# State of Research: Relevance of Computer Emergency Response Teams in Operational Technology

**Asiye Öztürk**
University of Wuppertal, Germany
Clavis Institute for Information Security

Asiye.oeztuerk@hs-niederrhein.de

**Abstract:** The increasing integration of Information Technology (IT) and Operational Technology (OT) in industrial environments has led to increased vulnerability to cyber threats. This article examines the need for a dedicated Computer Emergency Response Team (CERT) for OT to ensure the security, integrity, and resilience of critical infrastructure, particularly in the energy sector. OT is subject to specific challenges that differ from those in traditional IT networks. Cyberattacks on OT systems can not only cause financial losses, but also have a significant impact on physical security and the environment. A specific CERT for OT is necessary to address the unique characteristics of these environments. This requires expertise in industrial protocols, control systems and SCADA systems. The CERT for OT should be able to respond quickly to security incidents, perform forensic analysis and implement effective countermeasures to ensure business continuity. Research shows that implementing a specialized CERT for OT leads to improved threat detection, faster response, and more effective defense against attacks. In addition, this article emphasizes the importance of collaboration and communication between IT and OT security teams to ensure comprehensive system resilience. The following article provides a detailed literature analysis that comprehensively examines the current state of research on CERTs in the context of OT. The analysis of the relevant literature highlights the increasing threat to OT systems and emphasizes the specific requirements arising from the integration of IT and OT. By identifying research gaps and summarizing current findings, this article provides a comprehensive overview of the existing literature on this topic.

**Keywords:** Computer Emergency Response Teams, CERT, CRITIS, OT, Information security, Energy

## 1. Introduction

With the structural change in the electrical energy supply, numerous supply-related processes and procedures are increasingly being modified. The structural and technical modification of the future electricity supply affects the two fields of action of the electricity grid. The primary field of action can be characterized by the term “system” or “grid” and includes the predominantly electrotechnical and information technology functions that serve to ensure a secure energy supply and are used, among other things, in the context of grid operation and grid management. The secondary field of action “market” specifies the energy industry processes, which focus on the definition of products, business models, players, and roles. As a result of structural change, these latter fields of action are growing closer together. The interaction between the supply and demand of electrical energy will therefore be networked and regulated in future through the exchange of information at all grid levels.

One of the fundamental characteristic aspects of the energy transition is the paradigm shift triggered by the Renewable Energy Sources Act and the Paris Climate Protection Agreement towards the decentralization of electricity generation using renewable energy sources within the “grid” field of action. During the paradigm shift, nuclear and fossil primary energy sources are gradually being replaced by renewable energies. Offshore plants (wind farms) at sea and photovoltaic plants are the new large-scale producers that are connected directly to the extra-high voltage grid and are increasingly forcing conventional large-scale power plants off the grid. These feed the electricity they generate into the extra-high-voltage grid and transmit it over long distances to the high-voltage grid, where large, intensive industrial consumers are connected. Medium-sized energy generation plants are connected to the medium-voltage grid as producers and medium-sized consumers (e.g. hospitals), which feed in or draw their electricity from here.

Small producers such as biogas consumers who use animal and plant materials to generate energy are connected to the low-voltage grid and thus to the last level of the electrical distribution grid. End consumers who install photovoltaic systems on their roofs to generate electricity by converting solar energy are also connected. The gradual decentralization of electrical energy generation and the grid expansion required for this are placing new demands on electrical engineering and information and communication technology processes.

For example, the so-called transmission system operators (TSOs) and distribution system operators (DSOs), which act as active players in the energy supply, must reckon with new intelligent instances, the integration of which entails an increase in complexity. The second characteristic aspect of the energy transition is therefore the increasing degree of complexity (Dai et al, 2020, p. 565).

On the generation side, in addition to the actors described above, the TSOs and DSOs, there are numerous decentralized energy generation systems, which are currently estimated at around 3.7 million solar systems in Germany (CIO, 2024). This will result in the integration of volatile energy generation based on renewable energies, which means that the comprehensive installation and operation of intelligent monitoring and control systems on the generation side will play a key role. Furthermore, decentralization provides for the integration of so-called prosumers (producer + consumer), whose behaviour as "energy producers and energy consumers" no longer corresponds to the conventional passive role definition (BMWi, 2018, p. 107). This shows that in the future energy supply structure, a traditional separation between producers and consumers no longer seems appropriate and the typical producer-consumer image is increasingly disappearing. Accordingly, the increasing number of energy producers, energy consumers and grid users are equivalent to the increasing degree of complexity and can therefore be declared as the third characteristic of the energy transition.

A logical conclusion from the increasing number of grid users is the proportional increase in interfaces. With a manageable number of members, many grid users, market users and multidirectional interfaces, the energy supply system, which has been labeled obsolete, now defines new requirements that require additional dynamic system control and system monitoring. Another characteristic of future system interfaces is sector coupling, which contributes to the transfer of electrical energy to other sectors and can create synergy effects through efficient energy distribution (BMWi, 2018, p. 25).

To cope with the increasing level of complexity and thus ensure a safe and trouble-free power supply, new concepts and system structures must first be configured and implemented. This novelty must also be able to handle intelligent and dynamic monitoring and control of the multidirectional energy supply structure. The fourth aspect of the energy transition can thus be characterized under the term "digitalization". Digitalization addresses a broad spectrum of modifications that affect the following fields of application, among others:

- Electrical engineering
- Information technology
- Communication technology

Control technology networks electrical and physical signals, such as electrical voltage currents, with information technology hardware and software components. This allows physical signals and attributes in the form of logical measured values and system states (information technology) to be exchanged bidirectionally within a network via specific protocols (communication technology). Data is exchanged here between the central monitoring and control units (e.g. grid control center) and the decentralized field components (e.g. substations and transformer stations).

The focus of the future grid is therefore on the smart grid integration of producers, consumers and grid users, the aim of which is to ensure a sustainable, economical, and secure electricity supply. Similarly, Scheffler (2016, p. 13) defines the goal of the future energy supply system as the "networking and control of intelligent generators, storage facilities, consumers and grid equipment in energy transmission and distribution grids with the help of information and communication technology (ICT). The aim is to ensure a sustainable and environmentally friendly energy supply based on transparent, energy- and cost-efficient, safe, and reliable system operation".

The use of networked information technology and the increasing digitalization of the electrical supply structure thus serve to simultaneously ensure an intelligent, environmentally friendly, trouble-free, and secure power supply. While ICT processes are becoming more efficient with the use of ICT, the potential for ICT dependency is increasing at the same time.

## 2. Relevance of Information Security

An efficient energy supply is of crucial importance. An outage of electricity and gas would quickly have serious consequences, as public life and vital services would be affected. At the same time, the functionality of the energy supply is closely linked to well-functioning operational technology (OT). The increasing integration of interfaces in industrial environments (OT) has led to increased vulnerability to cyber threats.

In its policy brief "IT security in the energy industry" (2019, p. 3), the Virtual Institute Smart Energy (VISE) states that "the challenge posed by the convergence of process and control technology with information and communication technology systems (...) increases the potential threat of cyber-attacks. The fact that hardware systems in water or nuclear power plants, for example, have a very long service life and cannot simply be

replaced with more modern, more secure components for cost reasons, among others, does not improve the conditions".

Considering the increasing number of participants in the electricity grid of the future, this increased number of people involved, i.e. centralized and decentralized energy producers, energy suppliers and consumers, grid operators, metering point operators and service providers as well as customers in a grid, can be regarded as potential attack vectors for cyberattacks (VISE, 2019, p. 2).

The importance of information security is also reflected in the current legal landscape, which, following the introduction of the IT Security Act 2.0 (IT-SA) (July 2021), the publication of the Federal Office for Information Security Criticism Ordinance Part I (May 2016) and Part II (June 2017) and Section 11 (1a) of the Energy Industry Act, calls for the successive optimization and achievement of a minimum security level for Critical Infrastructure (CRITIS) in Germany, especially for the energy sector (FMI, 2016, p. 1).

The IT-SA refers to Section 11 (1a) of the Energy Industry Act and classifies network operators as operators of critical infrastructures. This classification is independent of the defined values set out in the Federal Office for Information Security Critical Infrastructure Ordinance. This type of consideration also implies the maintenance and safeguarding of information technology components that are used as part of grid operation and grid management.

The classification of the energy sector as a CRITIS explicitly emphasizes the importance of these entities as an active member of the German electrical energy system, particularly in the interest of compliance with electrotechnical and IT security. The primary focus is on securing and maintaining the energy supply and thus on the availability of electricity, which equivalently also requires the availability of electrotechnical and IT systems due to the technical interlocking. One of the key elements in ensuring the availability of OT systems (hardware and software components) is the effective cooperation and coordination of system administrators and IT managers. In addition, active monitoring of system behaviour is also part of this, as structured and organized processes enable a proactive and responsive approach to information security incidents. This approach is the reaction to dealing with the IT security incidents of the "Morris" cyber worm, which attacked a wide range of global OT systems in 1988. As a result of the serious cyberattack, the first Computer Emergency Response Team (CERT) approaches were conceived, which still exist today in different forms and variations (ENISA 2006, p. 8).

This research paper is dedicated to an in-depth examination of the current state of research in the field of Computer Security Incident Response Teams (CSIRTs) or CERT particularly regarding the energy sector. The terms CERT and CSIRT are used as synonyms in this paper. As already explained in the first chapter, the energy sector is characterized by increased procedural and technical interfaces, the effective management of which is of crucial importance in practice.

The importance of CERTs in the context of cyber security is becoming increasingly clear, especially in view of the growing complexity and frequency of cyber-attacks on critical infrastructures such as energy supply systems. These systems are characterized by a multitude of interfaces that include both procedural and technical aspects. Understanding and managing these interfaces is crucial to maintaining business continuity and minimizing risks.

By analyzing the current state of research and identifying best practices, the aim is to gain insights that can help improve the effectiveness and efficiency of CERTs in the energy sector. This is crucial to ensure the safety and reliability of the energy infrastructure and minimize the potential impact of cyber-attacks.

## 3. State of Research: Computer Emergency Response Team in the Energy Industry

A CERT is a team of IT security experts or specialists whose core process is to manage computer security breaches for a selected target group by offering preventive, reactive, and detective services. Preventive, reactive and detective services offered support the achievement of objectives. Preventive services provide support and information to prepare for attacks, problems, or events in advance. Reactive services are divided into two main core components:

- In the form of alerts or remote support processes aimed at identifying concepts for resolving incoming security incidents (analysis, coordination)
- In the form of on-site support processes or remote sessions (response, resolution).

Detective services support the continuous improvement processes. These include awareness-raising and training units, security audits and certifications, analyses (business continuity management and risk and vulnerability analyses).

A CERT can be established in various organizations or sectors, including government agencies, businesses, educational institutions, and critical infrastructure such as the energy sector. These teams can operate internally within an organization or externally as a service provider shared by multiple organizations.

The European Union Agency for Cybersecurity (ENISA) regularly publishes the CERT-Map, also known as the "European Union's National and governmental CSIRTs and their cooperation with ENISA", on its website and other relevant platforms (Öztürk, 2023, S. 78). The CERT Map provides an overview of the various CERTs and comparable institutions in the member states of the European Union. A current examination of this map shows, when selecting the energy sector, that as of the update 31.01.2024 there are a total of four CERTs that are specifically geared towards the energy sector (ENISA, 2024).


**Figure 1: CSIRT – Intentory: Selection of sector energy (ENISA 2024)**

However, the list is not exhaustive. A general search for CERTs for the energy sector has shown that in Austria the so-called Austrian Energy Cert, which provides specific services for the energy sector (Cert.at).

The following section examines the current state of research on the topic of CERT for network operators and members of the electrical power supply. The answer to this question is based on a comprehensive research analysis that focuses on written works. This includes primary and secondary literature, scientific papers, technical articles, and studies. Table 1 presents the results of this research: The list is the result of a thorough analysis of different databases combined with different keywords.

**Table 1: Literature analysis with databases**

| Results table work package | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Database** | **Absolute number of works recorded** | **Percentage share** | **Absolute number of eliminated shares** | **Percentage share** | **Reason for selection** | **Absolute number of selected works** | **Percentage share** | **Key words** |
| | | | | | | | | Computer Emergency Response Team |
| ACM | 49 | 100% | 15 | 31% | Duplicates | 34 | 69% | Cert |
| AIS | 100 | 100% | 56 | 56% | Duplicates | 44 | 44% | Computer Security Incident Response Team |
| IEEE | 169 | 100% | 83 | 49% | Duplicates | 86 | 51% | CSIRT |
| EBSCO | 12 | 100% | 1 | 8% | Duplicates | 11 | 92% | Incident Response Team |
| SPRINGER E | 64 | 100% | 9 | 14% | Duplicates | 55 | 86% | IRT |
| WISO | 1 | 100% | 0 | 0% | | 1 | 100% | Security Operations Center |
| SPRINGER D | 4 | 100% | 0 | 0% | | 4 | 100% | SOC |
| ECONBIZ | 8 | 100% | 4 | 50% | Duplicates | 4 | 50% | Cyber Defense Model (Modell) |
| **SUM** | **407** | | **168** | | | **239** | | |
| | | | | | | | | *Keywords were also combined with "concept, model + energy"* |

After selecting the duplicate files, a total of 239 papers containing the combination of keywords in their abstract were selected for analysis.

In the next step, these papers were analyzed in more detail, so that a total of 29 papers were selected that were classified as "relevant" and subjected to a semantic analysis in the next step.

As part of the content analysis, the following 31 research papers were examined in greater depth for the specific characteristics of CERTs in the energy sector.

**Table 2: Research paper on CERTs in the energy sector**

| Index | Author | Year | Title |
|---|---|---|---|
| 1 | ENISA | 2016 | Report on Cyber Security Information Sharing in the Energy Sector |
| 2 | NIS Policy 2.0 | 2023 | Network and information security policy 2.0 |
| 3 | NIS Policy | 2016 | Network and information security policy 1.0 |

| Index | Author | Year | Title |
|---|---|---|---|
| 4 | Holzleitner et al. | 2017 | European provisions for cyber security in the smart grid – an overview of the NIS-directive |
| 5 | ISO/IEC 27019 | 2018 | Information technology - Security procedures -Information security measures for the energy supply |
| 6 | Skopik et al. | 2018 | Cyber situational awareness in Public-Private-Partnerships |
| 7 | Martins et al. | 2019 | Specialized CSIRT for Incident Response Management in Smart Grids |
| 8 | CMU/SEI | 2003 | Handbook for Computer Security Incident Response Teams (CSIRTs) |
| 9 | CMU/SEI | 2004 | Steps for Creating National CSIRTs |
| 10 | ENISA | 2006 | Setting up a CSIRT step by step |
| 11 | CMU/SEI | 2006 | Action List for Developing a Computer Security Incident Response Team (CSIRT) |
| 12 | ENISA | 2007 | A basic collection of good practices for running a CSIRT |
| 13 | CMU/SEI | 2011 | Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability V. 2.0 |
| 14 | Huber et al. | 2018 | Introduction of an SME CERT in Austria |
| 15 | BSI | 2008 | National response plans: IT-Crisis Response in Germany |
| 16 | BMVIT | 2013 - 2015 | KIRAS project: Research Security. CERT communication model II |
| 17 | Huber | 2015 | Security in cyber networks. Computer Emergency Response Teams and their communication |
| 18 | New America | 2015 | National CSIRTs and Their Role in Computer Security Incident Response |
| 19 | CMU/SEI | 2016 | WHAT SKILLS ARE NEEDED WHEN STAFFING YOUR CSIRT? |
| 20 | Huber et al. | 2016a | Knowledge sharing and trust among Computer Emergency Response Teams - a European challenge |
| 21 | Huber et al. | 2016b | Study CERT Communication |
| 22 | Pospisil et al. | 2017 | Cyber security strategies - realizing goals through cooperation |
| 23 | ENISA | 2011 | CERT Operational Gaps and Overlaps |
| 24 | Hoyer et al. | 2006 | Critical success factors for a Computer Emergency Response Team (CERT) using the example of CERT-Niedersachsen |
| 25 | CMU/SEI | 2011 | Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability V.2.0 |
| 26 | Dartmouth College | 2017 | IMPROVING CYBERSECURITY INCIDENT RESPONSE TEAM (CSIRT) SKILLS, DYNAMICS, AND EFFECTIVENESS |
| 27 | ENISA | 2019 | Maturity Evaluation Methodology for CSIRTs |
| 28 | Energy Community | 2019 | Final Report - Study on cyber security in the energy sector of the Energy Community |
| 29 | ENISA | 2020 | SECTORAL CSIRT CAPABILITIES Status and Development in the Energy and the Air Transport sector |

| Index | Author | Year | Title |
|---|---|---|---|
| 30 | CMU/SEI | 2021 | The Sector CSIRT Framework Developing Sector-Based Incident Response Capabilities |
| 31 | Daniel Núñez-Agurto et al. | 2022 | Design of an academic CSIRT – A proposal based on strategic planning principles |

The works listed in 2 (see Table 2, indices 1 - 7) do not represent conceptual approaches or methods for CERT structures in the energy supply. In some points they merely underline the importance of this topic regarding the challenges to be expected in the energy transition.

In the "Report on Cyber Security Information Sharing in the Energy Sector", ENISA provides an insight into the development of CERTs, Information Sharing Analysis Centers (ISACs) and relevant initiatives for sharing information on cyber security incidents in the energy sector. Basically, ENISA analyzes existing regulations and functioning of the energy sector to derive how information sharing regarding CERTs can be improved in the future. The report is for informational purposes and does not present any specific methods or concepts that show how the exchange of information for CERTs could possibly look based on the results (ENISA 2016, p. 43).

A further examination of the works shows that there are various approaches to setting up CERT organizations (see Table 2, indices 8 - 14). However, no explicit conceptual process model for a CERT could be identified within the scope of the study that is either sector-specific or specifically addresses energy suppliers. The works listed above present procedures that enable the establishment of a CERT step by step. A closer examination illustrates that general and national institutions as well as SMEs are declared as the target group for the integration of the CERT organizational structure.

It also shows that ENISA is increasingly focusing on the establishment of new CERTs with the mission of securing the European information society by raising awareness of network and information security throughout Europe with the help of handbooks.

An analysis of the communication and cooperation models of CERTs illustrates that the topic of communication and cooperation plays an eminent role in the activities of CERTs, as, on the one hand, the increasing complexity means that an efficient and secure exchange of information and communication between the players in the digital supply infrastructure must be guaranteed and, on the other hand, incidents cannot always be resolved locally, so that the involvement of other units is required (Huber 2015, p. 54).

The listed theoretical works (see Table 2, indices 15 - 21) address the topic of communication and cooperation among CERT units for effective response, detection, and prevention of security incidents and present both empirical and conceptual approaches. Essentially, these works deal with efficient communication and cooperation between CERT units and emphasize the importance of this regarding the large number of actors that are generally required in the event of incidents. Fundamentally, this shows that there is currently no CERT that covers all services, meaning that the handling of security incidents requires different CERT units with different services (ENISA 2006, p.13).

According to Huber (2015, p. 55), “[t]he clear objective of cooperation for CERTs (...) is to obtain the support they need for their work”. None of these works show a targeted discussion of the CERT communication structure regarding the energy sector.

The GÉANT network's TRANSITS funding program (see Table 2, Index 16), which is also listed, supports the establishment and further training of CERT structures. It supports the training and further education of CERT employees and is sponsored by European associations such as ENISA and Forum of Incident Response and Security Teams (FIRST). The courses take place twice a year and are aimed at individuals or organizations (Huber 2015, p. 56).

Some of the literary works (see Table 2, indices 22 - 28) deal with increasing the quality of existing CERT structures and present best practices for continuous improvement processes and maturity models. Among other things, these works focus on the perspective of better CERT structures, success factors for setting up and operating a CERT and optimization options that are essential for the successful establishment of CERTs.

The last two papers (29 and 30) deal with studies on CERTs in the energy sector, but do not represent methods or research projects.

The paper in 31 deals with the development of an organizational model to support security processes in academic institutions during computer incidents. It includes a systematic literature review to identify relevant organization types, services, infrastructures, and procedures for the development of academic CSIRTs. Guidelines from ENISA and FIRST and principles of the Strategic Planning Process are applied to develop an organizational model, operational proposals for the CSIRT and research areas.

In addition to the theoretical research, existing empirical concepts and research models/projects will now be examined to answer the second sub-question.

**Table 3: Research projects and concepts on CERTs in the energy sector**

| Index | Association/authority/institute | Period | Research project? |
|---|---|---|---|
| 1 | Federal Ministry for Economic Affairs and Energy | 2000 - 2023 | No |
| 2 | Federal Ministry of Education and Research | 2000 - 2023 | No |
| 3 | Federal Network Agency | 2000 - 2023 | No |
| 4 | Fraunhofer Communication, Information Processing and Ergonomics (FKIE) | 2000 - 2023 | No |
| 5 | Fraunhofer Secure Information Technology | 2000 - 2023 | No |
| 6 | German Energy Agency | 2000 - 2023 | No |
| 7 | Network Technology/Network Operation Forum (FNN within the VDE) | 2000 - 2023 | No |
| 8 | Federal Office for Information Security | 2000 - 2023 | No |
| 9 | Research Power Grids | 2000 - 2023 | No |
| 10 | European Network and Information Security Agency | 2000 - 2023 | No |
| 11 | DFN-CERT | 2000 - 2023 | No |

Overall, it can be seen (Table 2, indices 1 - 11) that none of the bodies examined deal with the topic of CERT for network operators in their research projects. A review of the Federal Ministry for Economic Affairs and Energy Hanover Technical Information Library shows that the topics of CERT, the energy sector, virtual power plants and CRITIS are dealt with, but that no specific organizational model or research project is being carried out in this regard.

This result is also fundamentally reflected in the other sources. According to Huber (2015, p. 58), one possible reason for this could be that CERTs for CRITIS operators are still in the process of being developed, but that this development is difficult in practice because “ICT security considerations are very different for commercial IT systems and industrial control systems” (Huber 2015, p. 58). Actions carried out by the system operator in the control center, for example, usually require immediate action.

These actions can be, for example, shutting down or starting up certain systems, controlling the power supply and switching capacities and loads on and off. Traditional two-factor authentication methods usually fail here, as immediate action cannot be guaranteed.

## 4. Conclusion

In summary, the literature review shows that there are no dedicated research projects or approaches that specifically address the alignment of CERT services to the energy sector. Although there are general approaches to increasing information security in the energy sector, there is a lack of preventive, reactive and detective measures geared towards this sector. This is significant given the complexity and specificity of OT systems in this sector, which require special measures and expertise. The existing gap in research suggests that there is an urgent need to develop specific modeling approaches to ensure the safety and resilience of OT systems in the energy sector. The development of such approaches requires a comprehensive examination of the unique

challenges and threats faced by OT systems in the energy sector, as well as close collaboration between researchers, industry representatives and regulators.

Nevertheless, there is an urgent need for such projects in this sector. The energy sector is technically different from other sectors and therefore requires specific considerations in terms of information security. This industry operates complex infrastructures that are spread over wide geographical areas and include different types of energy sources and distribution systems. The integration of renewable energy sources and smart grid technology further increases the complexity and potential for attacks.

In addition, many assets and systems in the energy industry are highly outdated and may not be adequately protected against modern cyber threats. Therefore, it is crucial to conduct research projects that consider the unique technical aspects of the energy sector and aim to develop customized security solutions.

These projects should focus on identifying and addressing vulnerabilities in specific energy systems, developing security standards and guidelines for the industry, and training professionals in the unique challenges of energy security. Such targeted efforts can strengthen the energy sector's resilience to cyber-attacks and minimize the risk of serious impacts on society.

## References


BMWi (2018) “Sixth monitoring report on the energy transition. The energy of the future”, Federal Ministry for Economic Affairs and Energy, Germany, pp 1-190.

CIO (2024) “*How the promotion of solar energy will continue in 2024*”, [online] https://www.cio.de/a/wie-es-mit-der-foerderung-von-solarenergie-2024-weitergeht,3726505.

CMU/SEI (2021): “The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities”, 1-74.

CMU/SEI (2016): “WHAT SKILLS ARE NEEDED WHEN STAFFING YOUR CSIRT?” REV-03.18, pp 1-17.

CMU/SEI (2011): “Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0” pp 1-40.

CMU/SEI (2006): “Action List for Developing a Computer Security Incident Response Team (CSIRT) “, Carnegie Mellon, Software Engineering Institute, pp 1-9.

CMU/SEI (2004): “Steps for Creating National CSIRTs“, Carnegie Mellon, Software Engineering Institute, pp 1-26.

CMU/SEI (2003): “Handbook for Computer Security Incident Response Teams (CSIRTs)“, Carnegie Mellon, Software Engineering Institute, pp 1-223.

Dai, J., Li, Y., Zhang, T., Zheng, S., Zhou, X. (2020) “*Research on Optimal Decision-Making of Power Grid Flexible Reserve under New Situation*”, IEEE Sustainable Power and Energy Conference (iSPEC), Chengdu, China, pp 565-571.

Dartmouth College (2017): “IMPROVING CYBERSECURITY INCIDENT RESPONSE TEAM (CSIRT) SKILLS, DYNAMICS AND EFFECTIVENESS”, pp 1-17.

CERT.at (n. d.): “Mission Statement”, [online] https://cert.at/de/.

ENISA (2024): “CSIRTs by Country – Interactive map” [online] https://www.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map.

ENISA (2020): “Sectoral CSIRT Capabilities - Energy and Air Transport”, 1-62.

ENISA (2019): “ENISA Maturity Evaluation Methodology for CSIRTs”, pp 1-42.

ENISA (2016): “Report on Cyber Security Information Sharing in the Energy Sector”, European Union Agency for Cybersecurity, V. 1.1, pp 1-71.

ENISA (2011): “CERT Operational Gaps and Overlaps”, pp 1-73.

ENISA (2007): “PART I: A basic collection of good practices for running a CSIRT”, European Union Agency for Cybersecurity, pp 1-82.

ENISA (2006): “A step-by-step approach on how to set up a CSIRT”, European Union Agency for Cybersecurity, pp 1-86.

EU (2022): “NIS 2 Directive”, Official Journal of the European Union, 27.12.2022.

FMI (2016) *Ordinance on the Determination of Critical Infrastructures under the BSI Act (BSI Criticism Ordinance - BSI-KritisV),* Federal Ministry of the Interior.

Hoyer, S., Pomes, R., Wohlers, G., Breitner, H. M., (2006): Critical success factors for a Computer Emergency Response Team (CERT) using the example of CERT-Niedersachsen, Germany, pp 1-51.

Huber, E., Pospisil, B., Hellweig, O., Rosenkranz, W. (2018): “Introduction of an SME CERT in Austria”, in: P. Schartner - N. Pohlmann (Eds.) - D-A-CH Security 2018 – syssec, pp 142-150.

Huber, E., Hellwig, O., Quirchmayr, G., Donko-Huber, M. (2016b): Study CERT Communication”, in: In: BMVIT Research Security, KIRAS Study volume 3, Vienna, pp 1-12.

Huber, E., Hellwig, O. (2016a): Knowledge sharing and trust among Computer Emergency Response Teams - a European challenge”, in: Data protection and data security, pp 163-167.

Huber, E. (2015): “Security in cyber networks: Computer Emergency Response Teams and their communication”, Springer VS; 2015th edition, Germany.

ISO/IEC 27019:2020-08, Information technology - Security procedures - Information security measures for energy supply (ISO/IEC 27019:2017, corrected version 2019-08).

Martins, R.J., Knob, L.A.D., da Silva, E.G. et al. (2019): Specialized CSIRT for Incident Response Management in Smart Grids. J Netw Syst Manage 27, pp 269–285.

New America (2015): "National CSIRTs and Their Role in Computer Security Incident Response", pp 1-36.

Núñez-Agurto, D. et al. (2022): "Design of an Academic CSIRT – A Proposal Based on Strategic Planning Principles", in: Botto-Tobar, M., Cruz, H., Díaz Cadena, A., Durakovic, B. (eds) Emerging Research in Intelligent Systems. CIT 2021. Lecture Notes in Networks and Systems, vol 405. Springer, Cham.

Öztürk, A. (2023): Shared Service Processes for the Information Security in the Smart Grid of the Future, International Journal of Engineering and Technology, Vol. 15, No. 3, August 2023, pp 76-80.

Pospisil, B./Gusenbauer, M./Huber, E./Hellwig, O. (2017) Cyber security strategies - implementing goals through cooperation.

Scheffler, J. (2016) *Distribution grids on the way to an area power plant, legal framework, generators, grids*, Springer Publishing Berlin Heidelberg.

Skopik, F., Wurzenberger, M., Settani, G., Fiedler, R. (2015): Building national cyber situational awareness through incident information clustering. In: Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, UK, pp 1-8.

VISE (2019) Virtual Institute Smart Energy: "Policy Brief January 2019, IT security in the energy industry" Germany, pp 1-13.