Identifying and Managing Risks in Interconnected Utility Networks

The HyRiM Risk Management Process

Stefan Schauer, Sandra König, Martin Latzenhofer
Center for Digital Safety & Security
AIT Austrian Institute of Technology GmbH
Vienna, Austria
Email: {stefan.schauer, sandra.koenig, martin.latzenhofer}@ait.ac.at

Stefan Rass
Institute of Applied Informatics, System Security Group
Alpen-Adria Universität Klagenfurt
Klagenfurt, Austria
Email: stefan.rass@aau.at

***Abstract*— Critical infrastructures and especially their utility networks play a crucial role in the societal and individual day-to-day life. Thus, the estimation of potential threats and security issues as well as a proper assessment of the respective risks is a core duty of utility providers. Despite the fact that utility providers operate several networks (e.g., communication, control and utility networks), most of today's risk management tools only focus on one of these networks. In this article, we will give an overview of a novel risk management process specifically designed for estimating threats and assessing risks in highly interconnected networks. Based on the international standard for risk management, ISO 31000, our risk management process integrates various methodologies and tools supporting the different steps of the process from risk identification to risk treatment. At the heart of this process, a novel game-theoretic framework for risk minimization and risk treatment is applied that is able to deal with uncertainty by using distribution-valued payoffs. This approach is specifically designed to take information generated by various tools into account and model the complex interplay between the heterogeneous networks, systems and operators within a utility provider. It operates on qualitative and semi-quantitative information as well as empirical data, including expert opinions.**

Keywords-risk management; interconnected utility networks; game theory; ISO 31000

I. INTRODUCTION

Utility networks are critical infrastructures consisting of physical and cyber-based systems. The organizations operating these networks are providing essential services for society, e.g., the electric power production and distribution, water and gas supply as well as telecommunication services. A failure within a critical infrastructure has huge societal impact, as shown for example in [1] [2].

These infrastructures are heavily relying on Information and Communication Technology (ICT) as well as Supervisory Control and Data Acquisition (SCADA) systems for providing their services. As it has been shown in recent events [3] [4], ICT and SCADA systems are potential targets of cyber-security threats and may have vulnerabilities that attackers could exploit. Therefore, protecting and assuring availability and security is of the utmost importance for normal societal and business continuity.

In this context, risk management is a core duty in critical infrastructures. Current risk management frameworks [5]–[8] are mostly a matter of best practices, often focusing on one specific topic (e.g., the ICT area, SCADA systems or the physical utility layer). In particular, the aforementioned network-centric structure within utility providers relies on a high integration and a heavy interrelation between the different networks (cf. Figure 1). Hence, an incident in one network might affect not only the network itself but might also have cascading effects on several other networks as well. Standard risk management frameworks are often not designed to identify and assess these cascading effects, thus leaving them underestimated or even undetected.

In this article, we present a novel risk management process, which is specifically tailored to work on highly interconnected networks and take the aforementioned cascading effects into account. With this process, we go beyond the classical approaches in risk management and use a game-theoretic framework to identify an optimal set of risk mitigation measures. Therefore, we extend the well-known risk management process given in the international standard ISO 31000 by special tools. These tools support risk managers obtaining a holistic view of their organization, an in-depth identification of potential threats and a thorough analysis of the propagation of incidents together with their respective impacts. By integrating the collected semi-quantitative data into probability distributions or histograms, the presented process accounts for the intrinsic randomness given in this field of application. This utilization of distribution-valued payoffs represents also an extension to standard game-theoretic frameworks.

In the following Section II, we will give a short overview on the research already done in this field. Section III then describes the HyRiM Project in which the HyRiM Risk Management Process has been developed, in further detail. The ISO 31000 standard, which represents the basis for the HyRiM Risk Management Process, is sketched in Section IV. The core contribution of this work, the detailed description of the HyRiM Risk Management Process, is provided in Section V; the respective subsections describe each sub-step of the process. Section VI concludes the work.

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-582-1

II. RELATED WORK

In the past decade, risk and security management have become core parts of any company's day-to-day business. This is caused by the increasing number of attacks on cyber systems over the last years, where in particular critical infrastructures have moved in the center of attacker's attention. General standards for risk management (e.g., the ISO 31000 [5], ISO/IEC 27005 [6] or the NIST SP800-30 [7]) and security management (e.g., the ISO/IEC 27001 [9] or NIST SP800-37 [10]) as well as common business frameworks (e.g., COBIT 5.0 for Risk [8] or Octave [11]) provide a good approach to prepare organizations against the current threat landscape. Nevertheless, these standards and frameworks are quite generic and need a lot of tailoring to meet the specific requirements of critical infrastructures. Moreover, they represent best practice approaches with little or no mathematical basis for the assessment of risks.

For critical infrastructures, there are more specialized guidelines available, e.g. the NIST SP800-82r2 [12] or the ISA/IEC 62443 family of standards [13], covering the field of industrial control systems. Although these frameworks focus more on cyber-physical systems and thus intend to close the gap between those two worlds, they leave other aspects like organizational and human factors aside. Hence, they take some (more technical) parts of the critical infrastructure's network architecture into consideration but don't provide a holistic view on the whole organization as such. The HyRiM Project [14] described in the following section provides a more comprehensive view of these organizations and thus further improves the overall risk management.

III. THE HYRIM PROJECT

In the course of the FP7 project HyRiM ("Hybrid Risk Management for Utility Networks") [14], we are focusing on these sensitive interconnection points between different networks operated by a utility provider. The main goal is to define a novel risk management approach for identifying, assessing and categorizing security risks and their cascading effects in interconnected utility infrastructure networks. In more detail, we are concentrating on three major networks operated by utility providers, i.e., (cf. also Figure 1)

- the utility's *physical network infrastructure*, consisting of, e.g., gas pipes, water pipes or power lines;
- the utility's *control network* including SCADA systems used to access and maintain specific nodes in the utility network;
- the *ICT network*, collecting data from the SCADA network and containing the organization's business logic.

Additionally, we also include the *human factor and the social interrelations* (i.e., the social network) between employees, wherever possible. In other words, we choose a holistic or "hybrid" view on these networks, strongly emphasizing on the interrelations between them. Hence, we refer to our approach as "Hybrid Risk Management" and to the respective risk measures as "Hybrid Risk Metrics".

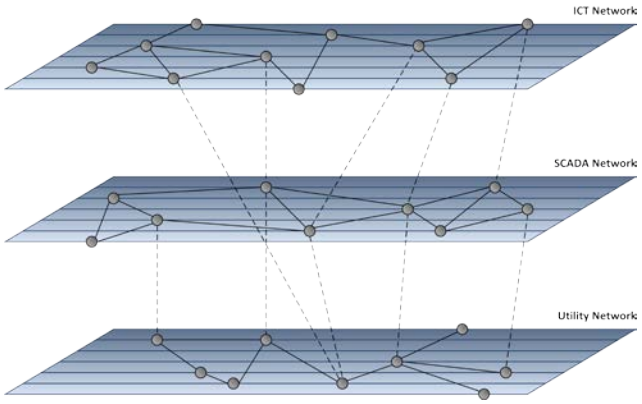

Figure 1. Interconnected networks operated by a utility provider

The risk measures developed in HyRiM are focusing on a qualitative approach to avoid the illusion of "hard facts" based on subjective numerical risk estimates provided by humans. Nevertheless, simulation tools based on well-defined mathematical frameworks like percolation and co-simulation are provided, which support the qualitative analysis with quantitative results.

Hence, our risk management process unifies the advantages of quantitative assessment with the ease and efficiency of a qualitative analysis and supports a qualitative assessment with a sound quantitative mathematical underpinning. The aim is to provide utility network operators with a risk management framework supporting qualitative risk assessment based on numerical (quantitative) techniques. In this way, the HyRiM project takes an explicit step towards considering security in the given context of utility networks based on a sound and well-understood mathematical foundation, ultimately supporting utility network operators with a specially tailored solution for the application at hand.

IV. THE ISO 31000 STANDARD

The international standard for risk management, ISO 31000 [5] describes the principles and guidelines for the implementation of risk management in organizations. It is based not only on the operational risk management process, but also on general organizational factors and their respective underlying structure. Therefore, the standard describes, to a large extent, a strategic risk management framework, which is constantly seeking to develop and improve the operational risk management process in the context of the defined principles.

A distinct characteristic of the ISO 31000 is the two-tier structure with a *risk management framework* on the one hand, and the *operative risk management process* on the other hand (cf. Figure 2). These two life cycles are linked by the framework's activity "implementing risk management". The risk management framework represents the top down approach, ensures the consistent embedding of risk management in the organization based on a quality management perspective. It follows an iterative and continuous improvement approach, i.e., the plan-do-check-act (PDCA) cycle. Furthermore, the operative risk management process supports the bottom-up approach, which puts the concrete risks in an organizational context,

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-582-1

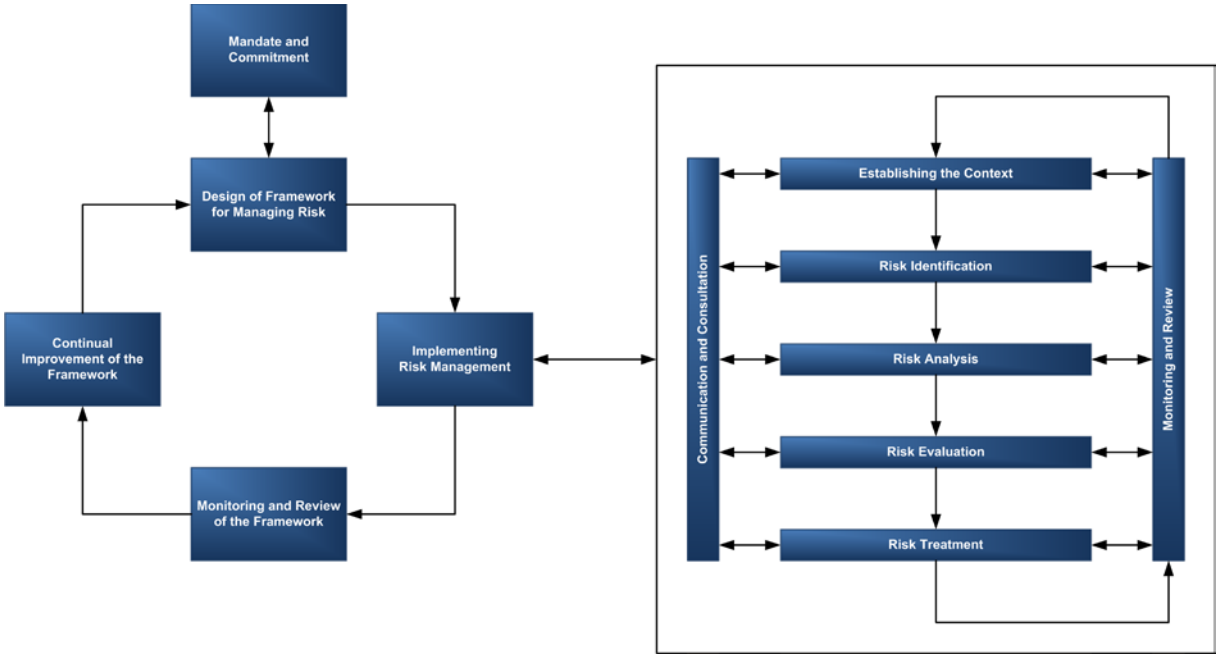

Figure 2. Risk management framework (left) and risk management process (right) according to ISO 31000 [5]

assesses and treats them. During the whole risk management process, two guiding sub-processes ensure communication and consultation as well as monitoring and review. The first one interacts with the stakeholders, the latter enables performance measure.

In order to support the PDCA-driven risk management framework, a strong and sustainable commitment of the organization's top management is required. Only with such a top-level commitment, a risk management policy is supported, objectives and strategies can be coordinated within the organization, indicators can be defined and legal and regulatory requirements can be met. Furthermore, this commitment also ensures that the necessary resources and responsibilities are allocated at all levels of the organization, the benefits are communicated to all stakeholders, and the framework for dealing with risks continues to be adequate.

The implementation of the risk management process describes the application of the risk management policy to the organizational processes including their schedule. Therefore, the following five generic steps are defined, which divide the operational risk management process into specific actions: *Establishing the Context*, *Risk Identification*, *Risk Analysis*, *Risk Evaluation* and *Risk Treatment*. In short, framework conditions for risk management in relation to the organization are specified in the beginning, followed by the identification of the potential threats together with their respective likelihood of occurrence and consequences. The resulting list of risks is assessed according to the predefined context of the organization and ranked according to its importance. This makes it possible to directly identify a procedure for risk management.

V. The HyRiM Risk Management Process

A. General Setting

The HyRiM Risk Management Process we are presenting here is tailored to organizations operating highly interconnected networks at different levels, such as utility providers or critical infrastructure operators. Therefore, the HyRiM process is compliant with the general ISO 31000 process for risk management [5] shortly introduced in the previous section and thus can also be integrated into existing risk management processes already established in the aforementioned organizations.

In detail, the operative risk management process of the ISO 31000 framework (cf. Figure 2) is adopted and each step of the process is supported with the tools developed in the HyRiM project. These tools cover different social and technical analysis techniques and simulation methodologies that facilitate the risk process. The relevant HyRiM tools have been identified and mapped onto the risk management process as shown in Figure 3. Since the ISO 31000 is a generic process and is often used as a template in other ISO standards itself (like in the ISO 27005 [6], the ISO 28001 [15] or others), the HyRiM process described here can also be integrated into these standards. This makes it possible to apply the HyRiM process to multiple fields of application.

The general framework applied in HyRiM to model the interplay between different networks is game theory. Game theory not only provides a solid mathematical foundation but can also be applied without a precise model of the adversary's intentions and goals. Therefore, a zero-sum game and a minimax approach [16] can be used, where the gain of one player is balanced with the loss of the other. This can be used to obtain a worst-case risk estimation.

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-582-1

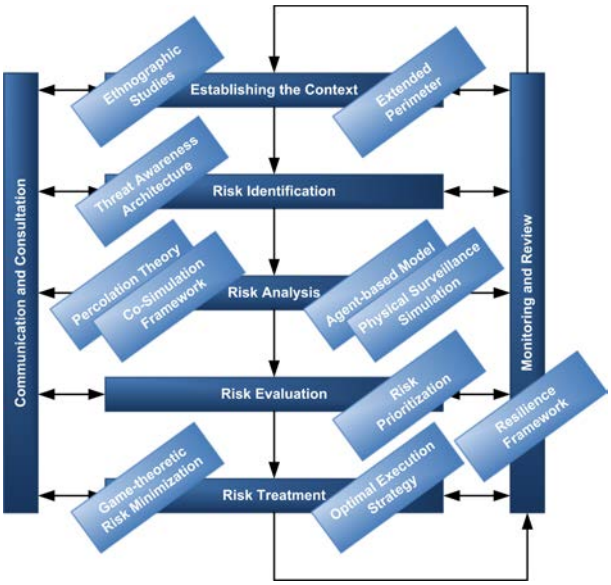

Figure 3. HyRiM Risk Management Process

The game-theoretic framework we developed in HyRiM [12] [13] also allows modeling the intrinsic randomness and uncertainty encountered in real-life scenarios. This is realized using distribution-valued payoffs for the game [19], as opposed to the standard modeling where security needs to be quantified in numeric terms; a task that is typically difficult and reasonable figures measuring security are hard to obtain. These payoffs are coming from both the percolation and the co-simulation, since those are stochastic processes and the results are described as distributions.

The output of the game-theoretic framework is threefold and includes the maximum possible damage that can be caused by an adversary, an optimal attack strategy resulting in that damage and an optimal security strategy for the defender. The optimal defense strategy is, in general, a mixture of several defensive (i.e., mitigation) activities. These activities, if implemented correctly, provide a provable optimal defense against the adversary's worst case attack strategy. The implementation can be simplified and guaranteed, for example, by the use of a job scheduling tool.

B. *Establishing the Context*

The HyRiM risk management process starts by defining the objectives which should be achieved and attempting to understand the external and internal factors that may influence the goal. This summarizes a description of the external and internal environment of the organization as well as detailed requirements for the risk management process itself.

The first step takes the information about SCADA and ICT communication networks (e.g., network architecture diagram), components of the utility network (e.g., architecture of the physical utility network layer), industrial control functions and information assets as input. Further, information about the social and organizational aspects as well as other necessary documentation that is relevant for the overall risk management context is also required. Whereas the technical aspects are often more or less documented within the organization, for analyzing the social aspects, we suggest using firsthand and more qualitative analysis techniques, like interviews or ethnography. This allows identifying the gap between the way policies and security measures are planned and should be implemented within the organization and how the organizational structure works in real life. In the HyRiM project, we applied such studies to obtain a holistic and in-depth view on the relevant infrastructures of the end user partners.

The main output of this step is a specification of the different networks (ICT, SCADA, social, etc.), their interdependencies among each other and a definition of the basic criteria for the risk management process as well as its scope, boundaries, and responsible parties.

C. *Risk Identification*

Risk identification involves the application of systematic techniques to understand a range of scenarios describing what could happen, how and why. Therefore, the infrastructure within the scope of the risk management process needs to be defined, including technical assets, organizational roles and individual personnel as well as their interdependencies. Based on that, potential vulnerabilities and threats can be identified.

As an input, this step requires a detailed specification of the organization's infrastructure relevant for the risk assessment process. This information is obtained from the previous step "Establishing the Context". The main objective of this step is to get an overview on the relevant aspects for a risk assessment. Therefore, firstly a list of assets has to be created, describing the subset of the organization's overall infrastructure under evaluation. Secondly, a list of asset-related threats needs to be extracted from the general set of potential threats in the organization's field of application. Further, specific vulnerabilities (not only from the technical area, but also from a general point of view) for these assets need to be gathered.

To avoid missing potential threats or vulnerabilities, a structured approach for risk identification has to be applied. Hence, a *Threat Awareness Architecture* [20], which is based on *Organizational, Technology and Individual* (OTI) viewpoints, was developed in the HyRiM project. This architecture comprises a three-stage process, including Situation Recognition, Situation Comprehension and Situation Projection. In this process, the OTI viewpoints serve as a basis and include not only the technical aspects but also cover policies and processes within an organization as well as how individual people behave under particular conditions. Thus, this architecture provides a holistic view on an organization's threat landscape and also specifies and collects structured information on threats and vulnerabilities. This information can be gathered and also shared with open source threat and vulnerability repositories to achieve a continuous exchange with other utility providers.

This step produces several outputs, including a structured representation (e.g., a network graph) of relevant assets and their interrelations, a list of open vulnerabilities and potential threats related to these assets.

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-582-1

D. Risk Analysis

Risk analysis deals with developing an understanding of each risk, its consequences and the likelihood of these consequences. In general, the level of risk is determined by taking into account the present state of the system, existing controls and their level of effectiveness. Whereas in a classical risk analysis approach both the consequences and the likelihood of an incident are aggregated into a single value, in the HyRiM process, both are described by distributions or histograms including all the relevant information coming from different sources. Hence, the more information is available to build up these distributions, the higher the quality of the results. Nevertheless, since most of the time only scarce information about potential threats and vulnerabilities is available within an organization, the HyRiM process is designed to work also with such limited information.

This step takes the list of potential threats and the list of the organization's assets together with their vulnerabilities as an input (resulting from the previous step "Risk Identification"). Based on this list, specific threat scenarios tailored to the organization's infrastructure are defined. These threat scenarios are evaluated according to their likelihood and consequences.

In general, there is a plethora of different methodologies for estimating the likelihood and consequences of a specific threat scenario. They range from simple questionnaires collecting expert opinions up to complex mathematical models. Especially in the context of utility networks, estimating the potential consequences of a threat often is quite complex due to the interconnected nature of the networks and the related cascading effects. Hence, for the HyRiM Risk Management Process, we suggest four specific simulation-based approaches, which are well-suited for utility networks: *Percolation Theory*, *Co-Simulation*, *Agent-based Modelling* and *Physical Surveillance Simulation*.

In particular, when looking at the different networks operated by a utility provider (cf. Figure 1) percolation theory [21]–[23] as well as co-simulation [24]–[26] can be used to describe the cascading effects spreading over the different networks. More precisely, percolation theory is particularly helpful when only high-level or sparse (e.g., qualitative) information is available [23]. In this case, the nodes and edges in the network graph from the previous step can be distinguished according to several characteristics. Based on these different types, a specific probability of failure is assigned to each type and the propagation of an error is modeled according to these probabilities. This model allows computing the probability that an error affects a significant number of components, i.e., it causes an epidemic or even pandemic, as well as how many nodes are indeed affected in this case.

If more details on the infrastructure and the communication between certain systems are known, a co-simulation approach can provide more accurate information about the spreading of a failure among these networks [26]. In this context, the overall network is represented in different tools, each responsible for simulating a part of the complex system. Then, the co-simulation framework models and manages the communication between these tools, e.g., by exchanging variables, data and status information. In this way, the separated simulations of the complex system are synchronized and the effects of an incident propagating over several systems in the different networks can be analyzed.

In case of threats against the physical infrastructure of a utility provider, e.g., the buildings, machinery, warehouses, tank depots, etc., a simulation framework for physical surveillance is more applicable. In this context, game theory is often used as a mathematical approach to model an intruder's behavior and to find optimal strategies to defend against specific scenarios [27]–[29]. A similar framework has been developed in the HyRiM project [14]. It takes the layout of the utility provider's premises, including the buildings and pathways connecting them and allows simulating the movements of an adversary entering the premises. In more detail, the adversary's capabilities, potential entry points and targets can be modeled. Additionally, the security measures (cameras, identity badges, etc.) together with the routes and routines of the security guards within the premises can be represented in the simulation. In this way, the framework allows reproducing and analyzing different attack scenarios together with the respective defensive actions. Using this framework, not only the potential physical damage caused by one or more intruders but also soft factors (like the effect of increased surveillance on the employees) can be estimated.

Complementary to these methodologies, agent-based modelling is much more focused on the societal impact of specific actions taken by an organization. Since utility providers are, in general, critical infrastructures, incidents happening within utility providers as well as the respective security actions can directly affect societal structures in a certain region. As shown in the HyRiM project, an agent-based model can be used to simulate such social response and provide an overview on the potential implications on society [30].

Taking the results of one or several of the simulation methodologies mentioned above, this step provides two unsorted lists as output, containing the consequences and likelihoods for each identified threat scenario. As already mentioned, the consequences as well as the likelihoods are represented as histograms to prevent the loss of important information.

E. Risk Evaluation

Risk evaluation involves making a decision about the level or priority of each risk by applying the criteria developed when the context was established (c.f. Section V.B above). In classical approaches, a cost benefit analysis can be used to determine whether specific treatment is worthwhile for each of the selected risks. In contrast, the game-theoretic model applied in the HyRiM process allows an optimization according to several tangible and intangible goals (i.e., not only costs but also soft factors like employee satisfaction or social response). Nevertheless, the result needs to be visualized in a well-known representation, i.e., a *risk*

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-582-1

matrix, to provide a high recognition value for top level management.

This step requires the compilation of the empirical histograms or distributions (or, more general, the probability mass functions) representing the likelihood and consequences of each of the threats as evaluated in the previous step "Risk Analysis". The input is created from data obtained from the aforementioned simulation approaches, i.e., percolation, co-simulation, agent-based modelling and physical surveillance simulation.

A general approach for risk evaluation is to compute the risk as the product "*consequence* × *likelihood*" and to order the results according to their magnitude. Due to the fact that we are dealing with histograms or distributions instead of single values, forming this product is not possible and the ordering becomes non-trivial. Hence, we need another way of ordering the consequences and likelihoods for each threat scenario. One solution for this is given by the stochastic $\preccurlyeq$-ordering, which has been introduced in [17] [18], and allows comparing two distributions (cf. [17] [18] for technical explanation of $\preccurlyeq$-ordering). By applying this ordering to the unsorted lists of the threat scenarios' consequences and likelihoods, is it possible to identify the risks with the most severe consequences and the highest likelihood. Unlike rankings based on values (only), this form of evaluation uses all available information, rather than relying on a lossy aggregation thereof (such as the product of likelihood and damage, which corresponds to condensing a distribution into its first moment only).

The main output of this step is a two-dimensional risk matrix including all risks according to their respective likelihood and consequences (cf. Figure 4). Based on this matrix, a priority list of all risks can be compiled.

F. Risk Treatment

Risk treatment is the process in which existing controls are improved and new controls are implemented. In classical risk management approaches, the aim is to apply these new or improved controls to reduce either the likelihood of a specific threat to occur or the magnitude of the consequences. The decision about which controls to implement is often a subjective one, carried out by the risk manager. In the HyRiM Risk Management Process, the goal is to identify the *optimal set of controls* to reduce the maximum damage that can be caused by an attacker to a minimum. In this context, the optimality of the resulting controls is given due to the game-theoretic algorithms developed in the course of the project [17]–[19].

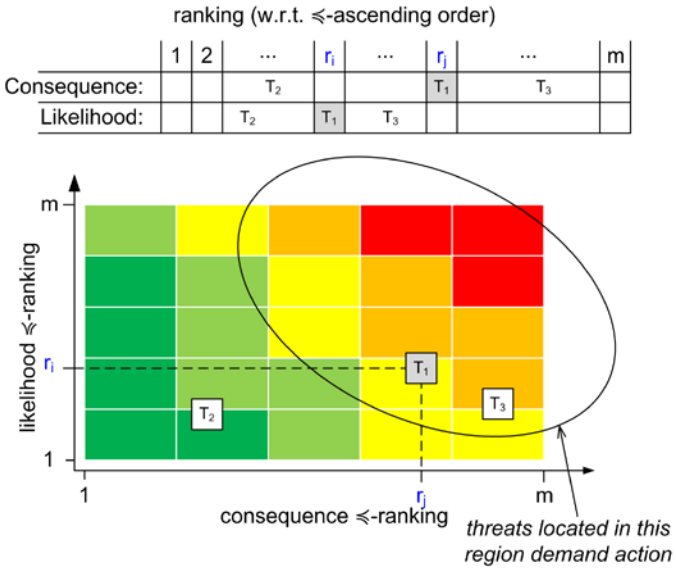

Figure 4. Illustration of the resulting risk matrix based on the two ordered lists for the consequences and likelihoods.

This step takes the list of risks resulting from the Risk Evaluation as input. The main goal is to identify an optimal treatment plan for risks with the highest priority. Therefore, the list of controls which can be implemented to counter a specific risk is evaluated according to their effect on the consequences. The game-theoretic approach applied here allows not only to identify the optimal choice of controls for a specific risk but also to cluster several risks with similar controls to identify the set of controls, which are most effective against all of the clustered risk. Additionally, the game-theoretic algorithm is capable of optimizing over different security goals, e.g., also taking the costs for implementing the controls into account.

To compute the optimal mitigation action, it has to be evaluated, how much a specific defense strategy affects a certain attack strategy. This is done by rerunning the consequence analysis for the organization's asset structure assuming that the specific defense strategy has been implemented. Therefore, the simulation approaches from Section V.D can be used again. The evaluation has to be done for all combinations of attack and defense strategies. The resulting table of the evaluated consequences (i.e., the payoff matrix) is then fed into the game-theoretic algorithm (cf. [18] for details on the computation of the game).

The output of this step is threefold: the first result is an optimal security strategy for the defender, pointing at the best choice of defense strategies. Those strategies can be pure (i.e., indicating one specific strategy) or mixed (i.e., several strategies have to be implemented with specific probabilities). The second output is an optimal attack strategy for the attacker identifying the neuralgic assets within the organization, and the third is the maximum damage that can be caused by an adversary. This information is then fed into a job scheduling tool, resulting in a well-defined sequence of mitigation activities implementing the optimal defense strategy.

G. Communication and Consultation

Concurrent to the five main steps of the risk management process (as described above), the Communication and Consultation step is performed. Therein, the main and partial results of the process are communicated to the respective stakeholders (as identified during the Establishing the Context step). This is a core part of the overall process due to the fact that the stakeholders, in particular the top level management, need to be kept well-informed about the results from the process. It is important to maintain awareness for the risk management activities, since their continued support

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-582-1

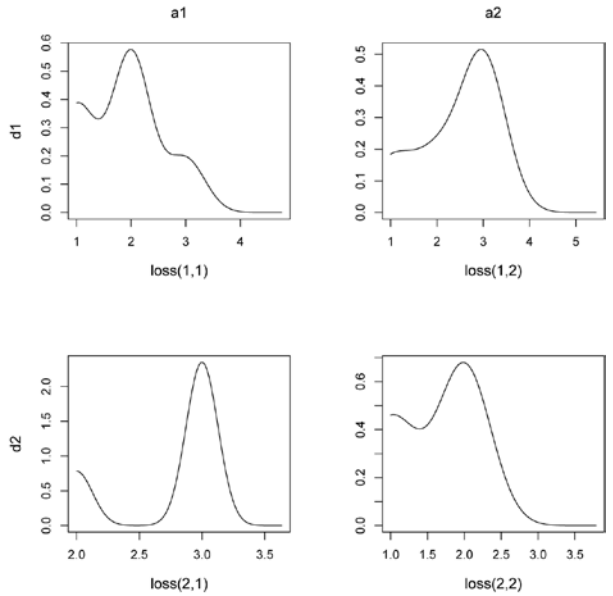

Figure 5. Example of a payoff matrix consisting of distributions (taken from [23])

for the risk management process is crucial for the overall risk management framework (cf. also Section IV about the ISO 31000).

H. Monitoring and Review

Besides the Communication and Consultation, a second step running in parallel to the five main steps of risk management is Monitoring and Review. This step represents a constant feedback loop, using the main and partial results from each step and evaluating their effectiveness. Although the outputs of the game-theoretic model are optimal (which can be proven mathematically), but any risk guarantee is only valid provided that the input data is accurate and the threat lists are exhaustive. Here comes another advantage of using payoff distribution models over normal numbers (as in competing approaches) into play: we can even account for rare and unexpected events, since the utilized distributions are based on input data, but by taking the tails of these distributions into account, we can capture extreme outcomes that have not been observed so far (e.g., zero-day exploits). In more detail, the inputs are based on the general organizational structure (cf. Section V.B), the list of potential threats and vulnerabilities (cf. Section V.C) as well as the estimation of the consequences and likelihood for each threat scenario (cf. Section V.D). If these inputs are not comprehensive enough or erroneous, the output of the risk treatment plan will also be incomplete. Hence, the correct implementation of the mitigation actions needs to be validated and their consequences on the organization needs to be compared to the effect estimated during the risk assessment process.

VI. CONCLUSION

In this paper, we presented a novel approach towards risk management for utility networks, the HyRiM Risk Management Process. This approach has been developed in the HyRiM project and extends the international risk management standard ISO 31000 by tools specifically designed to address the particular requirements of utility providers. As a main advantage over standard risk management processes like the ISO 31000, ISO/IEC27005, COBIT 5 for Risk or others, the presented risk management process accounts for the "hybrid" nature of utility networks, i.e., the strong and complex interrelations between the different networks operated by utility providers. To achieve that, several simulation techniques can be integrated into the process, for example, depending on the quality of the underlying information, to improve the analysis of the dynamics stemming from these interrelations and their resulting cascading effects. By including techniques from the field of social and human studies, not only technical but also individual, organizational and social impact of threats can be evaluated.

Further, the HyRiM Risk Management Process relies on a sound mathematical basis, building on game-theoretic concepts and algorithms, to improve mitigation actions to their optimum. This game-theoretic framework allows the estimation of the worst-case damage and the identification of the corresponding optimal mitigation strategy for a given set of potential threats. Hence, the HyRiM Risk Management Process has a clear advantage over standard frameworks, since those often rely on best practice approaches, lacking a general mathematical basis. Moreover, the notions of worst case damage and optimal defense strategy are well defined according to the game-theoretical framework.

In the course of the HyRiM project, the process' practicality and applicability have been evaluated in real-life use case scenarios. These scenarios include malware propagation in a power provider's cyber-physical network, an APT attack on a water provider's control room and a physical intrusion into an oil and gas refinery. The detailed scenarios will be described in [31].

ACKNOWLEDGMENT

This work was supported by the European Commission's Project No. 608090, HyRiM (Hybrid Risk Management for Utility Networks) under the 7th Framework Programme (FP7-SEC-2013-1).

REFERENCES

[1] S. Fletcher, "Electric power interruptions curtail California oil and gas production," *Oil Gas J.*, 2001.

[2] M. Schmidthaler and J. Reichl, "Economic Valuation of Electricity Supply Security: Ad-hoc Cost Assessment Tool for Power Outages," *ELECTRA*, no. 276, pp. 10–15.

[3] E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid," Washington, USA, 2016.

[4] J. Condliffe, "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks," 22-Dec-2016. [Online]. Available: https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/. [Accessed: 26-Jul-2017].

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-582-1

[5] International Standardization Organization, *ISO 31000: Risk Management – Principles and Guidelines*. Geneva, Switzerland, 2009.

[6] International Standardization Organization, *ISO/IEC 27005: Information technology - Security techniques - Information security risk management*. Geneva, Switzerland, 2011.

[7] G. Stoneburner, A. Goguen, and A. Feringa, *NIST SP800-30 Risk Management Guide for Information Technology Systems*. Gaithersburg, USA, 2002.

[8] ISACA, *COBIT 5 for Risk*. Rolling Meadows, USA, 2013.

[9] International Standardization Organization, *ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements*. Geneva, Switzerland, 2013.

[10] NIST, *NIST SP800-37 Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*. Gaithersburg, USA, 2010.

[11] C. Richard A., S. James F., Y. Lisa R., and W. William R., "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA, Technical Report CMU/SEI-2007-TR-012, 2007.

[12] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, *NIST SP800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security*. Gaithersburg, USA, 2015.

[13] International Society of Automation, "ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security." [Online]. Available: http://isa99.isa.org/ISA99%20Wiki/Home.aspx. [Accessed: 26-Jul-2017].

[14] "HyRiM | Hybrid Risk Management for Utility Providers." [Online]. Available: https://www.hyrim.net//. [Accessed: 26-Jul-2017].

[15] International Standardization Organization, *ISO 28001: Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance*. Geneva, Switzerland, 2007.

[16] M. Maschler, E. Solan, and S. Zamir, *Game Theory*. Cambridge University Press, 2013.

[17] S. Rass, S. König, and S. Schauer, "Deliverable 1.2 - Report on Definition and Categorisation of Hybrid Risk Metrics," Vienna, Austria, HyRiM Deliverable, 2015.

[18] S. Rass, "On Game-Theoretic Risk Management (Part One) – Towards a Theory of Games with Payoffs that are Probability-Distributions," *ArXiv E-Prints*, Jun. 2015.

[19] S. Rass, S. König, and S. Schauer, "Uncertainty in Games: Using Probability-Distributions as Payoffs," in *Decision and Game Theory for Security*, London, UK: Springer, 2015, pp. 346–357.

[20] A. Gouglidis, B. Green, J. Busby, M. Rouncefield, D. Hutchison, and S. Schauer, "Threat Awareness for Critical Infrastructures Resilience," in *Resilient Networks Design and Modeling (RNDM), 2016 8th International Workshop on Resilient Networks Design and Modeling*, Halmstad, Sweden, 2016, pp. 196–202.

[21] G. R. Grimmett, *Percolation Theory*. Heidelberg, Germany: Springer, 1989.

[22] S. König, S. Rass, and S. Schauer, "A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks," in *Secure IT Systems. 21st Nordic Conference, NordSec 2016, Oulu, Finland, November 2-4, 2016. Proceedings*, B. Brumley and J. Röning, Eds. Cham: Springer International Publishing, 2016, pp. 67–81.

[23] S. König, S. Rass, S. Schauer, and A. Beck, "Risk Propagation Analysis and Visualization using Percolation Theory," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, pp. 694–701, 2016.

[24] M. Faschang, F. Kupzog, R. Mosshammer, and A. Einfalt, "Rapid control prototyping platform for networked smart grid systems," in *Proceedings IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society*, Vienna, Austria, 2013, pp. 8172–8176.

[25] M. Faschang, "Loose Coupling Architecture for Co-Simulation of Heterogeneous Components," Vienna University of Technology, Vienna, Austria, 2015.

[26] M. Findrik, P. Smith, J. H. Kazmi, M. Faschang, and F. Kupzog, "Towards secure and resilient networked power distribution grids: Process and tool adoption," in *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*, Sidney, Australia, 2016, pp. 435–440.

[27] M. Aigner and M. Fromme, "A game of cops and robbers," *Discrete Appl. Math.*, vol. 8, no. 1, pp. 1–12, 1984.

[28] S. Bhattacharya, T. Başar, and M. Falcone, "Surveillance for Security as a Pursuit-Evasion Game," in *Decision and Game Theory for Security*, vol. 8840, R. Poovendran and W. Saad, Eds. Cham: Springer International Publishing, 2014, pp. 370–379.

[29] G. Hahn and G. MacGillivray, "A note on *k*-cop, *l*-robber games on graphs," *Discrete Math.*, vol. 306, no. 19–20, pp. 2492–2497, 2006.

[30] J. Busby, A. Gouglidis, S. Rass, and S. König, "Modelling security risk in critical utilities: the system at risk as a three player game and agent society," in *Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on*, Budapest, Hungary, 2016, pp. 1758–1763.

[31] S. Rass and S. Schauer, *Game Theory for Security and Risk Management: From Theory to Practice*. Boston, USA: Birkhäuser, to appear.

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-582-1