KONRAD ŚWIRSKI
Politechnika Warszawska
konrad.swirski@itc.pw.edu.pl

ISSUES OF CRITICAL INFRASTRUCTURE CYBER SECURITY IN THE POWER SECTOR

ABSTRACT

The article presents the problem of modern threats to critical IT infrastructure in the power sector (ICS – Industrial Control Systems) and the current status of global solutions, norms, standards and procedures and shows typical control systems protection strategies employed in the power sector. The emergence of advanced cyber-attacks against power control and distribution systems indicates a growing possibility of military attacks and malware prepared as a new forms of offensive weapons. Taking into consideration the possibility of using advanced techniques in cyber-attacks, most of the existing, commercial protection systems may be insufficient. It is necessary for critical infrastructure in the power sector to isolate systems from the outside world, which in turn could be inconvenient because it limits the possibility of remote process observation. In addition, solutions for the secure data communication are constantly developed and evaluated and this article presents in detail a secure communication solution for acquiring data from industrial DCS automation systems (power generation).

Keywords: *cyber security, critical infrastructure, IT OT, ICS, control systems*

STRESZCZENIE

Artykuł przedstawia problem cyberbezpieczeństwa infrastruktury krytycznej w energetyce (ICS – Industrial Control Systems) poprzez pryzmat możliwych zagrożeń, światowych rozwiązań, norm, standardów i procedur oraz pokazuje typowe strategie ochrony systemów sterowania w energetyce. Pojawianie się coraz bardziej zaawansowanych form ataków cybernetycznych na systemy stero-

wania związane z wytwarzaniem i przesyłem energii wskazuje na zwiększającą się możliwość ataków militarnych i malware przygotowanych jako nowa forma broni ofensywnej. Wobec możliwości wykorzystania bardzo zaawansowanych technik, większość obecnych, komercyjnych systemów ochrony może być niewystarczająca. Dla systemów infrastruktury krytycznej energetyki koniecznością staje się ścisła ich izolacja od świata zewnętrznego, co z kolei jest niewygodne, gdyż ogranicza możliwość zdalnej obserwacji procesu. Opracowywane i testowane są więc rozwiązania bezpiecznego sposobu przesyłania danych, a w niniejszym artykule zaprezentowane jest rozwiązanie bezpiecznej komunikacji dla pozyskania danych z przemysłowych systemów automatyki DCS.

Słowa kluczowe: *cyberbezpieczeństwo, infrastruktura krytyczna, IT OT, ICS, systemy sterowania*

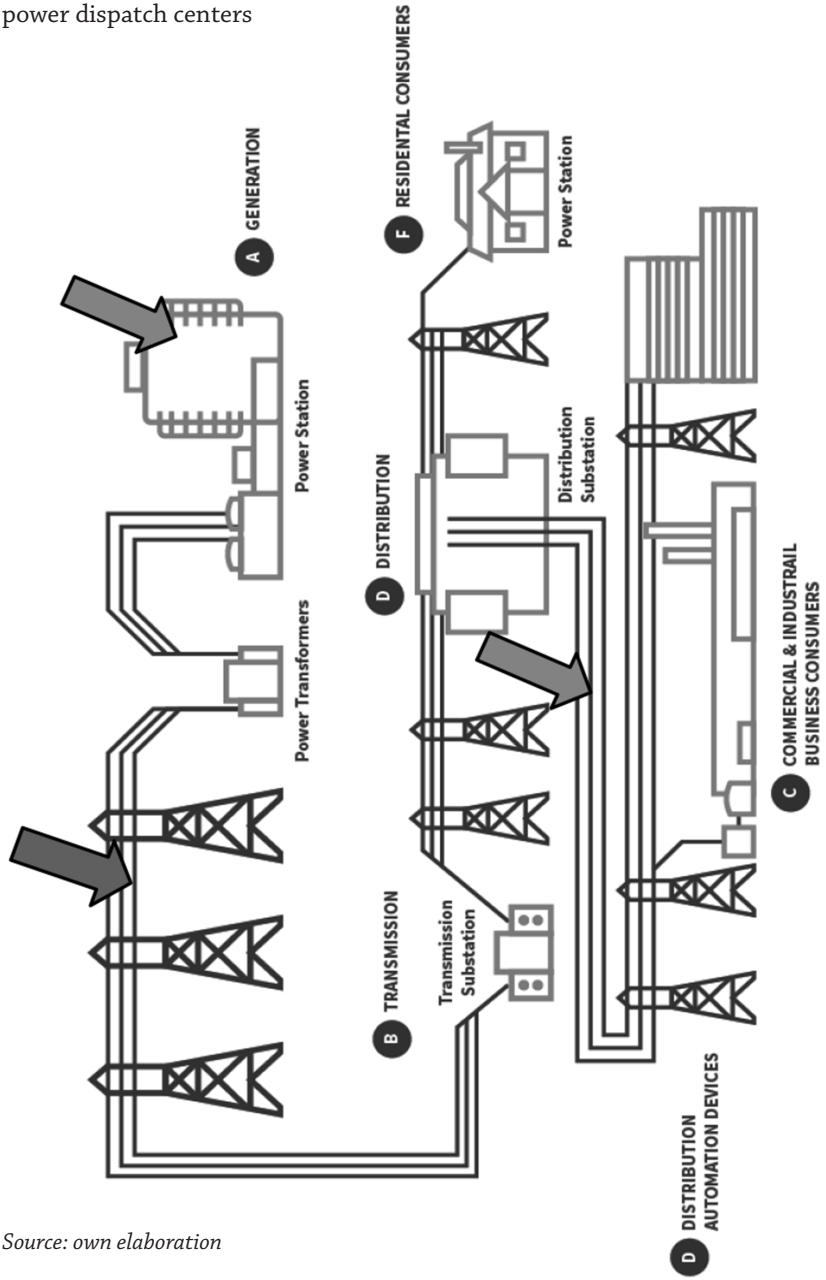
INTRODUCTION

Development of IT technologies and practically complete take-over of industrial process control by advanced automation systems has also been recognized by military doctrine. The ability to take down critical infrastructure of the enemy (which includes the electricity supply system, as the key element of the infrastructure) has been considered the top-priority defensive option as well as a new form of attack. Not surprisingly considerable resources were employed to develop sophisticated "cyber warfare", which was accompanied with increasing activity of criminal groups utilizing IT systems and the Internet for data theft or extortions. With time and with increasing dissemination of digital control systems in power plants, invisible components of the new cyber warfare, such as malware used to attack control system and to bring down the infrastructure, have become even more severe danger than conventional attacks. The year 2010 with Stuxnet attack, that is the attack on the Iranian control systems of uranium enrichment centrifuges, marked the start of a new era – the era of IT wars. Now power systems are facing more severe threats than bombs. Today, malware is perceived as one of the fundamental industrial problems and one of the most severe military threats [Bayar 2016] [Clarke, Knake 2012] and the cost of protection as well as the scale of potential damages caused by malware has been exponentially growing.

THE POWER SECTOR CRITICAL INFRASTRUCTURE AND DIGITAL CONTROL SYSTEMS – SCADA, DCS

The critical infrastructure spans a broad group of systems which are required by a modern state to function. Power sector holds one of the key

Figure 1.
Diagram of the power system with its key threats: of the Transmission System Operator (including National Power Dispatch Center), major power plants, regional power dispatch centers



Source: own elaboration

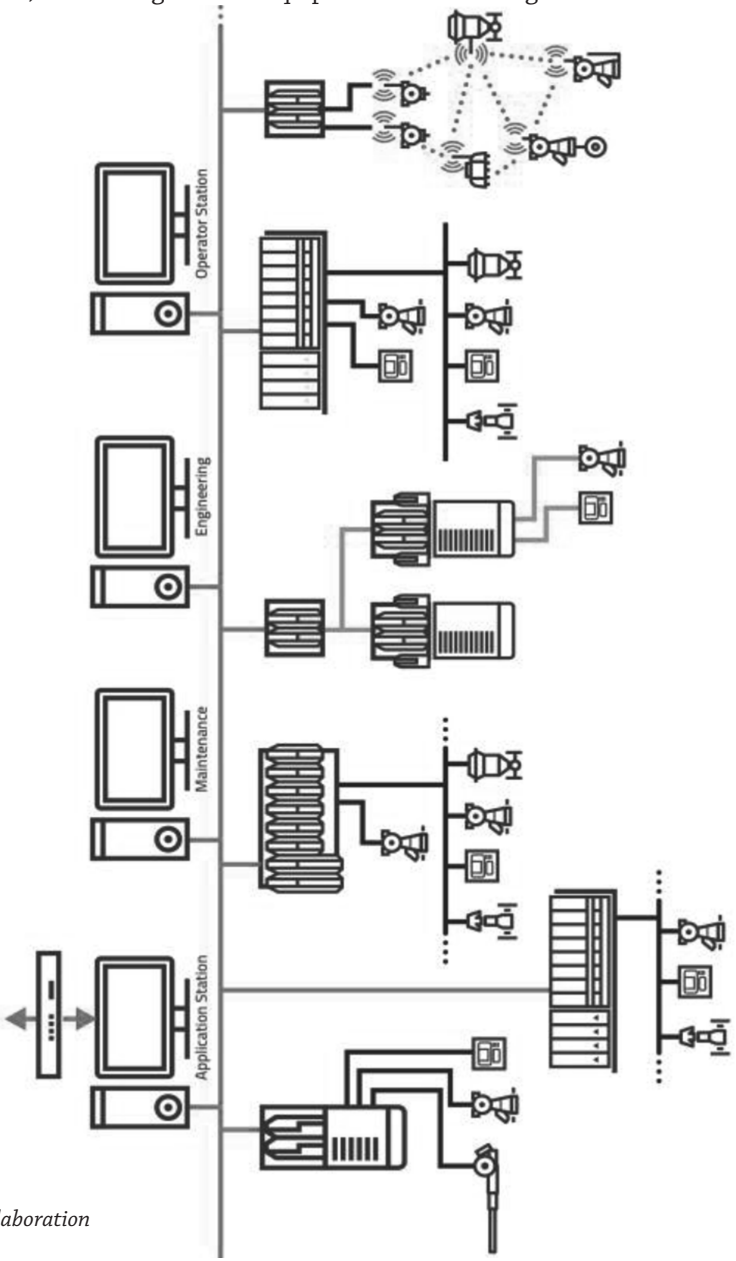
places in this group. From the perspective of system classes, it utilizes digital process control systems, usually referred to in governmental documents as SCADA, or named more accurately in the automation engineering nomenclature Supervisory Data Acquisition and Control (SCADA) systems or Distributed Control Systems (DCS) and is intended to automatically control or supervise various technological processes. According to the act on crisis management, automation systems and IT systems of this kind are responsible for supplying power, energy resources (gas) or water for industrial production (chemical production as well as in other sectors) and transmission pipelines (including oil, gas pipelines as well as industrial pipelines used for transporting hazardous substances). These systems are usually referred to in general as Industrial Control Systems (ICS) or Operational Technology (OT). However, the power sector plays a key role – the power supply system is centralized and practically lacks any energy storage capability. Consequently, potential attacks may result with total, uncontrollable loss of power supply capability over a wide area, i.e. a blackout. Other activities of control systems are limited to local monitoring of processes in specific industrial plants or networks and therefore potential threats affecting them (although with potentially severe financial consequences or life-threatening) have no such global impact. Power supply also affects operation of other critical infrastructure sectors (such as transport, telecommunication, health care, food distribution etc.) and the effect is instantaneous – and as such it may be considered a particularly attractive target in a offensive doctrine and in military plans. The key components in the electric power system, which in turn can cause threats, are the Transmission System Operator Infrastructure (supervision of transmission network, National Power Dispatch Center and power market organization), key centers of Distribution System Operators and of course DCSs of largest power units or central control room systems build in many power plants.

In process management systems of this type, it is important to understand the overall protection issues in terms of "safety" – that is ensuring protection for the proper execution of processes in contrast to less important in this case "security" – that is data security (as, for example, in the financial sector). The role of SCADA and DCS systems is to correctly regulate and to protect technological processes. Thus, the fact that these systems could be used "against own facilities" and that it is possible to intentionally damage the equipment using infected control systems shall

be considered a serious threat in the case of cyber attacks. It is therefore necessary to anticipate other types of attacks and potential threats than in other critical infrastructure sectors (e.g. financial sector) – which has been clearly proven by Stuxnet and other types of malware.

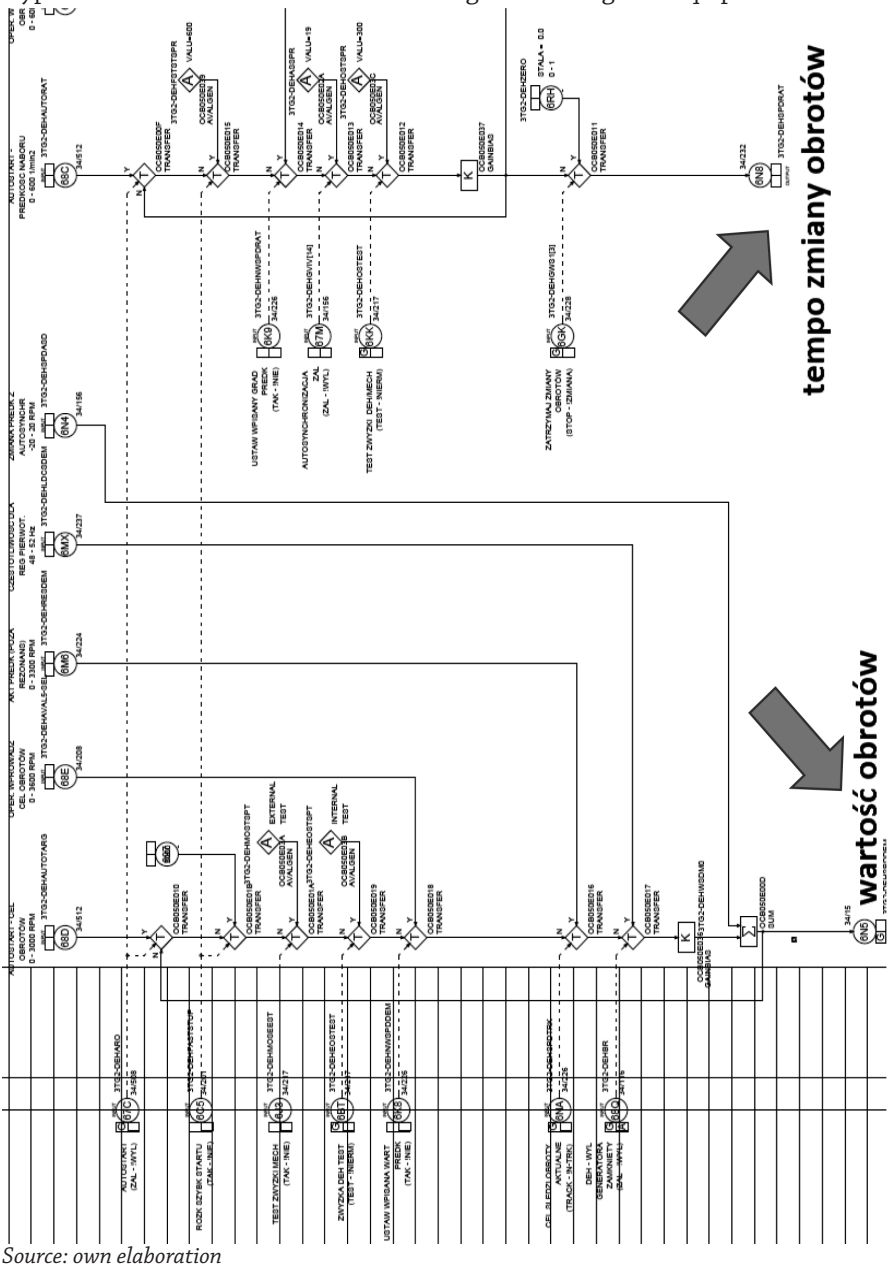
Systems, which are currently being commonly used to control the whole industrial and power infrastructure, appeared at the onset of the computer revolution. In 1970, Yokogawa and Honeywell concurrently developed first so-called Distributed Control Systems (DCS) which become the standard in on-line control systems. During the following years these DCSs were evolving and growing stronger. Today, they practically replaced power plant operators (the whole process from the start of a power unit, through its normal operation, up to its control in emergency situations is now handled automatically). At the same time, Programmable Logic Controllers (so-called PLCs) have been continuously developing and upgraded in terms of functionality. These are freely configurable controllers, that is electronic circuits, which control individual pieces of equipment used mostly in the industry and in discrete processes. In further stages of technological development these systems were connected with SCADA (Supervisory Data Acquisition and Control) systems. This abbreviation has also become a synonym for systems which collect data from distributed and remote locations, e.g. from the power grid. Currently, along with the pressure on costs reduction and on product standardization (e.g. utilization of standard components and operating environments, such as Microsoft Windows), differences between DCS, PLC and SCADA have been becoming less visible and apparent only for automation experts. For an outsider it all looks quite similar – that is as a some sort of an IT system which controls the equipment operation. System operation is also analogous – engineers are designing and developing so-called control algorithms (which describe how processes are to be controlled), they are using engineering computers running specialized, proprietary software, and algorithms are being then translated to computer programs, which are installed in controllers (control computers). The controllers then read process data (measurements from signals), process the data, supervise controlled process and by executing the control algorithm send settings to various actuators (valves dampers, etc.). It is essential for the physical equipment to operate within safe limits and that is ensured by protections and process interlocks – i.e. also computer programs which constantly check whether acceptable values have not been exceeded.

Figure 2.
Functional diagram of a DCS – controllers connected with a network (bus) and master operator workstations and engineering workstations; in some solutions a network (bus) connecting the field equipment is also distinguished



Source: own elaboration

Figure 3.
An example of a steam turbine rotational speed control algorithm (second pic.). Hypothetical malware could alter its settings and damage the equipment



Source: own elaboration

Today, the majority of controllers and engineering computers are in practice machines similar to desktop computers and running standard Windows operating systems (only some of the controllers use real-time operating systems), whereas the network interconnecting these computers to form DCS is almost exclusively classic Ethernet. Thus, access to the hardware is now possible for anyone knowledgeable in IT technology. And this is just one step away from a cyber attack, which may involve modification of actuators' settings (valves opening, altering engine rotation speeds, flap positions etc.) in a completely different way than under control algorithm supervision. We can therefore imagine a situation in which a control system, instead of supervising the power generation or transmission process may be used for a completely different purpose – that is to abort power generation, or even worse, to intentionally damage the generating equipment, bypassing its software interlocks and limit protections which finally may be sufficient sufficient to bring the power system down and cause potential blackout [Hadji-Janev, Bogdanoski, 2015].

CYBER SECURITY OF THE POWER SECTOR CRITICAL INFRASTRUCTURE

Until 2010 cyber security of power systems has not been very frequently considered a real threat but everything changed in 2010, after the Stuxnet incidents (malware which attacked and damaged the Iranian centrifuges used for uranium enrichment). The Stuxnet attack has been very well diagnosed and is described, for example, in [Hadji-Janev, Bogdanoski, 2015]. Stuxnet worked by gradually and covertly infecting digital systems of Siemens PLCs (Simatic S7 PLCs, which were programmed with Step 7 language and which utilized WinCC visualization systems – as that was the equipment used to control the Iranian centrifuges) and by continuously propagating onto successive controllers and engineering computers. Stuxnet exploited unknown vulnerabilities in Microsoft operating system and blocked its detection by typical anti-virus software. Having reached its target (engineering computers used to program Simatic PLCs), it detected relevant control algorithms and modified rotational speed settings of centrifuges in these algorithms – it re-programmed centrifuges spin up so as to damage them. Naturally, it also bypassed software protections preventing rotation speed from exceeding maxima and managed to accomplish that

in a way invisible to process engineers. It activated in a specific moment – i.e. it commanded execution of the modified algorithm, which resulted with mechanical damage to centrifuges which simply broke apart due to excessive rotational speeds.

Hence, Stuxnet was the first "cyber warfare" and marked the beginning of the new era [Farwell, Rogozinski, 2012] [Wilson, 2014], even if some authors are finding traces of first military attacks in attempts to paralyze public IT infrastructure undertaken several years before [Kaiser, 2015].

During following years information appeared about evolution of malware and detection of other threats with catchy names such as Duqu, Gauss or Flame. In 2015, energy supply in the Ukrainian distribution grid was aborted in consequence of attacks conducted using BlackEnergy software (which subsequently downloaded and activated KillDIsk). However, in that case the malware infection was caused by employees opening mislabeled files attached to e-mail messages and the attack was less elaborate than in the case of Stuxnet, as it only involved deletion of data from computer disks (which combined with likely incorrect configuration of the Ukrainian systems caused the described consequences). Today, attacks on computer systems of energy companies are occurring on daily basis [8]; however, all publicized cases were non-military actions or actions which just wanted to be perceived as such. Proliferation of the malware codes and means of attack from the military sector to the civilian sector has significantly facilitated this task for persons and groups trying to penetrate the power sector IT systems, although classic protections and separation of key systems seems to fulfill its protective task quite well. Unfortunately, today the most serious threat remains invisible as it is being developed by large teams developing offensive military systems utilizing new, unknown security vulnerabilities and combining the IT knowledge with the engineering knowledge.

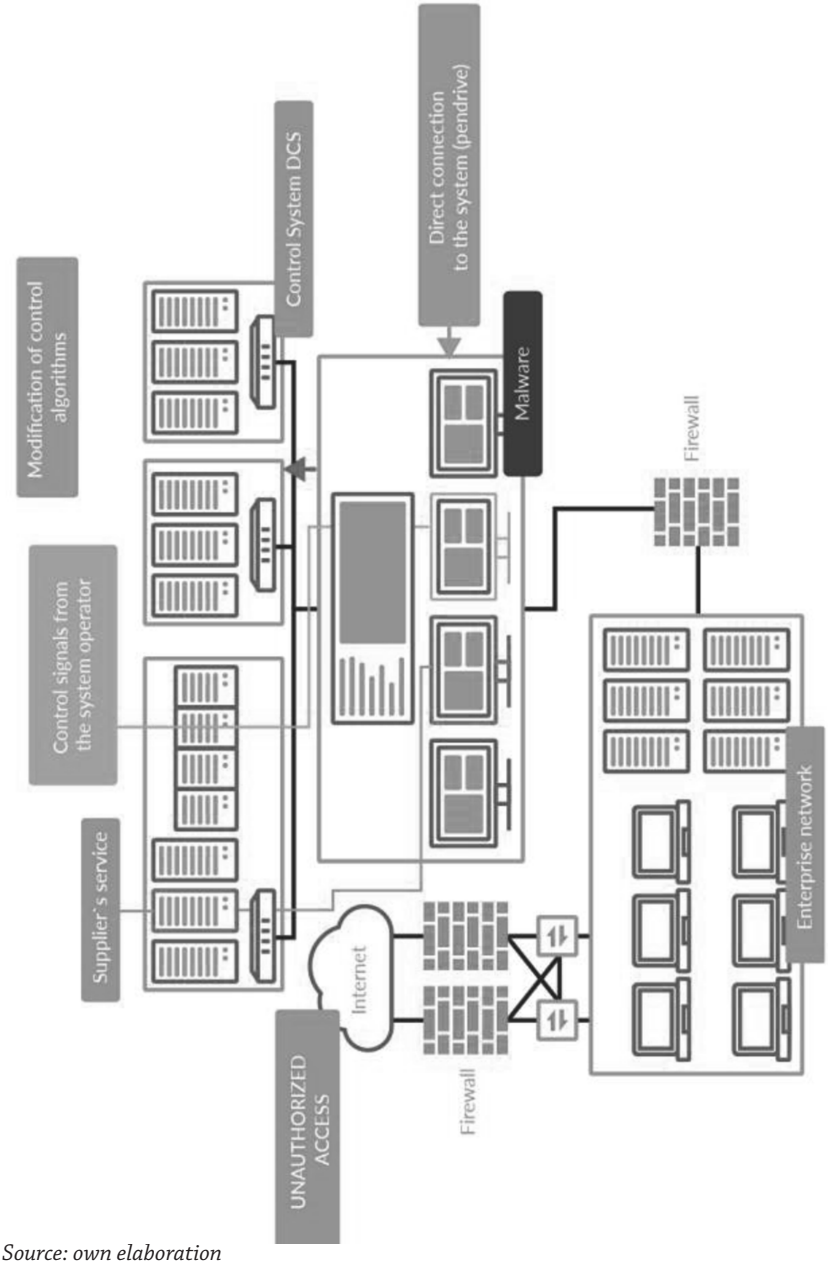
We may expect not only the increased intensity of attacks from varying origins (conducted by amateurs, professional private groups, professional private groups commissioned by businesses and by foreign states or by military IT organizations of other states or a combination of all of the above) either in daily system penetration testing practice or in the case of real conflicts and we should treat this as the first element of the hybrid war [Kaiser, 2015], [Wilson, 2014].

PROTECTION OF CRITICAL INFRASTRUCTURE IN THE ENERGY SECTOR

Since the beginning of industrial control systems implementation, and certainly since the emergence of threats such as Stuxnet, the basic strategy for information protection (ICS – Industrial Control Systems) has been to reduce the possibility of access and separate the control systems from computer networks and Internet access points [The NIS Directive..., 2016], as well as the use of specialized security platforms, in network management systems. In the case of DCS (power plants), the infection of control systems with malicious software can be carried out through direct physical access to the system (e.g. by connecting an engineering workstation to the PLC network or entering malware from a pendrive or other data carrier directly connected to the control system computers) or via contact points with external information systems. The first threat – physical access – has been gradually eliminated by the new system solutions, featuring for instance the inability to connect devices or external storage devices and by increasingly rigorous security policies for physical access to systems (procedures regulating who and how is allowed to use the system). As for the latter case, connection to other systems is eliminated or limited to specific communication methods. As a principle, the control system can operate autonomously (without any connection to the outside world), whilst the few information exchange points with other systems should be carefully controlled [GE Power Digital..., 2016].

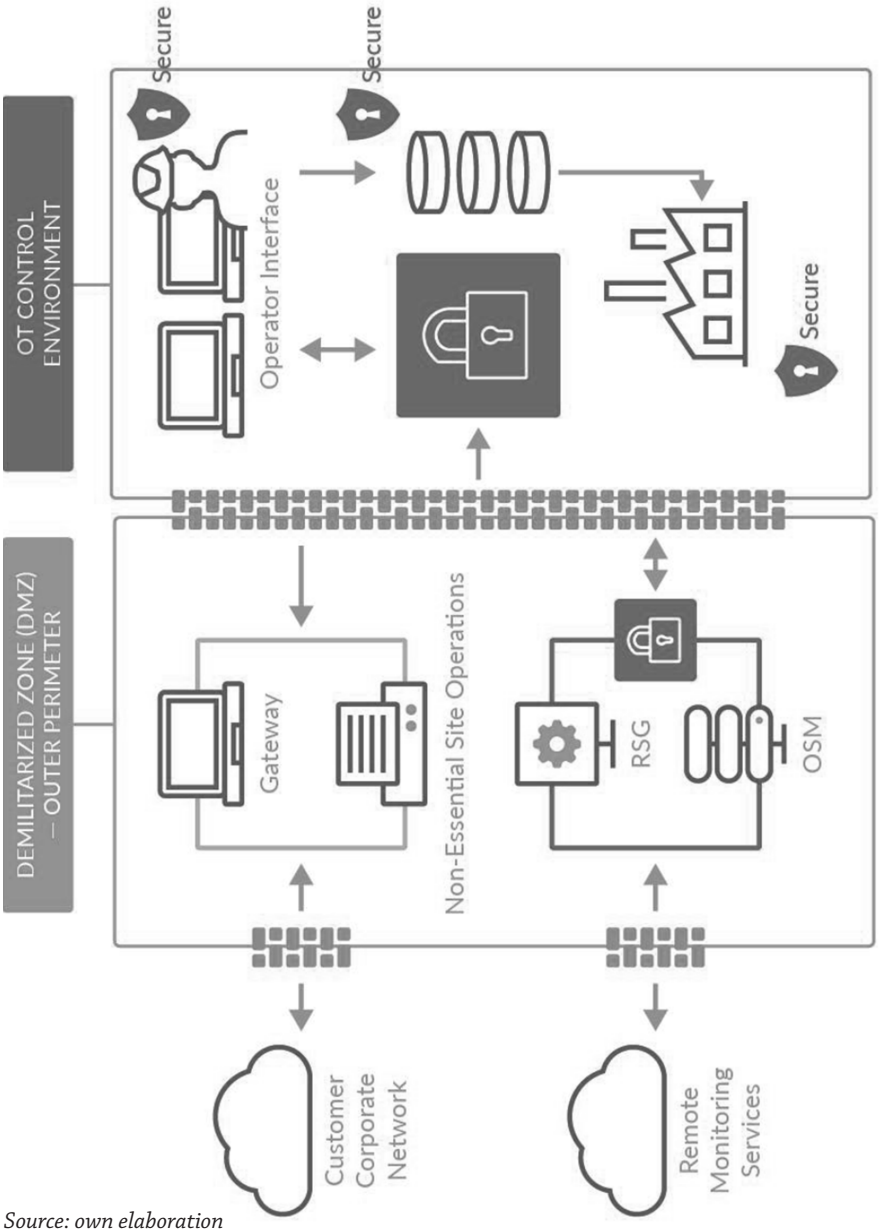
Therefore, in the case of well-supervised IT systems being a part of critical energy infrastructure there should be no possibility of uncontrolled connection between the technical networks (ICS) and other systems. In reality, this is not entirely feasible – DCS or SCADA systems must have a dedicated connection to the national management centers (e.g. in the case of power plants, with a Transmission System Operator for power units operating in ARCM (automatic regulation of frequency and power) systems, from which they receive special control signals controlling the desired operation level), in addition, there are service connections with automation system providers and connections used for process information transfer used by operation control or maintenance departments for diagnostic purposes or for global data analysis. Whilst the former information transfer points are specialized and dedicated networks and use dedicated communication

Figure 4.
DCS and potential attack routes



Source: own elaboration

Figure 5.
A typical mandatory model for separation of automation systems from external environment



Source: own elaboration

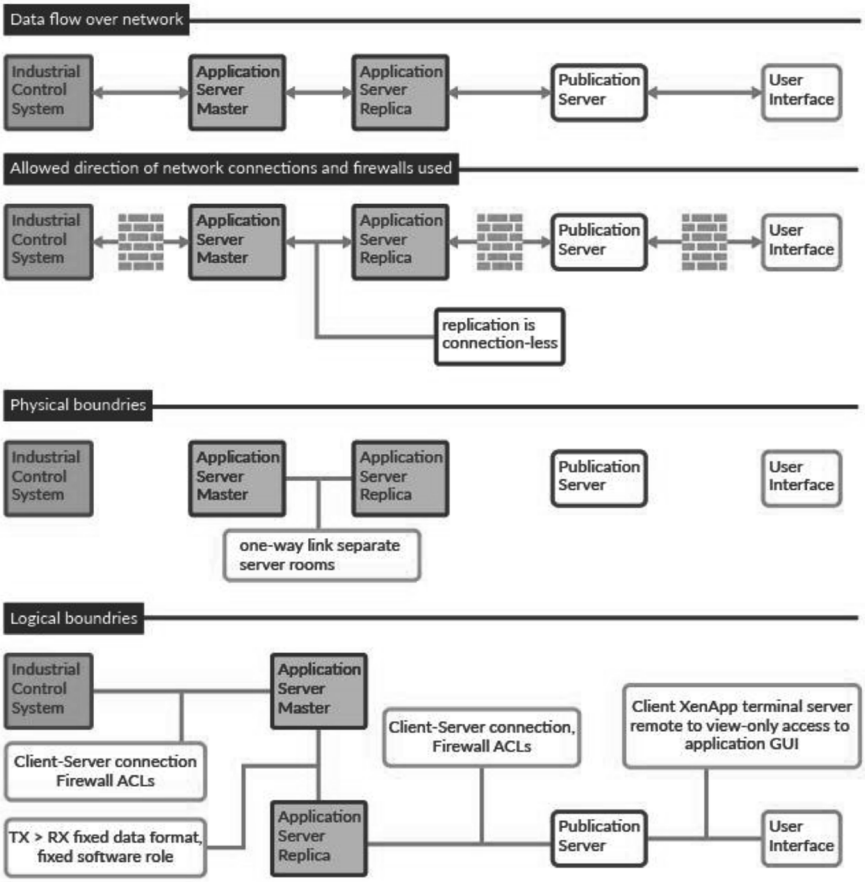
protocols or special authorization methods, the usual policy for information transfer from automation systems to local site (plant and corporate) networks typically does not comply with appropriate safety standards. It is that last integration element that is often the Achilles heel of security. Connections between the automation system and site networks are usually a "gray zone of responsibility" – between the supervision by the Department of Automation and IT Department of the company (therefore uncontrolled) and often utilizing standard, low protection data acquisition protocols (OPC), or even involve undocumented connections by local IT teams. As a result, the critical infrastructure element has many gaps and contains potential routes for security breach, perhaps not posing much danger in the case of common hacking attacks, but being extremely dangerous for potential advanced military threats. As a consequence, the key issue here is to allow process data access whilst isolating automation systems.

Nowadays, it is hard to imagine industrial installations without data access. The number of local area network users processing data at day-to-day work is constantly growing (process engineers, maintenance departments, operation control departments), the possibilities for business intelligence with the use of large data sets are increasing. The use of universal protocols (OPC UA, REST, SOAP) is growing, which, combined with the standardization of architecture of the control systems, increasingly relying on commercial hardware and software leads to the disappearance of previously present barriers (specific protocols and communication media and operating systems). Processing data with the use of mobile devices has also become a standard.

Data acquisition is therefore necessary, but this has to be combined with appropriate cyber-security solutions. It can be achieved with a comprehensive security protection application and industrial data security system, making use of:

- Real-time data replication from the control system with unidirectional connections
- Archive data replication from the control system with unidirectional connections
- Access application isolation with VDI processes (application/user's work environment virtualization)
- No local copies of data or software on user's workstations

Figure 6.
Main components and data flow in proposed solution (EDS Vault)



Source: own elaboration

Figure 6 above presents a detailed solution used by Transition Technologies SA (TT) for projects implemented in Poland and worldwide, mainly for power plants and industrial facilities equipped with Emerson Process Management OVATION control systems and TT proprietary EDS software. In order to ensure the operational security and information safety a multi-layer solution was developed, aimed at eliminating, whenever possible, threats relating to the security of control systems and at minimizing the risk of losing control over sensitive information. The schematic diagram below presents the solution's architecture.

Solution for ensuring the safety of control systems: The control system and the master application server are components of critical significance. The master application server is located in the DMZ of the control system network and dedicated to connect the control network with external systems in a controlled manner. All data from the control system network published within any lower security level network are transferred by the master application server – there is no other connection between the control system network and external networks of lower security levels. Communication between the master application server and lower security level networks is facilitated in an unidirectional connectionless mode. This means that there is no physical possibility to send a data packet from a lower security level network to the DMZ of the control system.

The unidirectional connection is ensured by a hardware solution or hardware connection, as well as the configuration of network layer. Among the supported solutions that ensure unidirectional communication, we can distinguish the so-called Data LEDs, unidirectional network adapters for passive listening or modified UTP network cables. The programming for the unidirectional communication channel includes ACL rules and/or SPAN operation mode of one of the ports, limiting the role of the port to copying packets from another port without the possibility to send. Hardware and configuration elements of unidirectional communication can be combined in order to eliminate certain possibilities for unauthorized change to bidirectional communication (e.g. by bypassing devices or changing the ACL rules). Unidirectional communication is used to replicate live and archive data between the master application server and its replica on the lower security level network side. The method to ensure information security: data is made available to end users with the use of VDI, which means that users use applications which do not run on their workstations, but run remotely, on an application virtualization server. The server used for application virtualization is Citrix XenApp, connected to the domain controller (the element not included in the diagrams), which is used to manage both the access rights for shared applications and the configuration of systems from which the end users access the shared applications. The end user host does not launch any access applications locally. The host for industrial data processing does not establish connection with the replica application server or any other network component of higher security level (i.e. control system network or DMZ subnet).

The industrial data processing/presenting application runs locally on publishing server, and only the user interface of the application is transmitted to the host operated by the user. The data acquired by the application running on the publishing server cannot be sent to the user's system via the channel used to share the application interface. Each application publication session is associated with the user's domain account in order to trace activity and to have the possibility to use access control policies, based on the role, time and place of access. In addition, integration with the domain controller allows the use of multi-factor user authentication mechanisms without affecting the structure of the solution. A domain controller (e.g. Microsoft Active Directory) manages access to the application server. Only devices managed by the domain controller (and devices of appropriate local security level – e.g. restricting the possibility of USB drive use, etc.) are able to access the application publishing interface (e.g. Citrix XenApp).

Despite the use of multiple hardware and software layers the solution maintains a low data transfer latency. Current values (measurements, alarms) are available in the EDS Terminal client application with a delay of approximately 1 second, compared to the data available on operator terminals of the control system. Therefore, this solution may be consider as a one of examples of modern data acquisition software architecture and is accepted and successfully tested according to the advanced international cybersecurity standards.

NORMS AND STANDARDS FOR CYBERSECURITY IN THE ENERGY SECTOR AND THE FUTURE

With the advent of computer threats, we witness the emergence of appropriate standards, procedures or recommendations. International experience shows that all countries are struggling to find the solution for structural problems connected to the development of optimal operational procedures. When analyzing the different approaches, it is worth to look at the following standards: NERC CIP V5 and NEI CIP (USA), CPNI SCADA (UK), CIGRE, JWG D2/B3/C2-01 (France) or VGB R175 (Germany). Apart from the diversity of both the systematics and the detailed norms (for energy) in each country, we also observe the efforts for unification by applying standards pertaining to particular devices (the European

industrial standards level) but here, however, it has been exclusively limited to selected issues of cybersecurity. Accordingly, European industrial standards for selected technology sectors such as IEC 62351 are being introduced in parallel with attempts to develop an industry-wide standard for automation (ISA99 Industrial Automation and Control Security) and the corresponding European IEC 62443 standard ("security for industrial measurement and control").

When analyzing the approach of particular countries to the problem of energy sector cybersecurity, the American procedures seem to be particularly interesting. The analysis of initial experiences on the market indicated the failure of the "voluntary" approach – a system of voluntary compliance with standards. Accordingly, given the expected scale of threats, it has been decided to move to a system of compulsory standard compliance. Supervision of energy (within the scope of cyber-security) under "The Energy Independence and Security Act of 2007 (EISA)" was submitted to the FERC (Federal Energy Regulatory Commission), and the organization in turn commissioned the development of a comprehensive system of procedures and standards of conduct to the North American Electric Reliability Corporation (NERC) NERC's Critical Infrastructure Protection Committee (CIPC). At the moment, the energy sector – utility power generation and transmission branches, with the exception of nuclear power sector, regulated by a separate set of standards – is subject to compulsory adherence to the so-called NERC CIP Ver.5 [North Amercan Electric ..., 2016] enforced by a system of financial penalties. Therefore, the energy sector is obliged to adhere to the cyber security requirements from their own resources, and under pain of financial penalties. It should be noted, however, that the procedures are relatively well developed and precise, and the compliance requirements rightfully relate in the first place to major facilities or installations having the greatest impact on the energy infrastructure and security (in the American nomenclature referred to as BES – Bulk Energy Systems, regulated by the appropriate NERC CIP 002). Today, the entire NERC CIP compilation comprehensively regulates the issue, relating to the definitions, the requirements of the industry and the nature of present risks and protection, both in terms of physical access and IT risks, to staff training and reporting incidents, and undergoes constant updating. The latest version of the standards is NERC

CIP 5, with its further modifications under way. The relevant procedures are CIP-002-5.1 BES Cyber SystemCategorization, CIP-003-6 Security Management Controls, CIP-004-6 Personnel & Training, CIP-005-5 Electronic Security Perimeter, CIP-006-6 Physical Security of BES Cyber Systems, CIP-007-6 Security Management System, CIP-008-5 Incident Reporting and Response Planning, CIP-009-6 Recovery Plans for BES Cyber Systems, CIP-010-2 Configuration Change Management and Vulnerability Assessments, CIP-011-2 Information Protection, CIP-014-2 Physical Security where, as evident, the CIP 7-11 procedures represent the typical problems addressed by IT operations (as with ISO 27000 standards), but the whole issue of security is treated more holistically.

The American solutions constitute a relatively coherent system, which involves the collaboration of the disciplinary CERT, the regulator and the organization responsible for issuing procedures. It seems that this is one of the best models to follow and possibly apply in Polish conditions.

Nevertheless, it should be noted that even the United States are far from complete consistency, because, for instance, cyber security at nuclear power plants is regulated by the relevant provisions of NEI (organizations associated with nuclear power) and for the recently relevant cyber-security issue of ”smart grid” FERC issued the NIST document (“Guidelines for Smart Grid Cybersecurity”). These procedures and standards also apply exclusively to electric power industry, as the gas industry for instance is subject to conditions as set out by the American Gas Association (AGA): Series of AGA12 reports, with the chemical industry being regulated by a yet different set of regulations. To sum up – even in the US it is being discussed whether the current system of organization and operation of the relevant services is appropriate and adequate for the risks and whether the critical infrastructure is secure against cyberattacks.

The newly adapted (July 2016) NIS Directive of the European Parliament and of the EU Council 2016/1148 dated July 6, 2016 – on measures to promote high common level of security of networks and information systems in the European Union should become an impulse (in Europe and Poland) for further development of a comprehensive information protection system for the energy sector. However, this is a “high level” directive – referring to the holistic view on the problem of cybersecurity and all sectors. From the perspective of energy sector it describes elements

that define the so-called "critical service provider" and includes enterprises *defined as in Art. 2, Item 35 of the Directive of the European Parliament and Council 2009/72/EC (1), which execute the function of "delivery" as defined in Art. 2, Item 19 of the directive*

- distribution system operators as defined in Art. 2, Item 6 of Directive 2009/72/EC
- transmission system operators as defined in Art. 2, Item 4 of Directive 2009/72/EC.

To sum up, the European experience today is based on a system of recommendations, the detail level of which varies depending on particular country. Procedures are created for particular devices, SCADA systems as well as particular sectors. The signaled desire for unification based on a single European procedure is probably the reason for lack of detail in the procedures as well as their substantially general scope – which contributes to difficulties in their practical application. Recommendations are still not mandatory and not regulated by any coherent system.

Comparing the international approach, it seems that European countries are at a stage that the US and Israel have long left behind – of noticing the great problem and the numerous threats connected to cybersecurity, but also the expectation that the issue will be resolved by manufacturers and users by voluntary complying to the standards. Therefore the recommendations in place are general and usually issued too late in order to respond to the market situation. It seems probable that one day the European countries will adapt the compulsory system, robustly formalized for each subarea of critical infrastructure. The key Polish IT systems for energy and gas supply are not protected against contemporary threats. In practice, only the "classical" and commercial security measures of relatively low proceduralization level are implemented – there are no standards of conduct, and if so, they are applied exclusively by particular businesses or constitute general practices, such as set out in ISO/IEC 27000 standards. In most cases, the industrial corporations' security policies focus on the safety of "information" and not the "process" and here also only standard practices are followed.

Looking pessimistically, considering the technology of power plant control and energy distribution, the systems nowadays in Poland are full of

gaps – related for instance to multiple connections to master systems (for data transfer). The landscape for other systems such as water or gas supply systems presents itself even worse. The entire set of practices for system changes does not live up to contemporary standards. The current approach (although changing) entails protection against common network threats and the use of modern but only commercial solutions for protection, omitting the importance of military threats (in the case of actual military conflict). As a result, the IT systems for critical installations are vulnerable in case of a modern conflict with the use of modern cyber warfare. Meanwhile, this issue is considered to be absolutely crucial in the security doctrines of the US, where well-developed standards are already in place. While this has not been a problem yet, as we have no reported incidents of control systems activation or successful cyber-attacks in Poland, it does not mean that the problem does not exist. Conversely, it seems that this is the final call before the rising tide of both criminal and military threats. Obviously, there have been first signs indicating that the cybersecurity problem exists and relevant systems must be secured. Energy industry organization have created appropriate bodies for their Information security management. In some cases their work is in accordance with the actual needs, however some of them limit exclusively to security audits. Some IT compliance departments of energy corporations are urgently seeking a specialized set of industry standards, which would allow to improve the security better than the general ISO procedures for IT.

The issue is evident in selected tender specifications by references made to foreign standards and documentation. Finally, we see the emergence of integrated security plans and models that aim at ensuring the continuity of the process by the use of backup and recovery. Recent months have shown a growing awareness of the major energy companies that sign agreements with the leading suppliers of audit and protection services, or even appoint their own CERT units. Unfortunately, the IT management is affected by constant personnel changes, and, as a consequence, changes or discontinuity regarding IT policies for particular businesses. In the absence of a global security strategy for critical infrastructure or any detailed industry standards for critical infrastructure of the energy sector, the strategy undertaken is a sum of actions by individual enterprises, without any comprehensive plan.

CONCLUSION

It seems that the adoption of the NIS [13] and the new revisions of cybersecurity strategies for the Republic of Poland [15], the revised version of the National Critical Infrastructure Protection Program [Rządowe Centrum ..., 2016] are subsequent steps that must lead to a further fundamental change in policy towards the protection of critical infrastructure in the energy sector. The appointment of National CERT must also result in the construction of a specialized "disciplinary" CERT – dedicated specifically to information systems for controlling the supply of gas, water, etc., as well as the adoption of some form of copy of the prescriptive American system, with robust standards for energy sector. Yet another step will be the necessary investments in which the energy sector companies will have to embrace the new standards under the pain of financial penalties We need to accept that predictable next (even hypothetical) military conflict will be a cyber clash with the use of software and advanced security systems.

Literature

Bayar T. (2016). *Cybersecurity in the power sector.* Power Engineering International.

Clarke R., Knake K. (2012). *Cyber War; The Next Threat to National Security and What to Do About It*. NY Ecco HarperCollins Publishers.

Falliere N., Murchu L.; W32.Sruxnet.Dossier, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [data dostępu: 16.09.2016].

Farwell J., Rogozinski R. (2012). *Stuxnet and the Future of Cyber War*. Survival 54.

GE Power Digital Solutions, 5 Security Imperatives for Power Executives, https://www.ge.com/digital/products/cyber- [data dostępu: 16.09.2016].

Hadji-Janev M., Bogdanoski M. (2015). *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare.* JVG Books LLC.

Kaiser R. (2015). *The birth of cyberwar.* Political Geography.

Kyung-bok L., Jong-in L. (2016). *The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd*. KSII Transactions on Internet and Information Systems Vol. 10.

North Amercan Electric Realiability Corporation CIP Standards, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx [data dostępu: 16.09.2016].

Rządowe Centrum Bezpieczeństwa Narodowy Program Infrastruktury Krytycznej, http://rcb.gov.pl/wp-content/uploads/NPOIK-dokument-g%C5%82%C3%B3wny.pdf [data dostępu: 16.09.2016].

Takebe T. (2014). *Trends in Industry Standards and International Standards for Industrial Automation Control System Security*. Yokogawa Technical Report English Edition Vol. 57 No. 2.

The NIS Directive of the European Parliament, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013PC0048 [data dostępu: 16.09.2016].

Wilson C. (2014). *Cyber Threats to Critical Information Infrastructure, chapter un Cyberterrorism: Understanding, Assessment, and Response, Chapter: Cyber Threats to Critical Information Infrastructure*. Springer-Swansea University.

Zespół międzyresortowy Ministerstwa Cyfryzacji, Założenia Strategii Cyberbezpieczeństwa dla Rzeczpospolitej Polskiej, https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf [data dostępu: 16.09.2016].