Journal of Energy

VOLUME 72 Number 1 | 2023

journal homepage: http://journalofenergy.com/

Cybersecurity of the Power Production and Distribution of Critical Infrastructure

Krešimir Kristić

***Summary* — The paper presents a structured, comprehensive and universally applicable approach to the management of cyber security of the power production and distribution of critical electricity national infrastructure. In his daily work, the author is competent for the protection and the resilience of the national electric power infrastructure against the threats from cyber space. The exposed approach and methods to the objective in question are successfully applied.**

***Keywords* — Critical Infrastructure, Cybersecurity, Electricity, Electricity Distribution, Power Production.**

I. Introduction

THIS paper addresses the generic vulnerabilities of production and distribution power systems in the field of cyber security and protection of the national power infrastructure.

In times of crisis and crisis situations, we feel the impact of electricity supply disruptions on all aspects of our lives, and we become aware of the dependence of civilizational achievements and the way we live on the constant availability of electricity.

We are also witnessing successfully carried out attacks from cyberspace on the critical power infrastructure of production and distribution systems, the consequent damages of which cause significant disruptions in the functioning of the society and economy due to interruptions in the supply of electricity to consumers. In doing so, vulnerabilities and new risks are increasingly used due to the combination of information technologies (IT) used primarily in business and in business processes, with operational technologies of industrial processes (OT) and new technological concepts such as IIoT (Industrial Internet of Things) and 5G connectivity. New emerging vulnerabilities caused by the deregulation of the electricity market with distributed electricity generation within the distribution system are also being exploited.

The key prerequisites for the efficient and effective implementation of cyber security activities and measures of the electricity infrastructure is knowledge about the vulnerabilities of protected objects – what is being protected, and knowledge about threats and attackers, i.e. from what and from whom the object should be protected.

(Corresponding author: Krešimir Kristić)

Krešimir Kristić is with HEP d.d., Ulica grada Vukovara 37, 10000 Zagreb, Croatia EU (e-mail: kresimir.kristic@hep.hr).

The paper describes the critical industrial processes of power and distribution systems in the context of their vulnerabilities due to cyber threats and groups of attackers with their goals.

Security in the business environment is a function of supporting the achievement of strategic business goals. The basic task, i.e. the mission of the business function of corporate security, is to enable a justified business request in a secure way. In the context of the operation of power and distribution systems [3,6], cyber security is primarily focused on ensuring reliability and availability, and on ensuring the contracted quality of electricity delivered to consumers [1]. The subject of this paper is an approach to the identification of relevant processes of power systems of hydroelectric power plants and thermal power plants and power distribution systems, primarily their vulnerabilities with associated threats that can adversely affect the operation of power systems from cyberspace and ultimately the quality, reliability and availability of power delivered to consumers [1- 6]. As for related works that cover certain specific similar segments, this work was designed based on a comprehensive top-down approach to economically justified protection of industrial automation and monitoring systems of power plants and electrical distribution systems, and it proved to be successful in application.

In the introductory part, it is necessary to explain the use of the terms and relationship between information and cyber security.

Information security in a business environment protects the most valuable business resource after employees, and that is - of course - information. The basis for this is the well-known Information Security CIA triad (Confidentiality, Integrity, Availability, CIA): confidentiality, integrity and availability of the information to be ensured. In this context, cyber security, which is focused on a set of threats only from cyber space against business valuable information, is actually a subset of information security [14].

In the field of protection of industrial processes (Operational Technology, OT) and Industrial Automation and Control Systems (IACS), the availability-continuity, integrity and confidentiality (AIC) of industrial production processes are primarily achieved by cyber security activities and measures, and only then, but no less important, related data, the bearers of relevant information, are protected.

In conclusion, the comprehensive Cybersecurity Program includes risk assessment, Business Impact Analysis (BIA) and enables the implementation of Information Security Management System (ISMS) activities and measures, which all together ensure the protection and elasticity of industrial processes of electricity production and distribution in relation to threats from cyberspace.

Section II. describes corporate Cybersecurity Program based

on the relevant sectorial regulations and laws, on the efficiently and economically established risk assessment, and on the results of the Business Impact Analysis (BIA) performed.

Section III. deals with Electricity Infrastructure Vulnerabilities, dealing with key industrial processes in production power systems as well as in distribution power systems with an emphasis on emerging risks of atomized production in the distribution system itself. Threats and attackers exploiting the vulnerabilities of power systems are also described in this section.

Section IV. Lifetime Management of Cybersecurity describes the establishment of Cybersecurity management, implementation in active production, and management at final termination of the operation. Chapter V. Conclusion stresses Cybersecurity Program and two important aspects: the need for simultaneous implementation of complementary activities of risk assessment and BIA and the need for further elaboration of the emerging risks arising from the atomized production of electricity in the distribution system.

The paper provides an answer on how to create a framework and implement the organizational and technical measures required for the protection of critical power infrastructure in an economically justified manner in accordance with regulatory rules and relevant legislation. The presented approach and methods according to the objective in question have been successfully applied in practice.

II. Cybersecurity Program

The implementation of activities and the application of cyber security measures of the electric power system ensure the continuity and integrity of production industrial processes. In production and distribution power systems, the goal is to achieve delivery reliability that results in available and high-quality electricity delivered to consumers.

By applying the relevant sectorial regulations and laws:

1. Directive 2016/1148 of the European Parliament and the Council of the EU on measures for a high common level of security of network and information systems throughout the Union (NIS Directive, NISD) [11],
2. Act on cyber security of operators of key services and providers of digital services, NN 64/18. in force from 26.07.2018. (ZKS) [12],
3. Regulation on cyber security of key service operators and digital service providers NN 68/18 (Regulation), and best practices primarily defined in families of standards:
4. ISA/IEC 62443 – security of industrial automation and control systems,
5. ISO/IEC 27000 – information security management system,
6. ISO/IEC 22300 – business continuity management system and
7. ISO/IEC 28000 – supply chain security management system,

and then in other applicable standards, a comprehensive and holistic cyber security program for industrial automation and control systems (Program), as shown in Figure 1, is defined and implemented.

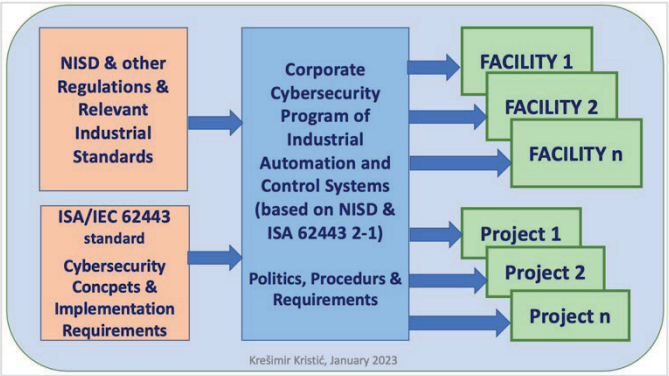

Fig. 1. Corporate Cybersecurity Program.

The NISD, i.e. its transposition into the national Croatian legislation ZKS and the Regulation operationalizing the ZKS, are a binding legal framework for all service operators (hereinafter referred to as the Operator) identified according to the criteria of the ZKS, of production and distribution of electricity of particular importance for the development of key national social and economic activities.

The NISD-ZKS regulation is the basis of the corporate cyber security program of industrial automation and control systems (the Program) because, in addition to the binding legal dimension with defined constraints, the NISD-ZKS regulation comprehensively and holistically defines the areas and activities in the Program:

- security management of network and information systems - management framework, organizational structure, establishment and documentation of management policy, implementation of internal controls;
- risk management - establishment of a risk management system, risk assessment, documentation on risk assessment, identification of equipment, persons and activities within which risk assessment is carried out, prevention, detection and resolution of incidents and mitigation of the impact of incidents;
- areas of protection of key systems - physical security and environmental security, security of supply, development and maintenance of key systems, management of contractual relationships, project management, management of outsourcing, management of structural assets, control of access to premises, management of changes in program assets, physical and logical separation of key systems , key system configuration, key system access control, key system vulnerability preventive checks, key system activity log, business continuity management, protection of data that is processed, stored and transmitted in the key system, protection against disruption of the availability of the key system, protection against malicious program code, reserve storage;
- notification of incidents - obligation to notify, incidents with a significant impact on the continuity of the provision of a key service, assessment of the impact of the incident on the continuity of the provision of a key service;
- notifications about incidents with a significant effect on the continuity of service provision - types of notifications, initial notification about an incident with a significant effect, interim report, final report on an incident with a significant effect, delivery of notifications about incidents with a significant effect, exchange of notifications;
- handling notifications about incidents with a significant effect - resolving incidents with a significant effect.

A. Risk Assessment

The purposefulness and economic justification of activities and measures during the implementation of the Program is ensured in accordance with Article 18 of the ZKS by implementing a risk assessment: "Operators of key services and digital service providers apply measures to prevent and mitigate the effects of incidents in proportion to the risk to which their network or information system is exposed". The usual risk assessment method is essentially:

- repository of relevant information assets (entities), preferably automatically recognized and updated in real time,
- identification of relevant vulnerabilities of each entity in the repository of information assets,
- identification of relevant threats for each recorded vulnerability,
- assessment of the impact of each realized threat and on
- determination of the probability of the realization of the threat and unwanted impact, which is actually a risk per definitionem.

Support for the efficient and effective implementation of risk assessment is achieved through the implementation and mutual integration of the applied information technology (IT) asset management system, i.e., the IT asset management system of the current level (January 2023) ITAM 2.0 (IT Asset Management, ITAM) and the governance, risk and compliance system (Governance, Risk, Compliance, GRC).

The automated integration of these two systems at the data level in real or near real time is important. Automatically detected and updated entities of information assets from industrial automation and control systems using the ITAM tool, are transferred to the GRC system grouped according to the criteria of a unique set of vulnerabilities and entered as a single entity in the GRC system. The transfer relation from the ITAM repository of information assets to the GRC system is *n: 1* grouped according to the criterion of an identical set of vulnerabilities of the entity registered in the GRC system. It is desirable that in the GRC system each registered entity has an up-to-date attribute of the number of individually detected assets in the ITAM system. ITAM enables detailed analytical insight into the relevant properties of each individually detected asset-entity, for example into all hardware components and into the licensing status of all installed software at each individual management and control workstation in the industrial automation and control system.

In addition to the aforementioned ITAM 2.0 and GRC system capacities, for the efficient and effective implementation of risk assessment, it is also necessary to provide the adequate skills, i.e., trained workers for the smooth implementation of the risk assessment process. Every relevant change in industrial automation and control systems should be followed by a risk assessment, both proactively in the change planning phase, and during the change implementation itself, which is an indispensable part of the standard change management procedure.

It must be emphasized that the ITAM system must be adapted to work in the environment of industrial automation and control systems to be functionally neutral, i.e., without affecting the operation and functioning of these systems, and thus, most importantly, without affecting the industrial process itself.

B. Business Impact Analysis BIA

While risk assessment results in a relatively static picture of the probability of adverse events in business and in business processes, Business Impact Analysis (BIA), which is the process of analyzing business processes and financial and operational impacts and consequences of disruptions or stoppages in processes and business, ultimately results managing the continuity of the operations [13].

The implementation of activities and the application of cyber security measures of the electric power system should ensure the continuity and integrity of production industrial processes. The simultaneous implementation of complementary activities of risk assessment and BIA analysis provides a comprehensive, complete and solid basis for achieving this goal. Even more so because the collected data and intermediate results in both procedures mutually facilitate and speed up the implementation and raise the quality level of the delivery of both procedures - both risk assessment and BIA analysis. A prerequisite for risk assessment is an up-to-date repository of information assets, while at the same time BIA, among other things, should address the resources necessary for the uninterrupted development of industrial production processes. Furthermore, the risk assessment ensures the timely recognition and implementation of preventive activities and security measures that will reduce the probability of occurrence of unwanted events in business, while the BIA should reduce the negative impact of these events, if they do occur.

There are three phases of BIA implementation:

I. data collection and confirmation with two key procedures

- a financial analysis of the impact/consequences that results in an assessment of the possible financial effects on the Operator in the event of work interruptions, i.e., disruptions and interruptions of key processes,

- an operational analysis of the impact/consequences with an assessment of the impact and consequences of process interruptions in a key area on the fulfillment of the operational goals, for example in electricity production the goal is to keep power oscillations at the level of acceptable standard oscillations [4],

II. the analysis being carried out

- identification of key business processes and target recovery time (Recovery Time Objective, RTO),

- by prioritizing critical processes according to RTO,

- identification of critical resources and RTO,

- by prioritizing critical resources according to RTO,

III. documentation and approval, whereby all results of the business impact analysis must be formally approved by the owner of the process, usually the director of the Operator, as shown in Figure 2.

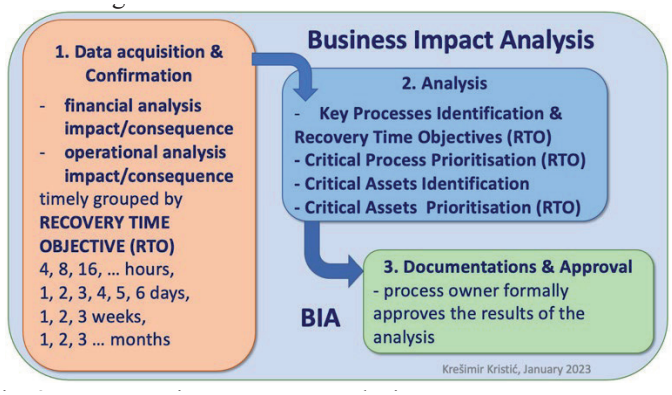

Fig. 2. BIA – Business Impact Analysis.

The key parameters for the definition of activities and the dynamics of the establishment and continuation of processes and operations within business continuity plans [13] and recovery plans for plant and equipment during business continuity management obtained by BIA analysis are:

• acceptable data loss - Recovery Point Objective, RPO

• Recovery Time Objective, RTO of critical process and operations

• the longest acceptable downtime - Maximum Tolerable Period of Disruption, MTPOD

as shown in Figure 3.

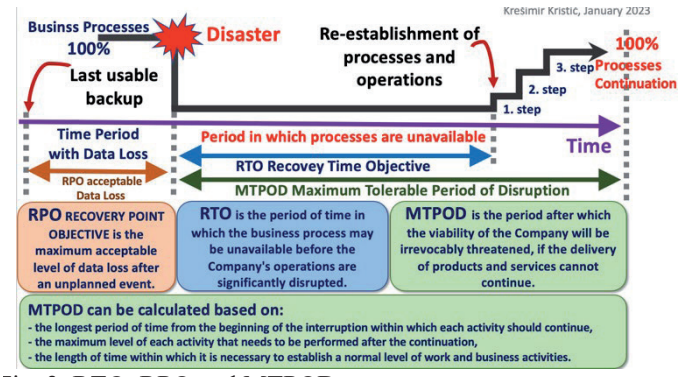

Fig. 3. RTO, RPO and MTPOD.

Based on these parameters, the plans define the dynamics of acquiring business resources and ensuring other conditions necessary for the re-establishment of business and production processes and for the continuation of business within the established RTO and MTPOD limits. The plans also define individual specialized teams with the minimum required number of relevant members for the smooth implementation of coordinated straight-line recovery activities of business and production industrial processes, such as the Crisis Management Team, the Damage Assessment Team, the Resource Assurance Team, the Crisis Communication Team and others. The plans define the types and frequency of simulation and other exercises of each individual team with an emphasis on the lessons learned during the implementation of the exercises (Eng. Lessons Learned), but inevitably also during real crisis situations, so that the necessary capabilities for efficient and effective crisis handling are ensured in addition to the necessary capacities and for continuous improvement of handling in crisis situations in the spiral PDCA cycle of continuous improvements (Plan-Do-Check-Act, PDCA).

C. Purpose of risk management and business continuity

By implementing the Program based on economically justified measures and risk reduction activities to an acceptable level, i.e. by implementing the Program based on the management of identified risks by their mitigation and on optimized and continuously improved business continuity plans and recovery plans for power plants and facilities, the purpose and goal of managing cyber security of the electricity critical infrastructure: delivery reliability, available and high-quality electricity delivered to consumers.

III. Electricity Infrastructure Vulnerabilities, Key Processes, Threats and Attackers

The inherent vulnerabilities of the traditionally defined electricity systems in relation to threats from cyberspace, primarily to industrial automation and control systems, are almost identical in production and distribution facilities, plants and areas regardless of the specifics of key processes. A significant number of these vulnerabilities are caused by organizational reasons, which are as follows:

- lack of a documented strategy and strategic directions for the development of the corporation's information system,
- the Information Security Management System (ISMS) has not been implemented in accordance with the basic ISO 27001 standard, and further to this vulnerability
- the procedure of the regular Administration's assessment of the state of security based on ISMS has not been introduced,
- there is no prescribed policy and/or procedure for the management of network devices, i.e., a policy for the use of network services,
- detection mechanisms on the network and on devices for process networks are inadequate,
- external contractors/service providers can cause problems during unannounced work on the information system. There is no formal periodic audit and supervision of the work of external suppliers, as well as their efficiency and safe way of working when accessing the information system,
- workers are not familiar with all the rules of information and cyber security during employment and can intentionally or accidentally cause damage due to ignorance,
- the absence and/or lack of usual functions and roles for information and cyber security in the member companies of the corporation does not contribute to the structured management of information and cyber security and weakens the response to possible information and cyber security incidents,
- there are no adopted internal acts for worker safety awareness,
- member companies of the corporation do not systematically conduct special training and education in the field of information and cyber security for those workers who have significant security roles and responsibilities,
- due to inadequately prescribed rules for protection against malicious software code (undocumented rules), protection management is difficult and incomplete,
- the patch management process is not documented or clearly prescribed, which causes vulnerabilities on systems due to shared responsibility or lack of information about vulnerabilities. For example, the consequence is the accelerated filling of memory on SCADA (Supervisory Control and Data Acquisition) systems due to badly applied patches,
- for all operational tasks of information and cyber security, responsibility is not clearly divided within the Operator and corporation in accordance with ISMS and the Program, and operational tasks are not performed, for example, maintenance of antivirus protection, hardening of network and server equipment,

- the lack of clear rules and instructions for the exchange of confidential information with external collaborators escalates especially in the implementation of projects by sending non-encrypted confidential information through unprotected channels, for example by e-mail and uncontrolled and security-questionable public services such as Jumbo mail, WeTransfer services, etc.,
- ineffective management of user access rights,
- there is no prescribed policy and/or procedure for the operation and management of mobile devices,
- lack of a defined and documented process for managing all types of changes in the information system (Change Management),
- there is no adopted internal act for managing the configurations of the information system,
- lack of a common template of basic security requirements that should be a standard component of tender documentation and contracts with external service providers and suppliers, etc.

Only then do the causes of vulnerability lie in operational procedures that are primarily mitigated by the implementation of measures at the technical level:

- operational and system records are not collected from all information system resources to the central system for detecting and reacting to anomalies (Security Operations Center, SOC),
- security hardening was not performed on the servers and unnecessary services were enabled,
- reliable authentication methods are not used, for example multi-factor authentication for remote access to the information system,
- parts of the information system do not use unique identifiers, but group generic user accounts, for example admin, administrator, root, etc.,
- regular checks of granted access rights are not carried out,
- activities for the maintenance of individual services are not recorded. An encrypted communication connection is used, but there are no strong authentication mechanisms for external connections or automatic closing of communication sessions in case of inactivity,
- inadequate supervision of the implementation of information classification rules without the use of software tools, for example tools for protection against data leakage (Data Leakage Prevention, DLP),
- the open communication connection is not automatically terminated after a long period of non-use, and potential attackers are left with the possibility of more time for malicious activity and compromising that relationship,
- etc.

In addition, it is necessary to emphasize and single out entire areas of new vulnerabilities in distribution power systems that arise from aspects of the service flexibility of the power distribution system, for example auxiliary services, aggregation and energy communities, e-mobility, balancing, congestion management and consumption management.

A. Key processes in production power systems

As part of the BIA analysis, key production and business processes in power systems are identified according to at least two criteria according to the criterion of unacceptable financial impact, i.e., damage due to disruption or interruption of the production process with regard to RTO, and according to the criterion of unacceptable operational impact of disturbances or interruptions in the supply of electricity for a duration longer than the established target RTO.

As a rule, the key processes in hydropower plants according to the above criteria are [6]:

- electricity production,
- preventive maintenance,
- corrective maintenance,
- periodic maintenance and repair,
- comprehensive planning and procurement in the widest scope of the Operator,
- production planning,
- safety management and system protection, occupational safety and fire protection.

While, as a rule, the key processes in thermal power plants are according to the two mentioned criteria:

- production of electricity,
- cooling of the production facility,
- production and preparation of water,
- preventive maintenance,
- corrective maintenance,
- periodic maintenance and repair,
- comprehensive planning and procurement in the widest scope of the Operator,
- planning and procurement of fuel,
- receipt and storage of fuel,
- production, planning and procurement of chemicals and
- safety management and system protection, occupational safety and fire protection.

B. Key processes in distribution power systems

According to the same criterion of unacceptable financial and operational impact in relation to the targeted RTO, the processes thus identified in power distribution systems are [6]:

- measurement and market support,
- remote control of the system,
- network management,
- telecommunications, and
- safety management and system protection, occupational safety and fire protection.

C. Specific vulnerabilities of distribution power systems

Emphasized and numerous peculiarities of the Program in the field of distribution power systems are determined by the binding

implementation legal framework primarily determined by the Law on the Electricity Market of the Republic of Croatia (NN 111/21, ZoTEE) and the complex relationship of dynamically changing and mutually influencing technological and market aspects of distribution power systems. ZoTEE is a fully harmonized national transposition of the Directive on common rules for the internal electricity market 2019/944 of the EU Parliament and the Council of June 5, 2019. and amendments to Directive 2012/27/EU (SL L 158, 14.6.2019).

ZoTEE ensures the implementation of a number of relevant acts of the institutions of the European Union, such as:

- Regulation on the integrity and transparency of the wholesale energy market (1227/2011 of the EU Parliament and Council of 25.10.2011. SL L 326, 8.12.2011),
- Regulation on the establishment of guidelines for capacity allocation and congestion management (EU Commission 2015/1222 of 7/24/2015 SL L 197, 7/25/2015),
- Regulation on management of the energy union and action in the field of climate (2018/1999 of the EU Parliament and the Council of 11.11.2018),
- Regulation on the internal electricity market (No. 2019/943 of the EU Parliament and Council of 5 June 2019, SL L 158, 14 June 2019).

Just these listed components of the binding implementing legal framework point to great challenges in practical application and implementation. If we add to this the complexity of the market and technological dimensions and the dynamic influence of all factors on a balanced and stable operation and the required flexibility of the power distribution system on a liberal and transparently regulated market, the necessity of recognizing, assessing and mitigating all newly arising specific risks is imposed.

The aforementioned complexity of both the market and even more technological dimensions of power distribution system operation is well and in detail illustrated by the ZoTEE-prescribed obligation to adopt numerous by-laws:

- Rulebook on general conditions for the use of the network and electricity supply,
- Rulebook on quality conditions of electricity supply,
- Rules on changing suppliers and aggregators,
- Methodologies for determining the fee for connecting to the electric power network,
- Decisions on the amount of the unit fee for connection to the network,
- Methodologies for determining the amount of tariff items for electricity distribution,
- Rules on non-frequency auxiliary services for the distribution system,
- Rules on congestion management in the distribution system,
- Network rules of the distribution system,
- Rules on connection to the distribution network,
- Rules for applying substitute load curves,
- Rules of non-standard services of the distribution system operator with the price list of non-standard services.

Furthermore, from the point of view of cyber security, it is also necessary to identify and manage a significant number of newly emerging specific risks arising from aspects of service flexibility of the electricity distribution system, for example auxiliary services, aggregation and energy communities, e-mobility, balancing, congestion management and consumption management. These open questions and challenges have yet to be adequately answered in view of the feedback and experiences from the implementation operational practice that are just emerging or beginning to arrive.

D. Threats and attackers

Attackers from cyberspace who exploit vulnerabilities in power systems and, in addition to system failures, are the primary threat source to the expected function of industrial automation and control systems, according to their capabilities and possibilities are:

- structured organizations,
  - state organizations - highly educated and equipped professionals on the state salary,
  - organized crime – mafias, gangs, criminal units,
- ideologically motivated groups,
  - terrorists - cyber terrorists, cyber militias,
  - ideological activists – cyber hacktivists, interest groups, sects,
- individuals and associated individuals,
  - specialized units and cyber mercenaries,
  - amateurs,
  - revenge - embittered and/or dissatisfied workers, dismissed workers,
  - pathological attackers – dishonest competitor, dishonest client, scammer, fraudster.

Threats (only three have been listed to illustrate the possible consequences), with which attackers can exploit electricity systems vulnerabilities are as follows:

- an uncontrolled plant shutdown with serious plant damage and long-term downtime, made possible by not using reliable authentication and poor management of user access rights, was caused by an embittered employee,
- ransomware, regardless of the capabilities and abilities of the attacker, causes, in the best case scenario, an unplanned shutdown of the system with a delay of several days for the restoration of the industrial automation and control system from backup copies, or in the worst case, a targeted written blackmail software or the use of undetected vulnerabilities (Zero-Day), whereby plants can be irreparably destroyed, and expensive recovery can take months,
- compromised encryption protection infrastructure of the Public Key Infrastructure (PKI) from state-sponsored attackers who, with sophisticated methods, have unnoticed acquired the possibility of complete hostile takeover, management, and control of the system, etc.

IV. Lifetime Management of Cybersecurity

Lifelong cyber security management of electricity systems is carried out in stages:

- establishment of cyber security management,
- active production implementation of cyber security activities and measures,

- management of cyber security during the final shutdown of the production facility.

A. Establishment of cyber security management

When establishing the cyber security management system of power systems, the ISMS implementation framework is based on the Information and Cyber Security Strategy, on the Program and on the organizational chart of ISMS according to the best practice embodied in the globally accepted standard, and on other internal acts that are required for an orderly and organized implementation of the Program and are derived from these umbrella documents according to the principle of subsidiarity, such as:

- Information and cyber security policies of the Operator,
- Rulebook on physical security and environmental security of key systems,
- Rules for ensuring the availability of equipment, materials, energy sources and other resources necessary for the regular and continuous functioning and maintenance of key systems,
- Rulebook on management of contractual relations and outsourcing in terms of risk assessment and supervision of service providers,
- Access control procedures to premises and key systems,
- Rulebook on the physical and logical separation of key systems from the rest of the infrastructure,
- Rules for monitoring and recording user activities on the key system,
- Rules for ensuring data protection in key systems,
- Rulebook on protection against computer attacks with the aim of ensuring the availability of the key system,
- Rules for ensuring the development and maintenance of key systems,
- Regulations on the establishment and Procedure of preventive checks of vulnerability of key systems,
- Regulations on the establishment and business continuity procedures of key services in cases of incidents and
- Regulations on the establishment and Procedures for management of backup data storage.

Wherein the term key system is used for industrial automation and control systems.

B. Active production implementation

The active production and implementation of lifelong cyber security management of the EES is reduced to the operational implementation of the Program in accordance with the best practice in terms of roles and responsibilities of the organizational chart of information security management according to the ISO/IEC 27001 standard, as shown in Figure 4.: Fig. 4. Organizational chart of the Corporate ISMS.

- The management of the corporation and the director of the Operator, manage information and cyber security at the strategic level, delegating the execution of the necessary activities and measures to the tactical level. ISMS is the function of the Corporate Management Board and Directors as a support mechanism for the achievement of strategic business goals,
- The organizational unit for information and cyber security, for example the Department for information and cyber security (Department), at the tactical business level establishes and organizes the ISMS - the information and cyber security management system, which is a tool of the corporation's management and Operator directors and proposes, prepares and organizes the implementation of measures within the ISMS. At the operational level of business, Department supervises the implementation of information and cyber security activities and measures and reports to the Corporate Board and Operators' Directors,
- Owners of business processes, who as a rule are also the owners of information assets and bearers/owners of related risks (Owner), have a key role in accepting the proposed activities and measures. The bearer/owner of the risk approves and accepts the proposed measures and activities of the Department. If the owner does not accept the proposed measures and activities because they negatively affect the flow of the business processes and operations, the Department is obliged to propose to the Owner acceptable compensatory organizational and/or technical measures to achieve the necessary targeted effect, as a rule of mitigation of relevant risks,
- Organizational units of IT, telecommunications and external contractual collaborators and partners implement technical measures and activities under the supervision of the Department that reports to the Owner, Operators' Director and to the Management Board.

C. Management at final termination of operation

All dynamic activities and measures from the production phase are successively and gradually reduced and finally completely abolished alongside with the planned and controlled reduction in the intensity of business activities and technological processes and the final complete shutdown of the power plant or of the power distribution system.

Specific activities in the field of information and cyber security area in this phase are as follows:

- ensuring adequate availability of technological, process, technical, economic and all other data in accordance with the terms of storage and archiving according to the relevant legal and regulatory provisions and according to the internal acts and provisions of the corporation and the Operator,
- safe and environmentally friendly disposal of used information and industrial automation and control systems and destruction of all storage media used in production, carriers of previously adequately archived information,
- reporting to the Corporation's Management and the Operator's directors on the dynamics of the implementation of specific activities from this phase of lifelong management of information and cyber security of industrial automation and control systems.

V. Conclusion

A complete and comprehensive Program based on current legislation and established standards is the basis of cyber security management of critical power infrastructure. Mutually complementary activities of risk assessment and the Business Impact Analysis (BIA) achieve a satisfactory level of industrial processes continuity of critical electric infrastructure. Vulnerabilities with associated risks against the continuity and integrity of the industrial processes of electricity production and distribution based on underlying national critical infrastructure, and newly created vulnerabilities as a result of the consequent deregulation and liberalization of the electricity market [7-10], such as the service flexibility of the electricity distribution system, aggregation and energy communities, e-mobility, balancing, auxiliary services, congestion management and consumption management, have yet to be incorporated and appropriately treated within the framework defined by the Program and presented in this paper.

References

[1] T. Tomiša, "Sustavi za trajni nadzor kvalitete napona u distributivnim mrežama", *35th International Convention IEEE MIPRO 2012*, Opatija, Croatia, 21-25 May 2012.

[2] M. Perić, Ž. Tomšić, T. Tomiša, J. Galešić, "Upravljanje energijom u industrijskim mikromrežama u tržišnim uvjetima", *Bosanskohercegovačka elektrotehnika*, Vol. 10, pp 78-88, 2016.

[3] I. Kuzle, "Dijagnostika u održavanju elemenata elektroenergetskog sustava", student textbook, Sveučilište u Zagrebu, FER, Zagreb, 2013.

[4] T. Plavšić, I. Kuzle, Regulacija napona i jalove snage kao pomoćna usluga sustava, *Journal of Energy-Energija*, Vol. 54, No. 5, pp. 385-396, 2005.

[5] H. Požar, "Osnove energetike I, II i III", Školska knjiga, Zagreb, 1992.

[6] H. Pandžić, "Održavanje proizvodnih postrojenja elektroenergetskog sustava u novim tržišnim uvjetima", *14. međunarodni simpozij "Elektroinženjerski simpozij (EIS 2007)": Dani Josipa Lončara*, Šibenik, Croatia, pp. 22-27, 03-05 May 2007.

[7] "Opći uvjeti za opskrbu električnom energijom", *Narodne novine*, br. 14, 2006.

[8] The European Parliament and the Council of the European Union, "Common rules for the internal market in electricity", *Directive 2003/54/EC*, 26 June 2003.

[9] "Zakon o tržištu električne energije", *Narodne novine*, br. 177, 2004.

[10] "Mrežna pravila elektroenergetskog sustava", Narodne novine, br. 36, 2006.

[11] The European Parliament and the Council of the European Union,: "Directive on security of network and information systems", *Directive 2016/1148/EC*, 6. July 2016.

[12] "Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga ", Narodne novine, br. 64, 2018.

[13] ENISA, https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/bi-analysis/conduct-business-impact-analysis?v2=1&tab=details, 25 January 2023

[14] NIST, „Glossary of Key Information Security Terms", NIST IR 7298r3, July 2019