Concept	Sketch	Degree of stereotypy	Justification	Category
Threat agent		36% 4/11	Derived from Use Case actor with darkened head depicting negative intentions.	Stereotype
		9% 1/11	Person, covering head with hood to remain untracked by security cameras, association with illegal activity. Modified to ensure distinction with Threat.	Refined prototype
		9% 1/11	Symbol of pirates, hackers are often described as pirates of 21 <sup>st</sup> century, reminds of illegal activity and danger.	Prototype
		9% 1/11	Black hat as symbol of bad guy, denotes contrast between good and evil. Eye mask added to evoke the image of Zorro and associate with vigilantes, known among other things for illegal activities.	Refined prototype
		9% 1/11	Guy Fawkes mask has gained widespread popularity after the "V means Vendetta" (2005) movie. Could be utilized to conceal face/identity, is strongly associated with the Anonymous hacker network. Hood removed as insignificant element.	Refined prototype






ISSRM Concept	Sketch	Degree of stereotypy	Justification	Category
Attack method		9% 1/11	Since bomb is a weapon, it could be directly used as attack method.	Prototype
		9% 1/11	Keyboard key as obvious tool for executing a cyberattack, black colour and skull with crossbones added to indicate danger	Refined prototype
		NA	Complete keyboard as the method for cyberattack, skull and crossbones added to indicate negative intentions.	Suggestion, based on prototype
		NA	Envelope denotes accessibility over distance, that is a trait of cyberattacks, familiar skull with crossbones added to indicate danger. Resulting symbol also bears resemblance to mail bombing.	Suggestion, based on prototype
		NA	Crosshairs as a common depiction of gun-sight, depicts attack method as well.	Refined prototype


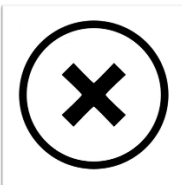


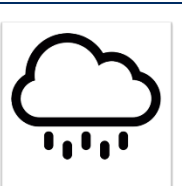
ISSRM Concept	Sketch	Support	Justification	Category
Threat		18% 2/11	Exclamation mark as a symbol of upcoming danger.	Stereotype
		9% 1/11	Handshake as indication of no weapon being hidden, black hand conveys danger and leads to believe that harm is about to be done.	Prototype
		9% 1/11	Follows the concept definition, hacker as threat utilizing computer as attack method.	Prototype
		NA	Similar to the previous prototype, skull with bones added to stress potential danger.	Suggestion, based on prototype
		NA	Follows the concept definition, humanlike figure with a bomb also resembles terrorist, and therefore threat.	Suggestion, based on prototype




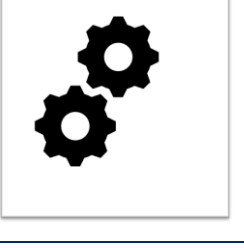

ISSRM Concept	Sketch	Degree of stereotypy	Justification	Category
Vulnerability		45% 5/11	Exclamation mark as a symbol of potential weak spot.	Stereotype
		9% 1/11	Link indicates potential weak spot in the chain that could be broken, impacting the whole chain. Also provides direct association with weak link as symbol of vulnerability point.	Refined prototype
		9% 1/11	Magnifying glass denotes search for potential vulnerabilities, added lock symbolizes secure state of the information systems.	Refined prototype
		NA	Key hole as potential weak spot of any lock, with lock here symbolizing secure state of the information systems.	Suggestion, based on prototype
		NA	Vulnerability is a weak spot, which is about to be endangered as it appears in the cross-hairs – immediate risk which should be mitigated.	Suggestion, based on prototype





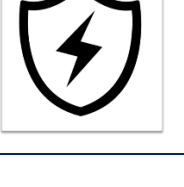







ISSRM Concept	Sketch	Degree of stereotypy	Justification	Category
Event		18% 2/11	Lightning as a symbol of potential immediate threat, aimed at vulnerability. Also adopted in BPMN in similar capacity.	Stereotype
		9% 1/11	Clock as point of time when event has occurred.	Prototype
		9% 1/11	Bell as real-world implementation of event notification.	Prototype
		NA	Calendar depicts certain date when event is about to occur.	Suggestion, based on prototype
		NA	Combination of threat and vulnerability, key whole was already proposed as symbol for vulnerability opened lock is utilized for threat.	Suggestion, based on prototype

ISSRM Concept	Sketch	Degree of stereotypy	Justification	Category
Impact		18% 2/11	Question mark as a depiction of potential consequence, also implies that it is used to denote what could happen.	Stereotype
		9% 1/11	Explosion cloud depict direct consequences of the risk, caused by a threat that is represented as bomb, also has strong associative ties to the impact in general.	Prototype
		9% 1/11	Negative consequences of harm done to Information system assets, skull and bones show that laptop is infected and unusable.	Prototype
		9% 1/11	Downward chart serves as a visualization of direct harm to business assets and dive in revenue.	Refined prototype
		NA	With lock serving as a metaphor for secure system, unlocked state indicates that an occurrence of the breach.	Suggestion, based on prototype

ISSRM Concept	Sketch	Degree of stereotypy	Justification	Category
Risk		18% 2/11	Exclamation mark as a sign to stay away from the potential harm and exhibit caution.	Stereotype
		9% 1/11	X mark indicates a concept of negation, transmitting the message to keep distance from the risk.	Prototype
		NA	Radiation hazard symbol denotes potential threat and similarly to previous symbols, advises to keep away.	Suggestion, based on prototype
		NA	Hand symbol offers same reasoning and is a variation of X mark, conveying the message of cautiousness and attention.	Suggestion, based on prototype
		NA	Rain cloud indicates potential risk and offers direct relation to an umbrella as risk treatment symbol, ensuring consistency.	Suggestion, based on prototype

ISSRM Concept	Sketch	Degree of stereotypy	Justification	Category
Risk treatment		27% 3/11	Shield serves as universal indicator of protection, directly associated with protection from risks.	Stereotype
		9% 1/11	Umbrella depicts protection from elements, and could be expanded to mean protection from any kind of risks. Additionally, umbrella offers a direct correspondence with a symbol of rain cloud, proposed for risk.	Prototype
		9% 1/11	Injection needle offers association with treatment in general, corresponding to the meaning of "treatment" as medical care.	Prototype
		NA	Combination of gears is meant to visualize the outcomes of successful treatment, and depicts system components working seamlessly.	Suggestion, based on prototype
		NA	Crossed tools symbol further expands the concept of treatment as medical care to treatment of the system components, as proposed tools could be used for mechanical repairs.	Suggestion, based on prototype

ISSRM Concept	Sketch	Support	Justification	Category
Security requirement		9% 1/11	Combination of shield and lock emphasise the secure state of the system which is intended to be achieved through security requirements.	Prototype
		9% 1/11	Amalgamation of checklist icon and shield with lock inside is meant to be an immediate representation of security requirement, with shield depicting security and checklist – respectively, requirements.	Prototype
		9% 1/11	Simplified representation of requirement as checkbox that is intended to be ticked.	Prototype
		NA	Proposes symbol could be considered as a combination of icons depicting security (shield) and requirement (checkbox), providing direct semantical meaning.	Suggestion, based on prototype
		NA	Lightning as a symbol of danger is contained within the shield – metaphor for secure state which should be achieved.	Suggestion, based on prototype

ISSRM Concept	Sketch	Support	Justification	Category
Control		18% 2/11	Ticked shield is meant to depict a secure system, obtained after the implementation of controls.	Stereotype
		9% 1/11	Proposed symbol is intended for drawing connections with the real world, since actual fence could be viewed as means to improve security and limit access to the specific area.	Prototype
		9% 1/11	Magnifying glass is depicted in a role of a tool that could be used to inspect and reveal potential problems, thus improving security.	Prototype
		NA	Fingerprint scanner was originally proposed for the security requirement. However, since it is a practical means to improve cybersecurity, depiction of control seems to be a better option.	Refined prototype
		NA	Firewall is one of first things that is associated with practical implementation of cybersecurity, and it is depicted here as globe(Internet) hiding behind the wall.	Suggestion, based on prototype

## XV. Questionnaire for Symbol Identification Survey

<p><b>Каков Ваш уровень образования ?</b></p> <p>Бакалавр (1 уровень) <input type="checkbox"/></p> <p>Специалист / Магистр (2 уровень) <input type="checkbox"/></p> <p>Кандидат наук / Доктор философии (3 уровень) <input type="checkbox"/></p> <p>Другой (пожалуйста, укажите) <input type="text"/></p>																													
<p><b>Каков Ваш пол ?</b></p> <p>М <input type="checkbox"/> Ж <input type="checkbox"/></p>																													
<p><b>Каков Ваш возраст ?</b></p> <p>-&gt; <input type="text"/></p>																													
<p><b>В каком географическом регионе Вы находитесь ?</b></p> <p>Страны Балканского полуострова <input type="checkbox"/></p> <p>Страны Восточной Европы <input type="checkbox"/></p> <p>Страны Балтики <input type="checkbox"/></p> <p>Другой (пожалуйста, укажите) <input type="text"/></p>																													
<p><b>Оцените Ваше знание языков моделирования (выберите один применимый вариант из 5 для каждого субвопроса)</b></p> <table border="1"> <thead> <tr> <th></th> <th>Затр. отв.</th> <th>Плохо</th> <th>Средне</th> <th>Хорошо</th> <th>Отлично</th> </tr> </thead> <tbody> <tr> <td>Unified Modeling Language (UML)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Блок-схемы</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Другой (пожалуйста, укажите)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>							Затр. отв.	Плохо	Средне	Хорошо	Отлично	Unified Modeling Language (UML)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Блок-схемы	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Другой (пожалуйста, укажите)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Затр. отв.	Плохо	Средне	Хорошо	Отлично																								
Unified Modeling Language (UML)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																								
Блок-схемы	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																								
Другой (пожалуйста, укажите)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																								
2																													

<p>Понятия, связанные с активами, представляют элементы, имеющие ценность для организации, и их потребности в безопасности.</p>					
<p><b>Бизнес активы</b> это актив, который представляет ценность для организации и должен быть защищен (нематериальные активы, напр. алгоритм, техн. план).</p>					
Какое из изображений является наиболее наглядным ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p><b>Информационный активы</b> это компонент или часть информационной системы, поддерживающей бизнес активы (напр. корпоративная сеть, сист. администратор).</p>					
Какое из изображений является наиболее наглядным ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p><b>Критерий безопасности</b> это свойство бизнес активов, характеризующее их требования к безопасности. Выражается в приватности, целостности и доступности.</p>					
Какое из изображений является наиболее наглядным ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Если у вас есть предложения по улучшению изображений рассмотренных понятий, пожалуйста укажите их.</p> <p>-&gt; <input type="text"/></p>					
3					






  

<p>Понятия, связанные с рисками, отвечают за определения рисков.</p>					
<p><b>Опасность</b> это возможная атака, которая направлена на информационные активы и может нанести ущерб (напр. хакер применяет соц. инженерию для получения пароля)</p>					
Какое из изображений является наиболее наглядным ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p><b>Уязвимость</b> это характеристика информационного актива, которая может быть дефектом с точки зрения безопасности (напр. отсутствие сигнализации).</p>					
Какое из изображений является наиболее наглядным ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p><b>Угрожающий агент</b> это действующее лицо которое обладает возможностью нанести вред информационным активам (напр. опытный хакер).</p>					
Какое из изображений является наиболее наглядным ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4					

<p><b>Метод атаки</b> это средство, с помощью которого угрожающий агент исполняет угрозу (напр. вторжение в IT систему).</p>					
Какое из изображений является наиболее наглядным ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p><b>Влияние</b> это потенциальные негативные последствия риска, которые после выполнения угрозы могут повредить активы системы (напр. раскрытие пароля).</p>					
Какое из изображений является наиболее наглядным ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p><b>Событие безопасности</b> это комбинация угрозы и уязвимости (напр. хакер использует социальную инженерию, полагаясь на неосведомленность жертв).</p>					
Какое из изображений является наиболее наглядным ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5					

**Риск** это комбинация угрозы с одной или несколькими уязвимостями, приводящая к негативному влиянию, которое вредит активам.

					
Какое из изображений является наиболее наглядным?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>






Если у вас есть предложения по улучшению изображений рассмотренных понятий, пожалуйста укажите их.

->






6

Понятия, связанные с обработкой рисков, определены и внедрены для их минимизации.






**Обработка риска** это решение о способах обращения с обнаруженными рисками (напр. корпоративная сеть не должна иметь прямого выхода в интернет).

					
Какое из изображений является наиболее наглядным?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Требование к безопасности** это условие, заданное для уменьшения рисков (напр. доступ пользователей должен регулироваться средствами аутентификации).

					
Какое из изображений является наиболее наглядным?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Результат** это практическая реализация требования к безопасности (напр. фаерволл, охранник офиса).

					
Какое из изображений является наиболее наглядным?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Если у вас есть предложения по улучшению изображений рассмотренных понятий, пожалуйста укажите их.

->

7



## XVI. Symbol Identification Survey – Results Analysis

<table border="1"> <thead> <tr> <th>Labels</th> <th># Business Asset</th> </tr> </thead> <tbody> <tr><td>1</td><td>6</td></tr> <tr><td>2</td><td>6</td></tr> <tr><td>3</td><td>9</td></tr> <tr><td>4</td><td>13</td></tr> <tr><td>5</td><td>3</td></tr> <tr><td>NA</td><td>2</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Business Asset	1	6	2	6	3	9	4	13	5	3	NA	2	<b>Total</b>	<b>39</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># IS Asset</th> </tr> </thead> <tbody> <tr><td>1</td><td>8</td></tr> <tr><td>2</td><td>16</td></tr> <tr><td>3</td><td>2</td></tr> <tr><td>4</td><td>4</td></tr> <tr><td>5</td><td>7</td></tr> <tr><td>NA</td><td>2</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# IS Asset	1	8	2	16	3	2	4	4	5	7	NA	2	<b>Total</b>	<b>39</b>
Labels	# Business Asset																																
1	6																																
2	6																																
3	9																																
4	13																																
5	3																																
NA	2																																
<b>Total</b>	<b>39</b>																																
Labels	# IS Asset																																
1	8																																
2	16																																
3	2																																
4	4																																
5	7																																
NA	2																																
<b>Total</b>	<b>39</b>																																
<table border="1"> <thead> <tr> <th>Labels</th> <th># Security criterion</th> </tr> </thead> <tbody> <tr><td>1</td><td>7</td></tr> <tr><td>2</td><td>11</td></tr> <tr><td>3</td><td>7</td></tr> <tr><td>4</td><td>7</td></tr> <tr><td>5</td><td>7</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Security criterion	1	7	2	11	3	7	4	7	5	7	<b>Total</b>	<b>39</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># Threat</th> </tr> </thead> <tbody> <tr><td>1</td><td>16</td></tr> <tr><td>2</td><td>16</td></tr> <tr><td>3</td><td>4</td></tr> <tr><td>5</td><td>2</td></tr> <tr><td>NA</td><td>1</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Threat	1	16	2	16	3	4	5	2	NA	1	<b>Total</b>	<b>39</b>				
Labels	# Security criterion																																
1	7																																
2	11																																
3	7																																
4	7																																
5	7																																
<b>Total</b>	<b>39</b>																																
Labels	# Threat																																
1	16																																
2	16																																
3	4																																
5	2																																
NA	1																																
<b>Total</b>	<b>39</b>																																
<table border="1"> <thead> <tr> <th>Labels</th> <th># Vulnerability</th> </tr> </thead> <tbody> <tr><td>1</td><td>13</td></tr> <tr><td>2</td><td>7</td></tr> <tr><td>3</td><td>4</td></tr> <tr><td>4</td><td>9</td></tr> <tr><td>5</td><td>5</td></tr> <tr><td>NA</td><td>1</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Vulnerability	1	13	2	7	3	4	4	9	5	5	NA	1	<b>Total</b>	<b>39</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># Threat agent</th> </tr> </thead> <tbody> <tr><td>1</td><td>1</td></tr> <tr><td>2</td><td>16</td></tr> <tr><td>3</td><td>10</td></tr> <tr><td>4</td><td>7</td></tr> <tr><td>5</td><td>5</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Threat agent	1	1	2	16	3	10	4	7	5	5	<b>Total</b>	<b>39</b>		
Labels	# Vulnerability																																
1	13																																
2	7																																
3	4																																
4	9																																
5	5																																
NA	1																																
<b>Total</b>	<b>39</b>																																
Labels	# Threat agent																																
1	1																																
2	16																																
3	10																																
4	7																																
5	5																																
<b>Total</b>	<b>39</b>																																
<table border="1"> <thead> <tr> <th>Labels</th> <th># Attack Method</th> </tr> </thead> <tbody> <tr><td>1</td><td>6</td></tr> <tr><td>2</td><td>6</td></tr> <tr><td>3</td><td>3</td></tr> <tr><td>4</td><td>20</td></tr> <tr><td>5</td><td>3</td></tr> <tr><td>NA</td><td>1</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Attack Method	1	6	2	6	3	3	4	20	5	3	NA	1	<b>Total</b>	<b>39</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># Impact</th> </tr> </thead> <tbody> <tr><td>2</td><td>10</td></tr> <tr><td>3</td><td>9</td></tr> <tr><td>4</td><td>11</td></tr> <tr><td>5</td><td>8</td></tr> <tr><td>NA</td><td>1</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Impact	2	10	3	9	4	11	5	8	NA	1	<b>Total</b>	<b>39</b>		
Labels	# Attack Method																																
1	6																																
2	6																																
3	3																																
4	20																																
5	3																																
NA	1																																
<b>Total</b>	<b>39</b>																																
Labels	# Impact																																
2	10																																
3	9																																
4	11																																
5	8																																
NA	1																																
<b>Total</b>	<b>39</b>																																
<table border="1"> <thead> <tr> <th>Labels</th> <th># Security event</th> </tr> </thead> <tbody> <tr><td>1</td><td>2</td></tr> <tr><td>2</td><td>1</td></tr> <tr><td>3</td><td>7</td></tr> <tr><td>4</td><td>14</td></tr> <tr><td>5</td><td>14</td></tr> <tr><td>NA</td><td>1</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Security event	1	2	2	1	3	7	4	14	5	14	NA	1	<b>Total</b>	<b>39</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># Risk</th> </tr> </thead> <tbody> <tr><td>1</td><td>19</td></tr> <tr><td>2</td><td>9</td></tr> <tr><td>3</td><td>1</td></tr> <tr><td>4</td><td>1</td></tr> <tr><td>5</td><td>6</td></tr> <tr><td>NA</td><td>3</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Risk	1	19	2	9	3	1	4	1	5	6	NA	3	<b>Total</b>	<b>39</b>
Labels	# Security event																																
1	2																																
2	1																																
3	7																																
4	14																																
5	14																																
NA	1																																
<b>Total</b>	<b>39</b>																																
Labels	# Risk																																
1	19																																
2	9																																
3	1																																
4	1																																
5	6																																
NA	3																																
<b>Total</b>	<b>39</b>																																
<table border="1"> <thead> <tr> <th>Labels</th> <th># Risk treatment</th> </tr> </thead> <tbody> <tr><td>1</td><td>13</td></tr> <tr><td>2</td><td>10</td></tr> <tr><td>3</td><td>4</td></tr> <tr><td>4</td><td>2</td></tr> <tr><td>5</td><td>5</td></tr> <tr><td>NA</td><td>5</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Risk treatment	1	13	2	10	3	4	4	2	5	5	NA	5	<b>Total</b>	<b>39</b>	<table border="1"> <thead> <tr> <th>Labels</th> <th># Security Requirement</th> </tr> </thead> <tbody> <tr><td>1</td><td>2</td></tr> <tr><td>2</td><td>5</td></tr> <tr><td>3</td><td>10</td></tr> <tr><td>4</td><td>2</td></tr> <tr><td>5</td><td>16</td></tr> <tr><td>NA</td><td>4</td></tr> <tr><td><b>Total</b></td><td><b>39</b></td></tr> </tbody> </table>	Labels	# Security Requirement	1	2	2	5	3	10	4	2	5	16	NA	4	<b>Total</b>	<b>39</b>
Labels	# Risk treatment																																
1	13																																
2	10																																
3	4																																
4	2																																
5	5																																
NA	5																																
<b>Total</b>	<b>39</b>																																
Labels	# Security Requirement																																
1	2																																
2	5																																
3	10																																
4	2																																
5	16																																
NA	4																																
<b>Total</b>	<b>39</b>																																

Labels	# Control
1	12
2	4
3	7
4	8
5	3
NA	5
<b>Total</b>	<b>39</b>

# XVII. Questionnaire for Validation Survey

### SRMSurvey

Welcome!

Feel like current security risk modeling notations have the potential for growth?  
Interested in contributing to the notational design?  
Passionate about making the domain of ISSRM and this world a better place?

We are currently working on improving intuitiveness and effectiveness of existing modeling notations, and would really appreciate your input. This survey should take about 25 minutes of your time.  
Your responses are voluntary and will be confidential. Responses will not be identified by individual. All responses will be compiled together and analyzed as a group.

There are 47 questions in this survey.

1  What is your gender?

Choose one of the following answers  
Please choose **only one** of the following:

Female  
 Male  
 Other

2  What is your age?

Choose one of the following answers  
Please choose **only one** of the following:

under 18  
 18-25  
 26-30  
 31-40  
 41-50  
 51-60  
 61 and over

3  In what geographic region are you currently located?

Choose one of the following answers  
Please choose **only one** of the following:

Balkans  
 Eastern Europe  
 Baltics  
 Other

4  What is your major (study program)?

Choose one of the following answers  
Please choose **only one** of the following:

Software Engineering  
 Computer Science  
 Informatics  
 Other

5  What is your educational level?

Choose one of the following answers  
Please choose **only one** of the following:

Bachelor (1st Cycle)  
 Master (2nd Cycle)  
 PhD (3rd Cycle)  
 Other

6  Please rate your modeling skills.  
Please choose the appropriate response for each item:

	NA	Poor	Fair	Good	Average	Excellent
How would you rate your familiarity with BPMN?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
How would you rate your familiarity with UML?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
How would you rate your familiarity with Secure Tropos?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7  Please find a BPMN diagram below.



This diagram depicts the process of a user registering an account in the software system. Upon registration, entered credentials are saved in the system's database. In compliance with personal data storage regulations, confidentiality of data should be ensured. However, since user data is stored as plain text, there exists a vulnerability which could be exploited by a hacker. Utilization of hacking techniques allows a hacker to obtain account data from the database, thus stealing personal information. In order to mitigate the vulnerability, data should be made unreadable prior to being inserted in the database. This can be achieved by introducing data encryption module.

8  Please match numbers of concepts (from 1 to 7), depicted in the BPMN diagram below, with their names. Each number corresponds to a single concept.



Please choose the appropriate response for each item:

	1	2	3	4	5	6	7
Business Asset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information System Asset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vulnerability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Attack Method	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security Requirement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Criterion	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Agent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



9  Please select a preferred symbol for Business Asset  
Please choose the appropriate response for each item:

		
Which symbol would you prefer?	<input type="radio"/>	<input type="radio"/>

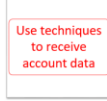

10  Please select a preferred symbol for IS Asset  
Please choose the appropriate response for each item:

		
Which symbol would you prefer?	<input type="radio"/>	<input type="radio"/>

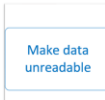
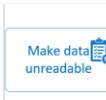
11  Please select a preferred symbol for Vulnerability  
Please choose the appropriate response for each item:

		
Which symbol would you prefer?	<input type="radio"/>	<input type="radio"/>


12  Please select a preferred symbol for Attack Method  
Please choose the appropriate response for each item:

		
Which symbol would you prefer?	<input type="radio"/>	<input type="radio"/>

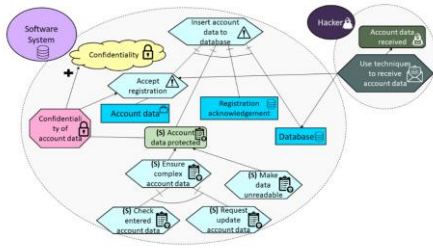
13  Please select a preferred symbol for Security Requirement  
Please choose the appropriate response for each item:

		
Which symbol would you prefer?	<input type="radio"/>	<input type="radio"/>

14  Please select a preferred symbol for Threat Agent  
Please choose the appropriate response for each item:

		
Which symbol would you prefer?	<input type="radio"/>	<input type="radio"/>

15  Please find a Secure Tropos diagram below.



This diagram depicts the process of a user registering an account in the software system. Upon registration, entered credentials are saved in the system's database. In compliance with personal data storage regulations, confidentiality of data should be ensured. However, since user data is stored as plain text, there exists a vulnerability which could be exploited by a hacker. Utilization of hacking techniques allows a hacker to obtain account data from the database, thus stealing personal information. In order to mitigate the vulnerability, data should be made unreadable prior to being inserted in the database. This can be achieved by introducing data encryption module.

16 []  
Please match numbers of concepts (from 1 to 8), depicted in the **Secure Tropos** diagram below, with their names. Each number corresponds to a single concept.

Please choose the appropriate response for each item:

	1	2	3	4	5	6	7	8
Business Asset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information System Asset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vulnerability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Attack Method	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security Requirement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Criterion	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Agent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

17 []  
Please select a preferred symbol for **Business Asset**  
Please choose the appropriate response for each item:

Account data

Account data

Which symbol would you prefer ?

18 []  
Please select a preferred symbol for **IS Asset**  
Please choose the appropriate response for each item:

Software System

Software System

Which symbol would you prefer ?

19 []  
Please select a preferred symbol for **Threat**  
Please choose the appropriate response for each item:

Account data received

Account data received

Which symbol would you prefer ?

21 [] Please select a preferred symbol for **Attack Method**  
Please choose the appropriate response for each item:

Use techniques to receive account data

Use techniques to receive account data

Which symbol would you prefer ?

20 [] Please select a preferred symbol for **Vulnerability**  
Please choose the appropriate response for each item:

Insert account data to database

Insert account data to database

Which symbol would you prefer ?

22 [] Please select a preferred symbol for **Security Requirement**  
Please choose the appropriate response for each item:

(S) Make data unreadable

(S) Make data unreadable

Which symbol would you prefer ?

23 [] Please select a preferred symbol for Criterion  
Please choose the appropriate response for each item:

Which symbol would you prefer ?

24 [] Please select a preferred symbol for Threat Agent  
Please choose the appropriate response for each item:

Which symbol would you prefer ?

25 [] Please find a Misuse Cases diagram below.

This diagram depicts the process of a user registering an account in the software system. Upon registration, entered credentials are saved in the system's database. In compliance with personal data storage regulations, confidentiality of data should be ensured. However, since user data is stored as plain text, there exists a vulnerability which could be exploited by a hacker. Utilization of hacking techniques allows a hacker to obtain account data from the database, thus stealing personal information. In order to mitigate the vulnerability, data should be made unreadable prior to being inserted in the database. This can be achieved by introducing data encryption module.

26 [] Please match numbers of concepts (from 1 to 8), depicted in the Misuse Cases diagram below, with their names. Each number corresponds to a single concept.

Please choose the appropriate response for each item:

	1	2	3	4	5	6	7	8
Business Asset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information System Asset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Impact	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vulnerability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Attack Method	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security Requirement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Criterion	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Agent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>


27 [] Please select a preferred symbol for Business Asset  
Please choose the appropriate response for each item:

Which symbol would you prefer ?


28 [] Please select a preferred symbol for IS Asset  
Please choose the appropriate response for each item:

Which symbol would you prefer ?



29  Please select a preferred symbol for Impact  
Please choose the appropriate response for each item:

	Personal information is stolen	Personal information is stolen 
Which symbol would you prefer ?	<input type="radio"/>	<input type="radio"/>



30  Please select a preferred symbol for Vulnerability  
Please choose the appropriate response for each item:

	Data stored as plain text	Data stored as plain text 
Which symbol would you prefer ?	<input type="radio"/>	<input type="radio"/>


31  Please select a preferred symbol for Attack Method  
Please choose the appropriate response for each item:

	Use techniques to retrieve account data 	Use techniques to retrieve account data 
Which symbol would you prefer ?	<input type="radio"/>	<input type="radio"/>

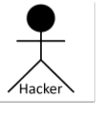

32  Please select a preferred symbol for Security Requirement  
Please choose the appropriate response for each item:

	Make data unreadable 	Make data unreadable 
Which symbol would you prefer ?	<input type="radio"/>	<input type="radio"/>

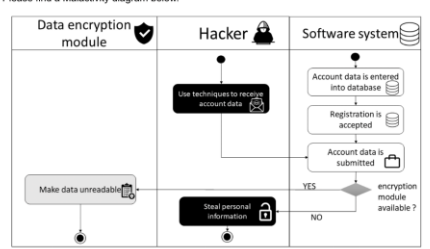
33  Please select a preferred symbol for Criterion  
Please choose the appropriate response for each item:

	Confidentiality of account data	Confidentiality of account data 
Which symbol would you prefer ?	<input type="radio"/>	<input type="radio"/>

34  Please select a preferred symbol for Threat Agent  
Please choose the appropriate response for each item:

		
Which symbol would you prefer ?	<input type="radio"/>	<input type="radio"/>

35  Please find a Malactivity diagram below.



This diagram depicts the process of a user registering an account in the software system. Upon registration, entered credentials are saved in the system's database. In compliance with personal data storage regulations, confidentiality of data should be ensured. However, since user data is stored as plain text, there exists a vulnerability which could be exploited by a hacker. Utilization of hacking techniques allows a hacker to obtain account data from the databases, thus stealing personal information. In order to mitigate the vulnerability, data should be made unreadable prior to being inserted in the database. This can be achieved by introducing data encryption module.

36 []  
Please match numbers of concepts (from 1 to 7), depicted in the Malactivity diagram below, with their names. Each number corresponds to a single concept.

Please choose the appropriate response for each item:

	1	2	3	4	5	6	7
Business Asset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information System Asset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Impact	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Attack Method	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security Requirement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Control	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Agent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

37 []  
Please select a preferred symbol for Business Asset  
Please choose the appropriate response for each item:

Which symbol would you prefer ?

38 []  
Please select a preferred symbol for IS Asset  
Please choose the appropriate response for each item:

Which symbol would you prefer ?

39 []  
Please select a preferred symbol for Impact  
Please choose the appropriate response for each item:

Which symbol would you prefer ?

40 [] Please select a preferred symbol for Attack Method  
Please choose the appropriate response for each item:

Which symbol would you prefer ?

41 [] Please select a preferred symbol for Security Requirement  
Please choose the appropriate response for each item:


Which symbol would you prefer ?

42 [] Please select a preferred symbol for Control  
Please choose the appropriate response for each item:

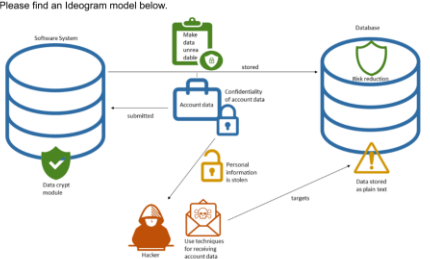
Which symbol would you prefer ?



43  Please select a preferred symbol for Threat Agent  
Please choose the appropriate response for each item:

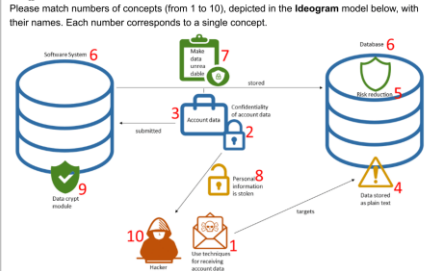
	Hacker	Hacker 
Which symbol would you prefer ?	<input type="radio"/>	<input type="radio"/>

44  Please find an Ideogram model below.



This diagram depicts the process of a user registering an account in the software system. Upon registration, entered credentials are saved in the system's database. In compliance with personal data storage regulations, confidentiality of data should be ensured. However, since user data is stored as plain text, there exists a vulnerability which could be exploited by a hacker. Utilization of hacking techniques allows a hacker to obtain account data from the database, thus stealing personal information. In order to mitigate the vulnerability, data should be made unreadable prior to being inserted in the database. This can be achieved by introducing data encryption module.

45  Please match numbers of concepts (from 1 to 10), depicted in the Ideogram model below, with their names. Each number corresponds to a single concept.



Please choose the appropriate response for each item:

	1	2	3	4	5	6	7	8	9	10
Business Asset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information System Asset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Attack Method	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Impact	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security Requirement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vulnerability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Agent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Risk Treatment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Control	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Criterion	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## XVIII. Validation Survey – Results Analysis

Expert users results

<b>Concepts</b>	# ideograDiagramSel_SQ001	
AtMet		16
<b>Labels</b>		<b>16</b>
<b>Concepts</b>	# ideograDiagramSel_SQ002	
Crite		11
SeReq		5
<b>Total</b>		<b>16</b>
<b>COncpts</b>	# ideograDiagramSel_SQ003	
BSA		15
ISA		1
<b>Total</b>		<b>16</b>
<b>COncpts</b>	# ideograDiagramSel_SQ004	
Vulne		16
<b>Total</b>		<b>16</b>
<b>COncpts</b>	# ideograDiagramSel_SQ005	
Crite		1
RiTre		15
<b>Total</b>		<b>16</b>
<b>COncpts</b>	# ideograDiagramSel_SQ006	
BSA		1
ISA		14
(пусто)		
<b>Total</b>		<b>15</b>
<b>COncpts</b>	# ideograDiagramSel_SQ007	
Contr		2
Crite		3
SeReq		11
<b>Total</b>		<b>16</b>
<b>COncpts</b>	# ideograDiagramSel_SQ008	
Impac		16
<b>Total</b>		<b>16</b>
<b>COncpts</b>	# ideograDiagramSel_SQ009	
Contr		14
RiTre		2
<b>Total</b>		<b>16</b>
<b>COncpts</b>	# ideograDiagramSel_SQ010	
ThAge		16
<b>Total</b>		<b>16</b>

<b>Concepts</b>	<input type="button" value="▼"/> # malact DiagramSelect_SQ001	
Contr		1
SeReq		15
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<input type="button" value="▼"/> # malact DiagramSelect_SQ002	
ThAge		16
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<input type="button" value="▼"/> # malact DiagramSelect_SQ003	
AtMet		16
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<input type="button" value="▼"/> # malact DiagramSelect_SQ004	
Impac		16
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<input type="button" value="▼"/> # malact DiagramSelect_SQ005	
BSA		3
Contr		13
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<input type="button" value="▼"/> # malact DiagramSelect_SQ006	
BSA		12
Contr		2
ISA		1
SeReq		1
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<input type="button" value="▼"/> # malact DiagramSelect_SQ007	
BSA		1
ISA		15
<b>Total</b>		<b>16</b>

<b>Labels</b>	<b># malact Basset</b>	
new		12
old		4
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># malact Isasset</b>	
new		13
old		3
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># malact Impact</b>	
new		15
old		1
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># malact AttackMethod</b>	
new		12
old		4
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># malact SecurityReq</b>	
new		16
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># malact Control</b>	
new		15
old		1
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># malact ThreatAgent</b>	
new		16
<b>Total</b>		<b>16</b>

<b>Concepts</b>	<b># misuseDiagramSelect_SQ001</b>	
BAS		15
ISA		1
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># misuse DiagramSelect_SQ002</b>	
ISA		1
ThAge		15
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># misuse DiagramSelect_SQ003</b>	
Crite		13
SeReq		3
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># misuse DiagramSelect_SQ004</b>	
Vulne		16
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># misuse DiagramSelect_SQ005</b>	
Crite		3
SeReq		13
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># misuse DiagramSelect_SQ006</b>	
Impac		16
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># misuse DiagramSelect_SQ007</b>	
AtMet		16
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># misuse DiagramSelect_SQ008</b>	
BAS		1
ISA		13
ThAge		1
(пусто)		
<b>Total</b>		<b>15</b>

<b>Labels</b>	<b># misuse Basset</b>	
new		11
old		5
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># misuse Isasset</b>	
new		14
old		2
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># misuse Impact</b>	
new		16
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># misuse Vulnerability</b>	
new		16
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># misuse AttackMethod</b>	
new		10
old		6
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># misuse SecurityReq</b>	
new		13
old		3
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># misuse Criterion</b>	
new		13
old		3
<b>Total</b>		<b>16</b>
<b>Labels</b>	<b># misuse ThreatAgent</b>	
new		13
old		3
<b>Total</b>		<b>16</b>

<b>Concepts</b>	<b># stDiagramSelect_SQ001</b>	
BAS		1
ISA		15
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># stDiagramSelect_SQ002</b>	
Crite		13
SeReq		2
Threa		1
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># stDiagramSelect_SQ003</b>	
BAS		15
ISA		1
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># stDiagramSelect_SQ004</b>	
Crite		2
SeReq		14
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># stDiagramSelect_SQ005</b>	
ISA		1
Vulne		15
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># stDiagramSelect_SQ006</b>	
ThAge		16
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># stDiagramSelect_SQ007</b>	
AtMet		15
Threa		1
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># stDiagramSelect_SQ008</b>	
AtMet		1
Crite		1
Threa		14
<b>Total</b>		<b>16</b>

<b>Labels</b>	<input type="button" value="▼"/>	<b># seqtro Basset</b>	
new			15
old			1
<b>Total</b>			<b>16</b>
<b>Labels</b>	<input type="button" value="▼"/>	<b># seqtro Isasset</b>	
new			16
<b>Total</b>			<b>16</b>
<b>Labels</b>	<input type="button" value="▼"/>	<b># seqtro Threat</b>	
new			14
old			2
<b>Total</b>			<b>16</b>
<b>Labels</b>	<input type="button" value="▼"/>	<b># seqtro Vulnerability</b>	
new			14
old			2
<b>Total</b>			<b>16</b>
<b>Labels</b>	<input type="button" value="▼"/>	<b># seqtro AttackMethod</b>	
new			12
old			4
<b>Total</b>			<b>16</b>
<b>Labels</b>	<input type="button" value="▼"/>	<b># seqtro SecurityReq</b>	
new			15
old			1
<b>Total</b>			<b>16</b>
<b>Labels</b>	<input type="button" value="▼"/>	<b># seqtro Criterion</b>	
new			14
old			2
<b>Total</b>			<b>16</b>
<b>Labels</b>	<input type="button" value="▼"/>	<b># seqtro ThreatAgent</b>	
new			14
old			2
<b>Total</b>			<b>16</b>



<b>Concepts</b>	<b># bpmnDiagramSelect_SQ001</b>	
BA		1
ISA		15
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># bpmnDiagramSelect_SQ002</b>	
Crit		1
SeReq		15
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># bpmnDiagramSelect_SQ003</b>	
BA		14
Crit		2
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># bpmnDiagramSelect_SQ004</b>	
BA		1
Crit		10
ISA		1
SeReq		1
Vuln		3
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># bpmnDiagramSelect_SQ005</b>	
ThAge		16
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># bpmnDiagramSelect_SQ006</b>	
Crit		2
Vuln		14
<b>Total</b>		<b>16</b>
<b>Concepts</b>	<b># bpmnDiagramSelect_SQ007</b>	
AtMet		16
<b>Total</b>		<b>16</b>

<b>Label</b>	<b># bpmn Basset</b>	
new		13
old		3
<b>Total</b>		<b>16</b>
<b>Label</b>	<b># bpmn Isasset</b>	
new		14
old		2
<b>Total</b>		<b>16</b>
<b>Label</b>	<b># bpmn Vulnerability</b>	
new		4
old		12
<b>Total</b>		<b>16</b>
<b>Label</b>	<b># bpmn AttackMethod</b>	
new		8
old		8
<b>Total</b>		<b>16</b>
<b>Label</b>	<b># bpmn SecurityReq</b>	
new		12
old		4
<b>Total</b>		<b>16</b>
<b>Label</b>	<b># bpmn ThreatAgent</b>	
new		13
old		3
<b>Total</b>		<b>16</b>

## Novice user results

<b>Concepts</b> ▾ # ideograDiagramSel[SQ001]	
AtMet	18
BSA	3
NA	1
RiTre	1
<b>Total</b>	<b>23</b>
<b>Concepts</b> ▾ # ideograDiagramSel[SQ002]	
BSA	1
Contr	2
Crite	7
Impac	2
ISA	3
NA	1
RiTre	1
SeReq	5
Vulne	1
<b>Total</b>	<b>23</b>
<b>Concepts</b> ▾ # ideograDiagramSel[SQ003]	
AtMet	1
BSA	12
Crite	1
Impac	3
ISA	4
SeReq	1
ThAge	1
<b>Total</b>	<b>23</b>
<b>Concepts</b> ▾ # ideograDiagramSel[SQ004]	
Crite	1
Impac	3
ISA	1
RiTre	1
Vulne	17
<b>Total</b>	<b>23</b>
<b>Concepts</b> ▾ # ideograDiagramSel[SQ005]	
AtMet	1
BSA	1
Contr	5
Crite	1
RiTre	11
SeReq	3
Vulne	1
<b>Total</b>	<b>23</b>
<b>Concepts</b> ▾ # ideograDiagramSel[SQ006]	
BSA	7
ISA	12
RiTre	2
Vulne	2
<b>Total</b>	<b>23</b>
<b>Concepts</b> ▾ # ideograDiagramSel[SQ007]	
Contr	3
Crite	4
SeReq	13
ThAge	3
<b>Total</b>	<b>23</b>
<b>Concepts</b> ▾ # ideograDiagramSel[SQ008]	
Contr	1
Crite	2
Impac	15
RiTre	3
Vulne	2
<b>Total</b>	<b>23</b>
<b>Concepts</b> ▾ # ideograDiagramSel[SQ009]	
BSA	1
Contr	11
Crite	5
NA	1
RiTre	4
SeReq	1
<b>Total</b>	<b>23</b>
<b>Concepts</b> ▾ # ideograDiagramSel[SQ010]	
AtMet	1
Contr	2
Crite	1
Impac	1
NA	1
ThAge	17
<b>Total</b>	<b>23</b>

<b>Concepts</b>	<b># maDiagramSelect[SQ001]</b>	
BSA		3
ISA		2
SeReq		18
<b>Total</b>		<b>23</b>
<b>Concepts</b>	<b># maDiagramSelect[SQ002]</b>	
BSA		2
Impac		1
ISA		2
ThAge		18
<b>Total</b>		<b>23</b>
<b>Concepts</b>	<b># maDiagramSelect[SQ003]</b>	
AtMet		20
Impac		1
NA		1
ThAge		1
<b>Total</b>		<b>23</b>
<b>Concepts</b>	<b># maDiagramSelect[SQ004]</b>	
AtMet		1
Contr		2
Impac		18
SeReq		1
ThAge		1
<b>Total</b>		<b>23</b>
<b>Concepts</b>	<b># maDiagramSelect[SQ005]</b>	
AtMet		1
BSA		1
Contr		15
Impac		2
ISA		3
SeReq		1
<b>Total</b>		<b>23</b>
<b>Concepts</b>	<b># maDiagramSelect[SQ006]</b>	
AtMet		1
BSA		9
Contr		5
ISA		5
SeReq		1
ThAge		2
<b>Total</b>		<b>23</b>
<b>Concepts</b>	<b># maDiagramSelect[SQ007]</b>	
BSA		8
Contr		1
Impac		1
ISA		10
NA		1
SeReq		1
ThAge		1
<b>Total</b>		<b>23</b>

<b>Labels</b>	<input type="button" value="▼"/> # maBasset[SQ001]	
new		18
old		5
<b>Total</b>		<b>23</b>
<b>Labels</b>	<input type="button" value="▼"/> # malsasset[SQ001]	
new		18
old		5
<b>Total</b>		<b>23</b>
<b>Labels</b>	<input type="button" value="▼"/> # maImpact[SQ001]	
new		19
old		4
<b>Total</b>		<b>23</b>
<b>Labels</b>	<input type="button" value="▼"/> # maAttackMethod[SQ001]	
new		17
old		6
<b>Total</b>		<b>23</b>
<b>Labels</b>	<input type="button" value="▼"/> # maSecurityReq[SQ001]	
new		17
old		6
<b>Total</b>		<b>23</b>
<b>Labels</b>	<input type="button" value="▼"/> # maControl[SQ001]	
new		18
old		5
<b>Total</b>		<b>23</b>
<b>Labels</b>	<input type="button" value="▼"/> # maThreatAgent[SQ001]	
new		19
old		4
<b>Total</b>		<b>23</b>

<b>Concepts</b>	# mcDiagramSelect[SQ001]	
BAS		10
Impac		4
ISA		7
NA		1
Vulne		1
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# mcDiagramSelect[SQ002]	
AtMet		1
Impac		3
ISA		1
ThAge		18
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# mcDiagramSelect[SQ003]	
BAS		1
Crite		11
Impac		1
ISA		3
SeReq		6
ThAge		1
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# mcDiagramSelect[SQ004]	
BAS		1
Impac		1
ISA		1
NA		1
SeReq		1
Vulne		18
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# mcDiagramSelect[SQ005]	
AtMet		1
BAS		2
Crite		6
SeReq		13
Vulne		1
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# mcDiagramSelect[SQ006]	
AtMet		2
Crite		2
Impac		12
NA		1
SeReq		2
ThAge		1
Vulne		3
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# mcDiagramSelect[SQ007]	
AtMet		18
Crite		2
Impac		1
ThAge		2
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# mcDiagramSelect[SQ008]	
BAS		8
Crite		2
ISA		10
NA		1
ThAge		2
<b>Total</b>		<b>23</b>

<b>Labels</b>	<b># mcBasset[SQ001]</b>	
NA		1
new		12
old		10
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># mclasset[SQ001]</b>	
new		21
old		2
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># mclImpact[SQ001]</b>	
new		19
old		4
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># mcVulnerability[SQ001]</b>	
new		19
old		4
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># mcAttackMethod[SQ001]</b>	
new		16
old		7
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># mcSecurityReq[SQ001]</b>	
new		9
old		14
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># mcCriterion[SQ001]</b>	
new		19
old		4
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># mcThreatAgent[SQ001]</b>	
new		16
old		7
<b>Total</b>		<b>23</b>

<b>Concepts</b>	# stDiagramSelect[SQ001]	
AtMet		1
BAS		8
ISA		10
NA		3
ThAge		1
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# stDiagramSelect[SQ002]	
BAS		3
Crite		7
ISA		1
NA		1
SeReq		8
Threa		1
Vulne		2
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# stDiagramSelect[SQ003]	
BAS		10
Crite		2
ISA		7
SeReq		1
Threa		1
Vulne		2
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# stDiagramSelect[SQ004]	
Crite		7
ISA		2
NA		1
SeReq		10
ThAge		1
Threa		1
Vulne		1
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# stDiagramSelect[SQ005]	
AtMet		1
BAS		1
Crite		3
ISA		1
NA		1
SeReq		2
ThAge		1
Threa		2
Vulne		11
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# stDiagramSelect[SQ006]	
ISA		1
SeReq		1
ThAge		16
Threa		5
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# stDiagramSelect[SQ007]	
AtMet		20
Crite		1
NA		1
ThAge		1
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# stDiagramSelect[SQ008]	
Crite		1
NA		1
SeReq		1
ThAge		3
Threa		12
Vulne		5
<b>Total</b>		<b>23</b>



<b>Labels</b>	<b># stBasset[SQ001]</b>	
new		19
old		4
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># stIsasset[SQ001]</b>	
new		18
old		5
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># stThreat[SQ001]</b>	
new		18
old		5
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># stVulnerability[SQ001]</b>	
new		22
old		1
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># stAttackMethod[SQ001]</b>	
new		20
old		3
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># stSecurityReq[SQ001]</b>	
new		19
old		4
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># stCriterion[SQ001]</b>	
new		20
old		3
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># stThreatAgent[SQ001]</b>	
new		20
old		3
<b>Total</b>		<b>23</b>

<b>Concepts</b>	# bpmnDiagramSelect[SQ001]	
BA		8
ISA		10
SeReq		1
ThAge		1
Vuln		3
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# bpmnDiagramSelect[SQ002]	
AtMet		3
Crit		3
ISA		3
SeReq		14
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# bpmnDiagramSelect[SQ003]	
BA		8
Crit		3
ISA		7
Vuln		5
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# bpmnDiagramSelect[SQ004]	
AtMet		1
BA		4
Crit		9
ISA		1
NA		1
SeReq		3
Vuln		4
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# bpmnDiagramSelect[SQ005]	
AtMet		2
SeReq		1
ThAge		20
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# bpmnDiagramSelect[SQ006]	
BA		1
Crit		8
SeReq		3
ThAge		1
Vuln		10
<b>Total</b>		<b>23</b>
<b>Concepts</b>	# bpmnDiagramSelect[SQ007]	
AtMet		18
BA		1
ISA		1
SeReq		1
ThAge		1
Vuln		1
<b>Total</b>		<b>23</b>

<b>Labels</b>	<b># bpmnBasset[SQ001]</b>	
new		22
old		1
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># bpmnIasset[SQ001]</b>	
new		17
old		6
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># bpmnVulnerability[SQ001]</b>	
new		15
old		8
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># bpmnAttackMethod[SQ001]</b>	
NA		1
new		17
old		5
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># bpmnSecurityReq[SQ001]</b>	
new		17
old		6
<b>Total</b>		<b>23</b>
<b>Labels</b>	<b># bpmnThreatAgent[SQ001]</b>	
new		20
old		3
<b>Total</b>		<b>23</b>

## XIX. Validation Survey – Results of Model Matching

Language	Concept	Icon-enriched notations									
		Novice users					Expert users				
		correct	in-correct	total	hit rate	semant. transp. coefficient	correct	in-correct	total	hit rate	semant. transp. coefficient
BPMN	Business Asset	8	15	23	34.78	0.24	14	2	16	87.50	0.85
BPMN	Information System Asset	10	13	23	43.48	0.34	15	1	16	93.75	0.93
BPMN	Vulnerability	10	13	23	43.48	0.34	14	2	16	87.50	0.85
BPMN	Attack Method	18	5	23	78.26	0.75	16	0	16	100.00	1.00
BPMN	Security Requirement	14	9	23	60.87	0.54	15	1	16	93.75	0.93
BPMN	Threat Agent	20	3	23	86.96	0.85	16	0	16	100.00	1.00
BPMN	Criterion	9	14	23	39.13	0.29	10	6	16	62.50	0.56
Secure Tropos	Business Asset	10	13	23	43.48	0.35	15	1	16	93.75	0.93
Secure Tropos	Information System Asset	10	13	23	43.48	0.35	15	1	16	93.75	0.93
Secure Tropos	Threat	12	11	23	52.17	0.45	14	2	16	87.50	0.86
Secure Tropos	Vulnerability	11	12	23	47.83	0.40	15	1	16	93.75	0.93
Secure Tropos	Attack Method	20	3	23	86.96	0.85	15	1	16	93.75	0.93
Secure Tropos	Security Requirement	10	13	23	43.48	0.35	14	2	16	87.50	0.86
Secure Tropos	Criterion	7	16	23	30.43	0.20	13	3	16	81.25	0.79
Secure Tropos	Threat Agent	16	7	23	69.57	0.65	16	0	16	100.00	1.00
Mal-activity Diagrams	Business Asset	9	14	23	39.13	0.29	12	4	16	75.00	0.71
Mal-activity Diagrams	Information System Asset	10	13	23	43.48	0.34	15	1	16	93.75	0.93
Mal-activity Diagrams	Impact	18	5	23	78.26	0.75	16	0	16	100.00	1.00
Mal-activity Diagrams	Attack Method	20	3	23	86.96	0.85	16	0	16	100.00	1.00
Mal-activity Diagrams	Security Requirement	18	5	23	78.26	0.75	15	1	16	93.75	0.93
Mal-activity Diagrams	Control	15	8	23	65.22	0.59	13	3	16	81.25	0.78
Mal-activity Diagrams	Threat Agent	18	5	23	78.26	0.75	16	0	16	100.00	1.00
Misuse Cases	Business Asset	10	13	23	43.48	0.35	15	1	16	93.75	0.93
Misuse Cases	Information System Asset	10	13	23	43.48	0.35	13	3	16	81.25	0.79
Misuse Cases	Impact	12	11	23	52.17	0.45	16	0	16	100.00	1.00
Misuse Cases	Vulnerability	18	5	23	78.26	0.75	16	0	16	100.00	1.00
Misuse Cases	Attack Method	18	5	23	78.26	0.75	16	0	16	100.00	1.00
Misuse Cases	Security Requirement	13	10	23	56.52	0.50	13	3	16	81.25	0.79
Misuse Cases	Criterion	11	12	23	47.83	0.40	13	3	16	81.25	0.79
Misuse Cases	Threat Agent	18	5	23	78.26	0.75	15	1	16	93.75	0.93
Ideogram	Attack Method	18	5	23	78.26	0.76	16	0	16	100.00	1.00
Ideogram	Criterion	7	16	23	30.43	0.23	11	5	16	68.75	0.65
Ideogram	Business Asset	12	11	23	52.17	0.47	15	1	16	93.75	0.93

Ideogram	Vulnerability	17	6	23	73.91	0.71	16	0	16	100.00	1.00
Ideogram	Risk Treatment	11	12	23	47.83	0.42	15	1	16	93.75	0.93
Ideogram	Information System Asset	12	11	23	52.17	0.47	14	2	16	87.50	0.86
Ideogram	Security Requirement	13	10	23	56.52	0.52	11	5	16	68.75	0.65
Ideogram	Impact	15	8	23	65.22	0.61	16	0	16	100.00	1.00
Ideogram	Control	11	12	23	47.83	0.42	14	2	16	87.50	0.86
Ideogram	Threat Agent	17	6	23	73.91	0.71	16	0	16	100.00	1.00

## XX. Icons Details

Icon Name	Author	Source	Link
Checklist	Aaron K. Kim	The Noun Project	<a href="https://thenounproject.com/term/checklist/316296/">https://thenounproject.com/term/checklist/316296/</a>
Shield	Marek Polakovic	The Noun Project	<a href="https://thenounproject.com/term/shield/304274/">https://thenounproject.com/term/shield/304274/</a>
Shield	To Uen	The Noun Project	<a href="https://thenounproject.com/term/shield/445820/">https://thenounproject.com/term/shield/445820/</a>
Hoodie	Sergey Demushkin	The Noun Project	<a href="https://thenounproject.com/term/hoodie/129183/">https://thenounproject.com/term/hoodie/129183/</a>
Skull	Stanislav Levin	The Noun Project	<a href="https://thenounproject.com/term/skull/217591/">https://thenounproject.com/term/skull/217591/</a>
Key in key-hole	flaticon	Freepic.com	<a href="https://www.freepik.com/free-icon/key-in-key-hole_729808.htm">https://www.freepik.com/free-icon/key-in-key-hole_729808.htm</a>
Hacker	Peter van Driel	Icon-finder.com	<a href="https://www.iconfinder.com/icons/1909691/crime_cyber_group_hacker_protect_security_skull_icon">https://www.iconfinder.com/icons/1909691/crime_cyber_group_hacker_protect_security_skull_icon</a>
Skull and Crossbones	Andrew Cameron	The Noun Project	<a href="https://thenounproject.com/search/?q=Skull%20and%20Crossbones&amp;i=1962">https://thenounproject.com/search/?q=Skull%20and%20Crossbones&amp;i=1962</a>

## **License**

### **Non-exclusive licence to reproduce thesis and make thesis public**

**I, Oleksandr Cherednychenko,**

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:
  - 1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and
  - 1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

### **Designing Visually Effective and Intuitive Modelling Notations for Security Risk Management,**

supervised by Raimundas Matulevičius,

2. I am aware of the fact that the author retains these rights.
3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **21.05.2018**