Cyber Security Protection and Defence Measures in the Electricity Transmission Networks in South-East Europe

Aleksandra Krkoleva Mateska[1], Petar Krstevski[1], Stefan Borozan[2]

Abstract – **The paper describes the practices for protection of information, control systems and assets by transmission system operators (TSOs) in the region of South-East Europe (SEE). Based on a survey undertaken among the TSOs of the SEE region, the paper indicates state of the art practices and future developments related to critical infrastructures in electricity transmission networks.**

Keywords – **transmission systems, critical information infrastructure, cyber security.**

I. Introduction

The operation of power systems relies on both legacy systems and new technologies. The existing electricity infrastructure is combined with sophisticated control systems and intelligent components with bi-directional communication capabilities. The information and communication systems represent an overlay to the conventional electricity systems and allow real time control in the operation of generation, transmission and distribution of electricity [1]. As the implementation of information systems and technologies in power systems becomes a necessity, it also increases the risks of cyber security threats and requires implementation of adequate protection measures that should reflect the multi-actor environment of the contemporary power systems [2].

The cyber-attacks in electricity systems potentially endanger the electricity supply chain, threaten other essential services because these systems cannot be disconnected as easily as other information technology systems. Furthermore, there is a growing interdependence among sectors and systems that enables threats to become a cross-border issue not only in the EU, but in other neighbouring countries.

The general challenges to the energy sector with regards to cyber security include [3]: grid stability in a cross-border interconnected networks; protection concepts reflecting current threats and risks; handling of cyber-attacks in Europe; effects by cyber-attacks not fully considered in the design rules of an existing power grid or nuclear facility; introduction of new highly interconnected technologies and services; outsourcing of infrastructures and services; integrity of components used in energy systems; increased interdependency among market players; availability of human resources and their competences; and constraints imposed by cyber security measures in contrast to real-time/availability requirements.

In fact, all the above-mentioned challenges are applicable to electricity systems, which is not the case for other energy sectors. This only implies that the operators of interconnected electricity systems with legacy and next generation technologies, operating in multi-actor environment, need to reassess their approach to cyber security issues, following the recommendations of relevant national authorities and international organizations.

This paper describes practices for protection of information and control systems and assets by transmission system operators (TSOs) in the region of South-East Europe (SEE). The investigation is based on a survey undertaken within the framework of the CROSSBOW project [4] and encompasses the practices related to information and control systems security of the TSOs of Bulgaria, Croatia, Greece, Romania Bosnia and Herzegovina, Montenegro, North Macedonia and Serbia. For confidentiality reasons, the eight TSOs that participated in the survey are anonymized, thus in the paper, instead of the company name, TSOx is used, where x is a number from 1 to 8.

II. Information System Security Legislation and Governance

A. Legislation and Practices in SEE

The above described challenges have to be addressed through transposition of relevant legislation, including the Directive (EU) 2016/1148 (NIS Directive) [5] and the Directive 2008/114/EC (Critical Infrastructure Directive) [6] as well as implementing numerous measures at utility level. The observed SEE region consists of countries that are EU Member States (MSs) as well as countries that are Contracting Parties of the Energy Community (EnC) and members of the Western Balkans 6 Initiative [7]. Therefore, the countries of the region represent a uniquely varied part of Europe and for that reason, may serve as an example of extension of frameworks, rules and practices that bring European Union (EU) closer to its adjacent regions.

The NIS Directive aims to increase the overall level of security of networks across the EU and to build a systematic approach in counteracting the possible threats to networks and information systems. Its transposition should enable the establishment of Computer Security Incident Response Teams, adoption of national cyber security strategies by each EU MS, as well as designation of one or more national competent authorities and a single point of contact on the security of network and information systems [5]. The NIS Directive

[1]Aleksandra Krkoleva Mateska, Petar Krstevski, are with the Ss Cyril and Methodius University in Skopje, Faculty of Electrical Engineering and Information Technologies, Rugjer Boskovic No. 18, Skopje, Republic of North Macedonia, E-mail: {krkoleva, petark}@feit.ukim.edu.mk.

[2]Stefan Borozan is with Elektrodistribucija DOOEL, 11 Oktomvri No. 9, Skopje, Republic of North Macedonia, E-mail: s.borozan2@gmail.com.

foresees minimum common planning requirements, exchange of information and common security requirements for Operators of Essential Services (OESs) and Digital Service Providers (DSPs) [5]. From the aspect of electricity systems, the NIS Directive affects the operational activities of TSOs, distribution system operators (DSOs) and electricity suppliers. These entities can be considered as OESs and therefore, are obligated to fulfil all the requirements related to information systems security and incident notification.

The Critical Infrastructure Directive fosters EU cooperation in identification and designation process for potential European critical infrastructures and regular review of the process. It sets the requirements for operator security plan and security liaison officer for each European critical infrastructure, identification of their critical assets and security solutions [6].

The transposition of these Directives is not obligatory for the Western Balkan (WB) countries. The investigations done in [2] show that WB countries lack a strategic and cooperative approach in identification of critical infrastructures, their protection, as well as providing necessary level of protection of networks and information systems. They all face the same potential risks as EU MSs, hence, there is a substantial need for these countries to develop legislation that is compliant with the relevant EU legislation. The Energy Community Secretariat has started initial activities to overcome regulatory gaps inside the EnC, as well as towards the EU. Among the first activities within the envisaged tasks are to identify current legal framework and if some of the measures from the above discussed Directives are already implemented by the EnC Contracting Parties [8].

B. Utility Information Systems Security Governance Model

The adoption of network security related legislation is one of the pillars for achieving functional high-level security in critical information infrastructures (CIIs). The second pillar consists of set of measures and actions to be performed by utilities, including TSOs, with the aim to complement the measures implemented on national/EU level.

The information systems security governance model presented on Fig. 1 is based on the recommendations of [9] and it shows that performing risk assessment and developing an adequate security policy based on the performed risk analysis is substantial for the security of any information system, including CIIs used by TSOs. Starting with identification of the CII whose failure impedes the essential service delivery, the OES (in this case TSO) sets up an information security system. The identification process may be operator driven or state driven, but the outcome is clear identification of these infrastructures [10].

The scope of the security measures [11] are the assets exposed to threats which when breached/failing can have a negative impact on the networks or services. In the context of TSOs, these assets include the SCADA systems, hardware, software and computer databases at national dispatching centres, communication links between the significant nodes within the high voltage transmission network, software platforms with access for end users and other information infrastructure. The overall information system security policy should be based on performing risk analyses and supported by a security management system. In fact, risk analysis is the essential tool that is used to build a consistent and adequate security policy. This policy should aim to set up the security strategy of the utility and to set references to all important information system security policies including the security accreditation process, security audit, cryptography, security maintenance, incident handling [9].

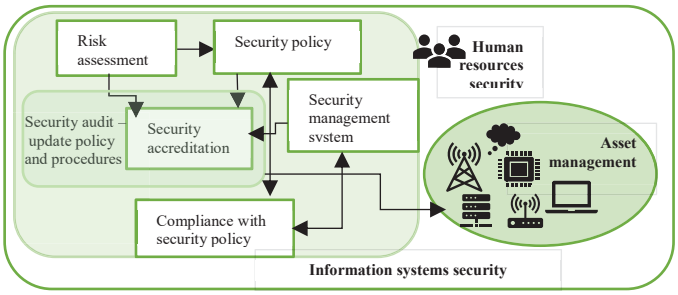

Fig. 1. Information system security, [2], [9]

The information security policy should lay out the accreditation process for the CII performed by the OES itself. The purpose of the process is to integrate the critical infrastructure in the security management system and formalize the processes. The accreditation process is used to map all the CIIs and apply adequate security measures. Within the process, a security audit to reassess the security policy and effectiveness of measures should be envisaged. The security of the system largely depends on the employees and contractors who should assume their responsibilities and on effective asset management.

III. INFORMATION SYSTEMS SECURITY PRACTICES IN THE REGION

A. Risk Assessment

Risk assessment is an essential tool for evaluating the potential cyber security threats to CIIs and assets. It is based on a pro-active approach, consisted of continuous monitoring and assessment, in a closed loop. As described in [11] the process should be performed during requirements definition, procurement, control definition and configuration, system operations, and end of system lifecycle, i.e. throughout the whole lifecycle of the infrastructure. The general risk assessment approach is to consider the possible threat, the vulnerability of the system and the consequence that the infrastructure and the system shall suffer due to the threat. The overall risk is determined using the following formula: risk = threat (probability) x vulnerability x consequence (impact). When the risk is assessed, then applying risk management techniques shall allow the utility to control, avoid, minimize or eliminate risks.

The survey on information systems security in SEE TSOs indicates that the companies are aware of the benefits of risk assessment in defining cyber security measures. However, regular performing of risk assessment is not a common

practice. Table I represents indicative summary of the results referring to risk assessment procedures. The "-" sign indicates that there are no developments related to the issues from the first column of the table, the "±" sign indicates that there are ongoing or planned activities for near future and the "+" signs show that adequate actions are implemented.

TABLE I
RISK ASSESSMENT PROCEDURES IN SEE TSOS

TSO	1	2	3	4	5	6	7	8
Perform risk assessment	±	+	+	±	-	±	+	+
Risk assessment is regular procedure	-	-	+	±	-	±	+	-
Measures implemented after risk assessment	-	+	-	±	-	±	±	+
Information security policy implemented	-	+	+	±	-	±	+	+
List of assets of critical infrastructures	+	+	+	+	-	±	+	+

As presented in Table I, half of the TSOs of the observed region perform risk assessment, but only two of them regularly. A general characteristic of the region is that the TSOs maintain lists of assets of critical infrastructures, which is essential aspect of the development of adequate security policy that refers to those assets. Although not all analysed companies implement risk assessment-based security policy, it should be noted that all of them implement security measures that are based on the assessment of the information and communication departments in the companies and common approach of TSOs in organizing their information infrastructure.

B. Protection

The set of cyber security measures consist of protective and defence measures. The protective measures encompass the information systems architecture, administration, identity and access management and maintenance. Concerning the architecture of the information systems [11], the operator should only connect equipment and/or install services and applications that are necessary for the functioning of the critical infrastructure. It should consider measures to segregate systems to avoid propagation of threats. However, when interfacing of systems is needed, the OES should apply additional measures for protection as traffic filtering (deny flows that aren't necessary for the functioning of the systems) in the CII to decrease the possibilities for a cyber-attack. A cryptography policy may be implemented to protect information confidentiality, authenticity and integrity in the infrastructure.

From the aspect of administration [11], OES should set up specific accounts for employees performing installations, configuration, management, maintenance and other system administration activities. These accounts should be used to connect to the system, after which administrator accounts should be used to perform the actual administration activities. Identity and access management include set of protective measures that minimize possibilities for unauthorized access to systems and processes related to CII. Unique accounts should be used as a part of the identification process. In addition, authentication credentials should be required for accessing systems and processes related to critical infrastructure.

Table II and III summarize the protection measures to minimize propagation of threats and of external access to the CIIs, respectively.

TABLE II
MEASURES TO MINIMIZE PROPAGATION OF THREATS IMPLEMENTED BY SEE TSOS

TSO	**System architecture – propagation of threats**
TSO1	Segregation, firewalls
TSO2	Implements adequate measures
TSO3	Secure protocol algorithms, advanced cryptography algorithms
TSO4	Security measures for e-mails and web traffic, sandbox solution for zero-day malware protection for network and email traffic
TSO5	Implements standard practices
TSO6	Segregation, firewalls, anti-malware, traffic filtering
TSO7	Segregation, LAN segmentation, traffic filtering, IPsec encryption
TSO8	Traffic filtering, cryptography

TABLE III
MEASURES TO MINIMIZE EXTERNAL ACCESS BY SEE TSOS

TSO	**System administration – external access**
TSO1	Secure VPN connections with authentication and authorization of access control
TSO2	Implements adequate measures
TSO3	VPN secure connections, personalized accounts with limited duration for specific tasks and access to dedicated isolated intranet zone
TSO4	Secure VPN connections with authentication and authorization of access control
TSO5	No reply
TSO6	Administration accounts with limited duration, complex passwords, and limited access, data backup, dedicated network for network administration
TSO7	Administration accounts with limited duration, dedicated network for network administration, authentication and encryption mechanisms
TSO8	VPN connections with authentication and authorization of access control

Table II shows that some of the protection measures are more common, as segregation, traffic filtering to control flows, firewalls and anti-malware. Similarly, as presented in Table III, the administration of critical infrastructure is usually performed using accounts that have some form of restriction (time duration limit, password protection, access restrictions). Concerning access rights, some of the end users implement (or

plan to implement) multifactor user authentication and some are using various access levels for different users.

The protection measures used for SCADA systems are summarized in Table IV.

TABLE IV
SCADA PROTECTION IN SEE TSOS

TSO	**SCADA protection measures**
TSO1	Segregation
TSO2	No internet access, firewalls, segregation
TSO3	Segregation, firewalls
TSO4	Dedicated firewall systems with next generation functionalities and comprehensive SCADA protocol support
TSO5	No reply
TSO6	Restricted network access for different services to one host, remote access via VPN allowed to dedicated serves only, dedicated network for system administration
TSO7	Segregation, LAN segmentation
TSO8	No internet access, closed network (segregation)

C. Defence

The defence of the CIIs includes implementation of measures for detection of threats, setting up logging systems on each CIIs to record events, as well as log correlation and analysis system. Detection of threats is the most important step in providing adequate system response. The second step is creating logs of events, especially for access, management of access rights and modifications of security policy. With appropriate log correlation and analysis system, the operator should be capable of data mining for events that have implications to security of CIIs. The summary of the results of the threat detection measures implemented by the TSOs in the observed region is available in Table V.

TABLE V
DEFENCE OF CIIS IN SEE TSOS

TSO	**Threat detection measures**
TSO1	Log analysis
TSO2	System control of network traffic
TSO3	Monitoring and logs
TSO4	Event or alarm logs
TSO5	No reply
TSO6	Event or alarm logs, threat detection systems
TSO7	Event or alarm logs
TSO8	System control of network traffic

It can be observed that all TSOs apply threat detection systems (mostly event logs and their analyses). However, the investigation showed that incident reporting procedures for some of the TSOs are subject of ongoing changes, which will be completed in near future. The notification procedures are under development and in two cases the ENTSO-E Wide Awareness System is implemented.

IV. CONCLUSION

The paper presents an overview of the various protective and defence measures implemented by the TSOs of the SEE region. The results show that risk assessment procedures should be implemented on regular bases and used to develop adequate security policies for the CIIs. The TSOs implement various protective measures to minimize propagation of threats or unauthorized access and to limit access to the CIIs and to protect CIIs from external parties. Stronger cooperation and regional approach to threat defence is required, especially related to notification of threats to relevant bodies in neighbouring countries. Further cooperation between TSOs and early implementation of the relevant EU legislation in the WB countries shall increase the security of CIIs in the observed region.

ACKNOWLEDGEMENT

The authors would like to acknowledge the support of colleagues from system operators, who took part in the survey to respond to the questionnaire and kindly shared their knowledge and experience. This research is supported by the EU H2020 project CROSSBOW (Grant Agreement no. 773430). This paper reflects only the author's views and neither the Agency nor the Commission are responsible for any use that may be made of the information contained therein.

REFERENCES

[1] M. S. Thomas, J. D. McDonald, *Power System SCADA and Smart Grids*, Boca Raton, CRC Press, 2015.
[2] V. Borozan, A. Krkoleva Mateska, P. Krstevski, R. Taleski, S. Borozan, "D3.2 Privacy and Data Protection in a Multi-Actor Environment", CROSSBOW H2020-773430, January 2019.
[3] EECSP, "Cyber Security in the Energy Sector- Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector," February 2018.
[4] CROSSBOW, available [Online] http://crossbowproject.eu/
[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[6] Directive 2008/114/EC – identification and designation of European critical infrastructures and assess-ment of the need to improve their protection.
[7] Memorandum of Understanding of Western Balkan 6 on Regional Electricity Marker Development and Establishing a Framework for Other Future Collaboration, 27 April 2017, Vienna, available [Online] https://energy-community.org/regionalinitiatives/WB6/MoU.html
[8] Energy Community, "Study on Cybersecurity in the energy sector of the Energy Community," Ljubljana, September, 2018.
[9] Cooperation Group, Reference document on security measures for Operators of Essential Services, 2018
[10] ENISA, "Methodologies for the identification of Critical Information Infrastructure assets and services," 2014.
[11] ENISA, "Smart Grids Task Force EG2 Deliverable - Proposal of a list of security measures for smart grids," 2013.