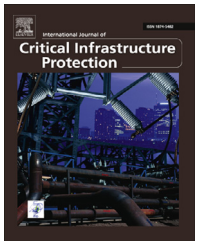
INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 18 (2017) 20–33

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/IJCIP



Cybersecurity protection for power grid control infrastructures

*Jacek Jarmakiewicz**, *Krzysztof Parobczak*, *Krzysztof Maślanka*

Faculty of Electronics, Military University of Technology, Kaliskiego 2, 01–476 Warsaw, Poland

ARTICLE INFO

Article history:
Received 3 March 2016
Revised 16 January 2017
Accepted 30 March 2017
Available online 20 July 2017

Keywords:
Power Grids
Industrial Control Systems
Power Grid Control
Cybersecurity

ABSTRACT

Modern power grid control systems are not isolated islands – disturbances in one system can cause instabilities or even blackouts in adjacent systems. Cyber attacks on power grids could result in significant economic losses. Indeed, cyber weapons have already targeted power systems in Europe.

This paper describes a cybersecurity protection approach for power grid control systems. It presents an analysis of a domestic power grid control system that emphasizes the identification of key elements of the infrastructure and their importance to power grid security. In addition, it provides a unique perspective based on experience with the system design process – from the identification of requirements to their application in operator control and supervisory substations. The paper also discusses how to verify the functionality provided by an implemented cybersecurity system. This approach is expected to assist in the design and implementation of power grid protection systems. Moreover, the approach can be adjusted to develop security systems for other critical infrastructure assets such as gas and chemical processing facilities, water and wastewater systems.

1. Introduction

The integration of the pan-European electricity transmission system, which began in 2009, has greatly influenced the reliability of operations, optimal management and sustainable development, the goal being to ensure the security of electricity supply and to meet the needs of the growing energy market [18]. As a result, the security of electric power generation and supply should be considered in the context of the entire continent.

The cooperation of domestic power systems is based on the European Network of Transmission System Operators (ENTSO-E) Agreement on International Cooperation, which was set up by 42 transmission system operators from 35 countries. The regulation [19] was made in anticipation of the adoption of legislative instruments in the Third Liberalization Package because of the need for transmission system operators to actively participate in rule setting for the European energy market. However, the integration process has been fraught with enormous challenges and threats to domestic systems. Of particular concern is the fact that disturbances in domestic power grids can propagate to external grids and negatively impact their stability.

The European electricity transmission grid and the European gas transmission network extend across national borders, which means that a failure of one portion of a network could propagate to other portions, potentially affecting several countries [16]. The cooperating domestic power systems, along with their foreign interconnections, must always maintain a balance between the energy generated and consumed. A sudden loss of generated power can disturb grid operations and damage generators, resulting in an electricity blackout to

* *Corresponding author.*
E-mail address: jjarmakiewicz@wat.edu.pl (J. Jarmakiewicz).

http://dx.doi.org/10.1016/j.ijcip.2017.07.002
1874-5482/

consumers in the local area or in a wide region. Recovering from a blackout could take several days or even several weeks, especially in the case of coal-fired power plants on which the Polish power sector is based [25,50,67].

A blackout in a given region and the inability to increase the capacity of energy sources could be caused by several events. In general, the possible events may be classified as: (i) technological events; (ii) environmental events; and (iii) human-induced events. Another classification involves four threat categories: (i) personal threats; (ii) physical threats; (iii) cyber threats; and (iv) environmental threats [64].

The 1998 power plant accident in Turów, Poland is an example of a random technical event where, due to the loss of load, the generator was torn out from the ground. Turów has turned out to be one of the biggest failures in the Polish power industry – building a new 400 MW generator with its automatic control infrastructure has been enormously expensive (more than one billion Euros) along with other consequences [26].

A solar eclipse in a large area, like the one that occurred in Europe on March 20, 2015, is an example of an environmental phenomenon that can cause a blackout [41]. To prevent blackouts, Italy and Spain terminated energy generation in all photovoltaic farms on the day of the eclipse [17].

Other environmental phenomena include earthquakes and tsunamis as in the case of Fukushima, Japan in 2011 [2]. However, a planned (and routine) disconnection on November 4, 2006 caused a power disruption in a German transmission system operator – the blackout affected more than 15 million customers in countries across Europe, including Austria, Belgium, France, Slovenia and Spain [67]. This blackout and others demonstrate that a single incident affecting a significant component of a power grid can affect electricity supply to regions, countries and even continents [16]. Unfortunately, such events are difficult to predict and mitigate.

Even more difficult to predict and mitigate are cyber attacks. The most spectacular attacks – such as Duqu [28], Stuxnet [22], Flame, Gauss [24] and BlackEnergy [39] – were politically and/or economically motivated and were financed by state-sponsored entities to be used against citizens, organizations and agencies in other countries [42,51]. In many instances, the attacking entities engaged individuals who were motivated by economic or ideological reasons. These attackers often had positions that gave them knowledge about and access to the targeted infrastructures that enabled them to launch attacks at the right moment. Such attackers can be discovered only after their actions produce negative effects.

In the case of the Ukraine blackout in December 2015, power systems were infected by the BlackEnergy malware [39], which leveraged a Secure Shell (SSH) backdoor [38]. Another attack using similar tools was directed at the Kiev airport [6,14]; in this case, the attack leveraged an infected Microsoft Word document [46]. Attacks against Turkish power systems and government and bank servers were executed in March 2015 [54]. In response to these attacks, in January 2016, Turkey supposedly conducted retaliatory cyber attacks against the Russian embassy in Israel [55].

A possible scenario involves an attack on control and supervisory substations (CSSs), field controllers and remote terminal units (RTUs) that use the IEC-870-5-104 protocol. By overwriting a buffer in device memory (e.g., buffer overflow exploit of an ABB PCU400 device described in Vulnerability Note VU#343971 [61]), a potential hacktivist, with access to the device network communications interface in the local-area network of a substation, could install malware that would enable him to control a group of remote terminal units. The attack would result in unanticipated load shedding by the generators that could induce an extensive blackout.

Another possible attack vector is the exploitation of vulnerabilities in supervisory control and data acquisition (SCADA) systems and human-machine interfaces (HMIs) such as those discovered in Siemens Tecnomatix software and described in ICS-ALERT-11-080-01 [30]. The malicious software could be delivered via an infected USB storage device or an infected laptop computer used by an employee during a maintenance operation. The attack could enable an attacker to control equipment in subordinate substations and potentially disable a national power grid.

The critical infrastructure – in particular, the power grid control system – is vital to every national economy. Inexpensive cyber attacks that target power grid control systems could impact entire countries or even a continent. This is why the design and implementation of cybersecurity protections for power grid control systems are vital. The potential impact of malicious actions could be reduced by monitoring internode traffic, continuously verifying compliance to protocol specifications and detecting anomalous control requests. The deployment of custom honeypots that emulate vulnerable intelligent electronic devices (IEDs) can provide insights into attacker motivation, behavior, techniques and tools before any real equipment is targeted. Additional layers for engineering access channel protection are also feasible; these could be achieved via monitored, virtualized access nodes instead of direct connections to substation equipment. Access should be provided only to legitimate operators and restrictions should be imposed on the sources and destinations of connections and traffic, and on the duration of maintenance operations; all the important actions should be recorded completely.

This paper describes a cybersecurity protection approach for power grid control systems that addresses the threats discussed above. It presents an analysis of a domestic power grid control system that emphasizes the identification of key infrastructure elements and their importance to power grid security. In addition, it provides a unique perspective based on the system design process – from the identification of requirements to their application in operator control and supervisory substations. Finally, the paper discusses the verification of the functionality provided by the implemented cybersecurity system.

2. Related work

An analysis of cybersecurity products for power control systems indicates that the market lacks integrated and comprehensive solutions despite the fact that manufacturers often claim that they have products that cover the entire cyberspace defense domain. Products designed for vulnerability assessments, penetration tests and holistic security audits are described in [63]; general information about solutions for protecting SCADA systems and the critical cyber infrastructure

are described in [64]. However, an analysis of these products only reveals general ideas about the architectures of the cyber protection systems; in most cases, the functionality is described without providing adequate implementation details.

The NERC CIP system [71] provides tools for cyber defense of power generation and critical infrastructure assets. According to the documentation, the system incorporates unidirectional security gateways of variable efficiency and various connection points to substations; the gateways are reportedly stronger than firewalls and have interfaces to an enterprise security information and event management (SIEM) system. However, the solution is designed for small- and medium-sized facilities and offers limited cybersecurity functionality and scalability. Moreover, the gateways introduce undesirable delays in a control network [48].

The Radiflow SCADA Security Portfolio [49], which is similar to the system described in this paper, incorporates a SCADA intrusion detection system (IDS), hardware edge router and gateways with integrated SCADA firewalls, virtual private networks (VPNs) and IPSec functionality. The system also includes a component that self-learns a SCADA network topology and an application that provides visualizations of network security events. The system is designed to detect anomalies and supervise the proper operation of control network elements. However, it requires a third-party security information and event management system for security event information processing, which leads to additional costs and introduces unpredictable vulnerabilities and interoperability issues. The system also incorporates mediation devices that convert the acquired data in various formats (e.g., HTTP, SNMP) to standard Syslog messages. Unlike other systems, it provides detailed information about important issues that arise in a power control network.

Tenable Network Security [62] recommends the use of its SecurityCenter application along with the Nessus tool to detect vulnerabilities, monitor traffic and identify events caused by unauthorized actions that may lead to resource compromises. The SecurityCenter application leverages passive vulnerability scanners and a log correlation engine.

The Israel Export Institute [32] lists several cybersecurity solutions for critical infrastructure assets; some of these solutions are designed to counter zero-day attacks on industrial systems. Other frameworks, tools and methodologies for cyber protection are described in [3,8,40,52,53,65]. Check Point Software Technologies [8] has developed a high-performance firewall with a virtual private network gateway and a SCADA intrusion prevention system (IPS).

Ultra Electronics 3eTI [66] offers a SCADA system solution that integrates several security tools. The solution processes security event data, alarms and alerts. However, the manufacturer concedes that the product is merely one component in a cyber defense system, not a comprehensive solution. The product requires additional security information and event management integration platforms and interfaces to provide the holistic situational awareness required in a power grid security control center.

An analysis of the available literature reveals that most efforts have focused on developing highly-specialized security solutions for industrial control systems. Sridhar et al. [56] discuss power grid infrastructure security, cybersecurity awareness and emerging research challenges. The latest control system security standards, guidelines and research are described in [37], with particular emphasis on European research projects. Methods and mechanisms for attack and anomaly detection are presented in [5,15,23,72], while research and development environments for evaluating cybersecurity solutions are discussed in [33,60,68]. Unfortunately, technical details about most of the proposed solutions and architectures are not released in order to protect intellectual property; this makes it difficult to assess the effectiveness of the security solutions.

3. Power grid system analysis

A power grid control system differs from a traditional information technology system in terms of its risk profile and mode of operation. The risks include impacts to human health and life, and environmental damage. A control system operates in a loop, which means that the sensors in electronic devices, switches, field breakers and generators are continually checked and the control strategy adjusts the actuators to maintain electrical characteristics such as angle, voltage and frequency stability within the desired ranges. Angle stability is related to the synchronization of generator rotor speed with system frequency. The sensors and actuators work in real time and the response time is critical; on the other hand, delays in information technology systems are more forgiving. Interested readers are referred to [58] for a comparison of industrial control systems versus traditional information technology systems.

This research conducted an analysis to identify the power grid elements that significantly impact the security of power grid control. Special attention was placed on control networks in power generation systems and high voltage transmission systems. The communications protocols are vital to power system control operations, especially for retrieving information from and sending control commands to field equipment. Control and supervisory substations are among the most important components of an energy infrastructure because they are crucial to power generation and delivery systems. Their importance is confirmed in an analysis performed on behalf of the European Commission [1].

Fig. 1 shows the multi-layer structure of the Polish power grid control system. The power system is centralized and energy generation is controlled by the Polish Power Grid Company JSC (PSE). PSE also serves as the transmission system operator (TSO) for the entire country. Energy is provided to customers by several competing distribution system operators (DSOs). The power system is divided into domains, where each domain is operated according to the business objectives of the distribution system operator. This fact has a significant impact on the design of a cybersecurity protection system – on one hand, the design must take into account the characteristics of the domains; on the other hand, it must ensure synergies via the exchange of security status data between the protected domains.

Power flows in the Polish power grid are controlled in real time by a load frequency control (LFC) system. The power supply method is centralized as a “secondary control process,”

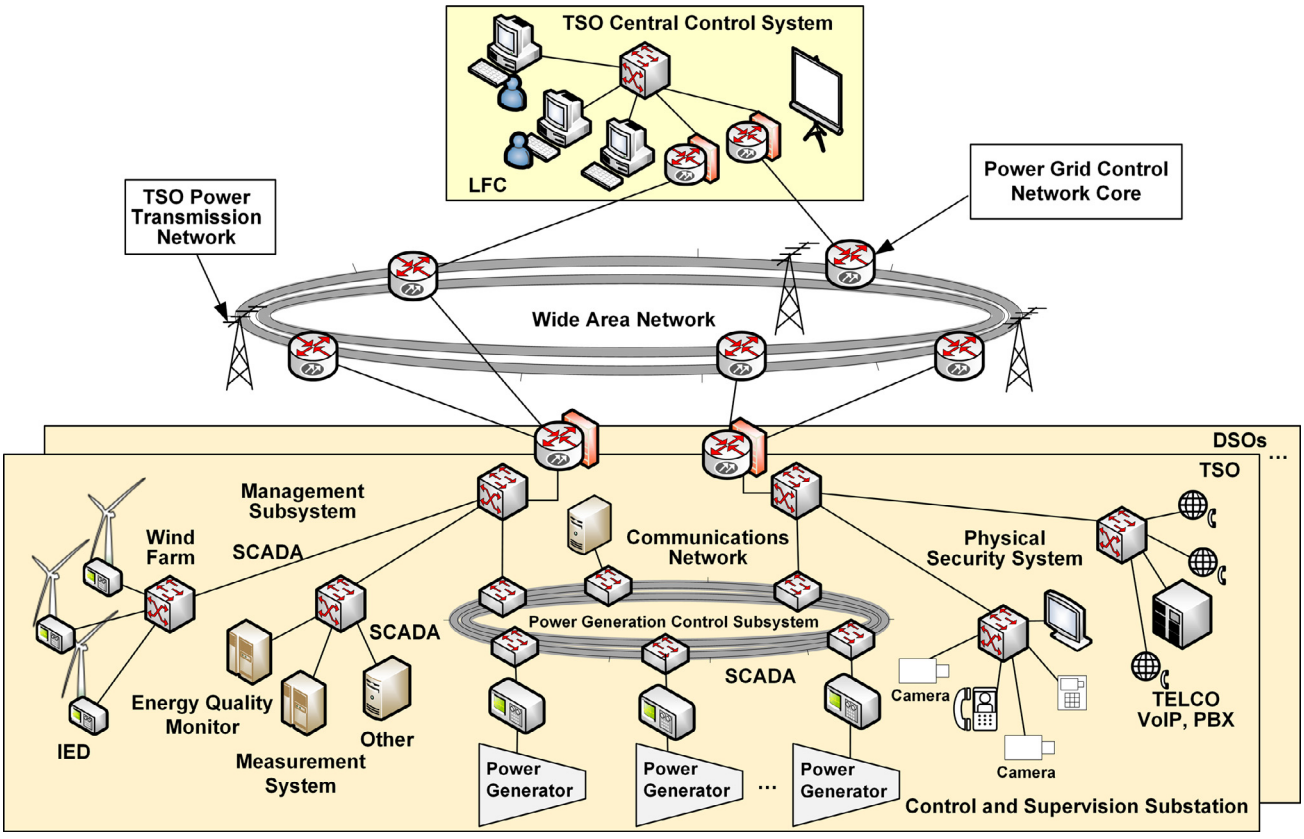


Fig. 1 – Multi-layer structure of the Polish power grid control system.

which means that the produced power is controlled by the central regulatory system. The power grid incorporates a combination of old and new control technologies. Several power generation facilities are more than 20 years old [31] and many of them still use analog devices. Nevertheless, the grid is being modernized and new intelligent electronic devices are replacing the older devices. The modernization improves power grid performance but paradoxically increases the vulnerability of the power grid to cyber attacks. Cybersecurity is a major issue for the power supply system because disturbances can have significant impacts on industry and citizenry.

The main task of energy services is to maintain the appropriate system settings in order to generate electricity that meets the ever-changing load demands of customers. Energy is supplied by power plants within 30 seconds from the moment a demand occurs [48]. In order to achieve this, the central control system (CCS) manages the energy supplied by power plants in real time. The load frequency control system is responsible for energy supply – it activates turbines and controls frequency and power. The central control system controllers operate in real time in a loopback mode.

Poland has 114 centrally-controlled generators in power plants [57]. Control messages are transmitted over an IPv4 network. SCADA protocol messages (IEC 60870-5-104 and IEC 61850) are encapsulated in TCP/IPv4 packets; this requires the network protocol stack to be implemented in every cybersecurity protection system. The control network is redundant and has a manual control feature.

The power grid enables electricity to be transported from sources through power lines and transformers to customers. Power transmission is supervised, monitored and performed at control and supervisory substations. The control and supervisory substations are critical elements of the national power grid infrastructure (Fig. 1). This infrastructure is susceptible to attacks due to its distributed nature and remote control features. SCADA systems installed in control and supervisory substations monitor and control field devices. Field devices control local operations such as opening and closing routes from energy sources to customers.

A security violation that results in inappropriate control could cause serious damage to power plants and large-scale blackouts. In addition to physical security, it is especially important to secure information and communications technology (ICT) and control systems. Tight time constraints for control data processing preclude the use of common encryption techniques in the power grid control system. Therefore, it is necessary to perform special monitoring of the data transferred to and from a control and supervisory substation.

A power grid control system typically evolves during the course of a cybersecurity protection system design process. Therefore, it is necessary to develop a reference model of the control system. The reference model in Fig. 2 shows the critical paths in the control system. Future power grid control system elements such as renewable energy sources are considered. The IP network in the control and supervisory substation is set up according to the modern transmission system operator

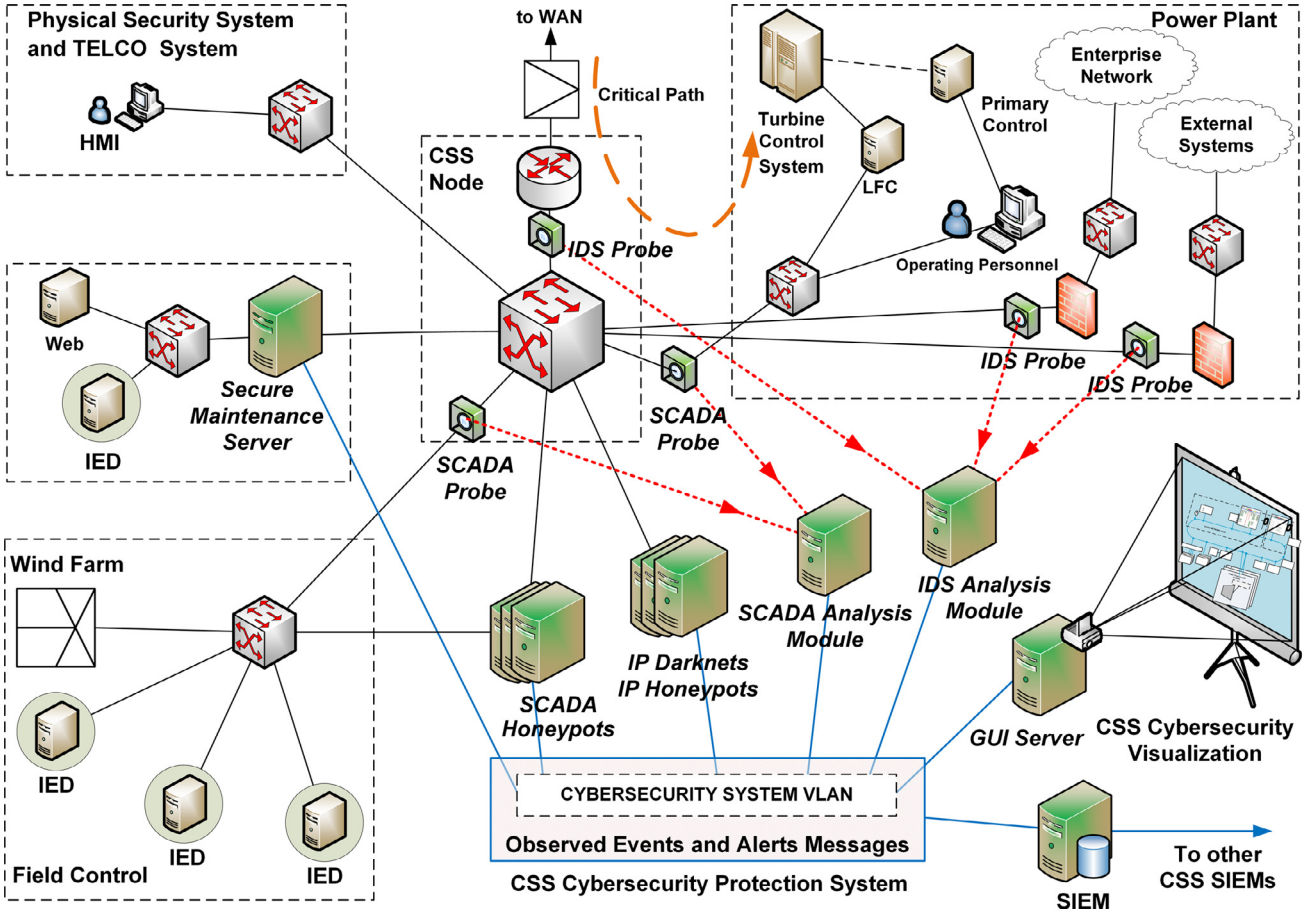


Fig. 2 – Power grid control system and the designed cybersecurity protection system.

station model [9]. The cybersecurity components, which are shaded green and labeled in italics, are described in detail in Section 5.

The operation and maintenance of control devices are also important issues that affect the design of the cybersecurity protection system. The control and supervisory substations typically comprise equipment from various manufacturers, making it necessary for external entities to be able to monitor and supervise operations in control and supervisory substations. It is especially important that the cybersecurity system detect unauthorized actions by authorized entities. It should also detect changes to the configurations of intelligent electronic devices, detect new equipment and software (e.g., USB drives installed in intelligent electronic devices and software upgrades) and store historical data about the use of resources.

4. Protection system requirements

In order to identify the cybersecurity protection system requirements, the following top-level objectives with regard to the technological infrastructure were elaborated with the assistance of a domestic transmission system operator:

- Creation of dedicated protection mechanisms that ensure an adequate level of cybersecurity against cyber crime.
- Continuous monitoring of cyber threats in the IP network infrastructure that supports power generation control and management subsystems.

The next step was to analyze the available literature focused on cybersecurity of industrial control systems. The literature specifies numerous high-level requirements such as data encryption, authenticated and authorized users, and anti-virus software [7,9,20,21,29,43–45,58,59,69,70].

Traditional information technology protection systems cannot be applied directly to control systems due to their tight real-time operational constraints. Their applications in industrial control environments require special precautions; in some cases, new customized security solutions are needed because traditional measures may not guarantee the secure operation of industrial control systems [13]. Moreover, in the case of power grid control systems, the cost of potential damage is too high to use off-the-shelf protection measures [58]. Additionally, a legacy solution such as MARS [27] may not be interoperable with control and supervisory substation components and other security solutions. Power grid control system implementations are not very different from each other, but no comprehensive and coherent view of a power grid security system exists.

Analysis of commercial cybersecurity solutions for power grid control systems conducted as part of this research

revealed that little, if any, information is released about comprehensive cybersecurity solutions for large-scale systems. Such solutions should be adapted to the properties of the power grid control system and should work synergistically with other systems that have already been installed. Indeed, protecting the highly networked and interdependent power grid infrastructure requires highly networked, holistic defenses.

The analysis yielded the following conclusions:

- A power grid control system is a centralized, multiply-redundant system.
- The business objectives of energy distributors are inherently conflicting; this is why they have to be covered by a data flow protection policy.
- In order to achieve synergy in a cybersecurity protection system, the exchange of safety messages has to be enabled between the various business entities. However, this must be controlled carefully using configurable cooperation profiles.
- The control and supervisory substations serve as interface elements between the power grid and energy producers and distributors. They are the critical elements of the power grid because the substations are responsible for ensuring the availability of energy to customers and ensuring appropriate loads on power generation facilities.

The conclusions listed above were used to formulate system requirements that take into account the limitations of a deployment environment. The MoSCoW methodology for requirements prioritization [10], which is used in project management and software development, was selected. MoSCoW is an acronym derived from the first letter of each of four prioritization categories: (i) must have; (ii) should have; (iii) could have; and (iv) would have.

More than 100 requirements were ultimately imposed on the cybersecurity protection system. Table 1 presents the requirements that were determined to be the most important and unique. The form of presentation was chosen to enhance the clarity and integrity of the security system with particular regard to interoperability with legacy cybersecurity solutions installed in the control networks of transmission system operators.

In the security system design process, the general requirements can be divided into those that are related to the operation of security elements and physical elements, and those that are related to good engineering practices in the administration of systems (e.g., authentication, authorization, encryption and user management). Supervisory mechanisms for all system processes should be considered to the extent possible. Moreover, it is good practice to organize the entries in the requirements list in a tree-like structure to maintain order and visualize the hierarchical associations between the entries as shown in the first column of Table 1. This representation also facilitates the transformation and management of the requirements in later development phases when using model creation and optimization tools such as Universal Modeling Language (UML) software. The developed system model enables each requirement to be assigned to the corresponding functions provided by the system components. This process facilitates an assessment of whether or not the designed system fulfills the requirements.

All the functional requirements listed in Table 1 correspond to the must priority category of the MoSCoW methodology. Additionally, requirements corresponding to all the implemented functions are assigned specific significance levels according to their roles in technological process correctness.

Technical conditions are important in addition to the business issues and conditions of cooperation between power system elements. In order to protect a power facility, information is required about the technologies that are used. Power grid control systems use two information models: (i) IEC 104; and (ii) IEC 61850, which has been introduced gradually; this has motivated the formulation of Requirement 1.1.2. The security of much of the power system depends on the success of threat detection in the control system (Requirement 1.1.2.1).

Consider, for example, the hierarchical dependencies of requirements in the cybersecurity awareness picture group. One of the elaborated high-level requirements (Requirement 3.2) can be ensured by implementing the functionalities that fulfill the lowest-level requirements (Requirement 3.2.1.1) directly. These are grouped in the Requirement 3.2.1 branch, which makes it possible to constitute additional requirements (not shown) to satisfy Requirement 3.2 adequately.

The requirements that result from the power grid control processes must not be ignored. Management processes that involve updating intelligent electronic device software and control and supervisory substations pose major threats. Unfortunately, the control and supervisory substations incorporate equipment from multiple manufacturers. It appears that controlling access to control and supervisory substations for maintenance purposes is impossible; however, maintenance processes can be supervised in an adequate manner by leveraging modern solutions such as virtualization technology. For this purpose, the requirements belonging to the engineering maintenance interface monitoring branch (Requirement 4.1) were formulated. During the formulation of the system requirements, the principle – that superior requirements resulting from the purpose of this work must be specified – was adopted. This has made it possible to define derivative functional requirements for which technical tests can be designed to confirm the implemented functionality.

5. Design and implementation

In designing the cybersecurity system, functional requirements were elaborated and formalized [47] in order to determine the technical cybersecurity measures that would be deployed. The security countermeasures for control and supervisory substations were driven by the functional requirements. Based on the analysis of the functional requirements, a notional architecture of the cybersecurity protection system was created [36]. The developed cybersecurity protection solution comprises several modules and, therefore, parts of the cybersecurity protection system may be used at each level of the power grid control system hierarchy.

Fig. 2 shows the cybersecurity protection solution for the power grid control infrastructure. The solution incorporates the following elements:

Table 1 – Key functional requirements of the developed cybersecurity protection system.

Req. no.	Requirement description	Leaf	Significance
Control system cyber attack detection and response			
1	Cybersecurity protection system must protect CSS LANs from remote cyber attacks.		
1.1	Cybersecurity protection system must support the elimination of attacks by preventing dangerous network traffic from reaching the destination.		
1.1.1	Cybersecurity protection system must support the blocking of attacks with known patterns.		
1.1.1.1	A traffic filter must be available to block known attacks in accordance with the configuration.	✓	*Medium*
1.1.2	Anomalous IED and SCADA (IEC 104, IEC 61850-MMS) over IP control traffic must be detected.		
1.1.2.1	Cybersecurity protection system must raise alarms upon detecting anomalous IED and SCADA (IEC 104, IEC 61850-MMS) over IP control traffic.	✓	High
1.1.2.2	Cybersecurity protection system must listen on all unused CSS subnet IP addresses in order to mimic SCADA systems using a honeypot decoy daemon.	✓	High
1.1.2.3	Cybersecurity protection system must listen on all unused subnets in CSS production systems (darknets).	✓	High
1.1.3	Overloading traffic (denial-of-service attacks) must be detected.	✓	*Medium*
1.2	All attack routes from multi-redundant directions must be secured.		
1.2.1	Network traffic that does not match the pre-configured patterns must be blocked.		Low
1.3	Security modules must deliver alarm notifications to the CSS SIEM system.	✓	High
Self-protection of cybersecurity protection system			
2.1	Cybersecurity protection system must monitor the structures and configurations of CSS LANs.	✓	Low
2.2	Cybersecurity protection system must monitor the operability of internal elements.		
2.2.1	Periodic "heartbeat" messages must be generated.	✓	High
2.2.2	Alarms must be raised when "heartbeat" messages from physical and software components are not received.	✓	High
2.2.3	Cybersecurity protection system must provide operators with information about the CSS security status.	✓	*Medium*
2.3	Security events must be registered in the cybersecurity protection system.		
2.3.1	Every administrative action on an element of the cybersecurity protection system must be registered with a non-modifiable record of the ID of the user who gained access.	✓	Low
2.3.2	Cybersecurity protection system must label security data and must supervise exchanged data.	✓	Low
2.4	Cybersecurity protection system must implement a remote registration service.	✓	Low
2.5	Correlations of event information must be made available from local and other CSSs, suggesting changes to the security configuration or other actions to the user.	✓	*Medium*
Cybersecurity awareness picture			
3.1	Cybersecurity protection system must support the sharing of knowledge about the security status of CSSs.		
3.1.1	Cybersecurity protection system must aggregate information pertaining to the local system and other collaborating CSS cybersecurity protection systems.	✓	Low
3.1.2	Cybersecurity protection system must collect, aggregate and exchange security information on its state with other CSS cybersecurity protection systems on demand and within the stipulated time constraints.	✓	*Medium*
3.1.3	Cybersecurity protection system must access information about the selected set of CSSs provided by other CSS cybersecurity protection systems.	✓	*Medium*
3.1.4	Cybersecurity protection system must exchange security information with collaborating CSS cybersecurity protection systems.	✓	*Medium*
3.2	Cybersecurity protection system must ensure the protection of federations and domains.		
3.2.1	Business interests of operators in different proprietary domains must be protected during the collaboration of CSS cybersecurity protection systems.		
3.2.1.1	The security policy between business entities must be followed.	✓	Low
3.3	Data transferred to external cybersecurity protection systems must be encrypted.	✓	High
3.4	Cybersecurity protection systems must mutually monitor the operability of other CSS systems.	✓	Low
3.5	Cybersecurity protection system must aggregate event information and alarms received from system elements and inform users.	✓	Low
3.6	Cybersecurity protection system must exchange alarms with other CSS cybersecurity systems.	✓	*Medium*
3.7	Cybersecurity protection system must monitor event logs and correlate data in order to detect threats.	✓	*Medium*
CSS engineering maintenance interface monitoring			
4.1	Cybersecurity protection system must provide secure access to substation resources through a centrally-supervised gateway.		
4.1.1	Cybersecurity protection system must implement mandatory access control of users of engineering maintenance interfaces.	✓	High
4.1.2	Cybersecurity protection system must provide non-repudiation by recording all the operations conducted via an engineering maintenance interface.	✓	*Medium*

(*continued on next page*)

Table 1 (*continued*)

Req. no.	Requirement description	Leaf	Significance
4.1.3	Cybersecurity protection system must provide mandatory access control for all devices accessed by an engineering maintenance interface based on a specified set of permitted IP addresses and time constraints.	✓	High
4.1.4	Cybersecurity protection system must monitor and analyze SCADA commands transmitted over an engineering maintenance interface and must generate alarms in the case of permission violations.	✓	High

- Probes based on Snort and Bro software that were adapted for the analysis of SCADA protocols (e.g., IEC 60870-5-104) in order to detect anomalies.
- Commercial intrusion detection/prevention system probes already deployed in control and supervisory substations.
- Honeypots, SCADA honeynets and darknets for monitoring, aggregating events and logging all detected threats and suspicious control network activities.
- Mediation devices (not shown) that convert and normalize messages received from legacy security systems and other security elements deployed in control and supervisory substations.
- Engineering maintenance interface access control module for monitoring and controlling all technical service activities, including video registration.
- Security information and event management system for gathering, analyzing and aggregating information received from cybersecurity protection elements.
- Databases for maintaining event and threat histories.
- Cybersecurity visualization module that processes security information and event management data in real time and provides support for mitigating threats and attacks.

All the elements of the system that collect security event information perform a two-tier security data exchange. Security events are reported by the system probes and the physical elements in which probes are installed. Physical elements (e.g. network infrastructure devices and legacy security solutions) report security events directly to the security information and event management system. The security information and event management system processes events in accordance with the implemented algorithms.

Each functional and system element mutually confirms its operability through periodic exchanges of authenticated heartbeat messages. Confirmations of the receipt of events and actions taken are initiated by the security system user, who closes the control loop. Automated reaction mechanisms are technically feasible for the power grid control system, but they are not implemented by the transmission system operator for procedural reasons.

Known attacks are detected (Requirement 1.1.1) using software such as Snort. However, standard information and communications technology security tools are generally inadequate in a power grid control environment. The cybersecurity protection system for such an environment should have an adaptive and configurable interface. The principle that any system that detects IP traffic anomalies should have an adaptive interface common to all non-standard systems is adopted. This interface is used by legacy security solutions (e.g., firewalls and intrusion detection/prevention systems) that are already deployed at the control and supervisory substations. Messages from external components are mapped to messages generally used in the system with the possibility of sending the original messages in case the security information and event management system needs to refer to the original messages. Messages sent by probes to a control and supervisory substation security system are exchanged independently of the power grid control system network.

SCADA system anomalies pose high risks; these risks should be minimized by using appropriately-designed probes. In order to address Requirement 1.1.2.1, probes for IEC 104 and IEC 61850 control traffic were developed. SCADA probes are among the most important components of the security system. The probes learn the profiles of authorized control messages (white list) and are then deployed in the operational mode in control and supervisory substations, where they detect anomalies from normal control behavior. Fig. 3 shows the security protection measures for a control and supervisory substation and the associated protocol stacks.

Alarms are reported to the security information and event management system and then to the system graphical user interface (GUI). Alarms are displayed differently depending on their threat levels. Alarm messages often are aggregated by probes due to their frequency. An adequate number of probes should be used in the case of multiple monitored SCADA devices. In order to diagnose and react to component failures, the system components must transmit authenticated heartbeat signals periodically (Requirement 2.2.1). The delivery of control data to control and supervisory substations may be hindered if a large traffic stream is generated by an unauthorized network element. Therefore, such events should be monitored at the network interfaces. When a traffic overload is detected, which could correspond to a denial-of-service attack (Requirement 1.1.3), a description of the event, including the response options, must be displayed on the security system graphical user interface. The system operator would then manually confirm the receipt of the event and take the appropriate actions.

The system can filter unauthorized malicious traffic. The power grid control system is logically separated from other (e.g., enterprise) networks. However, the leakage of non-production traffic (i.e., conventional IP traffic) to the control network is possible through deliberate or accidental misconfiguration of an edge network device or via self-updating software in a control and supervisory substation. Therefore, the network segments that are not involved in control should be provided with multiple regular and SCADA

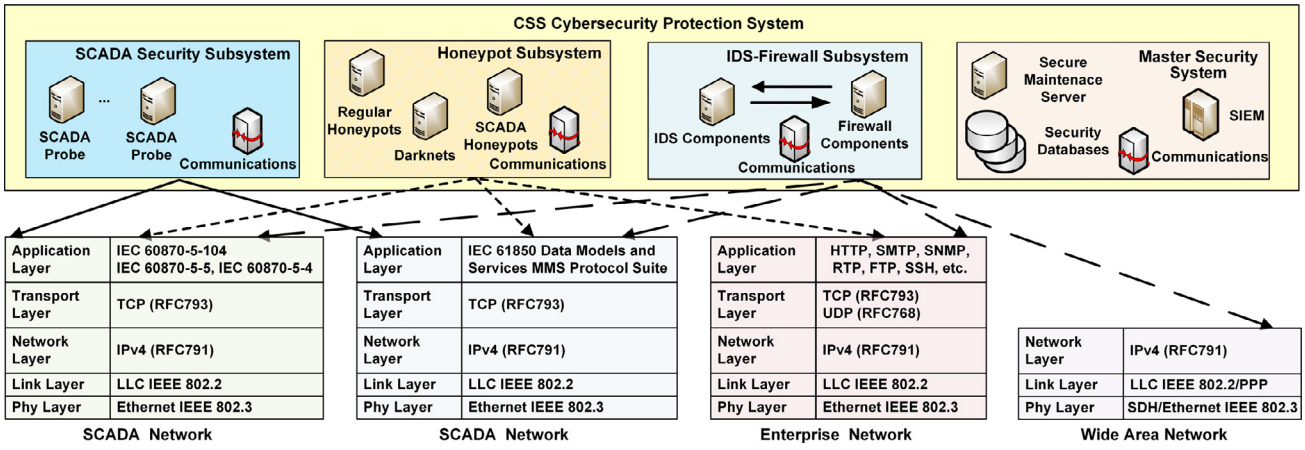


Fig. 3 – Security protection measures for a control and supervisory substation and the associated protocol stacks.

honeypots (Requirement 1.1.2.2) and darknets (Requirement 1.1.2.3) that cover the entire address space. These SCADA honeypots should mimic SCADA system operations and regular network services.

During the analysis of the control and supervisory substation environment, it became obvious that protecting administrative access to intelligent electronic devices is of crucial importance. A security daemon that monitors the operations of all remote users was developed (Requirement 4.1). The set of elements that can be accessed and the set of all possible operations were determined. All remote user operations are registered in non-modifiable records that also include the IDs of the remote users. All the events related to the monitored control system, cybersecurity protection system (CSPS) modules and physical entities must be delivered to and registered by the security information and event management system (Requirement 2.3). A human user interacts with the security system via a thin client and graphical user interface (Requirement 2.2.3). Multiple event occurrences are classified (Requirement 2.3.2) and correlated (Requirement 2.5). As a result, a comprehensive cybersecurity picture of the control and supervisory substation is created.

All cybersecurity protection system components interact with cybersecurity protection systems in other domains in accordance with the security policies stored in the domain controllers (Requirement 3.2.1.1). As shown in Fig. 4, the cybersecurity situational awareness picture of the federation is created by collecting and correlating security information from all the domains.

In order to verify the developed cybersecurity protection system, it was necessary to build an appropriate testbed on which attacks could be launched without causing any harm [33]. The testbed comprised three independent control and supervisory substations that belonged to two independent domains. Different security policies were developed for cooperation within a distribution system operator domain and for cooperation between two or more distribution system operator domains. Cybersecurity protection system elements were installed in each control and supervisory substation.

The domain cooperation mechanisms of the security systems were tested. The evaluation of the testbed is described in [33] and the verification results of some of the implemented cybersecurity mechanisms are described in [34]. Functional tests were performed for three environments (one domain, multiple domains and the deployment environment). The deployment was performed on a real control and supervisory substation at a PSE power transmission facility. Tests on the one-domain and two-domain environments iteratively provided a stable solution for the deployed cybersecurity protection system. The final solution was transferred to target station equipment for installation in the control and supervisory substation.

Functional tests were conducted prior to installation and the tests were subsequently repeated on the control and supervisory substation. The testing took more than 60% of the total implementation time. The functional testing of the security system was the most important stage before system deployment. Partial functional testing results are presented in [35].

Prior to performing each test, it was necessary to implement the functional testing plan. The prototype was evaluated as having a technology readiness level of 8 [4]. The functional testing documentation must include:

- Description of the testbed in which the functional tests were performed.
- Optional description of the specific conditions regarding the hostile activities in the local area network of the control and supervisory substation.
- List of functional test scenarios, including the test ID, test title, test priority, entry criteria, dependencies, covered requirements, step number, test case executed and exit criteria. Table 2 shows an example of a test scenario with all the values.
- Scenarios should be divided into stages of test execution, if necessary.

After the functional tests were formulated, they were executed in the testbed by a group of testers who had no connections with the developers. Table 3 presents an example of a test scenario and describes its results. The results of all the test scenarios are stored in a formal document called the

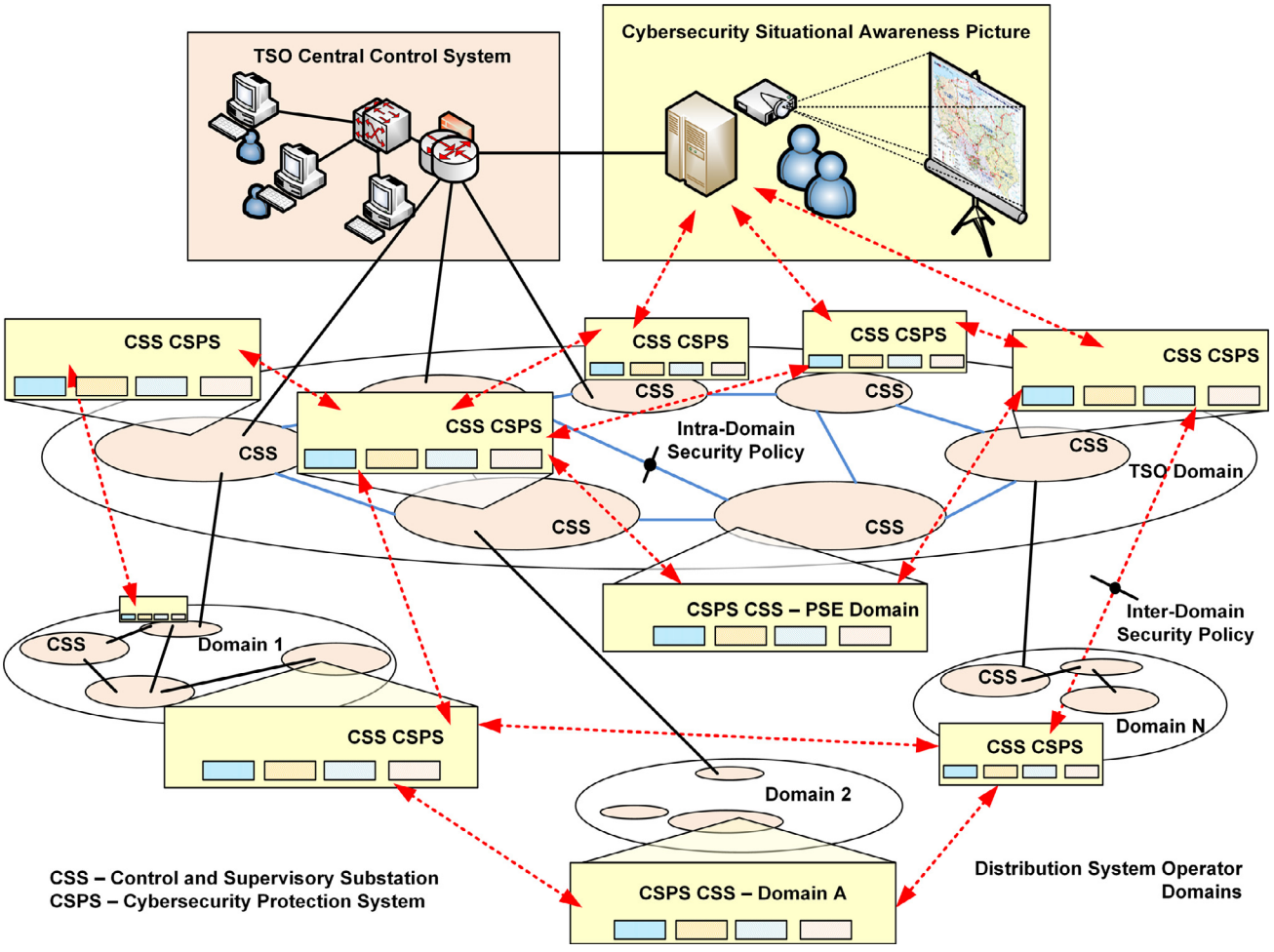


Fig. 4 – Federated multi-domain cybersecurity protection system for the power grid.

Functional Tests Report. This report includes the results of the functional tests compiled in a single table. After the functional tests have been completed, it is necessary to evaluate the readiness of the system. This step produces a table that maps all the functional tests to the requirement content and evaluation results (positive/negative).

6. Lessons learned

The design of the cybersecurity protection system was an iterative process that took more than one third of the time required for the entire implementation. Defining the protected facility turned out to be an important problem because the power grid operator standardized the architecture of its own control and supervisory substations that were to be protected. As a result, new system security functions materialized, such as those related to the secure access to the repair and maintenance system.

The formulation of requirements for the control and supervisory substations based on an evolving architecture was a continuous and iterative process. Consequently, the design and test phases overlapped partially, requiring continuous verification of the previously-elaborated requirements. Notably, there were many more problems to solve. Testing the security system was especially challenging. For obvious reasons, testing modules for threat detection, such as anomalies in IEC 104 and IEC 61850 traffic and filtering IP traffic in a control and supervisory substation under real-world production conditions, was impossible. If the system was to be operational, it was necessary to create a separate environment for integrating and testing the modules. Therefore, a testbed had to be developed for integration and functional testing [33].

It was also necessary to inject IP traffic, which was obtained from the real control and supervisory substations, into the testbed domains. In one of the domains, two control and supervisory substation environments were modeled. The domains were interconnected to reflect two distribution system operator business entities that exchanged security data. The data flow was controlled using configurable security policies. Collaboration of the cybersecurity protection systems between the domains produced synergies in the entire system – the distribution of security information enabled the preparation for and avoidance of threats, even if the threats had not been realized previously at a given location. The pre-deployment system environment turned out to be an

Table 2 – Example test scenario for the SCADA IEC 104 protocol probe.

Test ID	TS-04/1	
Test title	Response of the SCADA IEC 104 protocol probe to a malformed injected control packet.	
...		
Entrance criteria	SCADA probe is configured and runs in the promiscuous mode. Alarm processing module is active. SIEM system is available. Prepare the file with a malformed traffic sample for the network traffic generator.	
Dependencies	TS-02 – Initialization of the CSS cybersecurity protection system internal communications. TS-03 – Initialization of the SIEM functions of the CSS cybersecurity protection system.	
Covered requirements	Req. no. 1.1.2.1 – System must raise alarms upon detecting anomalous IED and SCADA (IEC 104, IEC 61850-MMS) over IP control traffic. Scope – SCADA IEC 104 protocol probe. Significance to the cybersecurity protection system. Req. no. 1.3 – Security modules must deliver alarm notifications to the CSS SIEM system.	
...		
Step no.	**Test case (TC) to execute**	**Expected result**
1	TC-01 – Enable the learning mode of the SCADA IEC 104 protocol probe for a period of time long enough to collect a traffic pattern.	SCADA IEC 104 protocol probe gained adequate knowledge about the syntax and semantics of messages exchanged between SCADA devices.
2	TC-02 – Change the mode of the SCADA IEC 104 protocol probe to the detection mode.	SCADA IEC 104 protocol probe operated in the detection mode.
3	TC-03 – Disconnect the monitored SCADA network segment from the CSS cybersecurity protection system.	SCADA segment was separated.
4	TC-04 – Connect the hostile traffic generator as a device that is monitored by the CSS cybersecurity protection system.	Hostile traffic generator was reachable by the SCADA IEC 104 protocol probe.
5	TC-05 – Initiate hostile traffic generation.	Hostile traffic was captured by Wireshark at the network interface of the SCADA IEC 104 protocol probe.
6	TC-06 – Check the security events and alarms in the local database related to the SCADA IEC 104 protocol probe.	An entry of the event was found in the SCADA IEC 104 protocol probe diagnostics file.
7	TC-07 – Find an event record corresponding to the detection of anomalies in SCADA protocol traffic in the CSS SIEM system.	An entry of the event was found in the CSS SIEM system.
Exit criteria	All the steps produced the expected results.	

important component that had to be developed and tested before installing any equipment in a control and supervisory substation.

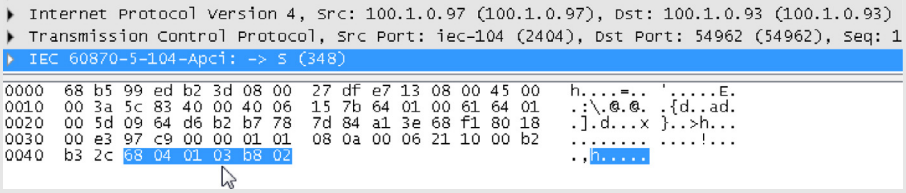
Several servers gathered and managed commands and responses from SCADA devices in the control and supervisory substations (e.g., IEC 104 and IEC 61850). A multiple server architecture was selected during the development and implementation phases due to internal data bus limitations concerning the data rate. It was possible to replace all the servers with a single unit powerful enough to handle the expected data stream processing rate and an adequate number of physical network interfaces. All the IP traffic in a control and supervisory substation was forwarded via a switch to the probes and honeypots. Enterprise IP traffic was also directed to and processed by intrusion detection systems and honeypots. The intrusion detection systems worked cooperatively with the control and supervisory substation firewalls (not shown in Fig. 2). A number of SCADA honeypots waited for unexpected incoming interactions via physical Ethernet interfaces set to the promiscuous mode. A portion of the IP address pool was used to emulate routers that redirected incoming traffic to decoy IP networks (i.e., darknets). All the interactions with emulated devices resulted in alarms being sent to the central server hosting the security information and event management system. After correlation, all the processed alarms and security events were presented to a remote human operator via a web browser.

7. Conclusions

Enhancing the cybersecurity of electric power grids is an important problem, especially in the light of current political and economic conditions in Europe [12]. Unfortunately, an analysis performed during the design and implementation of the cybersecurity protection system described in this paper indicates that limited knowledge of practical value is available about cybersecurity solutions for power grid control systems. Some security solutions have been developed for industrial control systems, but no standards or best practices exist for developing robust solutions for power grid control systems.

This paper has described a robust cybersecurity protection approach for power grid control systems. It presents an analysis of a domestic power grid control system that emphasizes the identification of key infrastructure elements and their importance to power grid security. In addition, it provides a unique perspective based on the system design process – from the identification of requirements to their application in operator control and supervisory substations. The paper also

Table 3 – Example test scenario results for the SCADA IEC 104 protocol probe.

Test ID	TS-04/1
Test title	Response of the SCADA IEC 104 protocol probe to a malformed injected control packet.
Responsible person	Krzysztof Parobczak, MUT
Date	September 5, 2015
Entrance criteria	SCADA probe is configured and runs in the promiscuous mode. Alarm processing module is active. SIEM system is available. Prepare the file with a malformed traffic sample for the network traffic generator.
Dependencies	TS-02 – Initialization of the CSS cybersecurity protection system internal communications. TS-03 – Initialization of the SIEM functions of the CSS cybersecurity protection system.
Step 1	{positive} Learning mode was activated on the SCADA IEC 104 protocol probe.
Step 2	{positive} Detection mode was activated on the SCADA IEC 104 protocol probe.
Step 3	{positive} Reachability to the SCADA segment was lost
Step 4	{positive} Hostile network generator was reachable in the SCADA segment.
Step 5	{positive} Hostile traffic was captured at the network interface of the SCADA IEC 104 protocol probe. The modified value is pointed to by the arrow in the following figure: 
Step 6	{positive} An entry of the event was found in the SCADA IEC 104 protocol probe diagnostics file; this is evidence of the occurrence of a malformed value in the control packet. The alarm message contained: source and destination IPv4 addresses of the SCADA devices in the CSS control network subnet; TCP ports, type of event and alarm priority; and the IPv4 address of the SCADA IEC 104 protocol probe in the cybersecurity protection system subnet. `Jul 21 23:15:10 pl.bipse.css05.scada_probe_IEC104 Sending alarm: ‘‘ip_src’’:[‘‘100.1.0.97,‘‘a_pro_4’’:[‘‘TCP’’],‘‘port_source’’:[2404],‘‘ip_dest’’:[‘‘100.1.0.93’’],‘‘port_dest’’:[54962],‘‘detector_probe_ip’’:‘‘172.20.5.102’’,’’a_det_e_id’’:’’pl.bipse.css05.scada_probe_IEC104’’},‘‘alarm_man’’:{‘‘alarm_time’’:1437513311711,‘‘alarm_msg’’:’’value_out_of_range’’,‘‘alarm_priority’’:‘‘crit’’`
Step 7	positive An entry of the event was found in the graphical user interface of the CSS SIEM system.
Result	{positive} A malformed value was detected in the IEC 104 control field of the SCADA packet. An alarm was sent to the CSS SIEM system and a notification was presented on the graphical user interface.
Summary	SCADA IEC 104 protocol probe detected a malformed value in the control packet sent to the SCADA device. All the requirements were met.

discusses the verification of the functionality provided by an implemented cybersecurity protection system.

The cybersecurity protection system described in this paper is intended to be used by transmission and distribution service operators for attack detection and controlled information dissemination. The system provides synergistic security impacts by leveraging knowledge about possible threats, locations of their sources and potential outcomes. The centralized situational awareness provided by the protection system is another key benefit, one that is realized by the underlying hierarchical domain architecture. Additionally, a mediation module simplifies integration with current and future security systems such as the Critical Infrastructure Warning Information Network (CIWIN) [11]. The modular design of the system supports customization as well as the implementation of advanced functionalities needed to secure an evolving power grid. It is important to note that, although the research has focused on the Polish power grid, the approach can be applied to design and implement power grid protection systems in countries around the world. Moreover, the approach can be adjusted to create robust cybersecurity protection systems for other critical infrastructure assets, including gas and chemical processing facilities, water and wastewater systems.

Acknowledgements

This research was sponsored by the National Centre for Research and Development as part of a research project focused on the national security and defense of Poland: System of Secure IP Communications Assurance in Electro-Energetic Control Networks (No. ROB 0074 03 001). The project involved personnel from the Military University of Technology, Research and Academic Computer Network, Asseco Poland and Military Communications Institute.

REFERENCES

[1] AEA Technology, Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector, Final Report to the European Commission Directorate-General Justice, Freedom and Security, Didcot, United Kingdom, 2009.

[2] H. Altomonte, Japan's nuclear disaster: Its impact on electric power generation worldwide, *IEEE Power and Energy* vol. 10(3), pp. 94–96, 2012.

[3] Alutech, SCADA and ICS Cyber Security Products, M.P. Negev, Israel (www.alutech-ics.com/products), 2016.

[4] M. Amanowicz, Eighth Technological-Level Readiness Assessment of the Cybersecurity System Prototype (in Polish), Internal Report, BIPSE Consortium, Warsaw, Poland, 2015.
[5] R. Barbosa, R. Sadre and A. Pras, Flow whitelisting in SCADA networks, *International Journal of Critical Infrastructure Protection* vol. 6(3-4), pp. 150–158, 2013.
[6] D. Bolton, Ukraine says major cyberattack on Kiev's Boryspil airport was launched from Russia, *The Independent* January 18, 2016.
[7] R. Campbell, Cybersecurity Issues for the Bulk Power System, Report R43989, Congressional Research Service, Washington, DC, 2015.
[8] Check Point Software Technologies, 1200R Rugged Appliance, San Carlos, California (www.checkpoint.com/products/industrial-control-systems-appliances), 2016.
[9] Cisco Systems, Cisco Connected Grid Solutions for the Substation, San Jose, California (www.cisco.com/c/dam/en_us/solutions/industries/docs/energy/substation_aag.pdf), 2012.
[10] D. Clegg and R. Barker, *CASE Method Fast-Track: A RAD Approach* Addison-Wesley Longman, Boston, Massachusetts, 1994.
[11] Commission of the European Communities, Commission State Working Document, Accompanying Document to the Proposal for a Council Decision on Creating a Critical Infrastructure Warning Information Network (CIWIN), SEC(2008) 2701, Brussels, Belgium, 2008.
[12] Council of the European Union, Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection, Brussels, Belgium, 2008.
[13] T. Cruz, P. Simoes, J. Proenca, M. Aubigny, M. Ouedraogo and A. Graziano, Improving cyber-security awareness for industrial control systems: The CockpitCI approach, *Journal of Information Warfare* vol. 13(4), 2014.
[14] Electricity Information Scaring and Analysis Center (E-ISAC), Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case, Washington, DC (ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf), 2016.
[15] N. Erez and A. Wool, Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems, *International Journal of Critical Infrastructure Protection* vol. 10, pp. 59–70, 2015.
[16] European Commission, Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection – Making European Critical Infrastructures More Secure, SWD(2013) 318 Final, Brussels, Belgium, 2013.
[17] European Network of Transmission System Operators for Electricity, Solar Eclipse March 2015: The Successful Stress Test of Europe's Power Grid – More Ahead, Policy Brief, Brussels, Belgium (www.entsoe.eu/Documents/Publications/ENTSO-E%20general%20publications/entsoe_spe_pp_solar_eclipse_2015_web.pdf), 2015.
[18] European Network of Transmission System Operators for Electricity, ENTSO-E Work Programme, 2015 through December 2016, Brussels, Belgium (www.entsoe.eu/Documents/Publications/ENTSO-E%20general%20publications/151218_AWP2016_Final_post_ACER_opinion.pdf), 2016.
[19] European Parliament and Council of the European Union, Regulation (EC) No. 714/2009 of the European Parliament and of the Council of 13 July 2009 on Conditions for Access to the Network for Cross-Border Exchanges in Electricity and Repealing Regulation (EC) No. 1228/2003, Brussels, Belgium, 2009.
[20] European Union Agency for Network and Information Security, Protecting Industrial Control Systems, Annex II, Survey and Interview Analysis, Heraklion, Greece (www.enisa.europa.eu/publications/annex-ii/at_download/fullReport), 2011.
[21] European Union Agency for Network and Information Security, Protecting Industrial Control Systems, Annex III, ICS Security Related Standards, Guidelines and Policy Documents, Heraklion, Greece (www.enisa.europa.eu/publications/annex-iii/at_download/fullReport), 2011.
[22] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Symantec, Mountain View, California, 2011.
[23] N. Goldenberg and A. Wool, Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, *International Journal of Critical Infrastructure Protection* vol. 6(2), pp. 63–75, 2013.
[24] A. Gostev, Kaspersky Security Bulletin 2012, Cyber Weapons, Kaspersky Lab, Moscow, Russia (securelist.com/analysis/kaspersky-security-bulletin/36762/kaspersky-security-bulletin-2012-cyber-weapons), 2012.
[25] Governor of West Pomerania, The Report on the Causes and Effects of the Energy Catastrophe by the Investigation Group Established by the West Pomeranian Governor's Decree No. 154/2008 of April 2 (in Polish), Szczecin, Poland (www.szczecin.uw.gov.pl/systemfiles/articlefiles/1466/20111202.120000.raport_koncowy-czesc_-1.pdf), 2008.
[26] Grupa PTWP, Building of 450 MW turbogenerator in Turow will be more expensive and time consuming in Polish, Katowice, Poland (budownictwo.wnp.pl/budowa-bloku-450-mw-w-turowie-bedzie-dluzsza-i-drozsza,262140_1_0_0.html), November 25, 2015.
[27] G. Halleen and G. Kellogg, *Security Monitoring with Cisco Security MARS* Cisco Press, Indianapolis, Indiana, 2007.
[28] G. Hogben and R. Leszczyna, DuQu: Briefing Note, European Union Agency for Network and Information Security Agency, Heraklion, Greece (www.enisa.europa.eu/media/news-items/duqu-analysis), 2011.
[29] F. Hohlbaum, P. Schwyter and F. Alvarez, Cyber Security Requirements and Related Standards for Substation Automation Systems, D2-02 B11, International Council on Large Electric Systems, Paris, France (library.e.abb.com/public/575ee5b396ceca41c1257a93002f7f3a/D2-02B11_en_Cyber_Security_requirements_and_related_standards_for_Substation_Automation_Systems.pdf), 2011.
[30] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Alert (ICS-ALERT-11-080-01), Siemens Tecnomatix FactoryLink Vulnerabilities, Idaho Falls, Idaho, January 17, 2014.
[31] International Electrotechnical Commission, Power Systems Management and Associated Information Exchange – Data and Communications Security – Part 10: Security Architecture Guidelines, Technical Report IEC/TR 62351-10:2012, Geneva, Switzerland, 2012.
[32] Israel Export Institute, The Israeli Cybersecurity Companies Data Base, Tel Aviv, Israel (itrade.gov.il/poland/files/2015/02/ISRAELI-CYBERSECURITY-COMPANIES.pdf), 2016.
[33] J. Jarmakiewicz, K. Maslanka and K. Parobczak, Development of cyber security testbed for critical infrastructure, *Proceedings of the International Conference on Military Communications and Information Systems* 2015.
[34] J. Jarmakiewicz, K. Maslanka and K. Parobczak, Evaluation of the cyber security provision system for critical infrastructure, *Journal of Telecommunications and Information Technology* vol. 4, pp. 22–29, 2015.
[35] J. Jarmakiewicz, K. Maslanka and K. Parobczak, The Functional Tests in Multi-Domain Systems Federation Environment – Plan and Report (in Polish), Internal Report, BIPSE Consortium, Warsaw, Poland, 2015.
[36] J. Jarmakiewicz, K. Maslanka, K. Parobczak, M. Glowacki and M. Wawryszczuk, The Architecture of Cybersecurity

Protection System for Power Grid Control (in Polish), Internal Report, BIPSE Consortium, Warsaw, Poland, 2013.
[37] W. Knowles, D. Prince, D. Hutchison, J. Disso and K. Jones, A survey of cyber security management in industrial control systems, *International Journal of Critical Infrastructure Protection* vol. 9, pp. 52–80, 2015.
[38] E. Kovacs, BlackEnergy malware used in Ukraine power grid attacks, *SecurityWeek* January 4, 2016.
[39] J. Leyden, Kiev airport goes dark after "BlackEnergy-linked" power outage, *The Register* January 18, 2016.
[40] Lofty Perch, SCADA and Control Systems Security, Markham, Canada (www.loftyperch.com), 2016.
[41] E. Marx, How solar-heavy Europe avoided a blackout during total eclipse, *Scientific American* March 24, 2015.
[42] E. Nakashima, Russian hackers suspected in attack that blacked out parts of Ukraine, *The Washington Post* January 5, 2016.
[43] National Cybersecurity and Communications Integration Center, Seven Steps to Effectively Defend ICS, U.S. Department of Homeland Security, Washington, DC (ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf), 2016.
[44] National SCADA Test Bed, A Summary of Control System Security Standards Activities in the Energy Sector, U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, Washington, DC (www.energy.sandia.gov/wp-content/gallery/uploads/CISSWG_Report_1_Final.pdf), 2005.
[45] Office of Energy Assurance, 21 Steps to Improve Cyber Security of SCADA Networks, U.S. Department of Energy, Washington, DC (energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf), 2002.
[46] J. Pagliery, Scary questions in Ukraine energy grid hack, *CNN* January 18, 2016.
[47] A. Patkowski, J. Jarmakiewicz and K. Liderman, Requirements for Cybersecurity Protection System for Power Grid Control System (in Polish), Internal Report, BIPSE Consortium, Warsaw, Poland, 2013.
[48] PSE Operator, The Requirements of Power Sources for Implementation of the LFC System (in Polish), Konstancin-Jeziorna, Poland (www.pse.pl/uploads/kontener/wymogi_JWCD_wersja_2%2B_2011%2B08%2B04.pdf) 2011.
[49] Radiflow, The Radiflow SCADA Security Portfolio, Mahwah, New Jersey (radiflow.com/products), 2016.
[50] C. Ruiz, N. Orrego and J. Gutierrez, The Colombian 2007 blackout, *Proceedings of the IEEE Power and Energy Society Transmission and Distribution Conference and Exposition: Latin America* 2008.
[51] D. Sanger and M. Mazzetti, U.S. had cyberattack plan if Iran nuclear dispute led to conflict, *The New York Times* February 16, 2016.
[52] SC3, Cyber Solutions, Alexandria, Virginia (www.sc3.com/services/cyber-solutions), 2016.
[53] SCADAfence, Smart Security for Smart Manufacturing, Be'er Sheva, Israel (www.scadafence.com), 2016.
[54] C. Sezer and E. Tuncay, Turkish banks fend off cyberattacks, some transactions hit, *Reuters* December 25, 2015.
[55] D. Sharkov, Turkish hackers down Russian Embassy website in Israel, *Newsweek* January 18, 2016.
[56] S. Sridhar, A. Hahn and M. Govindarasu, Cyber-physical system security for the electric power grid, *Proceedings of the IEEE* vol. 100(1), pp. 210–224, 2012.
[57] Stock Market Information Platform, Information on Power Grid Resources (in Polish), Warsaw, Poland (gpi.tge.pl/wykaz-jednostek), 2016.
[58] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams and A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, 2015.
[59] Swedish Civil Contingencies Agency, Guide to Increased Security in Industrial Information and Control Systems, Karlstad, Sweden (www.msb.se/RibData/Filer/pdf/27473.pdf), 2014.
[60] H. Takagi, T. Morita, M. Matta, H. Moritani, T. Hamaguchi, S. Jing, I. Koshijima and Y. Hashimoto, Strategic security protection for industrial control systems, *Proceedings of the Fifty-Fourth Annual Conference of the Society of Instrument and Control Engineers of Japan* pp. 986–992, 2015.
[61] C. Taschner, Vulnerability Note VU#343971, ABB PCU400 Vulnerable to Buffer Overflow, CERT, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania (www.kb.cert.org/vuls/id/343971), 2009.
[62] Tenable Network Security, Defend SCADA Networks with Continuous Network Monitoring, Columbia, Maryland (www.tenable.com/solutions/scada-security), 2016.
[63] Thales, Critical National Infrastructure: The Threat Landscape, White Paper, Basingstoke, United Kingdom (www.thalesgroup.com/sites/default/files/asset/document/thales-critical-national-infastructure-the-threat-landscape.pdf), 2013.
[64] Thales, Cyber Security for SCADA Systems, White Paper, Basingstoke, United Kingdom (www.thalesgroup.com/sites/default/files/asset/document/thales-cyber-security-for-scada-systems.pdf), 2013.
[65] Tofino Security, Tofino Xenon Security Appliance, Lantzville, Canada (www.tofinosecurity.com/products/tofino-xenon-security-appliance), 2016.
[66] Ultra Electronics 3eTI, Industrial Cyber Security, Rockville, Maryland (www.ultra-3eti.com/industrial), 2016.
[67] Union for the Coordination of Transmission of Electricity, Final Report, System Disturbance on 4 November 2006, Brussels, Belgium (www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/otherreports/Final-Report-20070130.pdf), 2007.
[68] U.S. Department of Energy, National SCADA Test Bed, Washington, DC (www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed), 2016.
[69] U.S. Department of Homeland Security, National Cybersecurity Protection System (NCPS), Washington, DC (www.dhs.gov/national-cybersecurity-protection-system-ncps), 2016.
[70] U.S. Department of Homeland Security and Centre for the Protection of National Infrastructure, Cyber Security Assessments of Industrial Control Systems, A Good Practice Guide, Washington, DC and London, United Kingdom (www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf), 2011.
[71] Waterfall Security Solutions, NERC CIP V5 Standards Position Unidirectional Security Gateways as Secure Alternatives to Firewalls and Network Intrusion Detection Systems, Rosh Ha'ayin, Israel (waterfall-security.com/wp-content/uploads/2015/12/wf-cipv5-ugw-details-v1.pdf), 2014.
[72] D. Yang, A. Usynin and J. Hines, Anomaly-based intrusion detection for SCADA systems, *Proceedings of the Fifth International Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-Machine Interface Technologies* pp. 797–803, 2006.