A Systematic Literature Review of Information Sources for Threat Modeling in the Power Systems Domain

Engla Ling^(✉), Robert Lagerström, and Mathias Ekstedt

Division of Network and Systems Engineering, KTH Royal Institute of Technology,
Stockholm, Sweden

{englal,robertl,mekstedt}@kth.se

Abstract. Power systems are one of the critical infrastructures that has seen an increase in cyber security threats due to digitalization. The digitalization also affects the size and complexity of the infrastructure and therefore makes it more difficult to gain an overview in order to secure the entire power system from attackers. One method of how to gain an overview of possible vulnerabilities and security threats is to use threat modeling. In threat modeling, information regarding the vulnerabilities and possible attacks of power systems is required to create an accurate and useful model. There are several different sources for this information. In this paper we conduct a systematic literature review to find which information sources that have been used in power system threat modeling research. Six different information sources were found: expert knowledge, logs & alerts, previous research, system's state, vulnerability scoring & databases, and vulnerability scanners.

Keywords: Threat modeling · Power systems · Cyber security

1 Introduction

Power systems are a crucial part of any country's infrastructure. Without the access to electric power, the consequences can be severe, for example, hospitals being unable to operate. It is essential that the security of power systems is kept, especially when they are added to the communication infrastructure as part of digitalization. One method of ensuring the security of the power system is to gain an overview of its vulnerabilities by creating threat models. Threat modeling is a method of assessing security of systems and is further described in Sect. 3. Threat models are suitable for power systems because current security assessment techniques for enterprise IT environments might not be available for power systems. Power systems combine Information Technology (IT) with

Funded by Swedish Centre for Smart Grids and Energy Storage (SweGRIDS), the Swedish Civil Contingencies Agency's Resilient Information and Control Systems research centre as well as the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907.

The original version of this chapter was revised: It has been changed to Open Access. The correction to this chapter is available at https://doi.org/10.1007/978-3-030-58295-1_8

© The Author(s) 2020, corrected publication 2021

A. Rashid and P. Popov (Eds.): CRITIS 2020, LNCS 12332, pp. 47–58, 2020.

https://doi.org/10.1007/978-3-030-58295-1_4

Operational Technology (OT) and there is often a combination of legacy and new techniques as well as equipment.

In this paper we find and discuss different information sources for vulnerability information when creating threat models for power systems. The aim is to contribute to the field of threat modeling in the power systems domain where finding reliable information to build a threat model is a crucial part of making sure that any conclusions drawn from the threat model is valid. It is not always clear how to find the information required to build a threat model and this article aims to aid in this process.

The research question is *What information sources have previously been used in research when generating threat models in the power systems domain?* The information sources have been found with a systematic literature review, i.e. a literature review where the process is carefully described so that the work can be repeated and avoid potential bias. This approach was chosen because there is a large amount of information in the research community, while in industry the created threat models are often not readily available being the potential security risk.

2 Related Work

The related work most closely related to this paper is “A review of cyber security risk assessment methods for SCADA systems” [8]. In that paper “SCADA” and “risk assessment” were used as keywords to find articles between 2004 and 2014. The authors found 24 articles according to these criteria. The difference between that study and this one is that they focused on all types of SCADA systems and on risk assessment. Cyber security risk assessment can be considered a broader term than threat modeling because the risk can be assessed by other means than with threat modeling. For example, it can be assessed by mathematical formulas. Another difference between cyber security risk assessment and threat modeling is that in risk assessment, the consequences of an attack are also taken into consideration. Even though the focus of that paper was not information sources, they presented it as part of their results. The authors found two different possible information sources, expert opinion and historical data. This is in contrast to this literature review paper where historical data was not mentioned in any of the articles and many more information sources were found. In addition, the different potential information sources were discussed in the article, indicating that the authors were aware that more than the two found by them exists.

Nazir et al. performed a survey for the techniques used to assess vulnerabilities of SCADA system [32]. Their survey was not a systematic literature review, but rather a collection of the most commonly used techniques including threat modeling. Some of the techniques that they discuss can be considered as information sources, for example using monitoring and test beds. They also discuss tools that can be used for gathering information. These tools are scanning tools, penetration testing, machine learning, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), honey pots, Security information and event management (SIEM), ethical hacking and forensic science.

3 Threat Modeling

Threat modeling has many different definitions [45], but it is typically defined as a technique where the different security threats for a system are modelled. Often they are modelled in order to run simulations. This allows you to find potential future attacks. In this way one can make sure that the system is secure by using a model of the system instead of the actual system.

There are multiple ways of how to represent a threat model. For example, attack trees that were made popular by Schneier [37] shows a successful attack as the goal node of a tree with different attack steps leading up to that goal node. According to his paper, the attack goals, attacks against those goals and the values of the nodes, that is, the difficulty of the attacks, are required to build the attack tree. This type of information to build attack trees or any other type of threat model can be found by using several different information sources. For example, one can derive the information from vulnerability databases, industry experts or base it on previous attacks. It is important that this information source is reliable so that the resulting threat model can be trusted. The threat model may be used to make decisions of where to assign the most resources to protect the system depending on the result and any mistakes could be costly.

4 Method

The scope of this systematic literature review is defined by the search query that was used and the databases that were searched. The keywords were chosen based on the best of our knowledge on what would be the most inclusive but also include relevant articles. The following search query with keywords was used: (**“attack graph” OR “attack tree” OR “threat model*”**) **AND (“power system” OR “energy system” OR “power grid” OR “smart grid”)**. The asterisk symbol means that the query will search for multiple variations of threat model, including “threat models” and “threat modeling”.

The databases IEEE, Springer link, Web of Science, Science Direct and Scopus were used in this systematic literature review. In total 260 articles were found, and the specific search queries with results are shown below. The search was performed on the January 24th 2020.

IEEE 76 results after a search by Metadata. The metadata consists of abstract, title and indexing terms. Indexing terms are keywords that have been defined by the author.

Springer Link 415 results that were manually narrowed down to 17 results. This was because the title, abstract and keywords had to be filtered manually since Springer Link does not support that search request.

Web of Science 45 results after searching based on Topic, which includes title, abstract, author keywords, and Keywords Plus. Keywords plus are keywords generated automatically by an algorithm. The algorithm creates keywords based on the titles of the articles references.

Science Direct 9 results found based on Title, abstract or author-specified keywords.

Scopus 113 results based on their “TITLE-ABS-KEY” search.

After duplicates were removed from the final 260 articles, 146 of them remained. These articles were narrowed down to 44 articles according to the following inclusion criteria:

- The article must focus on cyber security.
- The article must include a threat model or the method of how one was constructed.
- The threat model must be in the power systems domain.
- The article must mention at least one information source that was used to create the threat model.
- The article must be written in English.

When the final 44 articles had been found, they were divided into categories of information source.

5 Information Sources

In Table 1 the information sources that were found in each article of the systematic literature review is summarized. This section describes and discusses the different information sources as found by this systematic literature review.

5.1 Expert Knowledge

From the results, 11 threat models were generated by using expert knowledge. Expert knowledge means that the developers have gained information from experts regarding, for example, what they believe to be the most likely attack scenarios. These experts are not necessarily experts in security but they are rather experts in the power systems domain. There is one exception and that is one article that used hacking knowledge [15]. The information was found by reading about attackers describing their goals.

Most often there is little information regarding the experts, how many they are and their credentials [25,36]. This makes it difficult to validate their results. Even if the experts are well known in terms of their credentials it can be difficult to know how much to stress each expert’s opinion. In an article outside the scope of this review [22] the authors analyzed how to evaluate the correctness in expert knowledge judgement and how this could be used to weight in how much one considered a specific expert’s opinion. This opens up the possibility of using expert knowledge, while prioritizing knowledge put forward by reliable experts.

There are some articles that discuss the method itself and these methods are the Delphi method [6,7], brainstorming [40] or allowing the experts to model themselves [18]. The Delphi method is a process of anonymous scoring followed by open discussions and results iteratively. The authors that used the brainstorming method saw a possible weak spot because of its dependency on who is participating from the stakeholders [40]. However, they claim that this was

partly helped by the attending security experts. In the paper where the experts were allowed to model themselves they had some issues because the expert's modeling was not always in line with what could be translated easily to the threat modeling framework that they used [18].

One of the limitations of using industry experts is that they are often experts within one specific domain. This might make it difficult to model larger systems. This limitation was mentioned by [41]. In addition, they mentioned two other limitations. These are that the results are only valid during that instance and are constrained by the experts knowledge level. The authors expert knowledge reference group consisted of utility sector experts of Operational Technology (OT) systems. The experts were used to model the data flows. However, other information sources were used to create their attack graph because attack data was included in the framework that they used. In the threat modeling technique by Chen et al., a suggestion to this problem is presented where multiple smaller threat models are combined into one larger [5]. Each of the smaller threat models would be created by an industry expert in that domain.

Some articles use expert knowledge in combination with other information sources [15, 17, 41]. It can be easy to include expert knowledge because it may only be a question of asking an expert of their opinion. As seen in the articles of this systematic literature review, there are many different methods of how to include expert knowledge. This supports the fact that expert knowledge is easy to modify and adapt to your needs. However, one can question how to validate the results.

5.2 Logs and Alerts

A few articles use logged information as an information source. There are many different services that collect information about a system as logs and the resulting articles includes three of these different kinds of logs. One paper used information from archived IDS/IPS logs and alerts [15]. Another paper used event logs that they created themselves by running simulated attacks [14]. This might require a lot of time and skill to set up. An alternative could be to use historical data logs if that is available as Zhang et al. did [50]. Logs can be a very good source of information because there is often a very large amount of data that is collected. At the same time, it can be time consuming and require knowledge to go through all of the information.

5.3 Previous Research

The majority of articles found in this systematic literature review use previous research to find the different possible vulnerabilities or attacks on the systems that they model [4, 13, 16, 19, 23, 26, 28–30, 34, 46, 52, 53]. Previous research is also used in combination with other information sources [9–11, 20, 31, 41]. This previous research can consist of research articles or published reports. In most cases it is not exactly specified where the authors have used previous research and where they have made assumptions. This makes it difficult to validate their results.

Table 1. Information sources for power system’s threat models

Article	Expert Knowledge	Logs & Alerts	Previous Research	System’s State	Vulnerability Scoring & Databases	Vulnerability Scanner
[6]	●					
[7]	●					
[40]	●					
[18]	●					
[41]	●		●		●	
[5]	●					
[25]	●					
[36]	●					
[15]	●	●		●		
[17]	●				●	●
[50]		●				
[14]		●				
[52]			●			
[46]			●			
[30]			●			
[26]			●			
[29]			●			
[23]			●			
[19]			●			
[16]			●			
[53]			●			
[4]			●			
[28]			●			
[13]			●			
[34]			●			
[20]			●	●		
[31]			●		●	
[10]			●		●	
[9]			●		●	
[11]			●		●	
[39]				●		
[38]				●		
[27]				●		
[51]					●	
[47]					●	
[43]					●	
[42]					●	
[48]					●	
[35]					●	●
[49]					●	
[2]					●	●
[1]					●	
[44]					●	
[12]					●	

Previous research is however a valid information source where it is referenced properly because the source has often been peer-reviewed before publication.

5.4 System's State

Five of the articles used the state of the system that they want to model to evaluate the vulnerabilities or potential attacks. The state of the system can be to for example analyze the security implementations [15,27,38,39], make a forensics analysis [38,39] or look at configuration files [20].

There was a large variation of the type of information used from the system and how they used it found in this review. When using a system's state as an information source, no other resource or information is required except the system itself. This makes the information source easy to use. However, it might take time to collect the appropriate information and experts to be able to analyze the results accurately.

5.5 Vulnerability Scoring and Databases

17 articles of this systematic literature review was found to use vulnerability scoring or databases as an information source. Some of the articles use a combination of the scoring systems with the databases and some only use one of them. The most common scoring system as found in this review is the Common Vulnerability Scoring System (CVSS)¹ [42,43,47,48,51]. The CVSS is a scoring system that was developed by and maintained by Forum of Incident Response and Security Teams (FIRST). The authors in [21], outside the scope of this review, found that using CVSS alone does not perform well as an information source for threat modeling. While the authors in [24] found that in general CVSS can be trusted. In addition, their results also showed that if one considers all of the systems vulnerabilities and not only those with the highest CVSS score, the results were much more reliable. Some papers found in this review use a combination of calculating their own CVSS scores with vulnerability databases or other information sources [9–11]. Another example of a scoring system is the Common Weakness Enumeration (CWE) is a category system that also calculates a score for the weaknesses or vulnerabilities² [35]. The CWE includes all software weaknesses and not only vulnerabilities.

There are multiple different vulnerabilities databases that aim to categorize and explain vulnerabilities for different systems and these can be used as information sources when modeling. The ones found in this review are the U.S. National Vulnerability Database (NVD)³ [2,12,17,41,49], MITRE⁴ [31,44], several CERTs databases^{5,6,7} [1,12,44] as well as the Chinese databases Chinese National Vulnerability Database (CNNVD)⁸ [41].

¹ <https://www.first.org/cvss/> [accessed 28 April 2020].

² <https://cwe.mitre.org/> [accessed 28 April 2020].

³ <https://nvd.nist.gov/> [accessed 28 April 2020].

⁴ https://cve.mitre.org/cve/search_cve_list.html [accessed 28 April 2020].

⁵ <https://www.kb.cert.org/vuls/search/> [accessed 28 April 2020].

⁶ <https://www.cert.org.cn/> [accessed 28 April 2020].

⁷ <https://www.us-cert.gov/ics/monitors> [accessed 28 April 2020].

⁸ <http://www.cnnvd.org.cn/> [accessed 28 April 2020].

The positive aspect of using this information as a source is that a lot of information is readily available. This information source can also adapt easily to changes. If one is constructing a threat model with this source, it is possible to quickly update the vulnerability information if the scoring or database change. One downside of using the vulnerability scoring and databases is that this information has the possibility of bias. This is because there are experts who use their experience and knowledge to estimate properties that give vulnerabilities a specific score. It is difficult to know exactly where the articles gain the information, they might phrase it as “vulnerabilities can be found in vulnerability databases, for example X,Y,Z”. In these cases we assume that those are the databases used.

5.6 Vulnerability Scanner

A vulnerability scanner can automatically detect vulnerabilities within a system and three articles in this literature review used them as an information source [2, 17, 35]. In all of these papers, the vulnerability scanner was used in combination with another information source. A scanner may require time to set up, but it provides a lot of information that can often already be analyzed by the tool itself. Similar to the information source of previous research, it is not always clear to what extent the vulnerability scanning has been used. Sometimes the articles will give examples of vulnerability scanning tools that may be used, and in this can the assumption is that those tools have actually been used.

6 Discussion

Similar to any systematic literature review work, there is the possibility of changing the database, keywords and inclusion criteria that is used. For example, Google Scholar and arXiv could have been searched as well. The downside of using a database, such as Google Scholar, is that it includes other work such as e.g. student thesis reports in addition to peer-reviewed research papers. If we would search the full text of articles and not only the title, abstract and keywords then the result does not only show many more articles, but these articles may not be relevant for the research question.

Another limitation of this work that exists because of the nature of a systematic literature review is that some articles will not be included in the results. For instance, the terms “risk assessment” [33], “SCADA” [3] may be used instead of the search terms in this systematic literature review. However, if those search terms were included the review would result in many irrelevant articles. There may also be other information sources being used other than those included in published research. These might be information sources used by threat models created in the industry.

Possible future work includes looking into the relations between the different information sources and how some of them may overlap or complement each other. It could also be to look into information sources that exist in other domains and use these in the power systems domain. Future work could also be

to automatically keep this list of information sources up to date by utilizing the databases' API and some form of natural language processing solution. Planned future work is to use some of the found information sources to develop threat models for power systems.

7 Conclusion

In this article a systematic literature review was used as a method to find the different information sources that have previously been used in research when creating threat models in the power systems domain. Answering the research question, this systematic literature review found six different information sources. These are expert knowledge, logs & alerts, previous research, system's state, vulnerability scoring & databases and vulnerability scanners.

The many different information sources that have been used indicate that there is no standard method that is usually followed. The most common information sources that are used are expert knowledge, previous research, and vulnerability scoring & databases. As discussed in this paper there are many positive and negative aspects with all of the information sources. Because of the availability of information for these sources it might be beneficial to combine all three when creating a threat model in the power systems domain.

References

1. Anwar, Z., Shankesi, R., Campbell, R.H.: Automatic security assessment of critical cyber-infrastructures. In: 2008 IEEE International Conference on Dependable Systems & Networks With FTCS and DCC (DSN). IEEE Computer Society, Los Alamitos, June 2008
2. Beckers, K., Heisel, M., Krautsevich, L., Martinelli, F., Meis, R., Yautsiukhin, A.: Determining the probability of smart grid attacks by combining attack tree and attack graph analysis. In: Cuellar, J. (ed.) SmartGridSec 2014. LNCS, vol. 8448, pp. 30–47. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10329-7_3
3. Byres, E.J., Franz, M., Miller, D.: The use of attack trees in assessing vulnerabilities in SCADA systems. In: IEEE Conference on International Infrastructure Survivability Workshop (IISW 2004). Institute for Electrical and Electronics Engineers (2004)
4. Chang, Y.H., Jirutitijaroen, P., Ten, C.: A simulation model of cyber threats for energy metering devices in a secondary distribution network. In: 2010 5th International Conference on Critical Infrastructure (CRIS), pp. 1–7, September 2010
5. Chen, T.M., Sanchez-Aarnoutse, J.C., Buford, J.: Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans. Smart Grid **2**(4), 741–749 (2011)
6. Chen, Y.T.: Modeling information security threats for smart grid applications by using software engineering and risk management. In: 2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE), pp. 128–132, August 2018
7. Chen, Y.T., Huang, C.C.: Determining information security threats for an IoT-based energy internet by adopting software engineering and risk management approaches. *Inventions* **4**, 53 (2019)

8. Cherdantseva, Y., et al.: A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **56**, 1–27 (2016)
9. Dai, Q., Shi, L., Ni, Y.: Risk assessment for cyber attacks in feeder automation system. In: 2018 IEEE Power Energy Society General Meeting (PESGM), pp. 1–5, August 2018
10. Dai, Q., Shi, L., Ni, Y.: Risk assessment for cyberattack in active distribution systems considering the role of feeder automation. *IEEE Trans. Power Syst.* **34**(4), 3230–3240 (2019)
11. Dai, Q., Shi, L., Ni, Y.: A sponsor incentive attack scheme for feeder automation systems. *IEEE Trans. Smart Grid* **11**, 1440–1452 (2019)
12. Davis, K.R., et al.: A cyber-physical modeling and assessment framework for power grid infrastructures. *IEEE Trans. Smart Grid* **6**(5), 2464–2475 (2015)
13. Duman, O., Ghafouri, M., Kassouf, M., Atallah, R., Wang, L., Debbabi, M.: Modeling supply chain attacks in IEC 61850 substations. In: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–6, October 2019
14. Eibl, G., et al.: Exploration of the potential of process mining for intrusion detection in smart metering. In: ICISSP, pp. 38–46, January 2017
15. Garcia, L., Zonouz, S.: TMQ: threat model quantification in smart grid critical infrastructures. In: 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 584–589, November 2014
16. Grochocki, D., et al.: AMI threats, intrusion detection requirements and deployment recommendations. In: 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), pp. 395–400, November 2012
17. Guan, X., Ma, Y., Hua, Y.: An attack intention recognition method based on evaluation index system of electric power information system. In: 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), pp. 1544–1548, December 2017
18. Hacks, S., Hacks, A., Katsikeas, S., Klaer, B., Lagerström, R.: Creating meta attack language instances using ArchiMate: applied to electric power and energy system cases. In: 2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC), pp. 88–97, October 2019
19. Han, W., Xiao, Y.: Non-technical loss fraud in advanced metering infrastructure in smart grid. In: Sun, X., Liu, A., Chao, H.-C., Bertino, E. (eds.) ICCCS 2016. LNCS, vol. 10040, pp. 163–172. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-48674-1_15
20. Hawrylak, P.J., Haney, M., Papa, M., Hale, J.: Using hybrid attack graphs to model cyber-physical attacks in the smart grid. In: 2012 5th International Symposium on Resilient Control Systems, pp. 161–164, August 2012
21. Holm, H., Ekstedt, M., Andersson, D.: Empirical analysis of system-level vulnerability metrics through actual attacks. *IEEE Trans. Dependable Secure Comput.* **9**(6), 825–837 (2012)
22. Holm, H., Somestad, T., Ekstedt, M., Honeth, N.: Indicators of expert judgement and their significance: an empirical investigation in the area of cyber security. *Expert Syst.* **31**(4), 299–318 (2014)
23. Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., Shen, X.: Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Sci. Technol.* **19**(2), 105–120 (2014)
24. Johnson, P., Lagerström, R., Ekstedt, M., Franke, U.: Can the common vulnerability scoring system be trusted? A Bayesian analysis. *IEEE Trans. Dependable Secure Comput.* **15**(6), 1002–1015 (2016)

25. Khan, R., McLaughlin, K., Lavery, D., Sezer, S.: Stride-based threat modeling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pp. 1–6, September 2017
26. Lemaire, L., Vossaert, J., De Decker, B., Naessens, V.: Security evaluation of cyber-physical systems using automatically generated attack trees. In: D’Agostino, G., Scala, A. (eds.) *Critical Information Infrastructures Security*, pp. 225–228. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-99843-5_20
27. Liu, N., Zhang, J., Zhang, H., Liu, W.: Security assessment for communication networks of power control systems using attack graph and MCDM. *IEEE Trans. Power Delivery* **25**(3), 1492–1500 (2010)
28. Mander, T., Cheung, R., Nabhani, F.: Power system DNP3 data object security using data sets. *Comput. Secur.* **29**(4), 487–500 (2010)
29. Marksteiner, S., Vallant, H., Nahrgang, K.: Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling. *J. Inf. Secur. Appl.* **49**, 102389 (2019)
30. McDaniel, P., McLaughlin, S.: Structured security testing in the smart grid. In: 2012 5th International Symposium on Communications, Control and Signal Processing, pp. 1–4, May 2012
31. Nasr, E., Shahrour, I.: Evaluating wireless network vulnerabilities and attack paths in smart grid comprehensive analysis and implementation. In: 2017 Sensors Networks Smart and Emerging Technologies (SENSET), pp. 1–4, September 2017
32. Nazir, S., Patel, S., Patel, D.: Assessing and augmenting SCADA cyber security: a survey of techniques. *Comput. Secur.* **70**, 436–454 (2017)
33. Patel, S., Zaveri, J.: A risk-assessment model for cyber attacks on information systems. *JCP* **5**, 352–359 (2010)
34. Paudel, S., Smith, P., Zseby, T.: Attack models for advanced persistent threats in smart grid wide area monitoring. In: *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2017*, pp. 61–66. Association for Computing Machinery, New York (2017)
35. Radoglou-Grammatikis, P., Sarigiannidis, P., Giannoulakis, I., Kafetzakis, E., Panaousis, E.: Attacking IEC-60870-5-104 SCADA systems. In: 2019 IEEE World Congress on Services (SERVICES), vol. 2642–939X, pp. 41–46, July 2019
36. Ru, Y., et al.: Risk assessment of cyber attacks in ECPS based on attack tree and AHP. In: 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pp. 465–470, August 2016
37. Schneier, B.: Attack trees. *Dr. Dobbs’s J. Softw. Tools* **24**, 21–29 (1999)
38. Ten, C., Liu, C., Govindarasu, M.: Vulnerability assessment of cybersecurity for SCADA systems using attack trees. In: 2007 IEEE Power Engineering Society General Meeting, pp. 1–8, June 2007
39. Ten, C., Manimaran, G., Liu, C.: Cybersecurity for critical infrastructures: attack and defense modeling. *IEEE Trans. Syst. Man Cybern Part A Syst. Hum.* **40**(4), 853–865 (2010)
40. Tøndel, I.A., Jaatun, M.G., Line, M.B.: Threat modeling of AMI. In: Hämmerli, B.M., Kalstad Svendsen, N., Lopez, J. (eds.) *CRITIS 2012. LNCS*, vol. 7722, pp. 264–275. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41485-5_23
41. Vernotte, A., Vålja, M., Korman, M., Björkman, G., Ekstedt, M., Robert, L.: Load balancing of renewable energy: a cyber security analysis. *Energy Inform.* **1**, 5 (2018). <https://doi.org/10.1186/s42162-018-0010-x>

42. Wadhawan, Y., Neuman, C.: RL-BAGS: a tool for smart grid risk assessment. In: 2018 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), pp. 7–14, May 2018
43. Wadhawan, Y., Almajali, A., Neuman, C.: A comprehensive analysis of smart grid systems against cyber-physical attacks. *Electronics* **7**, 249 (2018)
44. Li, W., Jin, H., You, W.: Attack modeling for electric power information networks. In: 2010 International Conference on Power System Technology, pp. 1–5, October 2010
45. Xiong, W., Lagerström, R.: Threat modeling - a systematic literature review. *Comput. Secur.* **84**, 53–69 (2019)
46. Yan, J., Govindarasu, M., Liu, C.C., Ni, M., Vaidya, U.: Risk assessment framework for power control systems with PMU-based intrusion response system. *J. Mod. Power Syst. Clean Energy* **3**(3), 321–331 (2015). <https://doi.org/10.1007/s40565-015-0145-8>
47. Yeboah-Ofori, A., Islam, S.: Cyber security threat modeling for supply chain organizational environments. *Future Internet* **11**, 63 (2019)
48. Yu-de, Y., Shuilan, L.: Optimal prevention and control strategy against preconceive faults in electric cyber-physical system. In: 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), pp. 1–9 (2018)
49. Zhang, B., Li, Q., Zhang, Y., Liu, X., Ni, Z.: Generation of cyber-security reinforcement strategies for smart grid based on the attribute-based attack graph. *J. Power Technol.* **96**(3), 170–177 (2016)
50. Zhang, H., et al.: A multi-step attack detection model based on alerts of smart grid monitoring system. *IEEE Access* **8**, 1031–1047 (2020)
51. Zhang, Y., Wang, L., Xiang, Y., Ten, C.: Power system reliability evaluation with SCADA cybersecurity considerations. *IEEE Trans. Smart Grid* **6**(4), 1707–1721 (2015)
52. Zhang, Y., Xiang, Y., Wang, L.: Power system reliability assessment incorporating cyber attacks against wind farm energy management systems. *IEEE Trans. Smart Grid* **8**(5), 2343–2357 (2017)
53. Zhang, Y., Xiang, Y., Wang, L.: Reliability analysis of power grids with cyber vulnerability in SCADA system. In: 2014 IEEE PES General Meeting—Conference Exposition, pp. 1–5, July 2014

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.