Parametrization of Probabilistic Risk Models

Sandra König
Austrian Institute of Technology
Vienna, Austria
Sandra.Koenig@ait.ac.at

Abdelkader Magdy Shaaban
Austrian Institute of Technology
Vienna, Austria
Abdelkader.Shaaban@ait.ac.at

ABSTRACT

Probabilistic risk models are popular due to their ability to capture uncertainty. However, the parametrization of such models may be challenging, especially in the context of critical infrastructures where data is sometimes sparse. In this paper we propose different methods to parametrize a stochastic model of risk propagation depending on the amount of information available. Two of the approaches are illustrated with an example of a critical infrastructure and the application of the other methods is sketched.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

threat identification, risk modelling, parametrization, cascading effects, simulation

ACM Reference Format:
Sandra König and Abdelkader Magdy Shaaban. 2022. Parametrization of Probabilistic Risk Models. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3538969.3544454

1 INTRODUCTION

Risk models often contain stochastic components to capture the intrinsic uncertainty in risk assessment. Estimation of the model parameters, and especially of likelihoods, is one of the main challenges when applying such models. In the context of critical infrastructures, the task is even more challenging due to the common lack of data. In this article, we describe different approaches to parameter estimation and illustrate some of the methods for a fictitious example infrastructure. At the end, we provide an outlook of how these methods can be applied to a more evolved example, such as a pilot case in the EU funded project PRAETORIAN [17].

The analysis of an infrastructure (or infrastructure network) is supported by two tools: THREATGET allows a static threat identification [3], while Sauron [2] allows a dynamic analysis of consequences of a threat. While the threat identification requires qualitative knowledge, i.e., a formal model of the infrastructure and rules describing dangerous behaviour, the simulation of effects is based on a probabilistic model and therefore requires the estimation of numerical values (i.e., probabilities).

Threat modelling is a structured technique followed in this work for analysing potential security threats and determining how to address them. It is considered to be an essential action in the development of secure IT systems. It helps identify potential vulnerabilities early in the system development process to guarantee security-by-design [22]. As threats and vulnerabilities may occur in any system design, defining the proper security mitigation is necessary to be integrated with the system design to keep the security risk at an acceptable level. Microsoft introduced a Security Development Lifecycle (SDL) for security and privacy concerns during all development phases of IT systems [15]. Microsoft has incorporated threat modelling methodologies with the SDL by 1999 [24]. Multiple threat modelling methods have been developed to understand better the possible behaviours of current security vulnerabilities in information technology systems. Examples of this include STRIDE, PASTA, OCTAVE, Attack Trees, and a few others, all of which are discussed in [23], which also provides more details on each of these methods. The concept of threat modelling has been incorporated into various applications, including the Internet of Things (IoT), transportation, and others. The approaches of risk and threat assessment for the automobile industry have been explored in [14]. The same study also proposed a strategy to classify safety and security risks separately. A realistic and practical approach to threat modelling was described in [13], which extended the already existing tools for security analysis in the vehicular domain to support and illustrate the feasibility of this approach. Similarly, a technique for threat modelling is provided in [21] to conduct railway security assessments.

The THREATGET tool classifies potential cyber threats based on the STRIDE model. It is provided with a rule engine that automatically analyses all elements, communication channels, and relevant security properties to identify potential security weaknesses in the system model scheme.

Assessing consequences of an incident in a CI or in a network of CIs is a challenging problem due to the cascading effects that typically occur [8, 16]. These can hardly be described precisely, which is why probabilistic models are used frequently. Popular models include peroclation models [5, 12] and Markov chain models [18, 25]. A more general approach uses probabilistic Mealy automata [10] which is more suitable for incidents in CIs since they are triggered by some notification (e.g., an alarm).

2 PARAMETRIZATION OF PROBABILISTIC MODELS

This paper proposes several approaches to parametrize a probabilistic risk model depending on the amount of data available. The

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-9670-7/22/08.
https://doi.org/10.1145/3538969.3544454

different methods are illustrated with a model for assessing cascading effects in interconnected critical infrastructures (CIs).
A comprehensive overview of the situation of a network of CIs is provided through a (directed) graph model where each node represents a relevant component. The functionality of each component is described through a *state* variable $s \in S = \{1, 2, 3\}$ (generalizations to more states are straightforward). A 3-tier scale allows an intuitive visualization similar to a traffic light - the node is colored green if the node works fine (state 1), yellow if there are some problems (state 2), and red if it is not working (state 3). In the context of CIs, consequences are hard to predict precisely. It is practically impossible to capture all direct and indirect dependencies (also induced trough cascading effects) and identify all factor that influence the behaviour. Therefore, our simulation is based on a probabilistic model, more precisely, the behaviour of the nodes is described through a probabilistic Mealy automaton. The parameters of this model are the transition likelihoods of the automatons, i.e., the probabilities p_{ij} that an automaton switches from state i to state j, where $i, j \in S$.

The remainder of this section describes various methods for this parametrization task. Which method to choose is mainly influenced by the data available. If the assessment is based on discussion with experts, direct or qualitative estimation is possible. If additional information such as threat rules or simulation environments are available, it is possible to use more advanced estimation techniques. In the case where sufficient data is available (e.g., from log files), machine learning may be applied. However, even when using advanced techniques, experts evaluation is still indispensable. Besides availability of data, it is also worth considering the required effort, including working time of experts. Also, different methods may be used for different components depending on their relevance. For some components it may be sufficient to use rougher estimates and to accept lower accuracy of the estimates.

2.1 Direct Estimation

The simplest way to characterize the transition regime is direct estimation of the transition probabilities p_{ij} that a node changes its state from i to j. Such estimation is always subjective and in situations where data is sparse it is therefore prone to error. Whenever possible, multiple assessments should be collected and combined in a way that is not sensitive to outliers (e.g., choosing the median [11]). In the PRAETORIAN project, such estimates may come form CI operators involved in the use case scenarios and from domain experts. Their estimations will be hard-coded, so the model cannot be easily adapted.

2.2 Quantitative Estimation

One way to consider the uncertainty in human estimates is to let experts indicate how certain they are about their predictions. The predicted values are the most likely ones, but neighbouring values are also considered potential outcomes. Based on the confidence, the distribution over all possible states is of different forms, i.e., the weight put on other values increases when confidence decreases. Table 1 shows a way to map a prediction of the most likely value and the corresponding confidence to a distribution over the set $S = \{1, 2, 3\}$ where confidence is measured on a three-tier scale [9]. If experts are sure about their prediction, this is the only state with a positive probability. If experts have some doubts, direct neighbours get half of the weight as the predicted value. In the case where an expert is not able to predict the next state, a uniform distribution is used. This approach may be used in the PRAETORIAN project if several experts from the CI operators are available, but they are somewhat unsure about the estimations for the system's behaviour. This approach better integrates the expert's uncertainty into the modelling process.

Table 1: Distribution over all states depending on confidence

Prediction	High C.	Medium C.	Low C.
1	(1,0,0)	(2/3,1/3,0)	(1/3,1/3,1/3)
2	(0,1,0)	(1/4,2/4,1/4)	(1/3,1/3,1/3)
3	(0,0,1)	(0,1/3,2/3)	(1/3,1/3,1/3)

2.3 Identification of Similar Scenarios

In some situations, threats are explicitly characterized through variables, e.g., through the configuration of a system. In this case, the state of a node can be estimated through the number of scenarios that potentially caused a specific degree of disruption or loss. Let C be the set of all possible configurations and decompose this set into a union $C_1 \cup C_1 \cup \ldots \cup C_n$ where configurations in C_i cause an impact of i. The sets C_i are not necessarily disjoint since the variables will, in almost all cases, not capture all possible influencing factors; therefore, more than one impact level may be possible for a given configuration.

2.4 Counting Threats

In the situation where experts or tools support the evaluation of the threats an asset faces, the estimation of probabilities can be based on the number and type of threats that affect a specific asset. For a given configuration describing the current state of the node and potentially considering the states of neighbouring notes, the threats affecting an asset are evaluated to determine the new state of the node. In the simplest scenario, threats are just counted and then mapped to the number of states, i.e., if no threat occurs, the state is 1, some threats yield to intermediate states, and too many or even all possible threats yield to the worst state. However, it might also be relevant to include more information, such as the impact the threats have on the node. Similar to the decomposition of the configuration space in Section 2.3, it is recommended to decompose the set T of considered threats into a (not necessarily disjoint) union $T = T_1 \cup \ldots \cup T_n$ where T_i is the set of threats that trigger a node to change into state i. The transition probability p_{ij} is then estimated through the frequency of hitting the set T_j when the node is in state i.

2.5 Logistic Regression

If experts can provide their knowledge on a system and the related threats, the question is how to collect this knowledge that is often implicit. Experience from previous projects shows that even domain experts do not feel comfortable making precise estimates (particularly about probabilities). However, most experts can provide good

feedback on specific situations, e.g., judge if certain circumstances are dangerous or not. Therefore, a 'parametrization by example' is recommended, where different example configurations can be evaluated in terms of whether a threat occurs or not. It is not necessary to cover the full range of possible configurations, but the more data is available, the better. Such data can then be analysed by logistic regression [19]. This formal approach has the benefit that model diagnostic and plausibility checks are possible. However, it requires some effort to get this data. Data collection is eased by the fact that several domain experts can provide information on their domain (which actually increases the quality of the assessment). The most convenient data source for this analysis are simulation tools since they provide a huge amount of data that can be analysed statistically. More general, data from cyber or physical digital twins may be incorporated.

3 MODELING A WATER UTILITY SCENARIO

For illustration, we consider a simple model of a water utility provider using a SCADA (Supervisory Control and Data Acquisition) system to control the processes. Despite the many benefits of such control systems, the connection between cyber and physical domains opens the door for new threats, and attacks [7]. This section first describes how the interaction of components from the cyber and physical domain may put the system in a dangerous state, i.e., identifying potential threats. Then the consequences of such threats are assessed using a simulation tool based on a probabilistic risk propagation model [10]. The various parametrization methods described in Section 2 are applied depending on the available information.

3.1 Identification of Threats

In this work, we utilize THREATGET for modeling the considered scenario focusing on the interaction between cyber and physical domains (see [4] for a documentation of the tool and [6] for a formal description). Figure 1 illustrates the considered example. THREATGET is used to investigate and examine existing security measures for each system component and relevant assets in order to identify potential cyber threats. Assets are defined in the THREATGET model as a critical system component, such as hardware, software, data, or configuration, that has value for stakeholders and requires additional security protection procedures.

The figure combines cyber and physical domains and describes the interaction of data flow between these domains.

Cyber Domain: It refers to a data environment that includes networks, embedded, and host devices responsible for handling, monitoring, and storing data. The Supervisory Control and Data Acquisition (SCADA) component in the figure represents a complete embedded system that collects data from physical components and performs real-time processing to provide a set of commands that can regulate any changes in setpoints occurring in the physical domain. The gathered data might be stored in a secure database server, which would keep the data secure from any malicious activity. However, the database server's availability is considered one of the most challenging security concerns that need attention to ensure that data is available anytime. Furthermore, the availability

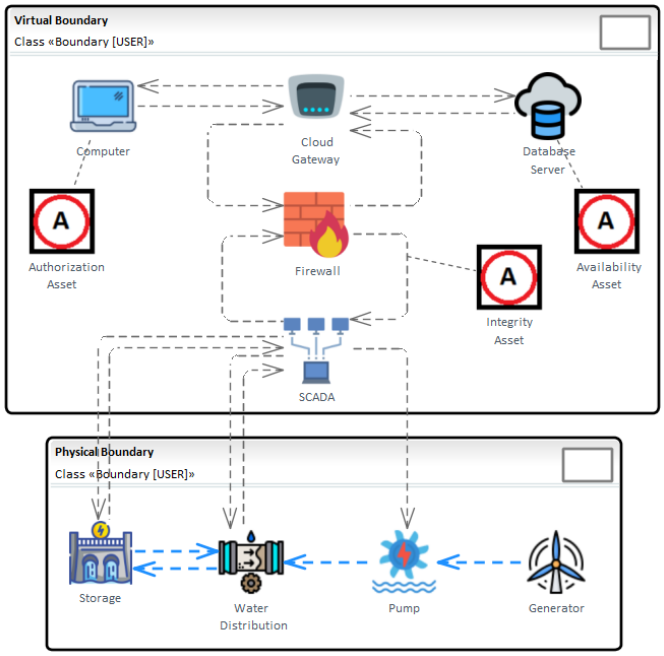

Figure 1: A THREATGET model for a water utility infrastructure

of the database server is regarded as a critical asset that needs additional security concerns to protect its continued operation. This asset is illustrated in the figure as an "A" letter connected to the server. Authorized individuals shall only handle the computer component in order to ensure secure and safe operation within the cyber domain's network. As a result, in this scenario, we define authorization as the critical asset that should be considered to ensure that authorized humans can control it for further activity. The network gateway is responsible for all data transmission, where the firewall inspects every data packet to provide high-level security policies capable of mitigating a wide range of cyberattacks. One of the most critical security concerns is the commend integrity of the SCADA systems, which should be addressed to avoid any negative impact on the normal operation of the whole system.

Physical Domain: As depicted in the figure, this domain contains a set of generic elements of the water utility infrastructure, consisting of a storage unit that stores the potable water or non-potable one for consumption and use. This water is then distributed by the water distribution centre responsible for distributing water from the centralized water plant to consumers. A water pump is also described in the model to increase the water pressure for the electricity generation process by a generator. The SCADA system in the cyber environment is responsible for managing and controlling these physical units, as described as communication between the physical and cyber environments.

3.1.1 Cyber attack Scenario. It is possible that unauthorized access to a computer may lead to the transmission of malicious data or code, which will impact the normal operation of the entire system.

When there are no authorization security mechanisms in place in a computer unit, an attacker can initiate a series of malicious operations against other components in the network. One of the expected possibilities is the flooding of the network with a massive amount of data to deny the service of the database server, which impacts the availability of the service. It is also possible that a set of malicious commands will be transmitted to SCADA systems, which will impact the normal operation of its capabilities for handling and controlling the physical environment. This type of cyber attack could have unanticipated consequences, such as the opening or closing of water gates or the shutting down of electrical generators, etc.

3.1.2 Physical Hazards. Physical or natural hazards are described as natural occurrences that have the potential to influence society and the human ecosystem [1]. Within this research, a set of multiple hazard scenarios is investigated and integrated to focus on the most relevant potential physical hazards that could have negative implications against physical components such as buildings, turbines, hydromechanical systems, etc.

3.2 Analysis of Consequences

In order to get a better understanding of the identified threats, it is helpful to simulate the consequences of the threats. In the following, we use a tool developed by the Austrian Institute of Technology (AIT) [2] to represent the network model of the considered system. The corresponding model of the water utility infrastructure is shown in Figure 2. It differs from the THREATGET model in Figure 1 since it is less focused on existing networks but rather on an abstract graph describing ways in which a problem can propagate (i.e., there is a directed edge from one node to another if a problem in one may affect the state of the other). Cyber components are represented as dots, physical components as squares and assets are represented as stars. Assets are special in that they are only affected by other components but do not forward threats (therefore, no transmission probabilities need to be defined).

The simulation method is based on a probabilistic model of cascading effects (described in more detail in Section 1). The main task to set up the simulation is to estimate the *transition probabilities* $p_{ij} = P(i \to j)$ that a nodes switches form state i to state j. These probabilities generally depend on the node and the considered threat. The way it is done depends on the data available (as described in Section 2). The amount of information depends on many factors, such as the type of node (e.g., it is easier to provide a lot of information on a technical device than on an entire infrastructure), the policy of a company, or the type of threat (e.g., there is few or no knowledge on zero-day attacks, while historical data may be available on natural disaster such as flooding).

Experience from previous projects showed that generally, more information is available for cyber assets than for physical assets. Therefore we recommend to use direct or quantitative estimation for physical assets (see Sections 2.1 and 2.2) while for cyber assets more advanced methods (as described in Sections 2.3 and 2.4) may be used. For the application of machine learning methods such as logistic regression (Section 2.5), a reasonable amount of data is needed, e.g., from a digital twin.

For the considered water utility, multiple threats can be identified

Figure 2: Sauron Model of Water Utility Scenario

as explained in Section 3.1. Table 2 shows some selected cyber and physical threats that have been identified in course of the analysis in Section 3.1. For illustration, we here focus on one physical and one cyber threat.

On the physical side, consider the increase in the water level due to flooding. For this threat, some historical data is available but due to factors such as climate change, the predictions come with intrinsic uncertainty. Therefore, a qualitative estimation (see Section 2.2) is applied. For the considered network, we assume that only the pump and the water distribution network are directly affected. For the pump we expect a change from 1 to 2 with medium confidence. If the pump already has a problem, the flooding will not make things better, i.e., we assume that things stay as they are or get worse with equal probability. That is, the transition matrix for the pump is

$$M_{pump} = \begin{pmatrix} 1/4 & 2/4 & 1/4 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & 1 \end{pmatrix}.$$

For the water distribution we expect a change from 1 to 3, also with medium confidence, and as for the pump no improvement if the original state is already 2 or 3. So the transition matrix for the water distribution (wd) is

$$M_{wd} = \begin{pmatrix} 2/3 & 1/3 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & 1 \end{pmatrix}.$$

On the cyber side, consider the communication integrity validity threat. This threat occurs if there is a connector from a source element to a target element where the target element does not have an input validation, but it holds an asset 'Integrity'. In THREATGET, this threat is identified if the attribute 'Input Validation' is not set to `yes`. For the considered example, this threat occurs on the connection between firewall and SCADA, if the attribute at SCADA is not set to `yes`, e.g., if it keeps the default value `undefined`. However,

Table 2: Selected cyber and physical threats according to THREATGET's outcomes

Cyber Threats					
#	Threat Title	Affected Elements	Affected Assets	Affected Connections	Violated Properties
1	Authorization of control system components	Computer and Virtual Boundary	Authorization Asset	————	Authorization
2	Lack of security capabilities of IIoT network device	Cloud Gateway and Virtual Boundary	————	————	Activity Logging and Anomaly Detection
3	Resource availability management	Database Server	Availability Asset	————	Anomaly Detection and DDoS Mitigation
4	Communication Integrity Validity	SCADA and Firewall	Integrity Asset	Connector from Cloud Gateway to Firewall	
Physical Threats					
#	Threat Title	Properties			
1	Shaking the water systems infrastructure due to earthquakes	Ground Tilting and Sesimometer Measures			
2	Increase the water level due to flooding	Drainage and Rerouting Water Flow			

the threat only occurs if there is an asset 'Integrity' related to the connection (i.e., only if we care about integrity, it is an issue if it can be exploited). In the Sauron model, edges to not have properties, instead we inserted an artificial node 'SCADA Data'. If there is a problem in the SCADA server, this might affect the stored data (i.e., in case of a malware attack), but the server might also have other problems (e.g., in case of fire data is not lost if there is a backup). Since occurrence of this threat only depends on the attributes of the SCADA node, we identify similar scenarios (Section 2.3) rather than counting threats (Section 2.4). As the threat is triggered through the value of just one attribute, there are only two sets of scenarios: one where 'Input validation' is set to `yes` (and others attributes such as activity logging or authorization take an arbitrary value) and one where 'Input Validation' is set to `no` or `undefined` (i.e., is different from `yes`) while other attributes are arbitrary. In the latter case, there is no threat and hence no state change happens (i.e., the transition matrix is the identity matrix). In the former case, the transition matrix may be estimated from further information about the threat. The THREATGET rule does not only describe when the threat occurs but also provides estimates on impact and likelihood (both measured on a 4-tier scale). Based on these two values, a risk level may be determined from a *risk matrix*, where the level is usually represented through colors from green (lowest risk for combinations of low impact and low likelihood) to red (highest risk for combinations of high impact and high likelihood). For the estimation of consequences, we apply a similar approach, just that instead of a risk level we determine a probability distribution over the states. Table 4 shows an example which the following intuition. The most likely value is determined as for a classical risk matrix, e.g., as shown in Table 3.

A distribution over all possible states can then be constructed based on the understanding that states 'close' to the predicted value are also possible in some situations, in particular if the likelihood is neither very low nor high (in these situations, we are more confident about our predictions). Therefore, in situations where the likelihood is low or medium, we assign half of the weight put on the state s to the neighboring states $s-1$ and $s+1$ (if these exist). The

Table 3: Most likely state depending on impact and likelihood

Impact/Likelih.	Very Low	Low	Medium	High
Negligible	1	1	1	1
Moderate	1	2	2	2
Major	1	2	3	3
Severe	1	2	3	3

corresponding distributions to the predictions from Table 3 are shown in Table 4.

Table 4: Distribution over all states depending on impact and likelihood

Impact/Likelih.	Very Low	Low	Medium	High
Negligible	(1,0,0)	(1,0,0)	(1,0,0)	(1,0,0)
Moderate	(1,0,0)	(1/3,1/3,1/3)	(1/3,1/3,1/3)	(0,1,0)
Major	(1,0,0)	(1/3,1/3,1/3)	(0,2/3,1/3)	(0,0,1)
Severe	(1,0,0)	(1/3,1/3,1/3)	(0,2/3,1/3)	(0,0,1)

The threat 'Communication Integrity Validity' has a severe impact and a medium likelihood. Therefore, based on Table 4 the transition probabilities form starting state 1 is $(0, 2/3, 1/3)$. As before, we assume no improvement if the original state is already 2 or 3 and we assume that in case of a problem (state 2), states 2 and 3 are equally likely (which may be refined in a more detailed analysis). So the transition matrix for SCADA is

$$M_{SCADA} = \begin{pmatrix} 0 & 2/3 & 1/3 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & 1 \end{pmatrix}.$$

The transition matrix of the node SCADA Data is most likely estimated from expert knowledge (e.g., the operator of the SCADA system).

4 CONCLUSION AND FUTURE WORK

Parametrization of risk models is possible in many ways, raining form heuristic to statistical methods. Which method is chosen usually depends on the available data, but in all cases it is important to explain the line of thinking and the assumptions that yielded the estimates.

In the course of the research project the considered examples will grow in size and complexity and advanced methods (such as the logistic regression) may be used if more data is available. In the context of critical infrastructures, data is often sensitive and experts are reluctant to provide any data. This problem is approaches in two ways. Where possible, digital twins of single components or entire infrastructures can be incorporated. In the future course of PRAETORIAN we plan to use these methods when analysing the use cases. If raw data is used for supervised machine learning methods, it can be shown that any guess of the (sensitive) dataset can be plausibly denied [20]. This allows the use of data such as log files to apply advanced methods.

ACKNOWLEDGMENTS

This work was done in the context of PRAETORIAN project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021274.

REFERENCES

[1] Federal Emergency Management Agency. 2022. *Natural Hazards | National Risk Index*. https://hazards.fema.gov/nri/natural-hazards

[2] AIT Austrian Institute of Technology. 2020. *SAURON Propagation Engine Editor*. https://atlas.ait.ac.at/sauron/#/

[3] AIT Austrian Institute of Technology. 2022. *THREATGET*. https://www.threatget.com/

[4] AIT Austrian Institute of Technology. 2022. *THREATGET Documentation*. https://documentation.threatget.com/21.10/index.html

[5] Benjamin Andreas Carreras, David E. Newman, Paul Gradney, Vickie E. Lynch, and I. Dobson. 2007. Interdependent Risk in Interacting Infrastructure Systems. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. 112–112. https://doi.org/10.1109/HICSS.2007.285

[6] Korbinian Christl and Thorsten Tarrach. 2021. The analysis approach of ThreatGet. https://doi.org/10.48550/ARXIV.2107.09986

[7] Antonios Gouglidis, Sandra König, Benjamin Green, Karl Rossegger, and David Hutchison. 2018. Protecting Water Utility Networks from Advanced Persistent Threats: A Case Study. In *Game Theory for Security and Risk Management*, Stefan Rass and Stefan Schauer (Eds.). Springer International Publishing, 313–333. https://doi.org/10.1007/978-3-319-75268-6_13

[8] Hengdao Guo, Ciyan Zheng, Herbert Ho-Ching Iu, and Tyrone Fernando. 2017. A critical review of cascading failure analysis and modeling of power system. *Renewable and Sustainable Energy Reviews* 80 (dec 2017), 9–22. https://doi.org/10.1016/j.rser.2017.05.206

[9] Sandra König and Stefan Rass. 2018. Investigating Stochastic Dependencies Between Critical Infrastructures. 11, 3 (2018), 250–258.

[10] Sandra König, Stefan Rass, Benjamin Rainer, and Stefan Schauer. 2019. Hybrid Dependencies Between Cyber and Physical Systems. In *Intelligent Computing*, Kohei Arai, Rahul Bhatia, and Supriya Kapoor (Eds.). Vol. 998. Springer International Publishing, 550–565. https://doi.org/10.1007/978-3-030-22868-2_40 Series Title: Advances in Intelligent Systems and Computing.

[11] Sandra König, Stefan Rass, Stefan Schauer, and Alexander Beck. 2016. Risk Propagation Analysis and Visualization using Percolation Theory. 7, 1 (2016). https://doi.org/10.14569/IJACSA.2016.070194

[12] Sandra König, Stefan Schauer, and Stefan Rass. 2016. A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks. In *Secure IT Systems. Proceedings of NordSec conference 2016, Oulu, Finland*. Springer International Publishing, 67–81. https://doi.org/10.1007/978-3-319-47560-8_5

[13] Zhendong Ma and Christoph Schmittner. 2016. Threat modeling for automotive security analysis. *Advanced Science and Technology Letters* 139 (2016), 333–339.

[14] Georg Macher, Eric Armengaud, Eugen Brenner, and Christian Kreiner. 2016. Threat and risk assessment methodologies in the automotive domain. *Procedia computer science* 83 (2016), 1288–1294.

[15] Microsoft. 2022. *Microsoft Security Development Lifecycle*. https://www.microsoft.com/en-us/securityengineering/sdl (Accessed on: June 20, 2022).

[16] Min Ouyang. 2014. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety* 121 (2014), 43 – 60. https://doi.org/10.1016/j.ress.2013.06.040

[17] PRAETORIAN Consortium. 2022. *PRAETORIAN*. https://praetorian-h2020.eu/

[18] Mahshid Rahnamay-Naeini and Majeed M. Hayat. 2016. Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach. *IEEE Transactions on Smart Grid* 7, 4 (Jul 2016), 1997–2006. https://doi.org/10.1109/tsg.2016.2539823

[19] Stefan Rass, Sandra König, and Stefan Schauer. 2021. Semi-automated Parameterization of a Probabilistic Model Using Logistic Regression—A Tutorial. , 438–484 pages. https://doi.org/10.1002/9781119723950.ch22

[20] Stefan Rass, Sandra König, Jasmin Wachter, Manuel Egger, and Manuel Hobisch. 2022. Supervised Machine Learning with Plausible Deniability. *Computers & Security* 112 (2022), 102506. https://doi.org/10.1016/j.cose.2021.102506

[21] Christoph Schmittner, Peter Tummeltshammer, David Hofbauer, Abdelkader Magdy Shaaban, Michael Meidlinger, Markus Tauber, Arndt Bonitz, Reinhard Hametner, and Manuela Brandstetter. 2019. Threat Modeling in the Railway Domain. In *International Conference on Reliability, Safety, and Security of Railway Systems*. Springer, 261–271.

[22] Abdelkader Magdy Shaaban, Christoph Schmittner, Thomas Gruber, A. Baith Mohamed, Gerald Quirchmayr, and Erich Schikuta. 2019. Ontology-Based Model for Automotive Security Verification and Validation. In *Proceedings of the 21st International Conference on Information Integration and Web-Based Applications & Services* (Munich, Germany) *(iiWAS2019)*. Association for Computing Machinery, New York, NY, USA, 73–82. https://doi.org/10.1145/3366030.3366070

[23] Nataliya Shevchenko. 2018. Threat Modeling: 12 Available Methods. https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html. (Accessed on: June 20, 2022).

[24] Adam Shostack. 2008. Experiences threat modeling at Microsoft. *CEUR Workshop Proceedings* 413.

[25] Sheng-Jhih Wu and Moody T. Chu. 2017. Markov Chains with Memory, Tensor Formulation, and the Dynamics of Power Iteration. *Appl. Math. Comput.* 303, C (June 2017), 226–239. https://doi.org/10.1016/j.amc.2017.01.030