Cyber Security strategies for the protection of Electrical Substations

Roberto Setola[1*] and Francesco Morelli[2]

[1] *Complex System & Security Lab, University Campus Bio-Medico of Rome, Rome,Italy*
[2] *ISACA Certified Information Security Manager (CISM), Italy*

Corresponding author

Abstract

The shift to widely distributed forms of energy generation and storage, requiring increased interconnectivity to geographically balance supply with distributed demand for electricity, creates a more complex electrical network. This complex network is generally labelled as the 'Internet of Energy' to stress the relevance that the digital components acquired in the electrical grid. But this introduces in the national electrical system new vulnerabilities related to the cyber risk. This paper illustrates the optimal approach that a TSO (Transmission System Operator) can adopt to manage such a risk in the electrical substations. Such an approach is based on the Zero Trust paradigm and is composed of technological, procedural and cultural elements in order to adequately manage cyber security issue all along the life cycle of any component..

Keywords

Cyber-security; Operational Technology; Cyber-Threat, Electric infrastructure, critical infrastructures

1. Introduction

The shift to widely distributed forms of energy generation and storage, requiring increased interconnectivity to geographically balance supply with distributed demand for electricity, creates a more complex electrical network. This complex network is generally labelled as the 'Internet of Energy' to stress the relevance that the digital components acquired in the electric grid. But this introduces in the electric grid new vulnerabilities related to the cyber risk. As noted by the World Energy Council [1] the resilience of the energy sector is greatly increased by digitalization as it enables the use of a complex and widening array of decentralized resources, improved efficiency, and enhanced abilities to detect threats, thereby increasing operational accessibility, productivity, sustainability, and safety. Unfortunately, at the same time, digitalization presents new challenges because a cyber events can affect operations producing severe degradation or even induce black-out.

The World Energy Council stressed that there are five factors that increase the vulnerability of the internet of energy, and specifically:

1) The rapid pace of innovation;
2) Technological complexity;
3) Data sharing and interconnectivity;
4) Rising cyberattack sophistication; and,

The sector's attractiveness as a cyber target.

In this paper we focalize specifically on the last two points due to their increased relevance because a wide range of malicious external actors target power grids motivated by financial goals, such as

ITASEC'22: Italian Conference on Cybersecurity, June 20–23, 2022, Rome, Italy
EMAIL: r.setola@unicampus.it
ORCID: 0000-0002-8792-2520 (A. 1); 0000-0001-7798-2936 (A. 2);

ransomware or intellectual property theft, or sometimes they aim to cause broader economic and social harm. In addition, like all organizations, energy companies can be collateral damage from an attack not directed at a specific company, such as fast-spreading malware like NotPetya attacks in 2017 and recently emphasized also by the Italian government CSIRT [2] in the framework of the consequences of the Russia-Ukraine war.

This fragility depends also by recent business-driven trends such as the standardization of protocols, the employment of off-the-shelves solutions and the augmented connectivity which significantly increased the vulnerable surface of industrial processes making them susceptible to be compromised via cyber-space as illustrated by the Aurora Project [3].

Episodes like Blackenergy 3 and CrashOverride which induced in 2015 and 2016 black-out in Ukraine [4,5] have shown that attacks of this fashion are possible but require the work of highly skilled and resourceful hackers. Even if impact of cyber-attacks remained far below the threshold of catastrophic events, cyber threat remains a crucial factor that jeopardizes the electric grid security.

However, they showed that targeting OT via cyber-space can lead to mechanical damage and that cyber-attacks involving kinetic consequences have become 'possible, available, significant and liable to disrupt the functioning of developed societies' [6].

The episode happened at Colonia Pipeline in 2022 showed that in the absence of an effective segregation between IT and OT system, malware can propagate also to operational system inducing also the showdown of the system.

This article will provide an overview of the approach that a TSO should adopt to improve the cyber resilience of a national High Voltage electrical grid.

2. National transmission grids

Electricity is not a storable commodity. It is therefore necessary to produce in each time instant the required quantity and distribute it through the system in such a way as to ensure that the demand and supply of electricity are always balanced, thus guaranteeing the continuity of service provision. This is a very complex task because electricity production and consumption are geographically located in different areas of the country, the consumption profile of users can only be partially estimated in advance, production (especially from renewable sources) may depend to a large extent on (unpredictable) weather conditions, and finally the state of the electricity grid must be taken into account to avoid overload conditions and to manage out-of-service events.

The management of electricity flows is known as dispatching and this activity is carried out by national Transmission System Operators (TSOs). These companies, which generally operate as national monopoly operators, manage the national transmission networks, i.e. those portions of the electricity grid that operate at high (36 kV - 150 kV) and extra-high voltage (220 kV - 380 kV) and are used to transfer significant amounts of electricity from generation plants and acquisition points from abroad to make it available to large users (generally connected to the medium-voltage network known as the distribution network to which domestic users are in turn connected on low-voltage networks). To this end, TSOs must constantly monitor electricity flows in order to ensure the instantaneous balance between available and used electricity at every point in the network. To do this, they have both the possibility of requesting a modulation in production capacity (limited to those power plants capable of dynamically modifying their production profile, such as hydroelectric and thermal power plants) or the disconnection of interruptible users, but above all to dynamically direct the flow of electric power in a manner consistent with instantaneous demand.

In Europe, all transmission grids are galvanically interconnected in order to ensure greater stability of the electric system and more effective management of electric power. This implies, however, that the actions taken by individual TSOs can have repercussions at the level of the European electricity system, with the consequence that any inappropriate actions can create even more or less extensive blackout events in other nations, as occurred in 2003 and 2006, hence TSOs have to cooperate exchanging information on electric status. To manage the power grid in the best possible way TSOs have equipped themselves with high-tech control systems, known as National Control Centers (NCCs). These centers represent the technological heart of the power grid overseeing all its operation and managing any anomality and critical situations. Specifically, NCCs, in addition to operating on the

modulation of electricity supply and demand (generation and consumption side), intervene on the grid's layout by dynamically changing its configuration through commands sent to the electrical sub-stations.

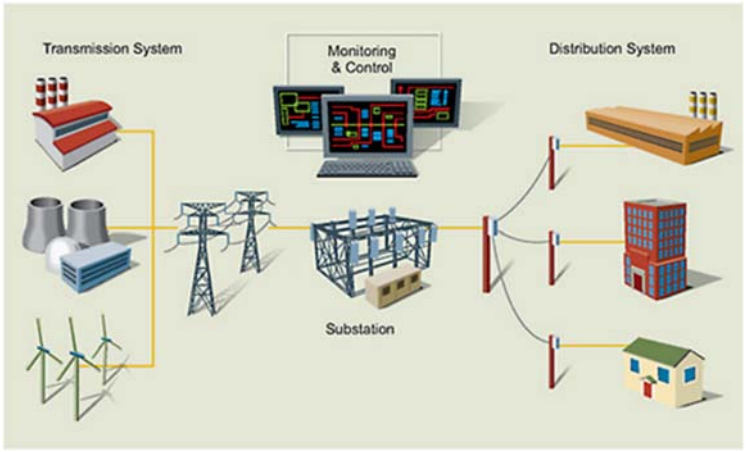

Figure 1: Schematic representation of TSO grid

Electric sub-stations are junction points where two or more branches of the electric grid, generally with different voltage, converge with the possibility of defining different configurations of the electric circuits in order to be able to direct the electric flow to instantaneously satisfy electrical constraints.

Modern substation architecture can be structured roughly in three-levels: process, bay and station [42, 43], as shown in Figure. 2.

The station level gathers information from the bay level devices for real-time supervision, monitoring and intervention by human experts. At this level are connected the computers dedicated to the supervision and management of the substation. It collects substation data like voltage, current, power factor etc. from the bay level devices and submit the control commands for the primary equipment (Circuit breakers) and collect the. Generally at Station Level there is one or more workstation used as HMI and for engineering purpose.

The bay level embedded devices control and interact with the process level equipment's. It acquires the data from the bay and then mainly act on the primary (power circuit) equipment of the bay. Generally a transformer with its related switchgear between the two busbars representing the two voltage levels forms one bay.

Process level extracts the information from sensors/transducers in the substation and to send them to upper level device. The other major task of process level function is to receive the control command from bay level device and execute it at the appropriate switch level. At process level there are different power devices like transformers, current/voltage transformers (CT/VT), circuit-breakers (CB), switch-gears, surge arresters, etc., which are essentially analog devices. Therefore, merging units (MU) are required to convert the analog signals, acquired/generated by the process level equipment, into digital signals. These information are transferred to the bay level, which comprises of the protection and control devices, which are embedded devices like DFRs, DPRs, IEDs, etc..

Modern substations are aimed to be more interconnected, leveraging communication standards like IEC 61850-9-2, and associated abstract data models and communication services like GOOSE, MMS, SMV. Such interconnection would enable fast and secure data transfer, sharing of the analytics information for various purposes like wide area monitoring, faster outage recovery, blackout prevention, distributed state estimation, etc. Such communication is mainly managed at station level.

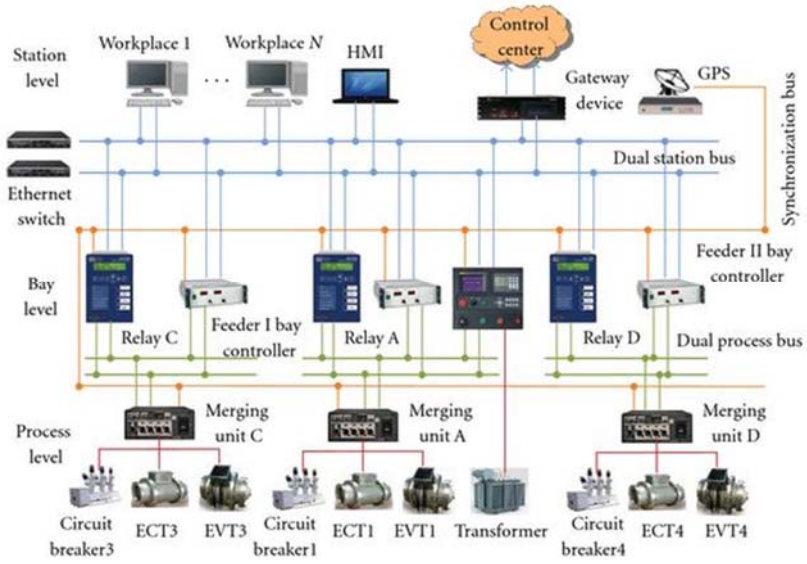

Figure 2: System architecture of the substation automation system in the 220 kV-132 kV transmission substation [41]

3. Operational Technology are inherently insecure

The acronym OT (Operational Technologies) refers to a set of interconnected systems that use physical elements, networks and communication protocols to perform industrial operations such as manufacturing, transportation and processing of goods [7]. Typical examples of OT are industrial control systems (ICS), control and data acquisition (SCADA) systems, and distributed control systems (DCS). These, despite being different and highly customized, are based on similar key components that enable them to perform three essential tasks: data acquisition, control and supervision, and command execution [8, 9, 10]. Such systems are generally designed to guarantee the safety of supervised processes, and to this end they have to be compliant with the time dynamic of the underline physical process this induces specific constraints on the maximum reaction time and the need to have high availability requirements.

OTs are generally characterized by the exchange of huge amounts of small information (limited-sized packets from a plethora of different sources) and high levels of determinism and very low latency. Thus, including elements such as encryptions, antivirus and firewalls means incorporating control routines that could affect the smooth running of activities by generating delays that, while quantitatively insignificant, make the control system less ready, preventing it from meeting the "hard real-time" requirements for which it was designed.

Another factor that undermines the implementation of security measures is the fact that the OT must operate continuously 24x365, which makes maintenance work extremely costly and problematic. Maintaining a system through the introduction of patches and updates requires infrastructure downtime [11], which implies that updating must be planned well in advance and cannot immediately follow path realise. In addition, patching is considered a risky task, as any change could produce unexpected effects. Preventing these effects would mean specific and targeted testing, the cost of which is often prohibitive [12].

Therefore, once installed and certified for safety, OTs remain in operation for up to 20 years with limited modifications, leading the operator to work with out-of-date software and inadequate assets with inherent instability, critical failure points, and security holes. Similarly, as reported in [13], only 10 percent of customers install patches and updates for programmable logic controllers (PLCs), leaving existing software with innate vulnerabilities susceptible to attacks [14].

As mentioned earlier, one of the primary needs for OT are the hard real time and high availability requirements which leaves little room for cybersecurity measures. In OT context, for a long time the

only protective barrier has been the so-called "*security through obscurity*" Previously, control systems were based on legacy systems running on networks that were physically isolated from company IT environment and without any connection with Internet and external networks [15, 16]. In addition, OT systems employed proprietary protocols unique to the industrial environment and tailored to the supervised industrial process. This isolation allows to promote a *security by obscurity* approach were the integrity of a system were "guaranteed" by the impossibility to physical access to the industrial network and by the difficulties to acquire in-depth knowledge of the proprietary software in use. As a result, industrial systems were considered reasonably immune to external cyber attacks and the main threat was perceived as insider [17], e.g. a "disgruntled worker" seeking revenge [15]. In fact, until 2010, the only cyber attack targeting control systems occurred in Maroochy Shire (Australia), where a former employer hacked the city's water control system and caused 800,000 liters of raw sewage to spill, resulting in significant environmental and economic damage [18].

Nowadays, OT-based sites can no longer rely on security by obscurity paradigm. In fact, modern processes, to improve efficiency, are largely based on off-the-shelf software and component and it is mandatory that OT networks can exchange data with company IT network or even be connected to internet to allow remote maintenance, monitoring and control. This imply that the OT devices used to control physical processes, which previously communicated through closed networks, are now connected not only to the corporate network but also to the Internet [19]. These developments are business-oriented and aim to meet growing operational needs. While they have dramatically reduced the cost of purchasing, installing, and maintaining OTs, as well as optimized the performance and maximized the availability of systems, the general trend to "connect the unconnected" [19, 20] has exponentially increased the vulnerable surface of OTs [21], with significant implications for cybersecurity [22].

This business-driven trends have led to a change in the nature of cyber-threats. In fact, if between 1982 and 2000 70% of attacks were internal, from 2000 to 2003 the number of attacks originated externally increased to 70% [23]. This progressive trend reversal is a direct consequence of the use for OT of off-the-shelf IT hardware and software included the use of commercial operative systema (e.g. Windows NT) and network protocol (e.g. TCP/IP) and it is unlikely to decrease in the future.

This elements, together with a significant increase in the frequency of cyber-attacks [24], have raised a great concern about the threats stemming from cyberspace. In 2009, a survey involving six hundred IT and security executives showed that most respondents held that a major cyber-operation involving as target the OT components of Critical Infrastructures was imminent [25].

Cyber-attacks might pursuit several goals. They could have a criminal nature, for example inflicting reputational damages [26] or locking data/system and ask for a ransom [27]. They could be business driven, thus with the aim of stealing valuable data or confidential information on production statistics, market strategies, drilling plans and pricing sheets [28, 29]. However, the most critical aspect of OT vulnerability is that cyber-attacks could have not only an economic impact, but also a kinetic one. Indeed, by modifying the normal functioning of a process, attackers are able to induce failures and mechanical break points. This was proved in 2007 with the Aurora Project, in which a cyber-attack targeting an industrial power generator was simulated [30]. As asserted in 2012 by the former U.S. Defense Secretary Leon E. Panetta, a successful operation could result in a 'cyber-Pearl Harbour' if a group gained 'control of critical switches' [31].

As concrete examples of such scenario, BlackEnergy 3 and CRASHOVERRIDE are considered to have originated power outages in Ukraine. The first attack manifested itself on the 23rd of December 2015 and caused a loss of power for six hours that affected around 225,000 customers. The adversaries used BlackEnergy 3 malware to pivot into the SCADA environment and take control of the operation. Once intruded, they leveraged the system to disconnect substations from the grid, which caused the blackout [32, 33]. Approximatively one year later, CRASHOVERRIDE, known also as Industroyer, deprived power to a part of Kiev and its surroundings for over an hour [34]. CRASHOVERRIDE allowed the attackers to take direct control of the substation breakers that were then opened, which provoked a temporary loss of power [32, 34].

An interesting peculiarity of these attacks is that it was not the malware which directly caused the loss of power. Both BlackEnergy 3 and CRASHOVERRIDE allowed the attackers to take control of the industrial operations and sent legitimate command to the substation, and such commands where able to induce anomalous behavior in the electric grid. In other terms the malwares were able to generate

a sophisticated sequences of legitimate commands which malicious interaction with the physical system provoked the outages [32, 45, 36]. This means that the main focus of the attack was not con the payloads themselves, but rather on the adversary's knowledge and ability to interact with the system [35]. In other words, if attackers find another entry-point into the industrial network, they would be capable of successfully repeating the attack regardless of the patches put in place by the defender.

4. Strategy for cyber-security of OT systems

In this paper we focalize on the cyber security of the electric substation. Such a motivation is based on the relevance that elements play for the stability of the electric grid. Indeed, as shown by the attacks in Ukrainian, a successful cyber attack is able to induce a blackout in large portion of population. Moreover being unattended and geographically dispersed sites generically located in rural areas with very low population density, their protection also from the physical point of view is a complex task. Finally the tight hard real time constraints which characterize the control schema, with maximum latency in the order of milliseconds, makes very challenging their cyber-protection.

However substations are, by their nature, comparable to distributed IT systems and, for this reason, they must be protected by implementing adequate organizational, process and technological countermeasures throughout their entire life cycle. Hence an adequate strategy to improve their cyber security involving all the components of the electric substation needs to be developed to guarantee the "construction" of a secure Cyber posture and the maintenance, until decommissioning, of the required level of protection.

This consideration should inspire any TSOs to create cyber resilient strategies which involve both technical and no-technical aspects and must be able to permeate all company divisions so that the departments dealing with substation procurement, operation, maintenance and decommissioning are fully involved and aware of the implications that failure to comply with cyber-security procedures could have in terms of negative effects on the electricity grid.

Such a strategy must include both cultural, procedural and technological elements. Even if in this paper we mainly focalize on the technological aspects, we consider mandatory to provide before a short description of the best practice that should be adopted to increase the cyber security culture in TSOs and about the procedure to manage the cyber security element along all the life cycle of any component of the electrical substations.

4.1. Cultural initiative and Cyber Security organization

To be able to implement an effective cyber protection strategy, it is mandatory that TSOs should have a dedicated structure to manage all the aspects related with the management of OT cyber security. Such a structure should have adequate decision-making autonomy and sufficient capacity to influence the various business processes in order to impose appropriate attention to cyber security issues in all decision-making and operational processes. Moreover, such a structure facilitates the development of a dedicated team with high skilled and specialization personnel with in-depth knowledge of both cyber and process issues.

Th e presence of a such a dedicated structure will ensure adequate governance and constant innovation of the cyber security architecture. This structure should supervision all the aspects related to the OT cyber issues and, among others, should:

- support the definition of security requirements in all the phases of the "life cycle" (design, acquisition, implementation, operation and decommissioning) of OT systems, components and services used to manage the high-voltage electric grid;
- ensure the constant development of defense and protection systems for the digital perimeter;
- carry out with adequate frequency cyber security assessment activities;
- guaranteeing centralized monitoring in real time of the cyber perimeters and ICT platforms (including those in the industrial sector);

- manage and coordinate security incidents in all their phases (detection, reaction, manage, forensic and post-event low up) included the management of relationship with law-enforcement and national cyber agencies;
- ensure the operation and ordinary and extraordinary maintenance of IT systems and applications in support of cyber security management activities;
- coordinate and promote corporate awareness & training initiatives in the cyber security area.

The last point should be one of the cornerstones of any cyber security strategy [37], this because human incorrect operation is at the base of almost 80% of Cyber Attacks successes [38]. In this regard, TSOs should develop campaigns to increase the digital culture and cyber security posture of the employers not only within the company, but also outside the company perimeter with suppliers and customers, thus increasing the awareness of all the actors involved, especially in the face of an exponential interconnection and sharing of digital data. Such initiatives should include, but not limited, specific training courses on cyber security issues for the personnel involving in the operation of OT and substation systems [39]. Moreover specific campaigns should be constantly carrying out to test the effective level of awareness of the personnel for cyber security issue [40].

4.2. Cyber Security procedure

How to manage cyber security issue in Electrical Substation must be codified within a specific standard in which a guideline is provided for the entire life cycle of digital station systems, consistently with the cyber security strategy. This to avoid to have multiple and potentially clashing requirements documents and also to have a repository where such information are collected and easily available. Such requirements have been inspired by the NIST 800-82 [8], but it is important to extended and customized the requirements on the base of the peculiarities of each environment in order to be immediately applicable to the specific TSOs' scenario. A factor that significantly affects this aspect is the different obsolescence level of the various technologies used within the substation, this because IT components, so as the OT components, have times of obsolescence much shorter than those of the electromechanical components.

An overview of the macro-areas that should be included in the standard is reported in the Table 1

Table 1
Standard for the Cyber Security of Digital Electric Substation Systems

Rule for	*Description*
System acquisition	policy regarding security check and constraints for software and hardware acquisition, development, integration, implementation and configuration. Elements that are not fully compliant with such criteria should not be installed in the OT environment
Configuration management and system integrity	set of activities focused on creating and maintaining the integrity of IT products and information systems, through the control of processes for initialization, modification and monitoring of configurations during the life of the element
System maintenance	checks regarding system maintenance, in particular regarding the presence of documentation and the regularity of maintenance interventions
Compliance and accreditation	continuous assessment procedures for the effectiveness of security controls and the implementation of privacy controls
Physical and environmental protection	measures to be taken to protect systems, buildings and related support infrastructures from accidental and malicious threats related with physical dimension and environment
Identification and authentication	guideline of the process that establishes the identity of an entity that interacts with the system. This element includes also the specification

	for access control, i.e. the process of granting or refusing specific requests for: • obtain and use information and related IT services; • access specific physical facilities
Traceability	set of activities to ensure the traceability of system operations and the availability of logs for legislation issue and for forensic activities
System and communications protection	rules for the implementation of security controls for any communication and data transfer
Contingency planning	provisional measures to restore services following an emergency or a system outage
Risk assessment	guideline of the process of identifying risks for operations, resources and individuals resulting from the operation of an IT system
Supply chain risk management	prescription for managing exposure to risks, threats and vulnerabilities in the supply chain and for developing strategies in response to the risks presented by third parties, by the products and services provided

As stressed by the last issue of the standard, it is mandatory that all the actors involved in the supply chain be actively involved in the risk analysis phase and for the management of the cyber security. Suppliers need to be compliant with cyber security technical specifications and to they have to guarantee an adequate level of cyber awareness. Moreover, in the supply contract should be explicitly included specific service level agreement (SLA) on the procedure to manage any situation when vulnerability are discovered/realized, specific procedures and time schedule to release and implement security patch, and also the procedure to manage specific contingency plan and to be involved in the risk assessment process.

4.3. Cyber Security architecture for Station

In line with the evolution of the Substation Automation Systems which have enabled various new functions (e.g. remote control), TSOs have to adapted their technologies and processes to ensure high protection and monitoring capacity of industrial systems.

Such approach should be inspired by the well-know principles of the *Security by Design,* i.e.:

- **Defense in Depth**: the cybersecurity strategy should be arranged as a series of different layered defense mechanisms each one characterize by peculiar mechanism and solution. In this scenario, if one mechanism fails, another immediately takes its place to counter an attack. This multi-layered redundant approach is able to increase the security of the entire system and addresses many different attack vectors;
- **Least-Privilege**: any user, person or software agent, is granted with the minimum levels of permissions that he/she needs to carry out his duties;
- **Deny-by-Default**: grants permission only what is explicitly authorized, while the rest is prohibited by default.

But it is important to implement the more innovative and recent approaches generally labelled as *Zero Trust* in compliance with the guidelines dictated by international industry standards such as, for example, NIST SP 800-82 [8] and ISO 27001: 2013. Inside a Zero Trust schema nothing, both internal and external to the network perimeter of an organization, is considered trusted by default,

A cornerstone element of this strategy is an effective segregation between IT and OT infrastructure (suggested also recently by Italian CISRT in response to the cyber risk related with Ukraine-Russia war). Such a segregation actually operates at two level from one side the IT network is segregated with respect to central OT network but also the central OT network is segregated from the OT networks distributed in the substations. This means that any malicious packed even if gained the access to the IT environment had to overcome two different type of firewalls before to be able to reach any single substation.

However, it must be considered that an attack can be carried out either by gaining physical access to the substation, which is generally unprotected, or by intercepting communications to/from the control center and the communications exchanged between substations. Hence the physical protection of a substation is the very first barrier to prevent a dangerous cyber attack and it should be carefully designed and continuously checked.

On the other side protecting communications is a challenge because only in some cases the substations are connected via proprietary fiber optics cable, while in general they use commercial or LTE links. However, the presence of a firewall is a useful tool to mitigate such a risk.

More complex is the protection of communication between substations, due to very stringent requirements on latency (generally less than 1 ms) that make unfeasible the presence of any on-line filtering component, i.e. this flow cannot generally be monitored by the firewall.

To partially overcome these difficulties, it is strongly recommended that each substation be equipped with an Anomaly Detection System (ADS) with signatures for industrial environments that, operating in parallel with the flow, is able to discover anomalous situations without interfering with the process.

The presence of the ADS, possibly integrated with the firewall in an Intrusion Prevention Systems (IPS), is also a protection mechanism for possible cyber attacks launched from the in-field devices by exploiting the connection with the 'bay' area.

In addition, it is useful to equip substation with control tools able to prevent unauthorized users or codes from accessing the station's computer. To this end, such a tools should:

- deny permission to execute any application or process not specifically approved (e.g. whitelisting);
- management of asset access policies based on the user's profile;

TSOs must be equipped with specific centralised asset management tools that guarantee the visibility of the network and technological elements of industrial systems.

The presence of a specific Cyber Threat Intelligence services for the industrial domain, is useful to promptly identify any external threats that put the company's information assets and critical services at risk. This allow to adopt pro-active measurements in order to prevent cyber attack.

Finally it is very useful to equip any substation with specific tools for carrying out vulnerability assessment campaigns (passive scanning on production environments, active scanning on test and experimental environments) in order to support the delivery of this instrumentation without create degradation in the operational environment.

In order to be more effective, it is strongly recommended to set up one or more test environments able to reproduce with high fidelity the architecture of the substations [40]. This test environment dedicated may be used to:

- check the effectiveness of patch and the absence of any side effect;
- analyze potential impact of malware or virus on the operation capabilities of the substation;
- experiment innovative technological security solutions;
- recreate real conditions of use suitable for experimenting with cyber security solutions to be used for the protection of assets;
- develop and experiment innovative communication procedures to support Cyber Security Awareness program
- create a Digital Twin of some portions of the industrial systems infrastructure, replicating the current operating ecosystem in order to carry out vulnerability analyzes and penetration tests.

5. Conclusion

In the framework of energy transition and network digitalization, the introduction of new technologies in the OT, IoT and Edge Computing fields brings great benefits and great opportunities for the evolution of the electricity system, but also inevitable new correlated cyber risks [39].

Cyber Security in TSOs is now an enabling factor for advanced planning, in the face of an ever-increasing complexity and unpredictability of threats, which require strengthening risk mitigation tools

and reducing reaction times to attacks. These objectives can be effectively pursued through an organization equipped with adequate technologies, processes and human resources.

The experience made by several TSOs confirms that an effective response to cyber threats can be given by a structure that manages the process end-to-end in an agile manner by using an operational strategy in which the mix of insourcing and outsourcing is dynamically modified in the safety principles and contributing to the achievement of the company's strategic objectives.

6. References

[1] World Energy Council "*Cyber challenges to the energy transition*" Report 2019 https://www.worldenergy.org/assets/downloads/Cyber_Challenges_to_the_Energy_Transition_WEC_MMC_2019.pdf

[2] CSIRT (2021) https://www.csirt.gov.it/crisi-ucraina-analisi-del-rischio-tecnologico-e-diversificazione

[3] Assenza, Giacomo, et al. (2020) "Cyber threats for operational technologies". *International Journal of System of Systems Engineering* 10.2: 128-142..

[4] Lee, R. M., Assante, M. J., & Conway, T. (2017). German steel mill cyber-attack. *Industrial Control Systems*, 30, 62;)

[5] Assante, M. (2018). Triton/TriSIS – In Search of its Twin. SANS Industrial Control Systems. 29 January. Available at: https://ics.sans.org/blog/2018/01/29/tritontrisis-in-search-of-its-twin

[6] Tabansky, L. (2011). Critical Infrastructure Protection against cyber threats. *Military and Strategic Affairs*, 3(2) 61-68

[7] Setola, R., Faramondi, L., Salzano, E., & Cozzani, V. (2019). An overview of Cyber Attack to Industrial Control System. *Chemical Engineering Transactions*, 77, 907-912.

[8] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security, *NIST special publication 800-82*, National Institute of Standards and Technology;

[9] Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G. & Ueda, K. (2016). Cyber-physical systems in manufacturing. *Cirp Annals*, 65(2), 621-641.

[10] Bhatkar, V. (2017). *Distributed Computer Control Systems in Industrial Automation*. Routledge.

[11] Cook, A., Janicke, H., Smith, R., & Maglaras, L. (2017). The industrial control system cyber defence triage process. *Computers & Security*, 70, 467-481

[12] McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5), 1039-1057 [13](Bodenheim, 2014)

[13] Engels, J. I. (2018). *Key Concepts for Critical Infrastructure Research*. Springer

[14] Galloway, B., & Hancke, G. P. (2013). Introduction to industrial control networks. *IEEE Communications surveys & tutorials*, 15(2), 860-880.

[15] Mansfield-Devine, S. (2019). The state of operational technology security. *Network Security*, 2019(10), 9-13.

[16] Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. *In Proceedings of the VDE Kongress* (Vol. 116, pp. 213-218)

[17] Hemsley, K., & Fisher, R. (2018). A History of Cyber Incidents and Threats Involving Industrial Control Systems. In *International Conference on Critical Infrastructure Protection* (pp. 215-242). Springer, Cham.

[18] Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *Design Automation Conference (DAC)*, 2015 52nd ACM/EDAC/IEEE (pp. 1-6). IEEE [20] (Knowles & al., 2015)

[19] Drias, Z., Serhrouchni, A., & Vogel, O. (2015). Analysis of cyber security for industrial control systems. In C*yber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, 2015 International Conference on (pp. 1-8). IEEE. [22] (Ani, He & Tiwari, 2017).

[20] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. I*nternational Journal of Critical Infrastructure Protection*, 9, 52-80.

[21] Kaspersky lab ICS-CERT, (2017). *Threat Landscape for Industrial Automation Systems* In The Second Half Of 2016, Kaspersky Lab. Available: https://ics-cert.kaspersky.com/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/
[22] McAfee, (2009). In the Crossfire: *Critical Infrastructure in the Age of Cyber War*. McAfee report. Available at: https://img.en25.com/Web/McAfee/CIP_report_final_uk_fnl_lores.pdf
[23] Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, 45, 58-74.
[24] Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, 31(4), 418-436
[25] North America Oli & Gas Pipelines, (2013). Discussing the Role of Cyber Security in OilAns Gas Pipelines. At: https://scholar.google.com/scholar_case?case=5478245559776905776&hl=en&as_sdt=0,5
[26] Wright, L. (2017). Economic Espionage and Business Intelligence. In *People, Risk, and Security* (pp. 91-105). Palgrave Macmillan, London
[27] Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Research Challenges for the Security of Control Systems. In *HotSec*
[28] Bumiller, E. and Shanker, T. (2012). Panetta Warns of Dire Threat of Cyberattack on U.S, *The New York Times*, 11 October 2012 available at: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html
[29] Lee, R. (2017 a). *CRASHOVERRIDE: Analysis of the threat to electric grid operations*. Dragos Inc., March
[30] E-ISAC (2016). *Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center* (E-ISAC).
[31] ESET, (2017). ESET discovers dangerous malware designed to disrupt industrial control systems. ESET – *Enjoy Safer Technology*. 12 June, Available at: https://www.eset.com/us/about/newsroom/press-releases/eset-discovers-dangerous-malware-designed-to-disrupt-industrial-control-systems/
[32] Conway, T., Lee, R. M., & Assante, M. J. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Electricity Information Sharing and Analysis Center. Available at: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[33] Cherepanov, A. (2017). WIN32/INDUSTROYER, A new threat for industrial control systems. *White paper*, ESET (June 2017).
[34] Assenza, G., Chittaro, A., De Maggio, M. C., Mastrapasqua, M., & Setola, R. (2020). A review of methods for evaluating security awareness initiatives. *European Journal for Security Research*, 5(2), 259-287.
[35] [Corradini, I. (2020). B*uilding a cybersecurity culture in organizations* (Vol. 284). Berlin/Heidelberg, Germany: Springer International Publishing.
[36] Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. *International Journal of Critical Infrastructure Protection*, 25, 14-35.
[37] De Maggio, M. C., Mastrapasqua, M., Tesei, M., Chittaro, A., & Setola, R. (2019). How to improve the security awareness in complex organizations. *European Journal for Security Research*, 4(1), 33-49.
[38] Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, 1(1), 32-74.
[39] Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, 8, 53-66.
[40] Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K., & Reddi, R. (2011). A control system testbed to validate critical infrastructure protection concepts. *International Journal of Critical Infrastructure Protection*, 4(2), 88-103.
[41] Lu, X., Wang, W., & Ma, J. (2012). Authentication and integrity in the smart grid: An empirical study in substation automation systems. *International Journal of Distributed Sensor Networks*, 8(6), 175262.

[42] Chattopadhyay, A., Ukil, A., Jap, D., & Bhasin, S. (2017). Toward threat of implementation attacks on substation security: Case study on fault detection and isolation. *IEEE Transactions on Industrial Informatics*, 14(6), 2442-2451.
[43] Gupta, R. P. (2008, December). Substation automation using IEC61850 standard. In Fifteenth *National Power Systems Conference (NPSC),* IIT Bombay (pp. 462-466).