



Cybersecurity issues in power systems

Zsolt Szabó

Óbuda University, Doctoral School on Safety and Security Sciences, Budapest,
Hungary
szabo.zsoltmihaly@uni-obuda.hu

Abstract: As a result of technological advances, humanity has become increasingly vulnerable to the operation of information systems. We have built ourselves an infrastructure system that supports our daily lives and makes them more comfortable, but these systems rely almost entirely on IT systems. However, with the development of information technology in the early 2000s, the level and number of remote management and convenience services provided by infocommunications has risen to such a level that there is almost no organization or company operating a critical infrastructure that is not connected to the World Wide Web. However, everything requires electricity. The electricity system has undergone significant change since the last decade: the path from electricity generation to the consumer is more complex and unpredictable with the spread of green energy. All of this absolutely highlights the key role of security of supply. The lecture and the related publication deal with the structure and basic technical knowledge of the electricity sector as a critical infrastructure area. The basics and infrastructure of electricity supply and the operation of the Hungarian electricity system are described. It deals with the control, protection, automation and communication systems of the electricity system. The publication is the examination of the cybersecurity issues in power systems as the greatest cyber security risk nowadays.

Keywords: power systems, critical infrastructure, electronic information systems, cybersecurity risks

1 Introduction

One of the main tools and channels of globalization since the 1990s, the explosive development of the Internet and mobile data communication technologies. The infocommunication systems and other electronic systems for example power systems pose threat serious security risks everywhere in the world. It is very important to note that the protection of electricity systems is a burning issue not only in terms of cybersecurity but also in all other respects, as we are talking about critical infrastructures.

The failure of a given system element can trigger an avalanche in the system due to interdependence, just think of the relationship between nuclear power plants,



internet service providers and banks as an example. Based on the topic raised we have two main questions, to which we are looking for answers:

- Will there be high quality and high secure power systems services available?
- Will there be cyber security conscious users?

2 The global trends driving the cybersecurity issues in power systems

However, since the development of information technology in the early 2000s the World Wide Web has used risen dramatically. We have built ourselves an infrastructure system that supports our daily lives and makes them more comfortable, but these systems rely almost entirely on IT systems (Kralovánszky, 2021). The electricity system is essential for our everyday lives, and the continuous supply of electricity has become a matter of civilization. As a vital component of the system, its impact on the population is extremely significant. That is why its protection is of paramount importance, as its continuous, intact operation is essential to the functioning of society.

However, potential operational problems in the electricity supply may not only affect the daily lives of the population, but may also affect other critical infrastructures, which is why we consider them to be the most critical critical infrastructure. Electricity has undergone tremendous development in recent decades. In the last century, it was still completely natural to check all instruments manually, record the data they measured on paper, and use the fewest digital instruments in the various processes. However, technological innovations and the opportunities they offer quickly spread to the sector, as it became possible to perform increasingly complex tasks in an increasingly shorter period of time, and the sector is now highly IT-dependent (Kralovánszky, 2019). As a result of technological advances, humanity has become increasingly vulnerable to the operation of information systems.

However, everything requires power systems.

Slogan: 'If there is electricity, everything is there!'

Hypothesis: 'Without IT, there is no electricity!'

The electricity system is indispensable for our everyday lives, and the continuous supply of electricity has become a matter of civilization (see Fig. 1). As a vital component of the system, its impact on the population is extremely significant. That is why its protection is of paramount importance, as its continuous, intact operation is essential to the functioning of society.

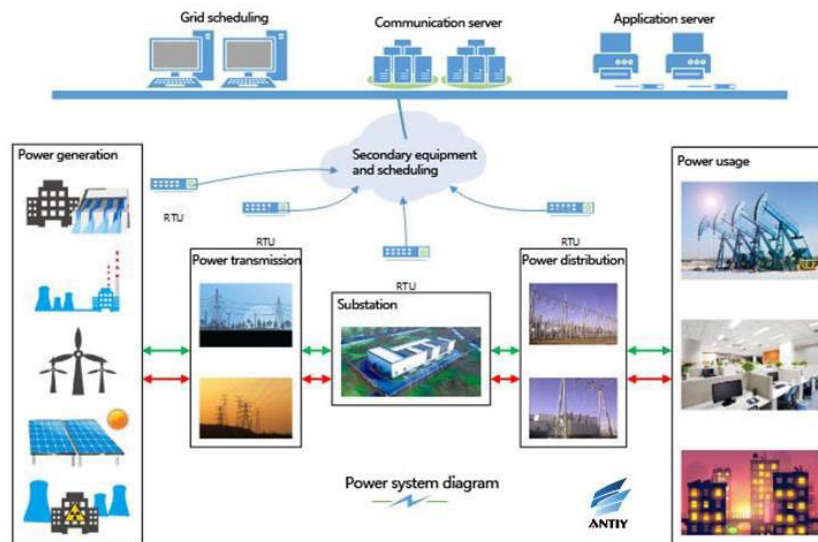


Figure 1 Power system diagram

Source: Antiy Labs (2016) available: <https://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks/>

However, potential operational problems in the electricity supply may not only affect the daily lives of the population, but may also affect other critical infrastructures, which is why we consider them to be the most critical critical infrastructure (Kralovánszky, 2021). Modernization, together with the impact of technological penetration, is also showing an increasing trend in the variety of attacks against them. As facilities that are particularly important for the operation of the state are currently regulated by technical means, special attention must be paid to their protection and safety. In the event that the technical equipment of the above facilities is not adequately protected, the object of the location's function may be compromised in the event of a cyber attack. The first precedent in our history for a cyber attack that caused a problem in an entire country occurred in Ukraine on December 23, 2015 (see Fig. 2).

The day before, as a result of a cyber attack, an electricity supply facility collapsed, leaving the majority of consumers unserved. Studying cases like this is important from a preventive point of view to avoid carrying out attacks like this in the future. It is known that the operation of critical infrastructures (for example: utilities, transport, etc.) is inconceivable without a continuous supply of electricity. Given this dependency, the electricity system can be considered, with a slight exaggeration, even the most critical infrastructure to be protected, including the continuous strengthening of its cyber security in line with current threats. As a concrete precedent, the cyber-attacks against the Ukrainian electricity (power) system in 2015 and 2016 provided a sobering signal. However, the number of cyber



© Szabó, Zs. (2021): Cybersecurity issues in power systems. In Kelemen-Erdos, A., Fehér-Polgar, P., & Popovics A. (eds.): FIKUSZ 2021 Proceedings (pdf) ISBN 978-963-449-274-0, Obuda University, Keleti Károly Faculty of Business and Management, 252 p. pp. 241-251., 11 p.
<http://kgk.uni-obuda.hu/fikusz>

security incidents in the energy sector has increased in recent years. These facts absolutely highlights the key role of security of power system (Görgey, 2020):

The lessons learned from the attacks on the Ukrainian electricity system have been presented and analyzed in a number of reports, studies and articles. Most of these cases have been examined from the cyber security the point of view. One of the possible reasons for this professional imbalance is that there is no current protocol for with incidents affecting the electricity system with cyber security and energy aspects together. Already the target choices of the 2015 attack indicated that the attacker had a thorough knowledge of the electricity supply process and its practical details. But when analyzing what happened in the 2016 attack, we know for sure, that although the attacker had a clear knowledge and plan for physically damaging the attacked power grid, the criminals could not cause actual physical damage due to their encryption error. The analysis of the 2016 attack showed that an effective analysis of a cyber attack on the electricity system is only possible in close cooperation involving all the disciplines affected by the attack, including electricity professionals. There had been no protocol for this integrated approach to incident investigations before this incident.

3 The risks and challenges of deploying power systems

Electricity has undergone tremendous development in recent decades. In the last century, it was still completely natural to check all instruments manually, record the data they measured on paper, and use the fewest digital instruments in the various processes. However, technological innovations and the opportunities they offer quickly spread to the sector, as it became possible to perform increasingly complex tasks in an increasingly shorter period of time, and the sector is now highly IT-dependent (Kralovánszky, 2019).

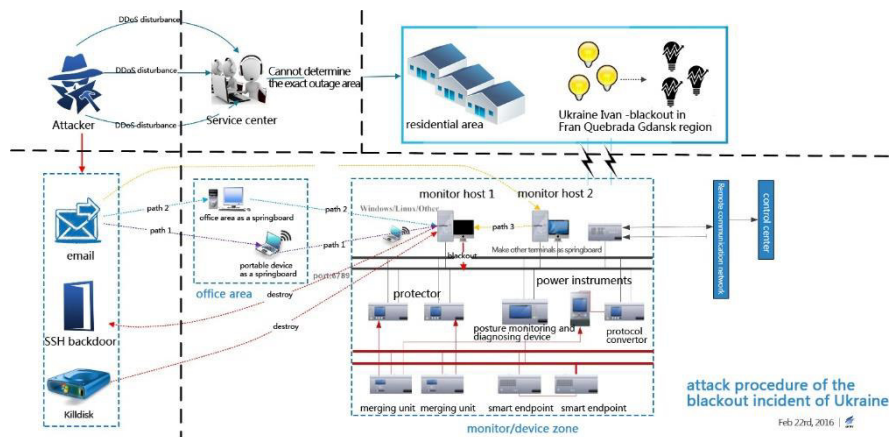


Figure 2 Attack procedure of the blackout incident of Ukraine

Source: Antiy Labs (2016) available: <https://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks/>

But as in all sectors, including electricity, the spread of new - computing - innovations has created more and more cyber security vulnerabilities, so much so that the possibility of cyber-attacks is now a growing threat to the sector. The first “warning” for this was given by Stuxnet in 2010 (David, 2013). The attack exploited 4 different Windows 0-day vulnerabilities to spread a malware and replaced the WinCC DLL with a man-in-the-middle attack against PLCs (Programmable Logic Controller) controlling uranium enrichment centrifuges. The significance of this attack lay in the fact that it was the first cyber attack that also caused physical damage to the attacked system. In 2016, an attack on the Ukrainian electricity grid took place along a similar principle (Antiy Labs, 2016).

On December 17, 2016, there was a 24-hour power outage in Ukraine, affecting nearly 250,000 households. The paralysis of the Ukrainian electricity network, like Stuxnet, was caused by a malware identified as Win32 / Industroyer (Todros, 2018). The attacker attacked the substation of the Ukrainian electricity system near Kiev (Pivnichna North). It should be noted that prior to the attack, several images and videos were uploaded to the Internet in connection with the renovation of the substation, which presumably facilitated the attack using OSINT (Open Source Intelligence) methods. The attack affected only one substation, but caused 200 MW of lost power. Industroyer/CrashOverride is a modular malware. Its danger lies in its ability to directly control the switches and circuit breakers of the power substation, so it can operate automatically, with the slightest manual intervention by attackers (Todros, 2018). It uses industrial communication protocols that are used in other supply infrastructures, transport management systems and other critical networks (water, gas) worldwide, so Industroyer/CrashOverride malware

can be used with virtually any change to attack any other ICS (Industrial Control System) (Pongrátz, 2020).

The key to this is to leave a backdoor open for an attacker to install, control, remotely connect to, receive, and send commands to. And the program code used by the malware shows that their writer has serious professional knowledge of how industrial control systems work. It should be emphasized that in the case of Industroyer/Crashoverride we are not talking about a single attack, but a series of attacks (Todros, 2018). It is also interesting to think about the fact that the extent of the damage caused by cyber attacks today does not depend on the attacker's abilities, but rather on his intentions.

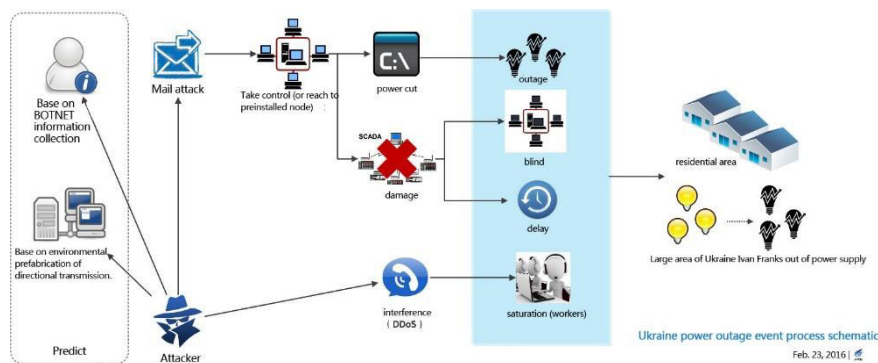


Figure 3 Summary of Ukraine power outage attacks

Source: Antiy Labs (2016) available: <https://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks/>

In terms of industroyer, therefore, much greater damage could have been done by the attacker (see Fig. 3). Yet Joe Slowik's analysis in 2019 shows that the attack would not have ended in disruption, but that the attackers may have had the additional goal of conducting a much larger-scale attack in parallel with disabling substation defenses (Slowik, 2019). According to Slowik, the attackers were prepared to disable more protection with DoS (Denial-of-service attack) attacks after Uskenenergo's work restored the service after causing the disruption, and then the substation equipment thus left vulnerable could even suffer fatal damage in the event of an overload. months, half a year, could have caused power outages. According to the analysis, this did not happen in the end just because the attackers made a mistake in developing the computer code used for the DoS attack (Pongrátz, 2020). That is, the attack was a series of attacks that presumably did not achieve their original purpose, presumably due to the attackers' fault. The vulnerability and inadequate protection of electricity systems has been repeatedly demonstrated, which has affected the daily lives of society. As I mentioned above, several images and videos were uploaded to the Internet prior to the attack, which may have helped make the attack more accurate. This is because, for political reasons, the media



gained insight into the substation, as the power at the time wanted to boast of the investment. This is a good example of the fact that electricity supply, like other critical infrastructure, should not be intertwined with political interests.

4 The human firewall and cyber awareness program

Last year and this year was a year of blackmail viruses, and all indications are that this type of threat has reached its peak. However, cybercriminals are not expected to give up this lucrative source next year, and will even expand the pool of opportunities. Experts predict that the number of newly discovered blackmail virus families will increase as criminals look for new targets: industrial systems and power systems will be targeted. Even the best-built enterprise system cannot be protected if only one person is responsible for security. Experts believe that the only solution is to regulate users. The most significant vulnerability is the human side (Szabó, 2018). What is the solution to the restructuring of the existing system? The answer seems obvious: on the one hand, new rules are needed, and, on the other, compliance with the rules needs to be promoted.

The 'human firewall' is more effective than anything else. It is not enough to deal with the 'human factor' at one level only. Secure corporate IT has more human aspects than you might think. So we need to look not only at systems, but also at people. The product of system you buy does not protect itself, even if you buy the best on the market. IT security is not a product but a state (Beláz - Szabó, 2020). It must be achieved, and, very importantly, further sustained through action; it must be operated. For proper regulation, information security must be ensured from hardware, software and communication, i.e. systems (physical layer), people (personal layer - training, what to do and why it is important) and processes (organizational layer - broken down into specific corporate actions; who pulls the plug, if necessary, who reports, etc.).

The critical issues are data leakage (when a colleague, for example, accidentally takes out sensitive data, e.g. sending a complete customer list instead of a quote) or denial of service. The latter can be crucial in the age of cloud computing. So the 'human factor' is an integral part of IT security. To increase the level of IT security in the organization, we need to keep our colleagues as well as the machines operating as necessary (Beláz - Szabó, 2020). That's why state-of-the-art computing says that the chain of security awareness for people, employees, is the human firewall - and in addition to the technical firewall, the human firewall must be made.' Based on the above, it is necessary to raise the security awareness and up-to-date information of the managers and employees of the organizations and to prepare them for the recognition of emergencies (ENISA, 2021). Based on international and domestic recommendations information security awareness



© Szabó, Zs. (2021): Cybersecurity issues in power systems. In Kelemen-Erdos, A., Fehér-Polgar, P., & Popovics A. (eds.): FIKUSZ 2021 Proceedings (pdf) ISBN 978-963-449-274-0, Obuda University, Keleti Károly Faculty of Business and Management, 252 p. pp. 241-251., 11 p. <http://kgk.uni-obuda.hu/fikusz>

material for users is warranted. The purpose of the training is not to communicate and account for lexical knowledge, but to transfer knowledge that can be used in practice.' The awareness program contains basic IT security knowledge and real-life examples. These can help you identify IT security risks and effectively contribute to the implementation of security measures to prevent dangerous situations, damage, and security. Our motto is: 'Understand, know, and do so.'

5 The cybersecurity manual for electricity

Finally, in the framework of the cooperation between SeConSys (Security for Control Systems) - in addition to mentoring National University of Public Service (NKI) and the Hungarian Electrotechnical Association (MEE) a Cyber Security Handbook for Electrical Industrial Surveillance Systems was published by the National Cyber Defense Institute. SeConSys is a new type of PPP (Public Private Partnership) collaboration to strengthen the cyber security of the electricity system. SeConSys collaboration has been defined by members as a platform without legal personality, as a voluntary, non-profit, form of professional collaboration for members. The current goal is to create a system of recommendations to strengthen the cyber security of the electricity system. The manual (see Fig. 1) is available on the SeConSys website (www.seconsys.eu) and can be downloaded from there.



Figure 4 The cybersecurity manual for electricity

Source: SeConSys (2020) available:

https://seconsys.eu/wp-content/uploads/2021/05/20201208_SeConSys_kezikonyv_final_ONLINE.pdf



Conclusion

Overall, Industroyer/CrashOverride malware is the fourth malware designed specifically against ICS (after Stuxnet, BlackEnergy, and Havex) and the first known malware created specifically to attack the power system. Its danger is raised to a high level by its modularity and high degree of autonomy. After Stuxnet, Industroyer/CrashOverride was the second malware targeting ICS that was able to disrupt ICS-driven physical processes without human intervention. Due to the current electricity situation in Europe, the conditions for conducting an APT (Advanced Persistent Threat) attack like the one above are more favorable than ever, as the resilience has been significantly reduced and the pronunciation of a single battery can cause a great deal of chaos in Europe. That is why preparedness against this type of attack would be particularly important, at least at national level, but even at European level. The material damage to civilian and state-owned companies is estimated at more than \$10 billion worldwide, but a critical infrastructure under the control of terrorist, unauthorized hacker groups could generate unforeseen dangers, disregarding national borders. If the smuggling of malicious code capable of blocking or manipulating the control system of a nuclear power plant succeeds, it could lead to a global problem, triggering a chain reaction that could have serious consequences. It is important that power plants, as critical infrastructure, meet the required information security requirements.

Some of the electricity systems in use today operate along infrastructure that has been in place for decades and is probably outdated to meet today's expectations, so it is important to keep modernization in mind. The aim should be to reduce and possibly eliminate the interdependence of critical infrastructures and to focus on protection. Reserves must be maintained that can be deployed in times of turmoil and will not allow chaos to prevail. It is very important to prevent or at least reduce disaster. It is true that this requires modern regulation and a lot of work, but it pays off many times over through the devastation that has been left behind. You need to be prepared to deal with external and internal crises with plans, exercises, ongoing training, and lifelike simulations. The main economic factors of the future are cities. Unfortunately, globalization and urbanization are facts that are very difficult to change. The cities high level of dependence on the infocommunication and power systems and the services they provide. The infocommunication and power systems and other electronic systems pose threat serious security risks everywhere in the world. Finally, we would like to make some suggestions:

- We recommend the minimum secure systems conditions that are essential to being in cyberspace.
- We recommend reinforcing the human firewall such as experience-based education.



References

- [1] Antiy Labs (2016): Comprehensive Analysis Report on Ukraine Power System Attacks. Downloaded: 26/11/2021. <https://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks/>
- [2] Beláz, A. - Szabó, Zs. (2020): The human firewall - The human side of cybersecurity. CYBER SECURITY REVIEW Szeptember pp. 1-7. Downloaded: 27/11/2021. <https://www.cybersecurity-review.com/wp-content/uploads/2020/09/Annama%CC%81ria-Bela%CC%81z-and-Zsolt-Szabo%CC%81-article-Cyber-Security-Review-online-September-2020.pdf>
- [3] Bonnyai, T. – Görgey, P. – Krasznay, Cs. (szerk.) (2020): Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve. SeConSys. NBSZK NKI. Budapest. ISBN 978-615-00-9827-2. pp. 1-243. Downloaded: 28/11/2021. https://seconsys.eu/wp-content/uploads/2021/05/20201208_SeConSys_kezikonyv_final_ONLINE.pdf
- [4] David, K. (2013): The real story of Stuxnet. IEEE Spectrum for The Technology Insider. 26 Feb 2013. Downloaded: 27/11/2021. <https://spectrum.ieee.org/the-real-story-of-stuxnet#toggle-gdpr>
- [5] ENISA (2021): Raising Awareness of Cybersecurity. November 29, 2021. Downloaded: 01/12/2021. <https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity>
- [6] Görgey, P. (2021): Kibertámadások Ukrajnában: áramszünetek és tanulságok (II. rész). Elektrotechnika 110. évfolyam 2020/11. pp. 22-24.
- [7] Görgey, P. (2020): Elkészült a villamosenergetikai kiberbiztonsági kézikönyv. Downloaded: 29/11/2021. <https://www.ludovika.hu/blogok/cyberblog/2020/12/22/elkeszult-a-villamosenergetikai-kiberbiztonsagi-kezikonyv/>
- [8] Joe, S. (2019): CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. Dragos Inc. August 15, 2019. Downloaded: 30/11/2021. <https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf>
- [9] Kralovánszky, K. (2021): A kibertér fejlődése (második rész) - Kiberműveletek és kritikus infrastruktúrák egyes kapcsolatai. Hadmérnök 16. évfolyam (2021) 1. szám 145-160. DOI: 1032567/hfTL2021.1.9. pp. 1-15.



© Szabó, Zs. (2021): Cybersecurity issues in power systems. In Kelemen-Erdos, A., Fehér-Polgar, P., & Popovics A. (eds.): FIKUSZ 2021 Proceedings (pdf) ISBN 978-963-449-274-0, Obuda University, Keleti Károly Faculty of Business and Management, 252 p. pp. 241-251., 11 p.
<http://kgk.uni-obuda.hu/fikusz>

- [10] Kralovánszky, K. (2019): A villamosenergia-rendszer kiberés nemzetbiztonsági kockázatai (1. rész). NEMZETBIZTONSÁGI SZEMLE 7. évfolyam (2019) 3. szám 40–57. • doi: 10.32561/nsz.2019.3.4 pp. 40-57.
- [11] Pongrátz, P. (2020): Incidens katalógus (2020 októberi állapot). Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve. NBSZK NKI. Budapest.
- [12] Monica, T. (2018): CRASHOVERRIDE: The Malware That Attacks Power Grids. Recorded Future January 10, 2018. Downloaded: 30/11/2021. <https://www.recordedfuture.com/crashoverride-malware-overview/>
- [13] Neumann János Számítógép-tudományi Társaság (2018): Gyurka bácsi és a „humán tűzfal”. Downloaded: 30/11/2021. <https://njszt.hu/hu/news/2018-06-18/gyurka-bacsi-es-human-tuzfal>
- [14] Neumann János Számítógép-tudományi Társaság (2014): Vasvári György portréja. Downloaded: 30/11/2021. https://www.youtube.com/watch?v=ewslw1ez0_U
- [15] Szabó, Zs. (2018): Cybersecurity issues in industrial control systems, IEEE 16th International Symposium on Intelligent Systems and Informatics: SISY 2018. IEEE Hungary Section, 2018. pp. 231-234.