Henryka Jormakka, Pekka Koponen, Heimo Pentikäinen,
Technical Research Centre of Finland

Hanna Bartoszewicz-Burczy
Institute of Power Engineering

Control systems of critical infrastructures, security analysis

The interconnected electrical transmission and distribution networks are geographically very distributed. Competitive energy markets, increase in distributed generation and use of renewable energy sources, and growing dependence on imported energy, increase the complexity of the operational level of the infrastructures controlling all the necessary processes. The infrastructures are operated from interconnected control centers via distributed Industrial Control Systems (ICSs) with the help of other information technology (IT) systems. The control systems have been for many years isolated from administrative corporate networks due to heterogeneous proprietary networks and security concerns. Now the situation has changed. Due to the increasing complexity and integration as well as the necessity to improve effectiveness of business in a highly competitive environment where fast communication and data exchange are crucial factors, the use of communication networks, open technologies and protocols in control systems for critical infrastructures is increasing.

The integration of the control network into the company business units and the connection with business partners supports new IT capabilities, but at the same time it opens the network to external threats typical for any information technology system. While security solutions have been designed for security issues of traditional IT systems, they have to be carefully adapted to the demands of an ICS environment. In spite of many common features and similarities, ICS differs from typical Internet-based information processing systems, including different threats, vulnerabilities and priorities. In IT systems data confidentiality and integrity is the main requirement. In traditional control systems it is the human safety followed by protection of the system processes to save from harm the environment and prevent financial losses, so system availability and integrity are the core priorities. ICS has also different performance and reliability requirements than IT systems. Especially in emergency situations fast responses in the interaction between the process, its automation and human operators are critical. Furthermore, the goals of efficiency and availability have a tendency to conflict with security in the design and operation of ICSs. For that reason, taking also into account that many old proprietary control systems (still operating) do not support security, it is important to re-evaluate ICS security architecture in order to mitigate the possibilities of electronic attacks. Adding to the complexity of the situation, IT security and control system expertise is usually not found within the same personnel. Therefore ICS and IT security experts need to cooperate closely, the more that the SCADA systems are high-profile targets for well trained attackers aiming at maximum damage with minimum personal risk.

Distributed industrial control system – overview

It is today possible to securely operate an insecure system encapsulated in a security architecture that uses layers of additional electronic and procedural measures to ensure that the probability of compromise of the system remains small. Electronic access can be protected by levels of firewalls and intrusion detection systems with data transfer architectures that exports externally relevant data to the outside while blocking any incoming request. Communication protocols can be secured using virtual private networks and associated authentication/authorization mechanisms at the network endpoints. Non-existing access controls at the console of the control system can be addressed e.g. by introduction of, potentially technically supported, operational policies and procedures that ensure that only authorized persons have physical access to the control system. However, the level of difficulty in improving security of an ICS varies, depending on the vulnerability. In case of some attacks, mitigation means mostly administrative decisions like defining correct access control rules, or defining correct security policy. In other cases, like integrity checking mechanisms, correct firewalls policy, network monitoring, segmentation and increased redundancy, it means some investments in new software or hardware, or constant staff education programs. Most challenging are the situations when one has to trade between system availability/integrity, which are essential in

case of ICSs, and security (examples of such cases are provision of scalable access control methods, or implementation and testing of updates) and therefore such situations require most effort and should be carefully studied.

To support the design and maintenance of ICS, a number of different initiatives dedicated to guidance on industrial automation systems security have been going on world-wide. An example is IEC (www.iec.org) that in different working groups addressed security issues for field buses or security profiles for secure communication in industrial networks and edited sets of relevant standards including IEC/TS 62351. Other examples are the National Institute of Standards and Technology (NIST) with its Guide to Industrial Control Systems (ICS) Security and similar documents, or Instrumentation, Systems, and Automation Society (ISA) creating guidance documents and standards [1] on introducing IT security to existing industrial control and automation systems. The control system architectures proposed by the different fora provide compulsory segmentation between control systems, company internal networks, and external connections. They promote layered, defense-in-depth solutions against cyber attacks and bring new opportunities for more secure modern, but also legacy systems adding an additional protection layer.

An example of a modern, distributed industrial system controlling electricity networks is presented in Figure 1., showing different sectors and communication links to different partners of an ICS. It illustrates separation between the control (SCADA LAN) and the administrative networks by the demilitarized zone (DMZ) - a separate network segment with firewalls to prevent traffic from passing directly between the two networks.The SCADA LAN houses among others the SCADA server and master terminal units (MTU) that collect information from remote terminal units (RTUs) and programmable logic controllers (PLCs) located in substations or other field sites. For the communication between the RTUs, PLCs and MTU, SCADA wide area networks (SCADA WANs) are used. Using these connections the control center is polling field devices for data or watches for interrupts coming from the field site alarm systems. Such centralized system enables operators to control and monitor large areas enabling remote maintenance or troubleshooting operations and management of distant sites. This is very crucial from the economic and service continuity point of view. For communication with other control centers or business partners private or public WANs are used.

The industrial control systems are moving into the direction of commercial off-the-shelf software and hardware products. These products are based on standard protocols such as e.g. Internet Protocol for communication between control systems and field devices, or commonly used operating systems like Microsoft Windows. The usage of COTS products reduces the costs of the systems, but at the same time increases the probability of electronic attacks through standardized interfaces and unnecessary functionality and code. Tools for conducting such attacks are commonly available on the Internet. While breaking into a remote IT system once required a lot of knowledge and skills, nowadays it is enough to download attack tools from the Internet and used them against interconnected servers. With time the tools are becoming more commonplace and easier to use, which means that less expertise and effort is required from an attacker. Except for tools made intentionally for launching illegal attacks, there are many “legal” devices and information that can be used for conducting attacks. This includes product manufactures’ technical specifications and network maintenance tools that are commonly used for data collection to analyze traffic, for network troubleshooting, or for configuration management.

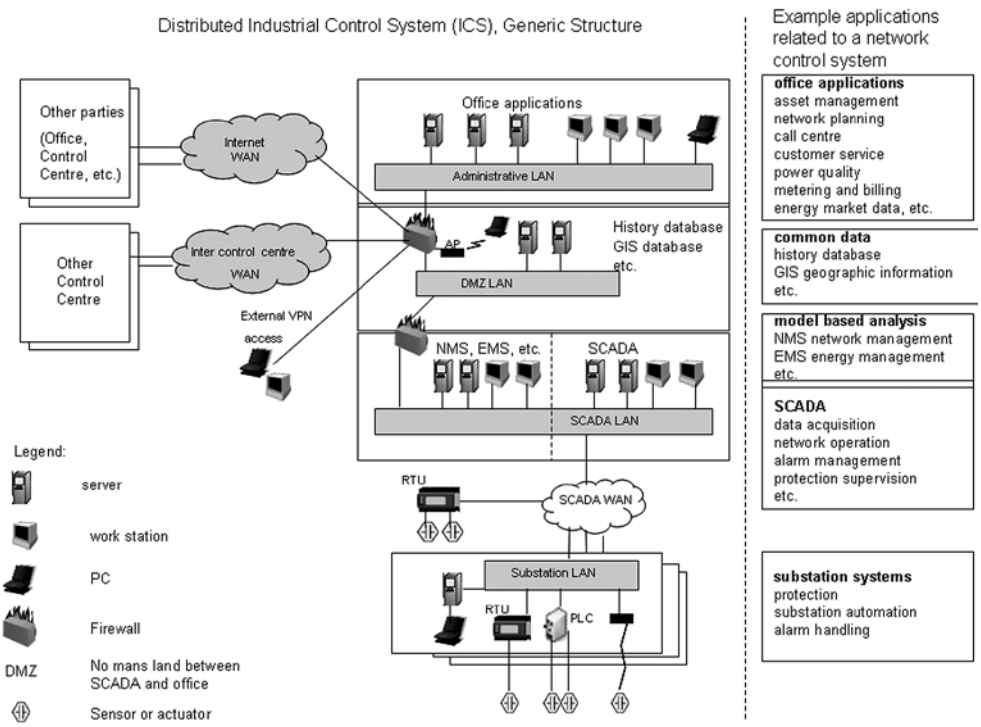

Fig. 1. Overview of Distributed Industrial Control System

Although much of the complexity in maintaining complicated systems can be avoided by division into separate units, it has to be remembered that compromising a computing resource that has access to a control system is the same as compromising the whole control system itself. Therefore to reduce the risk of malicious attacks, looking at the whole system as one unit, it is important to minimize the vulnerabilities of inadequate security layering and zones, improperly configured firewalls that divide the zones, lack of proper security monitoring, or inadequate security policies. In the following subsections, different, geographically distributed subsystems of the control system, as presented in Figure 1., will be investigated from the security point of view.

IT systems security and attack mitigation methods

Although much of the complexity in maintaining complicated systems can be avoided by division into separate units, it has to be remembered that compromising a computing resource that has access to a control system is the same as compromising the whole control system itself. This considers e.g. access via a wireless handheld device connected to an access point located in a DMZ, but also access through an unprotected field device, or virus infected terminal via VPN. Therefore to reduce the risk of malicious attacks, looking at the whole system as one unit, it is important to minimize the vulnerabilities of

- inadequate security layering and zones,
- improperly configured firewalls that divide the zones,
- lack of proper security monitoring,
- inadequate security policies.

In the following subsections, we will investigate different, geographically distributed subsystems of the control system, as presented in Figure 1, from the cyber security point of view.

SCADA LAN

In the past when the SCADA systems were working in standalone pattern, they were based on proprietary protocols, techniques and underlying control systems. Although now the situation is different, often in terms of information security the applied SCADA technology has not evolved enough to match this development. IEC 61850 protocols are used increasingly in conjunction with IEC/TS 62351, but insecure protocols are still commonly applied. Those application protocols used by the servers and workstations are mostly run on Ethernet and the TCP/IP protocol stack, or directly on TCP. To some extent they share the advantages, but also the negative features of a typical LAN. The difference is that the servers and workstations of a SCADA LAN are not used for general purpose computing, so they are not affected by applications such as e-mails, or Internet web browsers. Additionally, the hardware and software topology and configuration of a SCADA LAN is relatively static, so the usage patterns are basically known at the configuration time. However, there are hard restrictions imposed on the LAN. The communication is time critical and the system should be fully operating 24 hours per day. This may not be a problem, if redundancies are incorporated, but the hardware and software updates, antiviral checking and other changes have to be carefully planned. Except for the supervisory and control application software, some specialized protocols must run to provide reliable operation and management of the SCADA LAN. Those protocols, e.g. the Address Resolution Protocol, are the most frequent sources of attacks.

Some of the servers (e.g. the Historian) essential for control purposes have to be used by both – the control system and the administrative units. Placing them in the administrative network means that some insecure protocols (e.g. MODBUS, DCOM) will be used for communication with the SCADA LAN. On the other hand, placing those servers in the SCADA LAN means that such protocols like SQL, or HTTP have to be permitted to access the SCADA LAN servers. Additional sources of vulnerabilities are the connections to the administrative and substation networks which in case of improperly configured firewalls or incorrectly protected access to field devices may open the network for attacks.

As consequences of vulnerabilities of SCADA LAN can be mentioned such as infection of control network servers by malware disabling a safety monitoring system resulting in a lack of reaction to abnormal plant operation, making the system unavailable to system operators, as well as improperly schedule updates that may lock up the SCADA system and interfere with the service delivery to the customers. To mitigate the results of attempted attacks the following precaution methods should be applied.

Attack mitigation methods

Passwords that are well known sources of automated attacks and phishing, should be not disclosed to third persons and not send via networks in clear text. Securing devices with hard passwords slows down the attacker. The passwords should contain at least six case sensitive alphanumeric characters, and not forming any pronounceable name (to avoid dictionary attack). The number of failed access attempts to enter a password should be limited. [2] presents interesting data concerning comparison of time used for cracking password using brute-force and dictionary attacks in case of 4, 6 and 8 characters. The measurements were made for a typical substation controller, but the ratio of the time required in the above cases remains the same in case of any networked device.

Security policies should be developed and used. This refers to technical issues, but also to personal policies such as strict access control rules, or personnel training to increase safety and security awareness. The policies should be reviewed periodically to include countermeasures for new arriving threats, taking into account the system functionality and requirements. Because of the peculiarity of the SCADA system, it is possible that some of the vulnerabilities cannot be completely removed, as the resulting system would turn out to be inefficient, or even inoperable. In such cases the administrator must be provided with the possibility for controlling access in such a way that the vulnerability cannot be

exploited. For that e.g. filters, specific system configuration, or monitoring can be used.

New threats or system failures usually require software patching, updating, or upgrading. Those activities should be carefully planned not to interrupt the system operations. The optimal solution would be a parallel mirror system that could be switched on for the time of updates, otherwise used for redundancy as replacement of crashed hardware or software modules.

Placing in SCADA LAN servers that are shared with the administrative network should be avoided. Also, whenever appropriate, servers that are normally located in the business network and need to be used in the control network, need to be replicated on the control system network in order to minimize the amount of "look up" traffic that must pass from the control system through the electronic security perimeter to the business network. In general, servers used in both of the networks should be located outside of both of them. A better solution is to use the DMZ and locate there all the servers shared by the two networks, instead of two-zone solution (no DMZ, firewalls only). Using "hard coded" addresses on servers within the control system network will further reduce the need for out-bound traffic.

Access to all the unnecessary resources and services should be blocked. This is possible through use of perimeter devices (firewalls, proxies, filters) with access control lists. Only the necessary services should be enabled and only on per device rule. Network connections that bypass perimeter protection mechanisms should be eliminated. All direct remote access to the control LAN should be blocked.

The network servers and workstations should be regularly or continuously monitored for malicious activities. This may be based on monitoring of log files of the LAN devices, including firewalls protecting the LAN, in order to detect successful or attempted unauthorized access. Use of intrusion detection systems inside automation systems is not a daily practice. Some argue that typical IDS does not target automation specific protocols and for that reason will not detect attacks on that levels, instead confusing the operator in case of plant malfunction by sending additional alarms caused by the alarm messages of the control system. However, most attacks use typical IT, not SCADA specific protocols. Additionally, there exist some IDS that include rules for some automation protocols and the additional alarms will not appear if signature based IDS are used. The signatures have to be updated any time new signatures are developed following new discovered attacks. As IDS provides passive (monitoring) form of security protection, it is important to analyze the IDS log files frequently, to prevent an attacker from gaining access to the system before the log file is reviewed. Using multiple IDSs of different vendors enhances the system's security. All the IDS software should be tested before deployment to determine that it does not compromise, or make unavailable normal operation of the ICS.

Use of any unauthorized CDs, DVDs, and USB memory sticks on any node connected to SCADA LAN should not be permitted to prevent the insertion of malware. In all other cases, they should be scanned against malware. If drives/ports for the memory devices are not used for operational purposes, they may be disabled.

Components critical for the ICS operation should be identified. The system should be built with a small number of redundant diverse critical components using a fault-tolerant architecture, so that failures of individual components do not lead to failure of the system functionality. Single points of failure should be identified and risk assessment done.

Substations and field devices

SCADA field site, where the field devices are locked in unmanned remote cabinets, is one of the places from where an attack on a control system may be started. Often the devices physical security level is low due to the cost of large number of sites and the belief that a single device cannot cause a substantial damage. However, well-known vector attack (see [3]) using the remote device's network showed that this belief is not based on facts. The devices such as sensors, actuators, or valves as well as RTUs or PLCs located in substations and their communication links are part of the internal trusted domain, and some of them provide administrators with capabilities for remote maintenance access via laptops or other handheld devices using dial in or dedicated means like private radio, or public mobile cellular networks. For data collection and for communication they are using application-specific and often proprietary protocols which often do not include any security features. Even in the newest substations the IEC 61850-9-1/2 standard providing interoperability between equipment from different manufactures does not include security but refers to the IEC 62351-6 standard. For connection to the RTUs or PLCs the field devices/sensors use wired or wireless connections. The wires are vulnerable to physical destruction, reconnection of wires for message tampering and man-in-the-middle attacks, and eavesdropping. The physical destruction is usually detected fast by the existing fault-handling features of the systems, while intentional reconnection of the wires is of limited scope and therefore of limited interest to the attackers. In case of wireless communication the wired connections are replaced by radio frequency transmission. Due to lower installation costs and decreasing prices of communication, wireless connections continue to expand. In case of large number of devices field buses are used to connect them to controllers for the time-critical connections. Field bus protocols are optimized to provide fast access and many forms of redundancy are introduced to provide fault tolerance against random errors and equipment failures, but they do not offer security features against intentional attacks.

As the devices are part of a trusted domain, access into them can provide an attacker with an unauthorized access to the whole control system. Using control over a compromised device, the attacker may execute various procedures such as modifying data to be sent to the control station, changing the behavior of the field devices causing fault alarms, or on the contrary, not passing the data that should alarm the master station. Finally, he/she may scan the internal control network, what may be relatively easy as most likely the connections are not monitored for malicious traffic.

Attacks on substation may cause data interception and manipulation, DoS, or malware being installed through infected laptop of the substation LANs maintenance personnel. They can result in unnecessary disconnection of a power line without real reason, failure to break circuit as should happen due to the protection system, or in unauthorized changes to instructions for PLCs or RTUs. The latter may reduce transmission and distribution capacity and operational margins, increase losses, shutdowns or equipment damage due to under or over-voltages, etc. To minimize the effects of an attack, precaution methods should be applied.

Attack mitigation methods

Whenever possible, the substation devices should be protected by hard passwords, especially if wireless, or remote connections to the substation devices are allowed for maintenance and administration purposes. In that case strong authentication methods and access control should be used. In case of wireless connection the authentication should be mutual. Also the access point (AP) should be authenticated by the legitimate user in order to avoid false AP deployed by an attacker that can later reused the information (password and ID) illegally obtained from the user. As a support to provide security for the communication standards developed for control systems, the IEC/TS 62351 set of standards has been designed and should be used in future. It contains seven documents, out of which six (IEC 62351-1 to IEC 62351-6) are standards, the seventh, IEC 62351-7 has been issued as a Committee Draft and will eventually become a Technical Specification. These standards address different security objectives including authentication of entities through digital signatures, ensuring only authorized access, preventing eavesdropping, playback and spoofing, as well as providing some degree of intrusion detection. In some cases all of these objectives are important; in others, only some are feasible given the computation constraints of certain field devices, the media speed constraints, and the need to allow both secure and non-secured devices on the same network.

Portable equipment like laptops, USB memories, CDs used for direct access to the field devices should be scanned for malware before connecting to the device.

As in the case of the control equipment of SCADA LANs, the substation devices should be prepared for installation of patches that fix known errors as well as to replacement of crashed hardware modules. And, as in case of SCADA LAN, they should be scanned for malware detection. Components critical for the operation should be identified and the system should be built with a small number of redundant diverse critical components. Single points of failure should be identified and risk assessment done.

DMZ and connection to the administrative network

The SCADA LAN has to be well protected not only from malicious external and internal attacks, but also from unintentional damages caused by access from the administrative domain. In minimizing security risks the best solution is a DMZ, preventing direct traffic between the ICS and administrative networks, with separate authentication mechanisms. The DMZ contains firewalls guarding all access to and from the networks, and should include all the servers that contain the ICS data that needs to be accessed from the administrative network such as e.g. the Historian, but also a patch management server, an IDS, or other servers required for security of the control network. The databases in the servers may be connected to web-enabled databases located on the administrative network. Although the attacks on them are used mainly for stealing the data, they can be also used for gaining access to other devices through the server hosting the database. Alternative to DMZ, although not as effective solution is a set of firewalls between the SCADA LAN and the external networks.

The DMZ is also used for controlling remote client access, if such access to SCADA information is required. While direct connection between the SCADA server and remote client could be secured from data or identity interception by usage of virtual private networks (VPN), the risk of a compromised client device still remains. The control system administrator has no means for monitoring or enforcing security on the remote client, especially if it is under different organization's control. For such cases DMZ may offer protection in the form of terminal server, the external client connects to the terminal server located in the DMZ, which in turn uses another connection to the device of the control center to which the client aims to connect. The terminal server is under full control of the control network administrator. As it is not used for automated control system applications, it does not have strict real-time constrains and can be regularly patched, updated, or scanned for malicious software.

To main consequences of attacks on DMZ belong corruption of data critical for operational decision what can result in power plant operation failure by the control system not able to perform control and monitoring functions, corruption of data critical for business, or unavailability of operational or business services due to DoS attack caused by malware.

Attack mitigation methods

It is important to protect DMZs against vulnerabilities such as firewalls improperly configured, or insufficient IDS and firewalls logs. The DMZs should be customized according to the system functional and security requirements. Good practice is to use multiple firewalls from different vendors.

With a few exceptions, external access to the devices inside the control system should be allowed only via a DMZ and limited to necessary for the system functionality. As a rule the direct traffic incoming to SCADA LAN should be blocked and all traffic from either side – the control and administrative networks, could terminate at the servers located in the DMZ. For example, IEC 61850 protocol, might be used to communicate from the PLCs to the data historian, while HTTPS might be used for communication between the historian and administrative clients, neither crossing the two networks. In similar way any two other protocols could be used in the control-to-administrative network communication.

This reduces e.g. the chance of injecting the control network with worms, since the worm would have to use two different exploits over two different protocols. All unnecessary services/interfaces/ports should be blocked.

The direct traffic incoming to SCADA LAN should be monitored. Also the outgoing traffic passing a firewall should be limited to necessity only and monitored. All incoming and outgoing traffic should be source and destination-restricted on service and port basis to prevent the control network from being a source of spoofed communication. For each permitted direct incoming or outgoing data flow there should be a documented justification with risk analysis and a person responsible for the traffic monitoring.

If third party remote connections are permitted, the terminal server can be used to offer connection to the client and to mirror the server of the control center.

As the DMZ is the gateway to the control network, it should be guarded by always up to date antiviral software. If the IDS is signature based, the signatures have to be updated any time when new signatures are developed following new discovered attacks. All the IDS software should be tested before deployment to determine that it does not compromise, or make unavailable normal operation of the ICS. The antiviral system behavior should be also tested against critical situations, to assure that it does not send additional alarms caused by the alarm messages of the automation system.

In case if instead of DMZ there is only a firewall, or set of them, particular care needs to be taken with the firewall rule design. The rules should restrict traffic incoming to the SCADA LAN to a very small set of shared devices (e.g., the Historian) on the control network from a controlled set of addresses on the corporate network. Allowing any IP addresses of the administrative network to access servers inside the control network is not recommended. In addition, the allowed ports should be carefully restricted to relatively secure protocols such as Hypertext Transfer Protocol Secure (HTTPS). Allowing HTTP, FTP, or other unsecure protocols to cross the firewall, is a security risk due to the possibilities of traffic sniffing and modification. The firewalls should enforce user authentication and authorization allowing access to necessary nodes only and block the SCADA devices from access to the Internet.

Communication networks and remote connections

Maintenance and supervision of transport and distribution energy networks involves exchange of information between their different parts. The communication between SCADA and other IT systems, as well as communication with business partners, is done via wide area networks (WANs). In particular the networks are used (see Figure 1.) for communication between control center and substations (SCADA WAN), between different control centers of the same transmission or distribution operators, between different control centers of the different transmission or distribution operators and for communication with other business partners or remote offices. The infrastructure and the protocols of different networks vary, depending on the network coverage, age, usage pattern, or the energy transporting/distributing company size, ranging from private networks to the Internet. Depending on the type of the network, also the security threats may vary, however, most of them are common to all of the networks.

As SCADA devices may not support strong authentication methods, therefore direct remote support personnel connections to the SCADA LAN make the devices vulnerable to malicious attacks. Also field sites are often equipped with a remote access capability to allow field operators to perform remote diagnostics and repairs usually over a separate dial up modem or WAN connection.

The main vulnerabilities of the communication networks are lack of appropriate data encryption mechanisms, lack of redundancy for critical networks, network device configuration not stored or backed-up, security features provided by system vendors not implemented, updates not used.

The consequences of attacks can be corruption of data critical for operational decision resulting in power plant operation failure, delaying or blocking information flow which may make the network unavailable to control system operators, corruption of data critical for business operations, or corruption of user passwords and IDs (due to lack of encryption methods).

Attack mitigation methods

As most of the security attacks are caused via the communication links, to mitigate the risks, strict rules enabling communication should be established and followed. First of all, the SCADA environment should not be linked directly to the Internet and should not use the Internet to transfer information, unless a separate risk analysis will be conducted regarding DoS attacks and loss of the Internet infrastructure. Remote connections and wireless access points should not be allowed directly to the SCADA LAN, but through the DMZ and only with proper encryption and strong authentication of the users. Any unessential links between SCADA LAN and other networks should be blocked.

Although the main security measures may in many cases be authentication and access control, to mitigate such attack as man-in-the-middle, or data interception, insecure communication protocols can be secured by running them inside a secure tunnel provided by a virtual private network which provides confidentiality and integrity of the transmitted data. The latency introduced by cryptographic methods must not degrade the operational performance of the control system or impact personnel safety, therefore VPN devices avoiding latency problems, as offered by various vendors, should be used. As the main objectives of ICS are in order – system availability, data integrity and confidentiality, failure of a cryptographic mechanism must not create a denial of service. Therefore the use of cryptography should be determined after careful consideration. Additionally, it has to be remembered that VPN secures only the transport level protocols, but not the application level. To provide the latest, there should be used additional security measures such as the IEC 62351.

Network devices under the company control, particularly the networks separation points like firewalls and routers, should be monitored on a regular basis. Configuration of critical network elements that are under the company management should be backed-up. Based on potential consequences, also the appropriate restoration processes should be defined. A mixture of backup/restore approaches and storage methods should be used to ensure that backups are rigorously produced, securely stored, and appropriately accessible for restoration. Single points of failure should be identified and risk assessment should be evaluated.

As a rule only preauthorized equipment scanned for malware should be remotely connected to the SCADA network via DMZ. Otherwise, to decrease the risk, the usage of two computers sharing applications in series as presented in the DMZ section should be considered. Remote access should be enabled only when required, approved, authenticated and monitored. To prevent identity interception and data manipulation during communication, encryption should be used whenever possible or required. Third parties equipment should not be allowed to remotely access the devices of the SCADA LAN. If for operational reasons an exception has to be made, not only the equipment should be scanned for malware, but also the connection should be carried out under supervision and responsibility of an employer of the SCADA network owner.

Physical threats to electric systems

Except for cyber attacks, the electric systems are exposed to physical threats of different nature. The main elements of those threats are aging, exploited material used in various processes, random accidents, malfunctioning of an automatic protection system, natural events like storms, floods, fires, hurricanes or earthquakes, or intentional terrorist attacks. One more important factor and at the same time one of the biggest threats to the security of an industrial system is the threat posed by inside personnel which may result from unawareness, negligence, lack of competence, but also from a limited loyalty to an employer and sabotage. Additionally, the personnel itself may be under heavy stress or violent threat e.g. from different kind of criminals or even terrorist.

To mitigate consequences of the above mentioned threats, various countermeasures can be applied. To minimize accidental damages, there should be organized training courses for the personnel which should be sufficiently qualified with regular control of its competence. The staff should also be familiar with innovation processes and tools. It is especially important in a dispatcher work, for operators and supervisors.

Security policies and operating standards and procedures that clearly define rules and task for all employees and visitors should be strictly obeyed. Most of big power plants use several security perimeters such as the fence, control house building, alarm systems etc. Access to power plants is limited to employees, contractors, and visitors with entity-issued identification badges. Access into and out of critical assets is possible with controlled authorization procedures through measures such as keying systems, access card systems, CCTV etc. Nuclear power plants use more strict and complex security systems which require physical support and specific security measures. Small renewable power plants are equipped with security elements such as perimeter alarm system, security guard, monitoring etc., but some of them are unattended.

Substation that can be located in urban, rural, and industrial/commercial areas, usually have several physical security perimeters such as a fence, a control house building, security guard, alarm systems, a CCTV, motion detectors etc. Access to these critical substations should be limited and monitored, including authorization procedures. In case of overhead lines or underground cables transmitting electric power there exist a variety of systems such as SCADA/EMS to protect them from disruption and to limit losses.

The SCADA/EMS systems are also used for protection of control centers. Some of the control centers are collocated, but the tendency is to locate them in separate buildings of solid construction with and several access barriers such as an electronic entry system, entry card systems, locked doors with keyed entry, alarming, CCTV etc. and with controlled authorization procedures. A coordinated attack on selected control centers could result in long-term outages. To minimise this risk necessary are redundancies of physical equipment of control centers and communication networks in different configurations, which provide greater reliability, availability and quality to the highest possible level.

Redundancy is necessary not only in case of malicious attacks. Increased complexity of electric systems used for power transmission or distribution could lead to common failures, human errors during engineering, installation, modification, or maintenance and testing, therefore redundancy in such developed protection system gives additional possibility of reducing the consequences of failures. Also use of simulation models, threat scenarios, and system models to deal with the multiplicity of challenges helps to achieve expected level of preparation for potential physical attack or system failure.

Audit protocol

Security of energy control centers are being investigated in the EU project Octavio (Energy System Control Centers Security, an EU Approach). The objective of the projects is to improve the security of energy control centers based on establishing criteria and methodology to assess, audit and mitigate risks for electrical control centers and their interdependent ICT infrastructures. The project focuses on:

- provisioning of an accurate assessment regarding energy control centers cyber structure requirement
- defining security audit protocols for different control center levels
- testing audit protocols in at least three different functionality levels
- promoting collaboration schemes among energy and ICT network operators and authorities
- dissemination of results among EU security and energy communities.

Table1

An example of security audit protocol

Facility:		Identification:		Date:		
No (Code)	Entity	Activity	Security threat	Security concept	According to Octavio´s recommendations (Yes/No)	Comment
1 (3.4.1.1)	SCADA LAN	Authentication policy – password management	Passwords are not properly assigned, network compromised.	Passwords should be assigned to individual users, not to devices i.e. the same for all users.		
2 (3.4.1.2)	SCADA LAN	Authentication and access policies – password management	Passwords are used for too long time, network compromised.	Passwords should be regularly changed. The number of failed access attempts should be limited		

To achieve the above goals, security of energy control centers was reviewed for two types of energy infrastructures – electricity and gas. As a result, vulnerabilities of the systems and possible attacks caused by the vulnerabilities were identified. Following it, two sets of security requirements, one for each of the infrastructure type, mitigating possible attacks were proposed. The requirements were collected and grouped according to the entity to which they relate, e.g. SCADA LAN, DMZ, substation, etc. After testing it in cooperation with security experts ICS systems, the requirements will form a kind of a protocol that can be used for auditing security of energy control systems. The example of the protocol referring to authentication of users accessing SCADA LAN devices is presented in Table1. The code in the first row is related to the section of accompanied document in which the vulnerabilities and mitigation methods are discussed.

Conclusions

IT system controlling energy networks is, as any other IT system, as strong as it weakest point. Therefore security mechanisms should be built into the whole system from the very start of the system and should be monitored throughout the life of it. In this case security means not only encryption, authentication and strict access control, monitoring and audit of the infrastructure, prevention of denial of service, but also relates to security policies that supplement and enforce the security mechanisms.

While the security of energy control system is slowly improving, it has to be remembered that IT security alone is not enough. The whole power system should be designed fault tolerant and resilient. There is always probability of electronic attack to succeed, or even unintentional error can crash some part of the IT system. It is equally important to design the system in the way that restricts to local ones the potential consequences of an attack and have strict mitigation and recovery plans. Fortunately, even if security level of control system is still not sufficient enough, the performance and reliability of energy control systems is quite strong. Even if resilience and performance may be reduced, a well designed power system stays up even, if some control centers are destroyed.

This paper is based on the work carried out in the EU project Octavio (Energy System Control Centers Security, an EU Approach). The partners of the project are: Deloitte, S.L. (the project coordinator), AD Consulting, Naturgas Energía, S.A. from Spain, Center for European Security Strategies (Germany), Instytut Energetyki (Poland) and Technical Research Centre of Finland. The authors want to thank the project members for feedback and valuable discussions.

REFERENCES

[1] ISA SP99.: Integrating Electronic Security into the Manufacturing and control Systems Environment, Instrumentation, Systems, and Automation Society, ISA-TR99.00.02-2004, April 2004

[2] Oman P., Schweitzer E., and Frincke D.: Concerns about intrusions into remotely accessible substation controllers and SCADA systems, Schweitzer Eng. Labs, http://www.selinc.com/techpprs/6111.pdf, 2000

[3] Holstein D., Tengdin J., Wack J., Butler R., Draelos T., Blomgren P.: Cyber Security for Utility Operations, www.sandia.gov/scada/documents.htm, 2005

Octavio

This project has been supported by EUROPEAN COMMISSION, DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY (PREVENTION, PREPAREDNESS AND CENSEQUENCE MANAGEMENT OF TERRORISM AND OTHER SECURITY-RELATED RISKS Programme)

Octavio: Energy System Control Centers Security, an EU Approach