

Shared Service Processes for the Information Security in the Smart Grid of the Future

Asiye Öztürk

Abstract—With the structural change in the electrical energy supply, supply-related processes and procedures are increasingly being modified. Due to the gradual decentralization of electrical energy generation and the network expansion required for this, new requirements are being placed on the electrotechnical processes and the information and communication technology processes. A currently promising concept for solving these challenges in favor of transmission operators and distribution system operators is the integration of a so-called virtual power plant. Virtual power plants act as an integral part of the future electrical supply system between the critical infrastructure and the distribution network operators as well as transmission system operators in the field of remote monitoring and remote control of decentralized energy generation systems. With the classification of a virtual power plant as a critical infrastructure, the importance of these entities as an active member of the German electrical energy system in the interest of compliance with electrical and information technology security is explicitly emphasized. As a critical infrastructure, virtual power plants are committed to achieving a minimum level of information security. Chapter 6.1.3 of DIN EN ISO/IEC TR 27019:2020 recommends that virtual power plants maintain contacts with certain Computer Emergency Response Team organizations. However, it turns out that there is currently no organizational model for a computer emergency response team that focuses on virtual power plants in targeting its target group. Thus, the main goal of the present elaboration is the completion of a scientifically based approach, which deals with the efficiency of a possible solution to the problem of designing integrative security processes for the provision of Computer Emergency Response Team services, which is growing out of practical relevance to be solved in virtual power plants. The assumption here is that there is a need for research at this point about the challenges of the energy transition that have not yet been clearly presented.

Index Terms—Computer emergency response team, critical infrastructure, information security, virtual power plants

I. INTELLIGENT POWER GRIDS OF THE FUTURE

The structural and technical modification of the future electrical power supply affects the two fields of action of the power supply network. The primary field of action can be characterized by the term “system” or “network” and includes the predominantly electrotechnical and information technology functions that serve to ensure a secure energy supply and are used, among other things, within the framework of network operation and network management. The secondary field of action “market” specifies the energy management processes, which focus on the definition of

products, business models, actors, and roles. As a result of structural change, these latter fields of action are growing closer together. The interaction between supply and demand of electrical energy will thus be networked and regulated in the future via the exchange of information at all network levels [1].

Due to the gradual decentralization of electrical energy generation and the network expansion required for this, new requirements are being placed on the electrotechnical and information and communication technology processes. For example, the so-called Transmission System Operators (TSOs) and Distribution System Operators (DSOs), who act as active players in the energetic electricity supply, must reckon with new intelligent instances whose integration entails an increase in complexity. Thus, the second characteristic aspect of the energy transition is the increasing degree of complexity [2]. On the generator side, in addition to the players described above, the TSOs and DSOs, there are numerous decentralized energy generation systems, which are currently estimated at around 2.2 million solar systems in Germany [3]. This results in the integration of volatile energy production based on renewable energies, which means that the comprehensive installation and operation of intelligent monitoring and control systems on the generator side is of great importance. A logical conclusion from the increasing number of network users is the proportional increase in interfaces. The energy supply system, which has been marked as obsolete, now defines new requirements with a manageable number of members, many network users, market users and multidirectional interfaces that require additional dynamic system control and system monitoring. To do justice to the increasing degree of complexity and thus be able to guarantee a safe and trouble-free power supply, new concepts and system structures must first be configured and implemented. The focus of the future network is therefore on the intelligent network integration of producers, consumers and network users, the aim of which is to ensure a sustainable, economical, and secure power supply.

II. VIRTUAL POWER PLANTS AS A NEW ROLE DEFINITION

To be able to regulate the volatile load flow and generation situations, intelligent system interventions must be designed and implemented. Furthermore, the increasing importance of the role of the prosumer poses an additional challenge. The process of grid restoration now depends not only on the number of increasing players and decentralized systems, but also on the power consumption and power generation of the smart grid users. Here, an elaboration of concrete forecasts within the scope of the supply restoration concept is to be included.

A currently promising concept for solving the above

Manuscript received May 22, 2023; revised June 16, 2023; accepted June 30, 2023.

The author is with Clavis Institute for Information Security, Niederrhein University of Applied Sciences, Krefeld, Germany. E-mail: asiye.oeztuerk@hs-niederrhein.de

challenges is the integration of a so-called Virtual Power Plant (VPP). A VPP is a power plant that consists of several generating units, reactive loads or power storage systems and monitors the generated power and feeds it into the power grid in a bundle [4].

VPP are divided into the following four core components: controllable generation plants, weather-dependent feed-in generation plants, storage, and controllable loads [5].

III. INFORMATION SECURITY IN THE ENERGY SECTOR

If we look at the increasing number of people involved in the energy network of the future, this increased number of people involved, i.e., the central and decentralized energy producers, energy suppliers and consumers, network operators, metering point operators and service providers and customers in a network, can be seen as potential attack vectors for cyber-attacks are considered. On December 23, 2015, a targeted, meticulously planned cyber-attack on the Ukrainian power grid took place, after which three power distribution system operators with a high degree of automation were disconnected from their substations and local network stations. The attackers managed to install and execute malware on systems with obsolete software versions. At least 225,000 residents were affected by a power outage lasting several hours [6]. Due to the intentional compromise of the network control system WinCC (Supervisory Control and Data Acquisition (SCADA) system), which is used for remote monitoring and remote control of the decentralized units, the central processes in the network control center could no longer be executed. To compensate for the system failure and the restart of the substations, the switching operations had to be controlled manually on site in the substations. As a result, power was restored more slowly. The assumption that can be incorrectly derived from the above cyber-attack is the assumption or the conclusion that obsolete systems represent a potential attack vector due to their already outdated security mechanisms. In comparison, new IT systems (hardware) and software components can no longer prove these security gaps. In addition to technical weaknesses, there is also a weakness that functions in the role of humans. Because people are also defined as the most important risk factor. Examples such as BlackEnergy in the energy sector or WannaCry in the healthcare sector have shown the impact of not considering the human role as a hazard [7–10]. The IT Security Act 2.0 (IT-SiA) refers to Section 11 (1a) of the Energy Industry Act and classifies network operators as operators of Critical Infrastructures (CRITIS). This classification is independent of the defined values that are presented in the Federal Office for Security in Information Technology CRITIS regulation. This type of consideration implies the maintenance and safeguarding of the information technology components that are used within the framework of network operation and network management. This classification obliges energy suppliers to ensure and continuously maintain a minimum IT security level. according to the IT-SiA and according to § 11 paragraph 1a of the Energy Industry Act with the implementation of an information security management system according to the requirements of the international standards DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27002, and DIN EN ISO/IEC TR 27019 as well as IT requirements

-Security Catalog of the Federal Network Agency is to be achieved. Ultimately, VPP interact as an integral part of the future electrical supply system between CRITIS and the distribution network operators as well as transmission system operators in remote monitoring and remote control of the decentralized energy generation systems. With the classification of a VPP as CRITIS, the importance of these authorities as an active member of the German electrical energy system is explicitly emphasized, particularly in the interests of compliance with electrical and information technology security. The primary perspective is aimed at securing and maintaining the energy supply and thus the availability of electricity, which equivalently also requires the availability of electrotechnical and information technology systems due to the technical interlocking. One of the essential elements in terms of ensuring the availability of Information and Communications Technology (ICT) systems (hardware and software components) is the effective cooperation and coordination of system administrators and IT managers. In addition, the active monitoring of the system behavior is also part of it, since the structured and organized process flows enable a forward-looking and fast-reacting handling of information security incidents. This approach is the response to dealing with the IT security incidents of the cyber worm “Morris”, which attacked a wide range of global ICT systems in the late 1980s. As a result of the serious cyber-attack, the first approaches to a Computer Emergency Response Team (CERT) were designed, which still occur today in different forms and variations [11].

IV. COMPUTER EMERGENCY RESPONSE TEAMS IN THE ENERGY SECTOR

A Computer Emergency Response Team (CERT), also called Computer Security Incident Response Team is a team of IT security experts or professionals whose core process is to manage computer security breaches for a selected target group by offering preventive, reactive and detective services. Offered preventive, reactive and detective services support the achievement of goals. The fact that the topic of CERT is also an important topic in general based on empirical practice is shown primarily by the enactment of the so-called Network and Information Security Directive (NIS Directive 1+2), which is the first legal regulation to deal with the challenge of cyber security at European level was adopted in 2016 and version 2 will be published shortly. The guideline defines a common approach to information security and prescribes certain obligations and rules for CRITIS operators to establish a high level of security for network and information systems. To this end, the member states must, among other things, develop a national NIS strategy, introduce safety measures, and report major incidents. Each Member State must also set up one or more CERTs, which are responsible for tasks such as receiving cyber security incidents, issuing early warnings, responding to security incidents, and dynamically analyzing risks and incidents. However, the regulations of the guideline are universal and not designed explicitly for the energy sector [12].

Holzleitner *et al.* [12] analyzes the NIS Directive about the energy sector and state that certain regulations are in place, but do not apply specifically to the energy sector. Annex II of the directive lists the electricity and gas suppliers as well as

the electricity or gas distribution or transmission system operators as operators of essential services for the energy sector. Article 7 of the directive specifies requirements for the creation of a national strategy for network and information systems. The energy sector is also not explicitly mentioned here, so that the Member States can decide for themselves which of the measures are to be supported for individual sectors.

Chapter 6.1.3 of DIN EN ISO/IEC TR 27019:2020 therefore expressly recommends that VPP maintain contacts with certain CERT organizations. Since energy networks are very complex and, according to [12], require specific measures about their information security, it is first determined whether CERT models exist explicitly for the energy sector, which consider the special features, services, and infrastructure of this sector.

For this purpose, the CERT landscape in the energy sector is examined. For this purpose, the following research question is defined: What does the current national and international CERT landscape look like in the energy sector?

V. RESULTS

The sequencing of the CERT units is based on the table published by ENISA in [13]. ENISA is a center of excellence for cybersecurity in Europe and is based in Greece. Since its creation in 2004, ENISA has been actively contributing to a high level of network and information security in the Union, developing a culture of network and information security in society and raising awareness of network and information security. In the annual CSIRT inventory, ENISA provides an overview of the current situation of the CERT units in Europe. The CSIRT inventory contains a list of publicly listed CERT entities that can be traced using an interactive mapping tool.

The presentation of the individual mission statements and the services (Column Mission Statement & Services) is in turn based on the content specified on the individual websites of the CERTs, whereby the presentation is structured according to a uniform scheme. For a better understanding, the schematic structure of the CERT listing is first specified using the following listing (Fig. 1). A concise conclusion follows after listing the CERTs.

On this basis, in the next step, all internationally and nationally active CERT units were filtered and analyzed about their mission statement. A concise overview of the study follows (Fig. 2).

The evaluation of the national and international CERT units shows that the target group of commercial organizations ranks highest. These include organizations such as Siemens, the Lufthansa Group, the energy company E. ON and XING. A major reason for this may be the increasing integration of networked computer technology in the free market economy. Many commercial business models are now digital, so that IT plays an eminent role as a basic innovation in the generation of new business areas.

Regarding our object of investigation (sector energy) from an international perspective, there are six CERTs that specifically address the target group. In Germany there is currently no CERT specifically designed for the needs of players in the energy sector.



National	National CERTs (Germany) 
International	Internationally active CERTs 
Column: Description	CERT – name
Column: Mission Statement	The mission statement outlines the basic intentions and defines the objectives, scope and limits of the CERT and aligns its support concept with its potential target group.
Column: Constituency	The target group results from the assignment of the own information of the CERT organizations. These can be defined as follows:
CIIP	Critical Information Infrastructure Protection.
Commercial Organization	Commercial organizations. This includes only for-profit organizations.
Non-Commercial	Non-profit organizations. This includes only non-profit organizations.
Energy	Companies and organisations operating in the energy sector.
Financial	Companies and organizations operating in the financial sector.
Government	State and municipal organizations operating in the administrative and government sectors.
ISP Customer Base	Companies and organizations (Internet service providers) operating in the ICT sector.
Law Enforcement	State organizations operating in the administrative and state sectors in the field of law enforcement and prosecutors.
Military	Government organizations operating in the administration and government sectors in the defence and military sectors.
NREN	Government organisations assigned to the Research and Education Department.
Service Provider Customer Base	Companies and organizations belonging to the service sector.
Vendor Customer Base	Companies and organizations that are assigned to the logistics sector.
Column: DL	P – Preventive services R (1) – Reactive services R (2) – Reactive services remotely D – Detective services

Fig. 1. Schematic structure.



Constituency			Σ
CIIP	14	2	16
Commercial Organization	103	13	116
Non-Commercial Organization	10	0	10
Energy	6	0	6
Financial	74	4	78
Government	57	7	64
ISP Customer Base	45	1	46
Law Enforcement	4	1	5
Military	12	3	15
NREN	73	4	77
Service Provider Customer Base	38	7	45
Vendor Customer Base	24	2	26

Fig. 2. Results of the investigation.

At the current time of the analysis, the CSIRT inventory contains a total of 695 CERT entries worldwide. There are only 6 specific CERTs for the energy sector (Fig. 3).

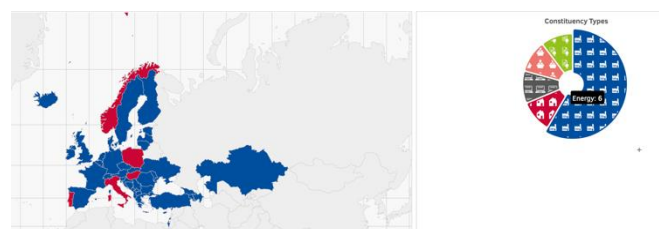


Fig. 3. CSIRT-Inventory: Sector energy [13].

Shared CERT services in the energy sector. The classic shared service concept describes an approach to providing internal services for multiple organizations by sharing resources. The shared services refer to supporting, thus non-value-adding and non-strategic services. Shared services are typically provided by shared service organizations (SSO), which can be assigned to the areas of IT and procurement, among other things [14]. The shared service approach, considering the required CERT services, can be presented as follows (Fig. 4):

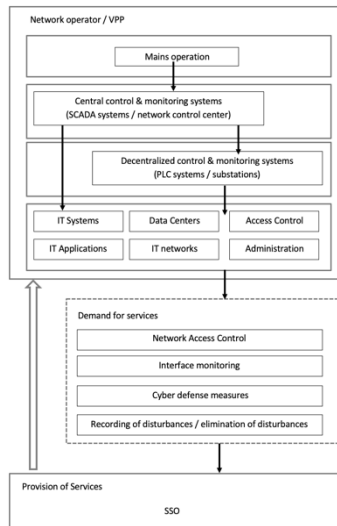


Fig. 4. Shared Service in network operation.

The technical requirement for the use of a CERT as a common cyber defense platform can be substantiated, among other things, by the fact that the complexity and dynamics of the current IT systems and cyber-attacks require a time-consuming and forensic investigation of the anomalies that have occurred. This results in significant costs for the organizations concerned. However, if one looks at the costs for the systematic analysis and elimination of security incidents in an operationalized manner, it becomes clear that the costs were largely invested in dealing with identical security issues [15].

The research [15] also states that security processes in companies such as the SSO process of the German Cyber Security Organization GmbH, which was founded as a subsidiary of Allianz, BASF, Bayer, and Volkswagen, have become far more cost-effective and effective and efficient solutions to cybersecurity problems. This approach serves to improve operational cybersecurity. On the one hand, organizations can integrate a much more cost-effective and therefore more economical security model, which allows for more effective and efficient solutions to cyber security problems. On the other hand, these constructs lead to the bundling of specialists and know-how forces and thus to an increase in synergies.

In addition to the efficiency and effectiveness of the professionalism and effectiveness of CERT organizational models, the economic consideration also plays a major role in the success of these models.

The economic orientation of CERT organizational models is different regarding to the organizational structure. One possibility is corporate CERTs, which were set up by the

organizations themselves for corporate purposes and are usually financed by them. These CERTs serve as the company's outsourced service providers. Parts of the services are thus outsourced to the internal department or organizational unit. Examples of company CERTs are the CERTs from Vodafone Group Services GmbH, IBM or XING. In addition to company CERTs, there are also global and national CERTs such as the CERT association, the Bayern-CERT or the CERT-NRW, which are financed by the state.

VI. CONCLUSION

What conclusions can be drawn from the results that have already been identified and evaluated, which point in detail to a factual deficit?

The presentation of the existing national and international CERTs and CSIRT entities listed in Fig. 1 leads to the following conclusion: A closer look makes it clear that the topic of CERTs for critical infrastructures represents little application in practice. A total of 16 CERT organizations deal with the target group of the CIIP both nationally and internationally. A specific consideration of the energy sector shows that only six out of a total of 695 CSIRT entries are assigned to the energy sector. [16] provides an important finding: Although CERTs are widespread in Europe and provide services for all areas of activity, very few focus on incident management and information exchange in the energy sector. [16] also justifies it by saying that the exchange of information and communication are more difficult and that understanding of the topic of information security does not have the required relevance and importance. The SSO approach serves to use shared resources. The advantages that result from this are, on the one hand, the effective solution of problems through a bundling of specialists as well as a presentation of all services that are offered by a CERT. In conclusion, the investigation shows that there is currently no standardized CERT model that takes up the specific requirements of a VPP at a high level of abstraction and treats them appropriately. Existing CERTs, which in their mission statement are explicitly aimed at the target group of energy suppliers, do not indicate any possible extensions or approaches to the subject of VPP.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

- [1] J. Scheffler, *Distribution Grids on the Way to the Area Power Plant*, Springer Berlin/Heidelberg, Germany, 2016.
- [2] E. Forstmeier and R. Hänlein "The power grid of the future," in *German Environmental Aid*, 2nd updated ed., October 2011, pp. 1–9.
- [3] Destatis. 2.2 million photovoltaic systems installed in Germany. [Online]. Available: https://www.destatis.de/DE/Presse/Pressemitteilungen/2022/06/PD22_N037_43.html
- [4] A. Öztürk and E. Koza, "A literature review to analyze the state of the art of virtual power plants in context of information security," in *Advances and New Trends in Environmental Informatics*, Wohlgemuth, V. Naumann, S. Behrens, G. Arndt, Eds. HK. Progress in IS. Springer, Cham, 2022.
- [5] VISE, "Regional virtual power plants," *Virtual Institute Smart Energy*, pp. 1–139, 2021.

- [6] X. Huang, Z. Qin, and H. Liu “Survey on power grid cyber security: From component-wise vulnerability assessment to system-wide impact analysis,” *IEEE Access*, vol. 6, pp. 69023–69035, November 2018.
- [7] E. Koza “Information security awareness and training as a holistic key factor—How can a human firewall take on a complementary role in information security?” in *Proc. International Conference on Human Factors in Cybersecurity, AHFE 2022*, AHFE Open Access, 2022, vol 53.
- [8] R. Rohan, S. Funilkul, D. Pal, and W. Chutimaskul, “Understanding of human factors in cybersecurity: A systematic literature review,” in *Proc. IEEE 2021 International Conference on Computational Performance Evaluation (ComPE)*, 2021, pp. 133–140.
- [9] J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph, “Towards an Improved understanding of human factors in cybersecurity,” in *Proc. of the 1st International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS) and the 5th International Conference on Collaboration and Internet Computing (CIC)*, IEEE, Piscataway, N. J., 2019, pp. 338–345.
- [10] M. Barrère, C. Hankin, N. Nicolaou, D. G. Eliades, and T. Parisini, “Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies,” *Journal of Information Security and Applications*, vol. 52, 2020.
- [11] ENISA European Network and Information Security Agency, “Establishing a CSIRT step by step” in Outcome WP2006/5.1, 2006.
- [12] M. T. Holzleitner and J. Reichl, “European provisions for cyber security in the smart grid—An overview of the NIS-directive,” *Springer Verlag Vienna*, vol. 1, pp. 14–18, January 2017.
- [13] ENISA. European network and information security agency: CSIRTs by country—Interactive map. [Online]. Available: <https://www.enisa.europa.eu/topics/incidence-response/csirt-inventory/certs-by-country-interactive-map>
- [14] C. V. Glahn and M. Schomann, “From shared services to portal services,” Ph.D. dissertation, Gabler/GWV Fachverlage GmbH, Wiesbaden, 2003.
- [15] Fraunhofer SIT Fraunhofer Institute for Secure Information Technology: Technical Report, “Position paper on cyber security in Germany,” Fraunhofer Verlag, 2017, pp. 1–22.
- [16] ENISA European Network and Information Security Agency, “Report on cyber security information sharing in the energy sector,” Version 1.1, November 2016, pp. 1–71.

Copyright © 2023 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited ([CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)).