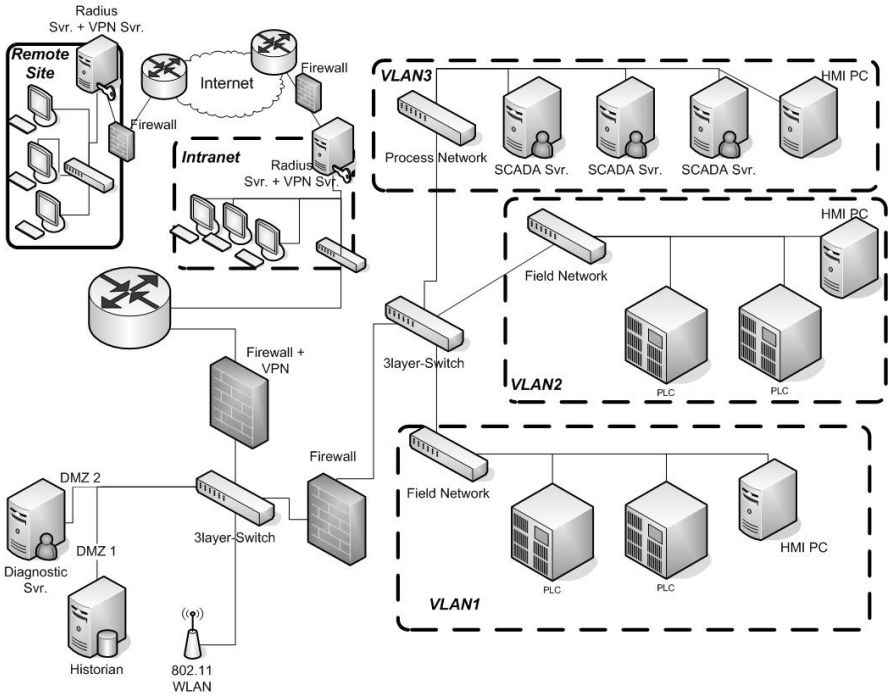
JRC Scientific and Technical Reports

ICT aspects of power systems and their security

Final Deliverable
Administrative Arrangement TREN/08/EC/S07.95052 CEIP

Marcelo Masera, Igor Nai Fovino, Bogdan Vamanu



EUR 24721 EN - 2011

JRC
EUROPEAN COMMISSION

ipsc
Institute for the Protection and Security of the Citizen

The mission of the JRC-IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: TP 210
E-mail: marcelo.masera@ec.europa.eu
Tel.: +39 0332 78 9238
Fax: +39 0332 78 9576

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC 63260

EUR 24721 EN
ISBN 978-92-79-19282-1
ISSN 1018-5593
doi:10.2788/46277

Luxembourg: Publications Office of the European Union

Printed in Italy

ICT aspects of power systems and their security

Final Deliverable

Administrative Arrangement TREN/08/EC/S07.95052 CEIP

Marcelo Masera, Igor Nai Fovino, Bogdan Vamanu

Action "Security of Critical Networked Infrastructures"
Unit "Security Technology Assessment"
Institute for the Protection and Security of the Citizen,
Joint Research Centre

15 November 2010

JRC EUROPEAN COMMISSION

ipsc Institute for the Protection and Security of the Citizen

Table of Contents

1 Introduction

This report provides a deep description of four complex Attack Scenarios that have as final goal to produce damage to the Electric Power Transmission System. The details about protocols used, vulnerabilities, devices etc. have been for obvious reasons hidden, and the ones presented have to be understood as mere (even if realistic) simplified versions of possible power systems.

In the last decade, with the use of computer and telecommunication technologies, power systems have begun to get connected to private and public networks. This evolution was possible due to the ready and affordable availability of off-the-shelves appliances and technologies. These communication solutions were adopted for the many advantages that they could provide to the operators, including easy access to all data produced in the installations. These data facilitates the different technical activities, and furthermore helped companies in the interactions with other operators and actors in liberalised markets. The unbundling of the power sector required the close interaction among industrial stakeholders, and among them and the different authorities and regulators.

Europe has seen the Interconnection of the national and regional power systems, offering an important number of benefits, such as sharing the reserves both for a normal operation and emergency conditions, dividing of the responsibility for the frequency regulation among all generators and a possibility to generate the power in the economically most attractive areas, thus providing a good basis for the power trade. Although this has reduced some negative features, on the other hand it has also introduced new problems – such as the potential for spreading of disturbances over large distances and thus paralyzing vast geographical areas etc. The application of information and communication technologies (ICT) has made possible these interconnections.

But the use of communication and networking technologies has another significant consequence: opening possibilities to security vulnerabilities and threats. Although access to data is extremely valuable, ICT normally used in electric power systems in the years 2000s are not secure: they were developed without security considerations, as it was not a significant requirement in the previous 30 years.

In the last months, the detection of the malware Stuxnet [76] has demonstrated how the security of control systems is at stake. The malware, probably produced by the cyber-army of one country for the resources and sophistication of the effort, is the first publicly-known malicious software program written specifically to exploit vulnerabilities in a SCADA system.

Security vulnerabilities can be exploited for disrupting the power grid operations, or for stealing commercially sensitive information. In addition, no system is 100% secure, and any connection or use of ICT implies security concerns [74]. Applications of computer and networking-based systems in power systems should be considered critical: their manipulation by antagonist malicious actors can cause great damage. Cyber attacks can result in frequency instability, voltage instability, angular instability, and other perturbations, which eventually could produce the closure of power systems and eventually provoke blackouts.

The reliability of the cyber layer is strictly related to its structure both in terms of architecture, protocols for data interchange and on the procedure for the backup and verification of data. Due to the increasing use of networking technologies, both for interlinking the field equipment with the control centers and the control centers among themselves, but also for interconnecting the different actors in the power system, the cyber layer is more vulnerable. On the one hand the cyber functions are more complex while still using in may cases off-the-shelf technologies, on the other hand they are exposed to malicious actors (insiders such as disgruntled employees, and external with different types of antagonists).

The reduction of the level of vulnerability is strictly related to the implementation of protective strategies (selectivity in case of the failure of components, coordination between devices in case of large scale events, coordination among protective and regulation systems…). However, cyber vulnerabilities will not disappear. ICT will be employed by power systems in an increasing manner, as they are essential for their efficient control and operation. The vulnerabilities and potential threats described here should be considered as an indication of the problems ahead, and the effort required for ensuring the resilience of power systems with respect to them.

The disruption of core business operations is the dominant security issue for electric power companies. Government and consumer pressure to keep electric systems operational have

forced the industry to invest in methods to maximize the reliability and availability of power. The expansion of remote access SCADA systems, the rise of on-line business, and the rapid integration of legacy systems have significantly increased the number of potential system exploits. At the same time, the potential cost of a security breach is proportionally growing. Some of the ways in which a security breach might negatively impact a power company are:

- Operational Disruptions
    - What is at risk is the reliability and availability of electricity throughout the power grid. An interference with the control systems can directly affect the operation of the system.
- Public Confidence
    - Competition has brought about an increased focus on customer service; thus, data about customer usage habits, payment, and demographics are crucial to utilities. Disruptions can severely affect those links.
- Corporate Reputation
    - Big and repetitive failures can greatly and immediately have a negative impact on the reputation of a company, with clear financial impact. Furthermore, these disruptions can affect the links with authorities and regulators.

With the current developments towards more effective and efficient power grids, including the planning of smart grids and super grids, the role and significance of ICT has further increased. The scenarios presented in this report can be applied to e.g. smart grid architectures. Nevertheless, it should be taken into account that more, and more complicated, scenarios could be elaborated in that context. Smart grids are more complex power grids with an intense use of ITC and many interacting stakeholders.

Many technologies and standards currently used in the power and ICT sectors will have to be adapted for assuring the security of smart grids [75]. This will have to be accompanies by an important scientific and technological effort.

2 The Electric power network framework

2.1 The power system

In power systems the physical layer is represented by the network hardware such as stations, lines, transformers and circuit breakers. The operation of the power system is managed at the highest level by a decision making layer characterized both by the implementation of automatic control actions and by human decisions. In between there is the cyber layer which is the natural interface connecting the other two layers, making possible the bidirectional communication among the physical and decision making layer (data field to the decision making and control actions to the physical)

A physical layer constituted by the bulk transmission system with all the related devices characterizes power systems. This physical layer acts as the support for the electricity transfer from the production sites to the final users. The transmission system needs to be operated in such a way to be kept feasible though proper control strategies, both human driven and automatic, that are transferred to the physical systems through ICT control and communication centers and devices (cyber layer of the system). In this section we will introduce the basic ideas about the physical layer and its operation needs while the following one will discuss the cyber layer.

In the physical layer, the network buses may differ greatly with respect to the role, the physical behaviour and the ownership. Roughly speaking we can differentiate the buses into for different types:

- *Transmission Stations (TS)*: are buses of the transmission network owned and operated directly by the Transmission System Operator (TSO) under its own responsibility.

- *Power Plants (PP*): are generation power plant in which energy is transformed from whichever form into electricity. They belong to various competing generation companies. Each company may posses various power plants connected to different

buses of the net.

- *Distribution Systems feeders (DS):* are buses, equipped with transformers, in which a Medium voltage distribution system is originated. Each Distribution System Operator (DSO) owns and operates as a monopolist the distribution system over a certain portion of territory, allowing all retailers to use the distribution net on an un-discriminatory basis. The same distribution company may have multiple feeding buses on the transmission network.

- *Large Utilizer (LU);* are buses to which are directly connected the utilizers that demand high power (> 5 MW)

The Remote Terminal Unit (RTU) represents the interface between the network buses in the physical layer, and the cyber layers. The RTU is basically a device equipped with a microprocessor and set of digital and analog input/output channels. Some buses are connected on a "one to one basis" to a dedicated RTU while several others can be grouped under the same RTU resorting to a gateway that simply concentrates the information from many buses in the same location, making them available for a RTU.

TS and LU buses are characterized by a dedicated RTU, while PP and DS buses are grouped, usually for generators and feeders belonging to the same company, below the same RTU connected (a single PP can manage information of power plants for almost 1000 MW). PP can also have, as well, a dedicated RTU in 2 different situations: a company owner of a single PP; power plants of some hundreds MW production, that require a big number of information (remote measurements, telesignals, alarms, level for load-frequency-control, level for automatic-voltage-regulation, …).

RTUs need to have a bilateral communications with the control centers through appropriate communication channels that can exploit various physical media (parallel-resonant circuit on power line, cupper telephone circuit, optic fibre, radio wave, and satellite communications). The communication networks involved in power systems operation and control are mainly:

- Normally TSOs have a dedicated network (TSON). TSON is a data network owned and operated directly by the TSO (for instance based on international standard

protocols, such as IEC 60870-5-104. The TSONs are telecom networks with some thousand points of data acquisition in the bigger European countries.

- Public Transmission Networks (PTN), the general purpose networks, owned and operated by Telecom Companies, can be (and are used in several European countries) used for data also from power systems.

The architecture of the control system of the transmission network is based on a clear separation between the function of command and the function of monitoring (/managing); the first one is attributed to the Switching Centers (SC) that are in charge of changing the configuration of the network acting on its devices (circuit breakers or disconnectors) and of assuring the safety of people working on HV lines/substations; the second function is attributed to Regional Control Centres (RCC) that supervise the network status and provide directions to the operator in the SC to act on the network devices. On the top of all that there is a unique National control centre (NCC) that guarantees the security of supply (e.g. N-1 security) for the national electric system and pursues the economical optimization of the operation, managing the ancillary services according to the “merit order”.

A significant quantity of information is exchanged between grid control centers and substations (TS, PP, DS, LU) and between control centers of neighbouring TSO. The information can be classified according to various criteria (time, networks…). The information directly managed by control and switching centers is called real-time information, which can be internal (national) or external (from neighbours area); the category of the non-real-time information concerns a considerable group of technical and administrative data, the most important of which are commercial information.

Each electrical infrastructure must integrate in the control processes both real-time and not-real-time information not only from the TSO but also from all the actors connected to the network (power plants, HV distribution substations and industrial consumers stations). “Real-time data collection” is a collection of data describing a current situation, which can be done periodically, on request or after a change of status or value, in order to support the TSOs in monitoring, coordinating and operating the transmission system. Operational security is assured by data and information interchange between substations, Control centers of the TSOs, Switching centers and automatic control systems.

In the ENTSO-E context, the TSOs' technical and operational data required for operation, planning and analysis of the interconnected transmission grid need to be handled under general rules concerning data confidentiality, acquisition, coordination and usage, the back-up procedures, intellectual property and hardship. All parties involved need to comply with the same rights and obligations to support ENTSOE's internal tasks and external communication policy.

The non-real-time information concerns the commercial transactions over the grid. The measurement systems are connected to various points of the grid itself with different purposes. The most important points are:

- Energy input points on the grid where power plants from generation companies are connected
- Energy withdrawal points and interconnection points of the distribution companies with the grid
- Interconnection points of with other countries.

The metering activity concerns are mainly focused on the bidirectional record of the flows over the previous points.

In a smart grid scenario, ICT in general, and networking and telecommunications in particular will be more extensively employed. Cybersecurity for smart grids will not only have to cover the basic functions for corporate networks and industrial automation, but also all the business functions among business stakeholders and end users. Specific issues that will have to be considered in addition to the ones described before are:

- Management of the smart grid market: including the interactions between the industrial actors, brokers, and the wholesale market and market clearinghouse;
- Links between industrial actors and end users: including meters, billing energy services interface, aggregators of retail energy providers and energy service providers;
- Actions at the customers' premises: such as management of appliances, electric vehicles, other related services (gas/water metering), etc.;
- Links among the power sector industrial actors.

This shows the long list of systems that will have to be protected and the different security

scenarios that will have to be properly assessed. A key point is the multiplicity of actors, each one autonomous in its own decisions. Therefore the interfaces among all of them acquire a strategic importance from the security viewpoint. These interfaces are technical (e.g. between control systems and communications equipment, between appliances and networks), and organisational (e.g. between industrial and market agents, and between them and end users). All these elements contribute to the security of the overall system.

2.2 Power Systems and Physical Threats

All the components of the power infrastructure can be subject to physical threats. At the same time, those components are also interconnected through communication networks (wired and wireless), which can be the objective of physical threats.

Accidental physical threats can be caused by natural events. Historically this is the most significant cause of outages. On the other hand, utilities know how to manage these situations based on their long experience. Power facilities are generally designed to minimize the impact and to promptly recover the service. Operational procedures are in place for quickly responding to storms and other natural disasters, and the responses are exercised periodically.

Deliberate physical attacks can cause serious damage to transmission lines, due to their fragility and to the impossibility to protect their whole extension. Transformers and communication towers are also very sensitive to physical attacks, but they are normally adequately protected. Of particular importance is the possibility to orchestrate multiple attacks to different components of the infrastructure. Due to the large geographical extent of such systems and to the fact that many constitutive elements are located in remote, isolated areas, multiple coordinated ‘easy to implement’ attacks may lead to great damage to the system as a whole. Well known are the activities of some terrorists groups against power infrastructures (e.g. ETA in Spain, groups in Colombia and the Philippines).

Accidental physical threats that can affect electric power infrastructures are:

- Hurricanes
- Tornadoes
- Wind (beyond design specifications)
- Earthquakes
- Snow/ice (beyond design specifications)
- Floods

- Static Electricity
- Extreme Temperatures
- Lightning
- Avalanches/slides
- Volcanoes eruptions
- Fires

Man-made physical threats can be: deliberate (fire, explosions, radio frequency interference), or accidental (spills, fire, erroneous mechanical/electrical malfunction, etc.).

2.3 Industrial Control Systems and Cyber Threats

A generic diagram of the components within a typical industrial control system is shown in Figure 1 [1].

Measurement variables are transmitted to the controller from the process sensors. The controller interprets the sensor signals and generates corresponding control signals that are transmitted to the process actuators. Process changes result in new sensor signals, identifying the state of the process, to again be transmitted to the controller. The Human Machine Interface (HMI) allows a control engineer or operator to configure set points, control algorithms and parameters to the controller. The HMI also provides displays of status information, including alarms and other means of notifying the operator of malfunctions. Diagnostic and maintenance tools, which are often made available via modem and Internet enabled interfaces, allow control engineers, operators and vendors to monitor and change controller, actuator, and sensor properties from remote locations [2].

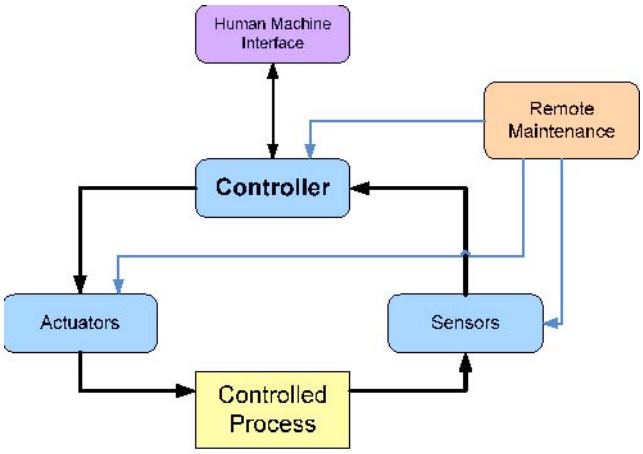


Fig. 1 – Generic Industrial Control System

2.3.1 Industrial Control Systems vs. ICT Systems

In the last decade, some aspects concerning the security of industrial control systems have come to light revealing some differences with the security approach commonly adopted in traditional ICT systems and networks. These differences have been identified and described by the ISA99 Committee [3] in its Technical Reports. There it is stated that the security plans for industrial production and control systems can in fact be developed on the basis of the experiences, plans and practices adopted in ICT systems. However, there are some critical differences from the operative point of view between the two systems that have a strong influence in the adoption of the required security countermeasures.

The differences can be summarized as follows:

- *Risks and consequences*. In ICT systems, the loss of files or documents can have an economical impact on the finances of the company. In an industrial system, the loss of data can have an impact on people security or on the integrity of installations or the environment where the plants are located, paving the way for other threats to the whole infrastructure.
- *Network Architecture*. In ICT systems the typical architecture is client-server and the critical data are stored only on the server-side, limiting the elements to protect. In an industrial system, there isn't a clear distinction between clients and servers, as the peripheral elements of the networks are both data source and receivers of commands from the other elements.
- *Availability*. ICT systems mainly work during office hours and ICT managers can schedule system maintenance and system reboots without affecting normal operations. Industrial systems must be continuously in operation and it is normally possible to perform maintenance on the system without stopping production lines.
- *Response Time*. Real-time applications are rarely used in ICT systems, thus the network performance is affected only by the total bandwidth and throughput on the physical links. On the contrary, industrial applications don't generate too much traffic on the network, but they require strict performance in terms of delay and jitter. In addition, during an emergency, the operators must response very quickly and often there is no time to perform strong authentication on the system.
- *Software*. ICT systems employ well-known operating systems and software packages running on general purpose hardware, thus their vulnerabilities are rather well known, and keeping the systems updated is a routine function. Industrial systems are normally based on proprietary software packages installed on dedicated hardware, and only the

manufacturers know how the system works. So, although it is possible to discover some system vulnerabilities, it is very hard to find a way to correct them. Typically, once a system is successfully installed and stable, it is never updated for fear to introduce instability and not guarantee the required level of reliability. In addition, it should be taken into account that there is a trend towards the adoption of typical ICT systems and network components (such as operating systems, protocols, etc.). This will result in the paradox of better knowing the vulnerabilities, while at the same time being more exposed to typical ICT threats.

3 ICT Threats and Vulnerabilities

Today's economy has become fully dependent upon ICT and the information infrastructure. A network of networks directly supports the operation of all sectors – energy (electric power, oil and gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, defence industrial base, food, agriculture, and postal and shipping. The reach of these computer networks exceeds the bounds of cyberspace. They also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars.

3.1 Threats

A spectrum of malicious actors can conduct attacks against critical information infrastructures. Of primary concern in this report is the threat of organized cyber attacks capable of causing debilitating disruption to critical infrastructures, economy, or even national security [4]. The required technical sophistication to carry out such an attack is high – and partially explains the lack of a debilitating attack to date. However, there have been instances where attackers have exploited vulnerabilities that may be indicative of more destructive capabilities.

Uncertainties exist as to the intent and full technical capabilities of several observed attacks. Enhanced cyber threat analysis is needed to address long-term trends related to threats and vulnerabilities. What is known is that the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving.

As an example, consider the "NIMDA" ("ADMIN" spelled backwards) attack. Despite the fact that NIMDA did not create a catastrophic disruption to the critical infrastructure, it is a good example of the increased technical sophistication showing up in cyber attacks. It demonstrated that the arsenal of weapons available to organized attackers now contains the capability to learn and adapt to its local environment. NIMDA was an automated cyber attack, a blend of a computer worm and a computer virus. It propagated across the USA with enormous speed and tried several different ways to infect computer systems it invaded until it gained access and destroyed files. It went from nonexistent to nationwide in an hour, lasted

for days, and attacked 86,000 computers.

Speed is also increasing. Consider that two months before NIMDA, a cyber attack called Code Red infected 150,000 computer systems in 14 hours. Because of the increasing sophistication of computer attack tools, an increasing number of actors are capable of launching nationally significant assaults against critical infrastructures. In peacetime they may conduct espionage on Governments, university research centres, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping information systems, identifying key targets, lacing infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems.

Cyber attacks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today, if the goal is to reduce vulnerabilities and deter those with the capabilities and intent to harm critical infrastructures [5].

Cyberspace provides a means for organized attack on infrastructure from a distance. These attacks require only commodity technology, and enable attackers to obfuscate their identities, locations, and paths of entry. Not only does cyberspace provide the ability to exploit weaknesses in critical infrastructures, but it also provides a fulcrum for leveraging physical attacks by allowing the possibility of disrupting communications, hindering defensive or offensive response, or delaying emergency responders who would be essential following a physical attack [6].

3.2 A Five-Level Problem

We present in the following the approach to the management of threats and mitigation of vulnerabilities in cyberspace taken in the U.S. National Strategy to Secure Cyberspace [7]. According to the referenced document, '… managing threat and reducing vulnerability in cyberspace is a particularly complex challenge because of the number and range of different types of users. Cyberspace security requires action on multiple levels and by a diverse group of actors because literally hundreds of millions of devices are interconnected by a network of networks.' A five levels approach is proposed for addressing the issue [7].

3.2.1 Level 1 – Home User/Small Business

‘Though not a part of a critical infrastructure the computers of home users can become part of networks of remotely controlled machines that are then used to attack critical infrastructures.‘ [7] Undefended home and small business computers are vulnerable to attackers who can employ the use of those machines without the owner’s knowledge. Such machines can then be used by third-party actors to launch for instance denial-of-service attacks on key Internet nodes and other important enterprises or critical infrastructures.

3.2.2 Level 2 – Large Enterprises

Large-scale enterprises (corporations, government agencies, and universities) are common targets for cyber attacks. Many such enterprises are part of critical infrastructures. Enterprises require clearly articulated, active information security policies and programs to audit compliance with cyber security best practices. According to the intelligence community, the networks of large enterprise will be increasingly targeted by malicious actors both for the data and the power they possess.

3.2.3 Level 3 – Critical Sectors/Infrastructures

A unified effort of organizations from different sectors (economy, government, academia) targeting the common cyber security problems is required for reducing the burden on individual enterprises. [7] states that ‘…such collaboration often produces shared institutions and mechanisms, which, in turn, could have cyber vulnerabilities whose exploitation could directly affect the operations of member enterprises and the sector as a whole. Enterprises can also reduce cyber risks by participating in groups that develop best practices, evaluate technological offerings, certify products and services, and share information. Several sectors have formed what are called following the USA’s terminology Information Sharing and Analysis Centres (ISACs) to monitor for cyber attacks directed against their respective infrastructures. ISACs are also a vehicle for sharing information about attack trends, vulnerabilities, and best practices.’

3.2.4 Level 4 – National Issues and Vulnerabilities

Some cyber security problems have implications and cannot be solved by individual enterprises or infrastructure sectors alone. All sectors share the Internet. Accordingly, they are all at risk if its mechanisms (e.g., protocols and routers) are not secure. Weaknesses in widely used software and hardware products can also create problems at the national level, requiring coordinated activities for the research and development of improved technologies.

Additionally, the lack of trained and certified cyber security professionals also merits national level concern.

3.2.5 Level 5 – Global

The worldwide web is a planetary information grid of systems. Internationally shared standards enable interoperability among the world's computer systems. This interconnectedness, however, also means that problems on one continent have the potential to affect computers on another. International cooperation is needed to share information related to cyber issues and, further, to prosecute cyber criminals. Without such cooperation, the collective ability to detect, deter, and minimize the effects of cyber-based attacks would be greatly diminished.

3.3 Vulnerabilities

The vulnerabilities of industrial ICT systems are the focus of several initiatives around the world. This is the result of the awareness about the urgency of the matter, and the lack of appropriate tools and means for dealing with the problem. In particular in the USA there have been a number of pioneer actions: the development of laboratories, test beds and test ranges for industrial ICT (e.g. the Idaho National Laboratory, the National SCADA Test Bed Program), the Cybersecurity Industry Alliance, the Chemical Cybersecurity program, etc.

In 2003, Sandia National Laboratories has engaged in vulnerability assessments of ICT systems with the main focus on control and automation systems used in critical infrastructures. The report [8] contains the results of the study, part of them being also provided in the sequel.

Most security vulnerabilities in infrastructure include failures to adequately define security sensitivity for automation system data, identify and protect a security perimeter, build comprehensive security through defence-in-depth, and restrict access to data and services to authenticated users based on operational requirements. Many of these vulnerabilities result from deficient or nonexistent security governance and administration, as well as budgetary pressure and employee attrition in system automation.

Also, the industry is largely unaware of the threat environment and adversary capabilities. Finally, automation administrators themselves cause many security deficiencies, through the widespread deployment of complex modern information technology equipment in control systems without adequate security education and training. Comprehensive mitigation

includes improved security awareness, development of strong and effective security governance, and amelioration of security vulnerabilities through the careful configuration and integration of technology.

The security of control systems depends upon five heterogeneous categories of elements, given in the sequel [8].

3.3.1 System Data

System security oriented towards data focuses on preserving the availability, authenticity, integrity, and confidentiality of data. Preserving these attributes ensures the reliable operation of the overall system.

3.3.2 Security Administration

Report [8] states that 'The administration constituent of a control system encompasses such non-automation functions as documentation and procedure. The cardinal element of documentation is the system security policy, which prescribes the goals and responsibilities for security.' The security policy is the origin for every other required administrative component, which subsequently prescribes procedures for system implementation, operation, and maintenance. Table 1 shows a list of common vulnerabilities related to security administration [8].

3.3.3 Architecture

The architecture of control systems refers to its control and data storage hierarchy. The architecture for the distribution of automation functionality is critical to reliability of the functional whole. At one extreme, the totally centralized authority for automation means that remote stations function as little more than boundaries for analog and digital control and measurement signals; this is the decades-old traditional model. At the other extreme, a completely decentralized authority resembles the agent model, where operations depend on the emergent behaviour of smaller entities with limited capabilities and viewpoints.

Category	**Vulnerability**
Policy	The control system has no specific documented security policy. This key vulnerability generates the proliferation of procedural and technical vulnerabilities
	The control system often has no specific or documented security plan
Procedures	Implementation guides for equipment and systems are usually absent or deficient

	There are no administrative mechanisms for security enforcement in the system lifecycle
	Security audits are rarely performed, if at all
Training	There is neither formal security training nor official documented security procedures
Configuration Management	Usually, there is no formal configuration management and no officially documented procedures. Hence, there are neither formal requirements, nor a consistent approach for configuration

Table 1 Common vulnerabilities related to control system administration [8]

Category	**Vulnerability**
Administration	Minimal data flow control is employed (e.g. minimal use of access control lists, virtual private networks, or virtual LANs)
	Configurations are not stored or backed up for network devices
	Passwords are not encrypted in transit
	Passwords exist indefinitely on network devices
	Passwords on devices are shared
	Minimal administrative access controls are applied
Hardware	There is inadequate physical protection of network equipment
	Non-critical personnel have physical access to equipment
	No security perimeter has been defined for the system that defines access points which must be secured
Perimeter	Firewalls are nonexistent or poorly configured at interfaces to external networks (that is, not related to control system)
	Control system networks are used for other kind of traffic
Monitoring & Logging	Firewall and router logs are neither collected nor examined
	There is no security monitoring on the control system network
Link Security	Critical monitoring and control paths are unidentified, complicating redundancy or contingency plans
	Control system connections over vulnerable links are not protected with encryption
Remote Access	Authentication for remote access is substandard or nonexistent
	Remote access into the control system network utilizes shared password and shared accounts
Wireless Connections	Wireless LAN technology used in control system network without strong authentication and/or data protection between clients and access points

Table 2 – Common vulnerabilities for control system networks [8]

3.3.4 Network

Control systems networks include all data transmission elements owned and administered by the infrastructure utility. Networking devices include lower-level end communications equipment (modems), advanced networking devices (routers, firewalls, etc.), and the link equipment itself (cables, rights-of-way, microwave dishes, etc.). Network functionality includes the capability of the network to deliver SCADA messages securely and reliably to support system operation. Table 2 shows a list of common vulnerabilities related to control system networks.

3.3.5 Platforms

SANDIA considers “Platforms” as encapsulating both the computing hardware (inclusive of specific industrial platforms) and software (like applications and operating systems) in control systems.

Table 3 shows a list of common vulnerabilities related to software and hardware platforms utilized in control system networks.

Category	**Vulnerability**
Software	Operating system security patches are not maintained
	Configurations are not stored or backed up for important platforms, including intelligent electronic devices (IEDs)
	Default operating system configurations are utilized, which enables insecure and unnecessary services
	Passwords are often stored in plain sight near critical systems
Administration	Power-on and screen saver passwords are not utilized
	Passwords are not encrypted in transit
	Passwords exist indefinitely on platforms
	Passwords on devices are shared
	There are no time limit, character length, or character type requirements for the passwords
	Minimal administrative access controls are applied
	Users have administrator privileges
	There is inadequate physical protection of critical platforms
Hardware	Non-critical personnel have physical access to equipment
	Dial-up access exists on individual workstation within the SCADA network
Monitoring & Logging	System logs are neither collected nor examined
Malware Protection	Virus checking software in uninstalled, unused, or not updated

Table 3 – Common vulnerabilities related to software and hardware platforms [8]

4 POWER SYSTEM CYBER THREATS

While on the one hand the massive use of use of ICT technologies has made possible a strong integration among the different elements of Power Systems (power plants, substations, transmission grids, business operations, etc.), on the other hand the new interconnections, layers, and communication links have introduced a not negligible set of new threats. Some of them, as showed for example in [78] [79], are directly inherited from the traditional ICT world (e.g. generic purpose worms, vulnerabilities of general purpose operating systems etc.) Others are peculiar of the Process Systems controlling power systems. The ICT security of control systems is an open and evolving research field.

Creery and Byres [80] presented an interesting high-level analysis of the possible threats to a power plant system, a categorization of the typical hardware devices involved, and some high level discussion about the intrinsic vulnerabilities of common power plant architectures. A Taxonomic approach toward the classification of attacks against energy control systems can be found for example in [82]. A more detailed work on the topic of SCADA security (Supervisory Control and Data Acquisition systems are the core of every industrial installation), is presented by Chandia, Gonzalez, Kilpatrick, Papa and Shenoi [81].

From a purely technical point of view, it is possible to claim that the cyber vulnerabilities affecting Power Systems can be classified as in the traditional ICT world:

- *Software Vulnerabilities*: vulnerabilities due to errors in the implementations of software applications (e.g. buffer overflows etc.);
- *Architectural Vulnerabilities*: vulnerabilities due to weaknesses in the architectural design of the ICT infrastructure;
- *Protocol Design Vulnerabilities*: vulnerabilities due to weaknesses in the design of the communication protocols;
- *Policy Vulnerabilities*: vulnerabilities due to a weak design or a weak implementation of security policies.

The severity of these classes of vulnerabilities (and of the related attacks) is strongly linked with the subsystem they affect. In what follows we provide a description of the main ICT

weaknesses of power systems, using as discriminator the subsystems affected. As a result, the vulnerabilities and attack scenarios presented will be grouped according to the following classes:

- SCADA system weaknesses
- Process Network weaknesses
- Control Centre weaknesses
- Network Layer weaknesses

The presented scenarios are generic enough to find application in almost all modern power system architectures.

4.1 SCADA protocol weaknesses

SCADA protocols (DNP3, Modbus, Profibus, OPC, IEC 60870-5/6 etc.) are used by field RTUs and PLCs to remotely exchange data and commands with the supervisory system. They constitute the backbone of every industrial system; in particular, the control flows in power systems embedded in the SCADA protocol flows connect the physical components in the field with the overall operational logic of the installation.

SCADA protocols were originally conceived to be used in serial communications and only later they were ported over TCP/IP and subsequently wireless communication. The porting of SCADA protocols over TCP/IP has obviously introduced new layers of complexity required for reliably managing the delivery of control packets in an environment with strong real-time constraints. In addition, it has opened new possibilities to attackers motivated to cause damage to target industrial systems. However, in this section the focus is not in investigating the vulnerabilities of the communication protocols used to transport the SCADA protocols (see for a discussion of network vulnerabilities section 4.4). We concentrate here our attention on the design weaknesses of the SCADA protocols. In particular, those protocols in their original formulation:

- Do not apply any mechanism for checking the integrity of the command packets sent by a Master to a Slave and vice-versa.
- Do not perform any authentication mechanism between Master and Slaves, i.e. every item could claim to be the Master and send commands to the Slaves.
- Do not apply any anti-repudiation or anti-replay mechanisms.

These security shortcomings can be used by malicious users for attempting to carry out different kinds of attacks:

- *Unauthorized Command Execution*: The lack of authentication between Master and Slave can be used by attackers to forge packets and send them directly to a pool of slaves.
- *SCADA-DOS*: On the basis of the same principle, an attacker can attempt to produce a Denial-of-Service by forging and sending meaningless SCADA packets, always impersonating the Master, and consume the resources of the RTU.
- *Man-in-the-Middle attacks*: The lack of integrity checks allows attackers to access the production network for implementing typical Man-in-the-Middle (MITM) attacks, modifying the legal packets sent by the master.
- *Replay Attacks*: The lack of anti-replying mechanisms allows attackers to re-use captured legitimate SCADA packets.

Finally, in addition to those classes of attacks, since anti-repudiation mechanisms are not implemented, it is hard to proof the trustworthiness of malicious Masters, which could have been compromised. In depth discussions on these vulnerabilities can be found in [83] [84] [85].

The impact of the successful exploitation of these weaknesses is immediately apparent: constituting the final, operational part of the entire regulation and control process, any malicious action can directly affect the industrial operation, with cascading effects on the citizens and on the companies owning the power system.

The existence of common vulnerabilities in different components of the power grid can be the cause of extremely dangerous events. In additions, it shows how the protection of the grid should incorporate security mechanisms in the communications network. In a power grid scenario, it will be normal to find the same software and hardware components repeatedly used in many systems. One recurring vulnerability will be exploitable by applying the same mechanism over and over again. This example shows how there is going to be the need for governance mechanisms for the patching and handling of vulnerabilities, linking vendors and users of technologies.

The recent detection of the Stuxnet worm, confirmed what presented in this section. This worm represents the first known example of malware ad-hoc developed for targeting SCADA systems: after infecting SCADA masters of a particular brand and model, it is in fact able to directly interact with the field devices (PLCs) to the point to be able to modify their internal

logic. More details on Stuxnet can be found for example in [76] [86].

4.2 SCADA protocol possible attacks

On this basis, the following are possible attack scenarios related to SCADA protocols.

- **SCADA Malware DoS scenario**: The goal of DoS attacks is to desynchronize (and, when possible, completely disrupt) the communication between Master and Slaves. In light of what presented before, for impairing the control communication stream it would be sufficient to inject a huge amount of SCADA packets against the Master or the set of slaves of the control system. A generic packet generator could be normally identified by Network Intrusion Detection Sensors, or by the anomaly detection engine of firewalls. Ideally, if the packet generator recreates the same traffic shape of some legitimate SCADA protocol traffic, it can circumvent the monitoring systems and interrupt the communication between Master and Slaves.

  In the following some infection triggers are listed:

  - Email-infection: the attacker, after gathering information about the hierarchical organization of the ICT security team in an organization, and about the process operators, forges an e-mail identical to the one usually sent for updating purposes (identical not only in the content, but also in terms of its format), with attached malware instead of a normal patch. In that e-mail, the attacker asks the operator to install the attached patch on a target Master, or on a PC in the same network. Once installed, the malware will start delivering massive amounts of well-formed SCADA packets to the slave, until the Master and the Slave are desynchronized.
  - Through Phishing Infection: Phishing attacks are typically mounted in one of the following ways: a) by means of a faked e-mail, displaying a link which seems to point to a legitimate site, but actually linking to a malicious website; or, b) by poisoning the victim's DNS server, thus making it possible to transparently connect to the malicious server. Usually the scope of these attacks is to steal the user credentials. The scenario can be slightly modified: the fake web server can contain a set of malicious scripts that activate the download and execution of the malware on the local machine from which the web page is accessed. The scenario develops as follows:

    1. By social engineering through a fake e-mail, or by poisoning the DNS of the process network, an operator is forced to visit an ad-hoc created web site

2. A set of scripts on the web-site, using some well known vulnerabilities of web browsers, download and execute of the operator PC the SCADA malware.
3. The legitimate SCADA traffic is interrupted.

- **SCADA DOS Worm**: the attacker creates a new worm that exploits some known software vulnerability or some zero-day vulnerability. This new worm carries in its payload the code of the SCADA DOS malware. In this way, every time the worm infects a new machine:

  1. It starts to spread itself by using the new host resources.
  2. It executes the SCADA DOS code.

  Below, the step-by-step infection evolution:

  1. From Internet the worm infects the PCs in the company Intranet
  2. If one of the infected PCs in the company Intranet is authorized to access one of the networks hosting the SCADA Servers or hosting any of the control devices, the worm spread itself through such networks.
  3. If the worm discovers SCADA Slaves in the network, it starts to send SCADA packets in order to desynchronize or completely interrupt the Master/slave Command Flow.

- **SCADA Unauthorized command execution scenario**: As SCADA protocols do not provide any security mechanism in order to protect the connections and the data flows, when a master sends a packet containing a command to a slave, this one simply executes it without performing any check on the identity of the master and on the integrity of the packet received. With the porting of SCADA protocols over TCP, this approach has obviously showed all its limits from the security point of view. In fact, since the slave can neither verify the identity of the sender of the commands to be executed nor its integrity, any attacker able to forge ad-hoc packets and having access to the network segment which hosts the slaves could force them to execute un authorized operations, potentially compromising the integrity or stability of the system. If the system is a critical infrastructure like a power plant, the potential damages could be catastrophic.

  The list of dangerous commands can be divided into two classes:

  - Normal commands: this class comprises all the commands normally used in the communication between Master and Slaves, like “open a valve, close the switch

etc.”; when used in the wrong context, they might cause damages (e.g. the attacker sends a “close valve command” which, due to the particular architecture of the system under attack, will have as result the increase of the pressure in a certain pipe.)

- Maintenance commands: the attacker uses commands designed for maintenance use.

In the following, taking as example the DNP3 SCADA protocol, we provide some examples of licit commands that be used for malicious objectives.

- The command *Reset Link* re-synchronizes the communication between a Master and a PLC. It is useful when a PLC restarts, but if sent during a regular transmission, it could introduce an inconvenient delay in the network.
- In the same way the functions *Reset User Process* and *Request Link Status* require an acknowledgement *ACK* from the PLC, which can easily flood a network if there are too many.
- The function code *Write (0x02)* linked with the object *Current Time (0x50)* allows to control the Master command delivery. By manipulating this function, an attacker can control the time synchronization of the PLC and potentially isolate it from the others.
- The functions code *Freeze and Clear (0x09)* and *Freeze and Clear no Ack (0x10)* store an object in a separate memory, and erase it from the on-time configuration of the PLC. With this command, an attacker forces a PLC, for example, to hide the evolution of the temperature in a power plant.

These examples are applicable to almost all the SCADA protocols such as IEC 60870-5 (which is under several aspects quite similar to DNP3).

Several can be the triggers of these attack scenarios; here we list two of them:

1. Direct access: the attacker is an insider (e.g. disgruntled operator), or in any case an actor that has physical access to the process/control networks. In that case: (a) he inspects the network in search of PLCs/RTUs; (b) he guesses the best sequence of commands to be sent in order to create a certain damage; (c) he writes a software able to send SCADA protocol packets; (d) he sends those packets to the PLCs/RTUs.
2. SCADA virus: As in the previous DOS attack scenarios, the attacker creates a malware able to send commands to the field devices. In that case, the malware, once it has reached the industrial process network will be able to substitute itself for the SCADA

server, and to virtually take the control of the SCADA system. The infection triggers in this case could be the same presented in the case of the DOS worm. Nai et. al. demonstrated the feasibility of this kind of attack in [77].

- **SCADA System data poisoning**: as a direct result of the intrinsic vulnerabilities of the SCADA protocol, attackers having access to the process network can easy impersonate a set of PLCs and provide false information to the SCADA server. The effect of this attack has a significant chain effect. In fact, since the information provided by the PLCs to the Master is aggregated and provided to the operational databases, and then used by the diagnostic systems and by the high level control centers, a similar attack could drive the operators in a completely wrong direction, with potentially catastrophic effects. A possible implementation of that attack scenario could be the following:

  1. The attacker (or the malware written by the attacker), perform a DOS against a set of PLCs in order to block the data flow between them and the SCADA Master.
  2. The attacker (or the malware) impersonates the blocked PLCs
  3. The attacker (or the malware) provides false data to the Master

  As in the previous case, in order to implement such an attack, the attacker needs an access to the process network, which can be physical, or obtained through a malware infection. This attack scenario, as well as the *OPC corruption scenario* presented in the next section, can be easily classified also as s*tate estimation attacks*, in the sense that their aim is to make the upper level control system fail in estimating the correct state of the field system.

- **Coordinated worm based SCADA attack:** This attack scenario is based on the same concepts presented in the previous examples. To make it realistic, although the vulnerabilities related to the different SCADA protocols are quite similar, we assume in this scenario that the field network uses Modbus. Moreover in this scenario, the attacker wants to hit the power grid simultaneously in different points. In the following we provide the description of the attack:
  1. The attacker collects as much information as possible about the ICT network structure of the power grid he wants to attack. Key information is the set of public IP addresses of the systems that provide the interface between the internal network of each control station and the external corporate network of the transmission system operators. This

information will be used to improve the effectiveness of the attack by better identifying the targets. Nevertheless, the attack would work also without this kind of information.

2. As in the previous scenario, the attacker, after having reverse-engineered Slammer, selects from the obtained code only the infection engine.
3. The attacker builds a new function that forges Modbus packets containing the function code “write discrete output register” (which basically sends a command to a field device like a switch, or a digital instrument). The payload of this function will tell the PLC to write the specified value into all the output discrete registers available.
4. On the basis of the information gathered by the attacker in the previous phase, the value to be written in the register should be the one that, if written on a register that corresponds to a field device that controls the “node connection”, causes its disconnection.
5. The new malicious code will have a delayed activation after the infection of the target machines: it will launch the malicious packets after a certain data, by checking the local clock. This will enable a coordinated attack by all copies of the malware.
6. The attacker merges together the infection engine of Slammer and the new code, obtaining a completely different virus for which there is no signature yet.
7. The attacker creates two versions of the malware: one will target the IP addresses retrieved during the first phase of the attack, and another will use a random address generator. In this way, also systems of which the attacker was unaware will possibly be infected.
8. The attacker releases the two versions of the malware “in the wild” (meaning in the corporate network for a targeted attack against a company – on the condition that the attacker has access to it -, or in the Internet, in a general attack against operators using that technology).
9. The malware will start to spread until reaching a target machine. Every time it reaches a new system, it starts to infect other systems in the neighborhood, and then silently puts itself in a dormant situation.
10. When the pre-defined data occurs, each piece of the malware resident in different machines or systems will wake-up and start to send the malicious Modbus packets against every possible IP address, starting from the ones in the same subnets, then proceeding with the ones in the nearest subnets and so on.
11. In a few minutes, entire lines of the grid will start to be disconnected by the PLCs executing the command received by the malware, and causing a coordinated loss of

power cuts.

4.3 Process Network weaknesses

The process network hosts the SCADA servers, the OPC servers (where used), the Builder servers (used to program the field devices) and the HMI. Compromising this level will enable the attacker to potentially take full control of one (or more) portions of the Power System. In what follows we describe some attack scenarios aiming at causing damages to the industrial installation.

- **OPC DOS**: the OPC servers (where used) act as a bridge between the SCADA server and the Control Network. A denial of service against them has the effect of completely separating the two networks, interrupting then command flow between Master and Slaves. It can be implemented in several ways:
  - Network DOS: the attacker sends a huge amount of meaningless packets to the network cards of the OPC server, which will not be able to deliver in time the SCADA traffic. This scenario can be implemented in different ways: (a) the attacker has direct access to the process network, and is able to run a traffic generator. In order to accelerate the effects, it could use for example a UDP packet generator (as it is easier to generate a huge amount of traffic using UDP instead of TCP); (b) the attacker can use some malware which by infection is able to reach the process network and perform a DOS against the OPC server
  - Application based DOS: in this case the attacker might take advantage of one of the typical vulnerabilities of windows systems in order to take down the server.

- **OPC corruption and poisoning**: the OPC server is typically a MS-Windows machine, with the typical vulnerabilities of that kind of system. An attacker might be able to take advantage of those vulnerabilities and corrupt the OPC server. In that case, it would be able to:
  - Send unauthorized commands to the PLCs;
  - Send false data to the Master (poisoning the data provided to the operators);
  - Interrupt the communication flow between Master and Slaves.

- **OPC protocol corruption**: the OPC communication protocol is far from being completely secure. Authentication and integrity mechanisms exist, but they are not always applied. For that reason an attacker (or a malware) having access to the process network, might be able to directly interfere with the communication channel between the SCADA master and the OPC server. In this way, an attacker can violate the integrity of the packets, modifying the command flow or poison the data flow. In both cases the net effect may be extremely dangerous. An attack scenario in that case might involve a DOS against the OPC server (to stop it from answering to Master requests) and impersonation (the attacker inject fake OPC traffic spoofing the identity of the OPC server). The effects of those attacks can, again involve data falsification and unauthorized command execution.

- **SCADA Server DOS**: A denial of service against the SCADA Master is extremely dangerous. This server controls directly the PLCs and more generally the process driving the industrial installation. If an attacker would be able to block it, the whole industrial system might run into a critical state. Moreover, the information flow between the process network and the higher level of the system (up to the operators and other decision makers) will be interrupted. As in the case of the OPC server, this malicious scenario can be generated either through a classical network DoS (the attacker in that case needs to have direct access to the process network, or needs to use some malware able to reach that network), or by taking advantage of some software vulnerabilities.

- **SCADA server corruption**: the effects of a SCADA server corruption can be extremely negative. If an attacker can take control of this system, he will be able to perform many kinds of malicious operations: (a) unauthorized command execution, (b) data poisoning, (c) system halt, etc. Several studies (see for example “ICT Security Assessment of a Power Plant, a Case Study", Nai, Masera and Leszczyna, Second Annual International Conference on Critical Infrastructure Protection, 2008) showed how computer systems in industrial process networks have usually a low patching speed. This directly implies that the window of opportunity opened by the vulnerability of these systems in relation to new threats is always large enough to permit a well-determined attacker with sufficient resources to take advantage of it. In this scenario, we can assume that one of the installed software in the SCADA server would be vulnerable to one or more attacks (e.g. buffer overflow, format string attacks etc.) allowing the attacker to gain control of the system. The scenario, as usual, is based on the precondition that the attacker has access to the server,

or to the network used by the server.

- **SCADA Server data flow corruption**: the communication protocols used by the SCADA systems are usually not protected via authentication and integrity mechanisms. An attacker might be able to interfere with those data flows (the flows between the SCADA server and the HMI, or with the related databases and other servers). In these cases the possible damages can be caused in the following ways:
  - An attacker can provide false information to the HMI, in order to hide some other malicious operation in act in the control network.
  - An attacker can modify the content of the command flow, making the PLCs to execute unauthorized or dangerous operations.
  - An attacker can modify the content of the data flow between the SCADA server and the databases, poisoning the information flow from the field to the operators and other decision makers.

  The scenario can be easily implemented if the attacker has access to the process network (he can for example perform a DoS against the SCADA Server and then send in its name unauthorized commands or data). In addition, this scenario can be implemented by creating an ad-hoc virus, which, once reached the process network, performs the same kind of operations.

- **HMI corruption**: the HMI provides the local interface to the operator. Its corruption can affect the operability of the system, but the impact would always be limited, since the operators will always be able to directly operate the SCADA server, bypassing in this way the HMI. The kind of attack scenarios against this system are basically the same described for the SCADA server.

4.4 Control Centre Network attacks

The control centre network hosts normal PCs which might act as HMI, in order to enable the operators and the decision makers to access to the industrial installation (i.e. to access to the databases). Those systems are usually also connected, directly or indirectly, to the Internet. This implies that they are easily accessible to attackers. However, these PCs usually have stricter patching and security policies. However, virus infections, or other classical attacks, are always possible. Once an attacker is able to gain control of one of these systems, he will

have to obtain the credential of one of the users authorized to access the remote system. This can be done in different ways (e.g. by using key loggers etc.). If in possession of the authorized credential, the attacker will then be able to perform a large number of malicious operations:

- Injection of malicious software in the remote process network
- Poisoning of the databases
- Infection of the diagnostic systems
- Network DoS against the exchange server switch (to block the traffic coming from the process network)
- Access to the process network
- Injection of malicious SCADA packets into the process network

4.5 Network Layer attacks

Power Systems rely heavily on the underlying ICT network layer. Attacks against switches, routers, and networks might have serious impact on the efficiency and on the control functionalities of the power system. It is possible to classify those attacks in:

1. Network interference/noise: injection of ah-hoc crafted streams of packets aiming at creating noise on the network (e.g. Packet Flooding Attacks, Short Burst DOS and more sophisticated). The level of exposure of the different subnets of the Power System to this threat is quite different. The field networks are usually less exposed (but more susceptible), since they constitute the deeper and farthest from external interferences part of the network. The network devices interconnecting the different subnets are instead the more exposed. The potential effects of attacks depend on the local target: if the field devices are the target, the net effect will be the disconnection of a local portion of the network. On the other hand if the attack takes as target the interconnections between the different subnets, the impact might be more extended.
2. Single implementation vulnerability attacks: they aim at exploiting a vulnerability peculiar of a particular model of network devices, due to implementation errors. Those vulnerabilities usually have as main results: to turn-off / slow down the network device, to modify the network device configuration. Depending on the type of vulnerability exploited, an attacker might be able to re-route packets, crash the network devices, and inject new ad-hoc crafted packets.
3. Protocol Related Vulnerabilities: aiming at taking advantages of some

design/implementation weaknesses of the network protocols used. Power Systems employ other communication protocols, e.g. the TCP/IP suite is widely used. In the following a list of the possible classes of attacks related to TCP/IP is provided:

- TCP SYN attacks
- IP Spoofing
- Routing attacks (Routing Information Protocol (RIP) based)
- ICMP attacks
- DNS attacks

All these classes of attacks can be used as bricks to mount more complex scenarios for carrying out DOS, to inject fake packets, or to re-route the traffic.

As described in Section 3, the communication among different parts of the Power System WAN, when using communication lines provided by third parties (i.e. ISPs) relies on the use of MPLS. The Multi Protocol Label Switching provides a mechanism for routing the network traffic in a more efficient way, providing at the same time segregation functionalities. It is largely used by the ISP providers to guarantee high quality of service to the network traffic of some customers. The devices involved in communications using MPLS can be classified in two classes: the devices that are part of the MPLS Core Architecture, and the devices outside the core. If an attacker has access to devices outside the core, it might be successful in performing the following attacks:

- Rogue Path Switching
- Rogue Destination Switching
- Enumeration of Label Paths
- Enumeration of Targets
- Label Information Base Poisoning

All these attacks can be used in the specific case Power System to interfere with the legitimate control traffic. In particular, the last one can be used to perform an extensive Denial of Service. If an attacker has access to devices inside the MPLS core all the previous scenario remain valid but their impact assumes a higher magnitude. More details about MPLS and its vulnerabilities can be found in [87].

5 Security Risk Assessment

5.1 Analysing cyber threats

Securing computer systems that control industrial production and distribution is vital for the protection of key components of critical infrastructures and the health of the associated economies at risk. Current systems are designed first and foremost to meet performance, reliability, safety and flexibility requirements. Yet, as these systems are steadily integrated with information and communication technology (ICT) solutions to promote more advanced functionalities, corporate connectivity and remote access capabilities, serious new vulnerabilities are being introduced into operational system components [77] [82].

Cyber attacks on industrial production and distribution systems, including electric, oil and gas, water treatment and distribution systems, could endanger public health and safety as well as invoke serious damage to the environment. Attack on any industrial control system could also result in serious financial implications including loss of production, generation or distribution of a product, or compromise of proprietary information and creation of liability issues.

As shown in 2.2.1, real-time computer control systems used in industrial control applications have many characteristics that are different from traditional information processing systems used in business applications. Primary among these is the design for efficiency and time-critical response. Security in these systems is generally not a strong design driver and therefore has tended to be bypassed in favour of performance and control requirements. Furthermore, the goals of safety and security sometimes conflict with the design and operation of control systems [10] [11] [12].

Furthermore, due to the increasing interconnection among systems and organisations, the probability and potential impact of security breaches have grown heavily in recent years. Because of the complexity of the security issues and the rapid pace of change, the decision makers must identify, assess, weigh, and establish priorities for threats and vulnerabilities and to identify and evaluate options for action. In summary, it is necessary to:

1. Understand the threats involved
2. Appreciate vulnerabilities

3. Make timely, coordinated, and effective actions

Of great importance is the assessment of malicious threats, and in particular those deriving from terrorist actors.

Garrick et. all [13] offer a methodology for quantitatively assessing the risks of terrorism to make the right decisions for countering them. The overall framework for action is composed of the following procedures:

- Step 1 Information gathering and processing
- Step 2 Risk assessment
- Step 3 Decision-making and action implementation

5.1.1 Information Gathering and Processing

The prerequisite for risk analysis is to have adequate supporting information. Therefore, it is necessary to gather observations, evidence, proofs, and other relevant data from various sources and convert them into a numerical form suitable for risk assessment (Step 2) and for the subsequent decision analyses (Step 3). The questions addressed in these steps are:

- **Which threats should be considered the most serious based on existing evidence?**
- **What supporting information can be obtained for the analysis of those threats?**

Obviously, these first two steps aim at screening out the less important threats so that resources can be concentrated on the more serious, more credible ones.

5.1.2 Risk Assessment

The most likely malicious attack scenarios, including their potential consequences, should be identified, analyzed, and developed based on the information gathering and processing phase. Risk assessment entails a three-part process:

- **Threat assessment**
  - includes the analysis not only on the intentions and capabilities of the malicious actors, but also of the potential targets and aggressive means delivery systems;
- **System analysis**
  - refers to the system being attacked and the need to define successful operation of the system as a baseline for knowing how the system can fail or be destroyed;

- **Vulnerability assessment**
  - is the response of the system to the threat and includes the appraisal of the consequences.

This step is crucial as risk analyses are essential to making the right decisions.

5.1.3 Decision Making and Actions Implementation

Decision analysis involves determining the risks, costs, and benefits of different alternatives available to the decision makers. Good decisions are strongly dependent on the risks analysis process. The decisions making is followed by the implementation of actions.

The general aforementioned framework, along with other state-of-art security issues contemporarily concerned in power system, will be specifically recounted in the subsequent sections.

5.2 The case of the electric power system

5.2.1 Information Gathering and Processing

i. Defining the System

The objective is to define the system being analyzed in terms of what constitutes normal operation, what constitutes anomalous states, and which are the points of vulnerability. This will serve as a baseline for the risk assessment and the operation of the systems. The purpose is to understand how the system works so deviates from normal, successful operation can be easily identified. Once the system is understood, vulnerabilities that require special analysis can be identified.

In the case of the electrical grid, the main components are:

- *substations*,
- *transmission lines (especially the extra high-voltage transmission lines)*,
- *SCADA systems*, and
- *Energy Management Systems (EMS)*.

Each of these components represents a potential point of vulnerability and therefore must be characterised. The characterisation should look at the structural elements (i.e. the topology and interconnection among components), their functionality, and their operational behaviour under different conditions.

For the characterisation the questions include but are not limited to:

- Is the generating capacity in the grid sufficient to meet load demands during peak periods?
- Which substation(s) supply the majority customers?
- Where could there be potential bottleneck(s)?

ii. Characterizing the Threat

Once the system is described, the threats associated with it can be identified and characterized.

A threat is defined as “a potential cause of an unwanted incident which may result in harm to a system or organization” [14]. In more general terms, it connotes an initiating event that can cause harm to a system or induce it to fail.

The Common Criteria [15] characterizes threat as a 4-tuple: a threat agent, a presumed attack method, the vulnerability exploited by the attack and the asset under attack. According to this definition, threats are defined with reference to specific vulnerabilities and assets. For the sake of discrimination, [16] characterizes a threat by a 3-tuple, the threat agent, the threat mode and the threat determinant.

NERC developed five colour-coded threat alert level definitions addressing both cyber and physical security [17][18]. Each level represents an increasing degree of potential threat, ranging from low-green, guarded-blue, elevated-yellow, high-orange to severe-red. The threat alert level does not have to apply consistently to all corporate locations and assets. A company could specify a unique threat alert level for a particular region, city, or type of facility.

Considering the intimate connections between power systems and society’s other infrastructures, [19] has summed up the threats of power system into three categories:

- Those that can be related to attacks **upon the power system**.
    - In this case, the electricity infrastructure itself is the primary target – with outages rippling into the customer base.
- Those that can be related to attacks **by the power system**.
    - The ultimate target is the population, using parts of the electricity infrastructure as a weapon.
- Those that can be related to attacks **through the power system**.

- The target is the civil infrastructure in this case.

Modern security threats have increased in both the physical and cyber areas, characterized from inadvertent (natural disaster, equipment failure etc) to malicious (hackers attack, warfare etc).

- **Physical Threats:**
  - Numerous physical methods, such as facility break-ins, weapon attacks, or bomb explosions, could be used to damage the elements of power system with varying degrees of damage to the network and the region.
- **Cyber Threats:**
  - A cyber attack could be planned, coordinated, and carried out from almost anywhere in the world where there is a connection to the Internet. The cyber systems in power industry mainly consist of two categories — the control system and the management information system. The former mainly refers to the SCADA/EMS system; the latter includes all the management and information software in power industry. An important concept relevant to cyber attack is information security, it is defined as the preservation of confidentiality, integrity and availability of information [20].

5.2.2 Risk assessment

Risk is measured in terms of *scenarios* (what will happen), *likelihood* (how likely it is to happen), and *consequences* (what the results would be). The parameter selected for measuring risk is based on the probability of the success rate of different levels of damage.

Risk assessment is an integral part of the electricity sector's definition of *critical infrastructure* [21] [22] [23]. The final objective is to support risk management in safeguarding the essential components of the electric infrastructure against physical and cyber threats. As the grid interconnects different operators and countries, the assessment and management of risk has to be done in a manner consistent with both industry and industry-government partnerships, while sustaining public confidence in the electricity sector. The most difficult part of the risk assessment process is the development of realistic, quantitative estimates for the likelihood of each potential failure, including consistent evaluations of the uncertainties in each estimate.

i. Constructing Scenarios

The malicious attacker and the risk analyst must both think in terms of scenarios or

sequences of events. This is the core of the risk assessment. The scenarios show how specific damage levels can result from physical attacks on the system hardware, cyber attacks on system controls, and combinations of these attacks [24] [25].

It is convenient to structure malicious attack scenarios from the point of view of the system that is attacked. The first step is to develop a diagram describing the *success scenario* that leads to a successful end-state or normal operating procedures for the system without the intervention of a terrorist event. The second step is to develop the meaningful *initiating events* that could disrupt the normally operating system and assess their likelihoods. The likelihood of attack scenarios is quantified in terms of three explicit and quantitative interpretations — *frequency*, *probability*, and *probability of frequency*.

- **Frequency**:
    - The frequency of the recurrent scenario can be expressed in occurrences per day, per year, per trial, per demand, etc.
- **Probability**:
    - If the scenario is not recurrent, that is, it happens either once or not at all, then its likelihood can be quantified in terms of probability. It is the degree of credibility of the hypothesis in question, based on the totality of relevant evidence available.
- **Probability of frequency:**
    - If the scenario is recurrent, and therefore has a frequency, but the numerical value of that frequency is not fully known, and if there is some evidence relevant to that numerical value, then Bayes Theorem [26] [27] can be used to develop a probability curve over the frequency axis. This 'probability of frequency' interpretation of likelihood is the most informative, and thus is the preferred way of capturing and quantifying the state of knowledge about the likelihood of a defined scenario.

Specific scenarios that will be developed further are (1) a physical attack on the electrical grid; and (2) a complementary simultaneous cyber attack on the electrical grid.

i.1 Physical Attack Scenarios

Figure 1 shows an example of the systematic thought process used to develop the attack scenarios and to assign their consequences to the damage levels. Branches can be added to account for other protective barriers in each system. The purpose of this exercise is to create

a comprehensive framework for identifying vulnerabilities and in turn make better decisions.

i.2 Cyber Attack Scenarios

The cyber attack can be divided into five phases [13]:

1. *Discovery phase.*

   It begins with the identification of potential targets (mostly via the Internet). This could be done using search engines by typing in keywords, and then assemble the critical information, such as IP addresses, about these electric utility companies.

2. *Launch platform acquisition.*

   Cyber attacks are typically carried out through a series of computers, which makes it very difficult to trace the source of the attack, even if it has been discovered. The attackers would arrange administrative privileges on the computer systems with vulnerabilities and then go dormant, covering their tracks by deleting log entries and using other stealth techniques. In this manner, they would compromise a series of computer systems from which they could launch their cyber attacks remotely.

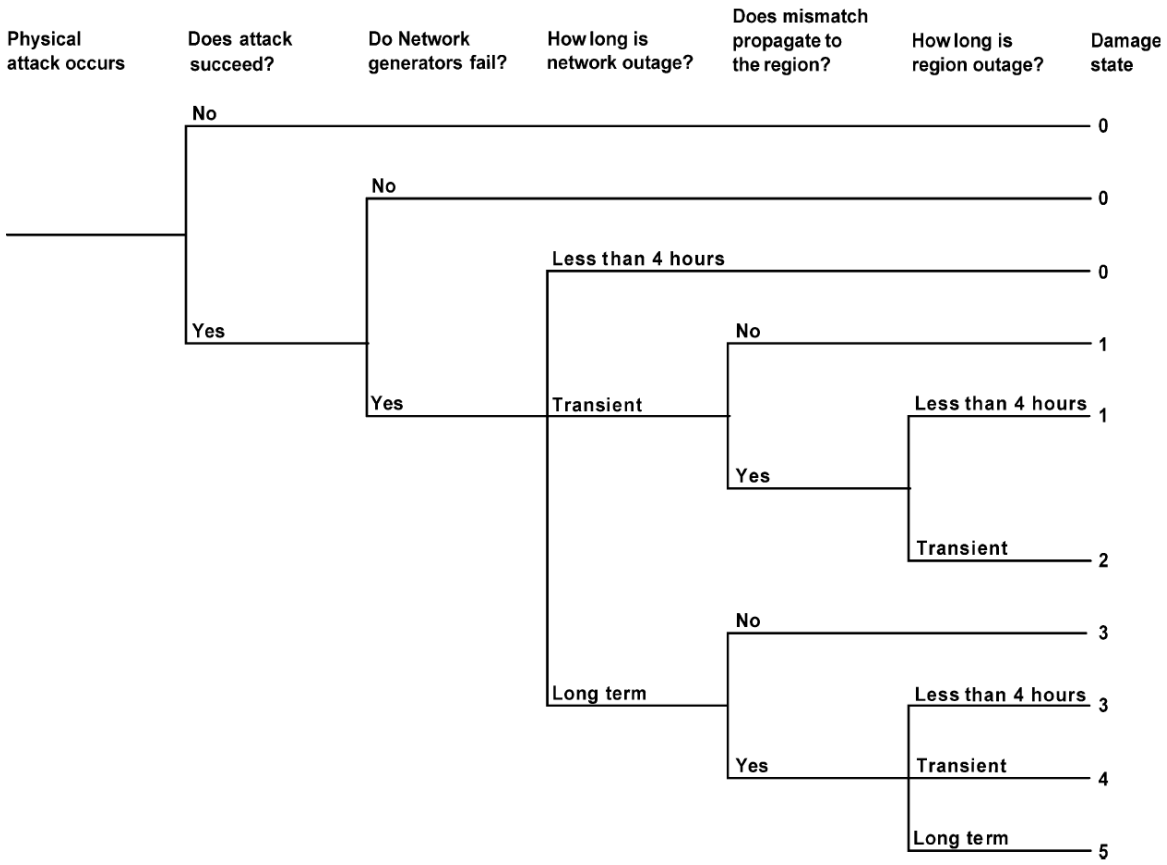


Fig. 2 - An example of thought process for attack scenarios

3. *Target selection.*

   Once an electric utility had been selected as a target, the attackers would activate some of the computers exploited in the platform acquisition phase, transferring the prowl tools that are readily available on the Internet to the compromised computers. When these tools are successful, they can install a number of surveillance/reconnaissance tools that would automatically cover up any sign that the utility computer had been compromised.

4. *Target reconnaissance and compromise.*

   In this phase, the cyber attackers would attempt to assess the number of other computers in the network that 'trust' the computer system compromised in the previous stage and to what extent. They could then use these trust relationships to inspect other computer systems on the network, as well as to discover other local networks. The cyber attackers might also install packet sniffers to listen in on network traffic for packets destined for ports specific to a particular SCADA system. Once they found SCADA port traffic, they could identify the computer systems being used as SCADA systems.

5. *Initiation of an attack.*

   The final step would involve compromising one or more of the computer systems that run the SCADA system. Once the SCADA system was compromised, the amount of damage inflicted on the components of the power grid reachable by the compromised SCADA system would depend on the attacker's knowledge of electric power systems.

We can form a simple cyber attack scenario with respect to the example in i.1. According to figure 1, one possible way to achieve damage state 4 is first to bring down the network (by a physical attack), and then to override or block the regional SCADA protection and control systems (by a cyber attack) so that frequency stabilization, load shedding, and islanding protocols or automatic supplies from other interconnected regional grid could not be quickly implemented or provided. Thus, the failures of one network can cascade throughout the regional grid. If the major regional tie-lines remain connected to the attacked network, the entire grid may be quickly collapse [28].

In fact, most cyber attacks are multistep attacks composed by a set of attack actions. The paper [29] proposes an algorithm for constructing attack scenario based on modelling multistep cyber attacks.

i.3 Results Assembly

Once the individual scenarios have been quantified, they can be assembled into risk measures. This is a matter of combining all scenarios that terminate in a specific damage category.

The results take the form of the graph in figure 3, which shows the curve for a single scenario or a set of scenarios leading to a single consequence. Each scenario has a probability-of-frequency curve quantifying its likelihood of occurrence.

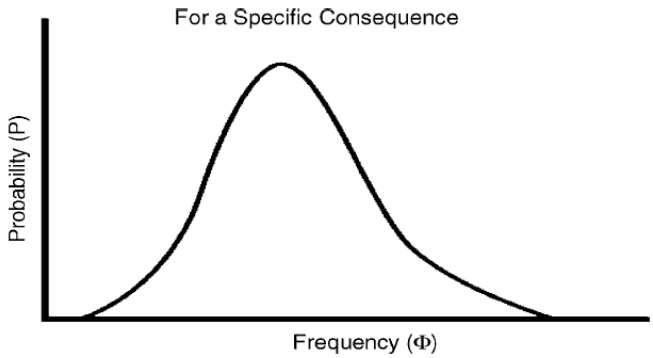


Fig. 3 - Probability-of-frequency curve

Showing different levels of damage requires a different type of presentation. The most common form is the classical risk curve, also known as the frequency-of-exceed curve. This curve is constructed by ordering the scenarios by increasing levels of damage and cumulating the probabilities from the bottom up in the ordered set against the different damage levels. Plotting the results on log-log paper generates curves, as shown in figure 4.

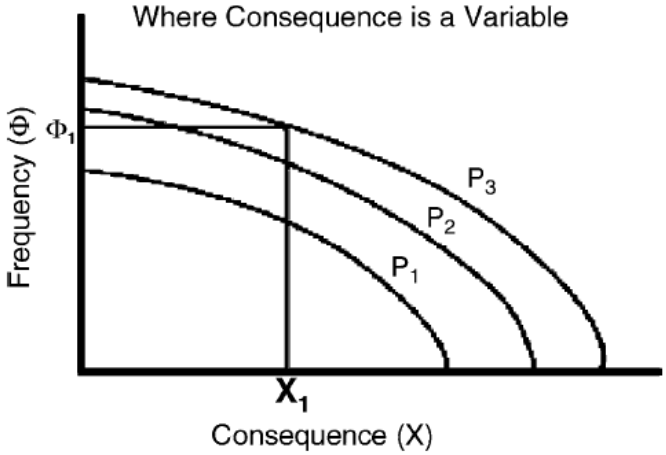


Fig. 4 - Risk curve for varying consequences

Suppose P_3 has the value of 0.95, that is a probability of 0.95, and suppose we want to know the risk of an X_1 consequence at the 95% confidence level. According to the figure, we are

95% confident that the frequency of an X_1 consequence or greater is Φ_1: The family of curves (usually called percentiles) can include as many curves as necessary. The ones most often selected in practice are the 5th, 50th, and 95th percentiles.

It's necessary to notice that although Figs. 3 and 4 can provide a perspective on the actual risks and in establishing priorities for threats, targets, and vulnerabilities, the most important thing is to rank the importance of contributors to a risk by analyzing the curves in Figs. 3 and 4.

ii. Threat and Vulnerabilities Assessment

Based on the assembly results, by linking the threat assessment with vulnerability assessment, we would be able to answer questions such as which threats and vulnerabilities can be matched in a given power grid; what are the contributing factors and how do they rank in importance; what actions will have the biggest payoff in terms of risk reduction for the amount of resources invested. These answers are the key points to make decisions or develop countermeasures when system is confronting the risk.

The threat assessment includes events and activities leading up to the attack but does not assess or speculate on the malicious actors' decision to initiate the attack. The threat analysis generates the initiating events for the vulnerability assessment. In other words, the output of the threat assessment is the input to the vulnerability assessment.

Vulnerabilities are the faults that might result in accidental events, or that might expose the system to threats [30]. The sources of vulnerability include natural disasters (e.g., earthquakes, hurricanes, and winter storms), equipment failures, human errors in the design, configuration, operation or maintenance of the system [31].

The main task of vulnerability assessment is to evaluate the level of system strength or weakness relative to the occurrence of an undesired event. USA's DOE has conducted a number of vulnerability assessments for energy infrastructure providers. The suite of tasks that are often included in the vulnerability assessment can be summarized as [32]:

- Evaluate the threat environment:
    - Characterizing the threats, combining with an appreciation of the value of the assets and systems, and impact of unauthorized access and subsequent malicious activity.
- Information network architecture assessment:
    - Providing an independent analysis of the enterprise assurance features of the

information network(s) associated primarily with infrastructure control systems, such as SCADA and EMS [33] [34] [35].

- Cyber security assessment, including penetration testing of information systems:
    - Utilizing active scanning and penetration tools to identify network vulnerabilities that might be easily exploited by a determined adversary. Additionally, there is strong interest in determining whether access can be gained to critical applications.
- Physical security assessment:
    - Evaluating the physical security systems in place or planned, and to identify potential physical security improvements for the sites evaluated. The physical security analysis include access controls, barriers, locks and keys, badges and passes, intrusion detection devices and associated alarm reporting and display, closed circuit television (assessment and surveillance), communications equipment (telephone, two-way radio, intercom, cellular), lighting (interior and exterior), power sources (line, battery, generator), inventory control, postings (signs), security system wiring, and protective force.
- Operations security assessment:
    - Denying potential adversaries information about capabilities and intentions of the host organization.
- Review administrative policies and procedures.
- Physical asset analysis:
    - Examining the systems and physical operational assets to ascertain whether vulnerabilities exist.
- Impact analysis:
    - Evaluating the impact on market and/or system operations associated with exploiting unauthorized access to critical assets.
- Risk characterization:
    - Providing a structure under which options developed in the previous tasks can be compared and evaluated.

Vulnerability assessment is a research topic that is gaining academic interest. Quantitative measures based on different approaches, such as vulnerability index [36], graph theory [37] and game theory [38] [39], are presented in a large amount of easy-to-access reference papers. Since it’s impossible to provide an exhaustive or an all-inclusive list here, this report won’t go further on this subject.

iii. Making Decisions

Generally speaking, to avoid physical attacks, one plausible action to consider would be to improve the security of the elements (substations, transmission lines etc) identified as the principal contributors to long-term outages for the power grid by the risk assessment.

Another key high-priority technology for countering physical attacks is adaptive intelligent islanding [19]: When major disruptions occur on a power system, the transmission network automatically responds by breaking into self-contained islands, according to fixed procedures established well in advance. Such procedures have not generally been updated since the onset of deregulation and will not be adequate for dealing with a terrorist attack on multiple carefully chosen targets. Rather, we need a more flexible islanding method that can react instantaneously to attack conditions, taking into account the location and severity of damage, load status, and available generation.

To avert cyber initiated attacks, strategies could be taken to reduce the uncertainties in the risk analysis and to find ways to discourage repeated attempts. Nowadays, several classes of commercially available products can be used to protect against cyber attacks. The first class is a number of computer firewall products that can recognize and deflect cyber attacks by restricting all incoming and outgoing network traffic unless the administrator of the firewall designates it. A second class of security devices, intrusion-detection systems, monitors incoming and outgoing network traffic for digital signatures of known cyber attack tools and ploys.

However, utility decision makers face a number of challenges in the security area [40]. Therefore, it's impossible to give a universal rule for how to make decisions when confronting the malicious attack, but standards and guidelines issued by government agencies, industry organizations and electricity utility operators could be used as a good reference baseline point. Furthermore, looking into some industrial successful efforts will also give insight into how to provide the needed coordination and establish a unified response to cyber threats.

6 Relevant standards and Guidelines

6.1 Standards

The importance of the security aspects in the electric power field is confirmed by the constitution of security working groups by standard organizations, such as IEC TC57 WG 15. WG 15 published the Technical Report 62210 [41] which may be considered a valuable approach for introducing security in power system control.

Based on the ideas in IEC TR 62210 [41] and taking into account the more commonly applied security standards (Common Criteria [15] and ISO/IEC 17799 [20]), CESI-JRC present a methodological approach to analyze the security of systems by identifying its assets, their vulnerabilities, the threats that might exploit the latter by means of attacks or accidental means, and the losses that could be caused [16].

Similar to ISO/IEC 17799, ISA [42] provides generic guidance in two reports. One report [43] deals with security technologies, and the other [44] discusses how to develop a security program for Manufacturing and Control Systems.

In response to the increasing cyber and physical threats to electricity industry facilities, assets, and personnel, NERC devised a standardized set of protective measures [45] based on national security plans and guidelines developed by other agencies [17] [18], on the basis of which, EPRI offers guidelines that an electric power company can use to develop or enhance its own threat alert level response plan [46]. This guideline along with its companion reports, EPRI Report 1001639 [47] and EPRI Report 1008396 [48], provide a scope of information to the decision makers, who could in turn devise their own countermeasures against a particular threat.

The Urgent Action Cyber Security Standard 1200 adopted by NERC in 2003 specifies actions to be taken to protect utility systems in 16 areas, such as access control, information protection, personnel training, incident response, and recovery planning, among others. This standard has been extended and modified for development into a set of permanent cyber security standards: CIP-002 through CIP-009. NERC also offered the corresponding implementation plan for these cyber security standards [49].

Operating a reliable information security system is an important cyber security-related issue.

The standards of [20], [50], [51] give any organization a good basis to build an information security management system framework and implement security controls to fulfil security requirements. And in a similar way, any power utility could use the same basis and adapt security controls for its own needs, where [20] provides a sound check list of a great number of issues to be dealt with for proper handling of information security. However, the standards do not focus on control systems domains within the electric power industry and it is left to each power utility to adopt, adapt, or develop adequate policies and procedures to these domains [52] [53].

Many associated system operators regulate their own standards in terms of security and reliability. Take the strong-interconnected power grid UCTE as an example. According to UCTE Operation Handbook [54], the information security can be enhanced by the following measures:

- All data exchanged must be transmitted over the Electronic Highway (EH) in sequence and in a timely manner. The EH is a private network dedicated to the electricity sector to be used by TSOs only.
- EH transfers only UCTE-approved operational and electricity market data between TSOs.
- EH shall use only protocols and formats approved by the responsible body of UCTE.
- EH has no direct connection to the Internet.

In addition to the guidelines and standards above-mentioned, comprehensive discussions about security issues in power grid can also be found in [19] [39] [55] [56].

6.1.1 Common Criteria

Identifying threats is one of the core components of Security problem definition. CC puts the security issue in a threat-asset relationship. [57], states that ‘a threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset).

The threat agents are defined as ‘entities that can adversely act on assets.’ The threat is defined as a high level of abstraction. Thus, a threat agent may be anyone of the following: hackers, users, computer processes, TOE (Target of Evaluation – the IT system being assessed), development personnel, and accidents.

In turn, threat agents may be further described by aspects such as expertise, resources, opportunity and motivation. They may be described as individual entities, but in some cases it may be better to describe them as types of entities, groups of entities etc.

The same document defines Assets as entities that someone places value upon. To be more specific, some examples of what may be considered as assets are give in the sequel: contents of a file or a server; the authenticity of votes cast in an election; the availability of an electronic commerce process; the ability to use an expensive printer; access to a classified facility.

Adverse actions are actions performed by a threat agent on an asset. These actions influence one or more properties of an asset from which that asset derives its value.

The mentioned document also makes several recommendations on countering the threats. Thus, ‘countering a threat does not necessarily mean removing that threat, it can also mean sufficiently diminishing that threat or sufficiently mitigating that threat [57]. The possible actions to counter the threat are removing, diminishing and mitigating the effects. Several examples of possible countermeasures are given in Table 4.

An attack potential (AP) estimation methodology is proposed for vulnerability assessment in [58]. The method should be used based on the threat profile developed during Security Problem Definition / Security Target (ST). The following is a short introduction of the main definitions and concepts involved. The following are in line:

- AP should be determined in consideration of the threat environment and the selection of assurance components
- AP of the attackers of the TOE is generically characterised as Basic, Enhanced-Basic, Moderate or High.
- The primary role of the attack potential is to determine whether or not the TOE is resistant to attacks assuming a specific attack potential of an attacker during vulnerability assessment.
- Attack potential is a function of expertise, resources and motivation.

According to [58] ‘Motivation is an attack potential factor that can be used to describe several aspects related to the attacker and the assets the attacker desires. Firstly, motivation can imply the likelihood of an attack - one can infer from a threat described as highly motivated that an attack is imminent, or that no attack is anticipated from an un-motivated threat. Secondly, motivation can imply the value of the asset, monetarily or otherwise, to either the attacker or the asset holder. An asset of very high value is more likely to motivate an attack compared to an asset of little value. Thirdly, motivation can imply the expertise and resources with which an attacker is willing to effect an attack.

The following factors should be considered when characterizing the attack potential:

1) Time taken to identify and exploit (Elapsed Time); the total amount of time taken by an attacker to identify that a particular potential vulnerability may exist in the TOE, to develop an attack method and to sustain effort required to mount the attack against the TOE. When considering this factor, the worst case scenario is used to estimate the amount of time required. The identified amount of time is as follows:
   a) less than one day;
   b) between one day and one week;
   c) between one week and two weeks;
   d) between two weeks and one month;
   e) each additional month up to 6 months leads to an increased value;
   f) more than 6 months.

Removing	Removing the ability to execute the adverse action from the threat agent.
	Moving, changing or protecting the asset in such a way that the adverse action is no longer applicable to it.
	Remove the threat agent (e.g. removing machines from a network that frequently crash that network)
Diminishing	Restrict the ability of a threat agent to perform adverse actions.
	Reduce the likelihood of an executed adverse action being successful.
	Reduce the motivation to execute an adverse action of a threat agent by deterrence.
	Restrict the opportunity to execute an adverse action of a threat agent.
	Requiring greater expertise or greater resources from the threat agent.
Mitigate the effects	Making frequent back-ups of the asset
	Insure an asset
	Obtaining spare copies of an asset
	Ensure that successful adverse actions are always timely detected, so that appropriate action can be taken.

Table 4. Possible threat contermeasures – Compiled from [58]

2) Specialist technical expertise required (Specialist Expertise); the level of generic knowledge of the underlying principles, product type or attack methods (e.g. Internet protocols, Unix operating systems, buffer overflows). The identified levels

are as follows:

- Laymen are unknowledgeable compared to experts or proficient persons, with no particular expertise;
- Proficient persons are knowledgeable in that they are familiar with the security behaviour of the product or system type;
- Experts are familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type.
- The level “Multiple Expert” is introduced to allow for a situation, where different fields of expertise are required at an Expert level for distinct steps of an attack.

3) Knowledge of the TOE design and operation (Knowledge of the TOE); specific expertise in relation to the TOE. This is distinct from generic expertise, but not unrelated to it. Identified levels are as follows:
   - Public information concerning the TOE (e.g. as gained from the Internet);
   - Restricted information concerning the TOE (e.g. knowledge that is controlled within the developer organisation and shared with other organisations under a non-disclosure agreement)
   - Sensitive information about the TOE (e.g. knowledge that is shared between discreet teams within the developer organisation, access to which is constrained only to members of the specified teams);
   - Critical information about the TOE (e.g. knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking).
4) Window of opportunity;
5) IT hardware/software or other equipment - the equipment required to identify or exploit vulnerabilities.
   a) Standard equipment is readily available to the attacker, either for the identification of vulnerability or for an attack.
   b) Specialised equipment is not readily available to the attacker, but could be acquired without undue effort.
   c) Bespoke equipment is not readily available to the public as it may need to be specially produced (e.g. very sophisticated software), or because the

equipment is so specialised that its distribution is controlled, possibly even restricted or very expensive.

The document further details the assessment methodology. This is not presented here, since it gets out of the scope of this report.

6.1.2 ISA (Instrument Society of America)

ISA is a leading, global, non-profit organization that sets standard in the automation field. Inside ISA, a specific committee (SP99) has been created [3]. This committee will establish standards, recommended practices, technical reports, and related information for implementing electronically secure manufacturing and control systems, and for the security practices and assessment of their security performance. The Committee's focus is to improve the confidentiality, integrity, and availability of components or systems used for manufacturing or control and to provide criteria for procuring and implementing secure control systems.

ISA99 published its Part 1 standard, ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems: Concepts, Terminology and Models*, [59] in late 2007. This Part 1 standard serves as the foundation for all subsequent standards in the ISA99 series.

Also in late 2007, ISA99 published an updated version of its technical report, ANSI/ISA-TR99.00.01-2007 *Security Technologies for Manufacturing and Control Systems*. [60] This technical report provides an assessment of cyber security tools, mitigation countermeasures, and technologies that may be applied to industrial automation and control systems regulating and monitoring numerous industries and critical infrastructures.

The final ISA99 series will consist of 6 parts. It is being adopted as the basis of other standards, such as IEC 62443.

6.1.3 ISO (International Organization for Standardization)

ISO, in conjunction with IEC (International Electrotechnical Commission), forms the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interests.

The International Standard ISO/IEC 27001 [61] has been prepared to provide a model for establishing, implementing, operating monitoring, reviewing, maintaining and improving an

Information Security Management System (ISMS). The adoption of ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple ISMS solution.

This International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS. An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process. The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach". The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

1. understanding an organization's information security requirements and the need to establish policy and objectives for information security;
2. implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;
a) monitoring and reviewing the performance and effectiveness of the ISMS; and continual improvement based on objective measurement.

This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes. Figure 2 illustrates how ISMS takes as input the information security requirements and expectations of the interested parties, and through the necessary actions and processes produces information security outcomes that meet them.

The International Standard ISO/IEC 27002 [62], which replaces the standard ISO/IEC 17799, provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining ISMS. Information security is defined within the standard as the preservation of confidentiality (ensuring that information is accessible only to those authorised to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability

(ensuring that authorised users have access to information and associated assets when required).

The standard contains the following twelve main sections:

1 Risk assessment
2 Security policy: management direction
3 Organization of information security: governance of information security
4 Asset management: inventory and classification of information assets
5 Human resources security: security aspects for employees joining, moving and leaving an organization
6 Physical and environmental security: protection of the computer facilities
7 Communications and operations management: management of technical security controls in systems and networks
8 Access control: restriction of access rights to networks, systems, applications, functions and data
9 Information systems acquisition, development and maintenance: building security into applications
10 Information security incident management: anticipating and responding appropriately to information security breaches
11 *Business continuity management*: protecting, maintaining and recovering business-critical processes and systems
12 *Compliance*: ensuring conformance with information security policies, standards, laws and regulations

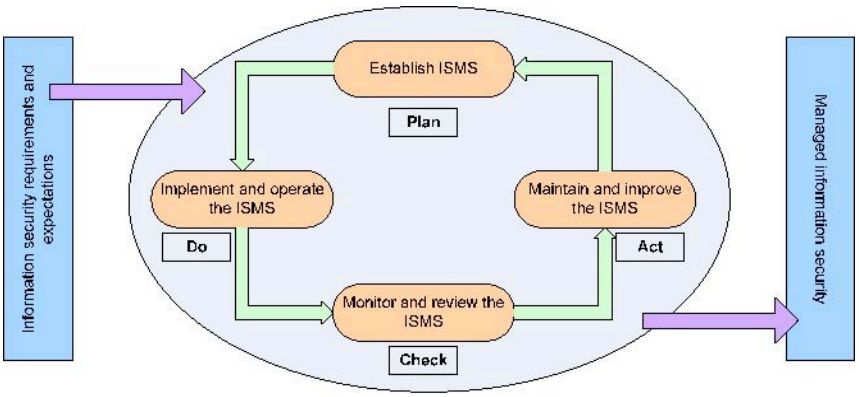


Fig. 5 – Plan-Do-Check-Act model applied to information systems

Within each section, information security controls and their objectives are specified and outlined. The information security controls are generally regarded as best practice means of

achieving those objectives. For each of the controls, implementation guidance is provided.

6.1.4 NIST

The US National Institute of Standards and Technology is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology.

In the security field, NIST has been developing standards for cyber and physical assessment and protection.

i. NIST 800 series

NIST Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.'

Three of the 800 series have been identified as relevant for our topic. These are:

i.1 Guide to Industrial Control Systems (ICS) Security (NIST 800-82)

The document provides guidance for establishing secure industrial control systems (ICS). The document focuses on supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and Programmable Logic Controllers (PLC). The document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

The document states that numerous sources have to be taken into account when considering potential threats to ICS. These include hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, natural disasters as well as malicious or accidental actions by insiders. ICS security objectives typically follow the priority of availability, integrity and confidentiality.

The control system incidents are classified in three broad categories:

i. Intentional targeted attacks such as gaining unauthorized access to files, performing a DoS, or spoofing e-mails (i.e., forging the sender's identity for an e-mail)

ii. Unintentional consequences or collateral damage from worms, viruses or control system failures
iii. Unintentional internal security consequences, such as inappropriate testing of operational systems or unauthorized system configuration changes.

The document propose a ICS risk assessment methodology in accordance with the more general IT systems methodology provided in Special Publication 800-30 Risk Management Guide for Information Technology Systems.

i.2 Risk Management Guide for Information Technology Systems (NIST 800-30)

The document defines risk management as the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. NIST 800-30 provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. Risk is defined as a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

The risk management approach in this document is to integrate risk assessment throughout all the 5 phases of System Development Life Cycle (SDLC) – Initiation, Development and Acquisition, Implementation, Operation and Maintenance, and Disposal.

A 9 steps risk assessment methodology is proposed as for being applied in each of the SDLC phases:

- Step 1 - System Characterization
- Step 2 - Threat Identification
- Step 3 - Vulnerability Identification
- Step 4 - Control Analysis
- Step 5 - Likelihood Determination
- Step 6 - Impact Analysis
- Step 7 - Risk Determination
- Step 8 - Control Recommendations
- Step 9 - Results Documentation.

Threat identification phase (Step 3) leads to defining a threat statement characterizing the system. 'The threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits)'.

Natural threats (e.g., floods, earthquakes, storms) should also be taken into account.

The threat statement should be developed based on reliable information from different sources, among which 'government and industry organizations' that 'continually collect data on security events' thus 'improving the ability to realistically assess threats. Sources of information include … intelligence agencies (for example, the Federal Bureau of Investigation's National Infrastructure Protection Centre), Federal Computer Incident Response Centre (FedCIRC), Mass media, particularly Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org'

As resulting from the proposed methodology, an important source of information when identifying the threats is previous incident / attack related data collected in the past. NIST also provides a set of recommendations and support documentation for assisting organizations in mitigating the risks from information security incidents by providing practical guidance on responding to incidents effectively and efficiently in 'Computer Security Incident Handling Guide' NIST 800-61.

i.3 Computer Security Incident Handling Guide (NIST 800-61)

The document presents general incident response guidelines that are independent of particular hardware platforms, operating systems, and applications. Specifically, it includes guidance on establishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing, and handling incidents.

An incident is defined as "*a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."* The benefits of having an incident response capability are pointed out as:

- Responding to incidents systematically so that the appropriate steps are taken
- Helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information, and disruption of services
- Using information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data
- Dealing properly with legal issues that may arise during incidents.

From the attack/effect viewpoint the approach taken in this document tackles the security issue from a different perspective than the ones in the documents above. The document supports recognizing the incident by the system's symptoms. In other words, the document

addresses the monitoring facet of system security.

The importance of communicating with other outside parties is stressed out throughout the document. Details of an incident should be communicated not only to reporting incidents to organizations, but also ‘other involved parties, such as the organization’s Internet service provider (ISP), the ISP that the attacker is using, the vendor of vulnerable software, or other incident response teams that may be familiar with unusual activity that the handler is trying to understand.’

A 4 phase incident response process is proposed for handling incidents, starting from initial preparation through post-incident analysis. Recommendations are given for each.

1. Preparation
    a. Preparing to handle incidents
    b. Preventing incidents
2. Detection and Analysis
    a. Incident categories
    b. Signs of an incident
    c. Sources of Precursors and Indications
    d. Incident analysis
    e. Incident documentation
    f. Incident prioritization
    g. Incident notification
3. Containment, Eradication and Recovery
    a. Choose a containment strategy
    b. Evidence gathering and handling
    c. Identifying the attacker
    d. Eradication and recovery
4. Post-incident activity
    a. Lessons learned
    b. Using collected incident data
    c. Evidence retention

The general procedure is detailed for 4 main classes of incidents (denial of service, malicious code, unauthorized access, inappropriate usage and multiple components).

6.1.5 NERC

The North American Electric Reliability Corporation, NERC, has as its mission to ensure the reliability of the bulk power system in North America. To achieve that, they develop and enforce reliability standards, among other activities. NERC is a self-regulatory organization, subject to oversight by the U.S. Federal Energy Regulatory Commission and governmental authorities in Canada.

In the last years NERC has produced a set of standards that are mandatory for all the actors in the US power infrastructure.

i. Security Guidelines for the Electricity Sector: Control System Cyber Security Incident Response Planning. Threat and Incident Reporting

According to NERC, “the purpose of this guideline is to describe this reporting process and encourage organizations to promptly report suspicious activities, threats or acts of sabotage, vandalism or terrorism”.

Moreover, the guidelines are intended to encourage organizations to report significant security threats or incidents to the Electricity Sector – Information Sharing and Analysis Centre (ESISAC), pointing out common benefits the different organizations may get from (promote a timely and actionable response in order to prevent the attack or mitigate the consequences on public health and safety, the environment and the economy; minimize negative impact on organization repair costs, revenues, productivity, customer service and public trust; and demonstrate diligence and due care by the organization on behalf of the electricity sector.

A critical facility is defined as any facility or combination of facilities, that if severely damaged or destroyed, would have a significant impact on the ability to serve large numbers of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the energy grid or would cause significant risk to public health and safety.

According to the document, the security threats and actual incidents should be reported to law enforcement (e.g., local, state/provincial, FBI/RCMP), government agencies and regulators as is necessary or required (e.g., at the state/provincial or federal level), the Electricity Sector’s Information Sharing and Analysis Center (ESISAC); and other electricity sector entities (e.g., control areas, reliability coordinators, regional transmission operators, independent system/market operators).

The information to be reported by the power infrastructure actors will vary according to the

specific circumstances and availability of the information, but should include:

- date, time and location of the incident
- brief description of incident
- impact on critical infrastructure, public health and safety, environment
- expected duration of impact, or time to restore
- cause, if known
- reporting individual and organization, and contact information for follow-up
- law enforcement involvement

ii. Security Guidelines for the Electricity Sector: Control System Cyber Security Incident Response Guideline

These guidelines address the potential risks that can impact some electricity sector organizations and provides practices that can help mitigate the risks. The document states the importance of having an incident response plan and provides guidance in creating one. However certain decisions about how to manage the incidents are to be made before the actual developing of the plan.

The plan stresses out one of the key aspects in managing the attack: how to react to an attack in terms of the 'forensic' aspects: 'The plan should consider the merits of immediate response by blockage of a detected intruder as well as a delayed response that allows tracking the intruder access up to a certain point. The delayed response view purports to allow an entity time to assess the intruder's entrance strategy, tactics and possible installations, scope of attack, and how to utilize the current incident for future prevention. Entities must weigh the pros and cons of both options when first embarking on the development of an incident response plan and delineating decisions. However, the entity must recognize that the actions put forth in the second view exposes the critical cyber systems to prolonged risk during the monitoring and assessment activity. (…) Additional decisions and discussions will need to address the trade-off between rapid system restoration and collection of evidence required for law enforcement proceedings (e.g., by chain of custody and quality of collection processes, tools, and proper documentation).'

The following represents a sequence of events that may be used to respond to a cyber security incident:

1. <u>Analyze the Incident</u>

   The incident should be analysed if it meets any of the criteria outlined in the definition

stage of the program setup. If there are multiple symptoms or potential causes/sources, then the events need to be “triaged” or ranked by critical importance regarding escalation and remediation.

2. Respond to the Incident

   Regardless of the method chosen to respond to incidents (i.e., rapid restoration or collection of evidence), at this stage an effective Incident Response Plan should endeavour to:

   a. Ensure no further damage can/will be done

   b. Contain and compartmentalize existing problem/intrusion

   c. Keep records of actions taken to aid in learning, reporting, and prosecuting

   d. Save and archive logs from impacted systems, IDSs (Intrusion Detection System) and firewalls.

3. Escalate as Appropriate

   If after initial implementation of the solution the incident is not contained, a pre-determined escalation plan should be invoked to augment the people and resources used to combat the issue.

4. Communicate

   When the analysis phase determines that the there is a reportable incident, then the communication channels must be opened. However, depending on the level of severity of the incident, different communication paths and plans may be appropriate for different situations. Further communication as the situation develops may be necessary, and in any case a summary report once the cyber security incident is resolved should be provided to all individuals at all levels involved in the escalation. Communication could include representatives of departments such as: legal, Human Resources, Marketing, Public Relations, Business Managers, existing security groups, such as physical security, audit or risk management departments, IT and any other employees or team members affected by the cyber security incident or its investigation.

5. Resolve the Incident

   Resolve the threat agent and negate the vulnerability. At this point a post-cyber security incident report should be developed. The report itself should include

information, such as:

- Incidence reference number
- Report author and contact information
- Summary of systems or assets involved
- Description of activity
- Supporting documentation or logs of activity
- Description of resolution
- Lessons learned

The documentation of the cyber security incident that can be reported will be kept for three calendar years. Contents of the report should include:

- How the cyber security incident was contained
- The cause and source of the compromise
- Elapsed time from compromise to detection
- Elapsed time from detection to containment of the threat
- Costs associated with the cyber security incident
- How much (if any) down time was caused
- How future similar cyber security incidents will be prevented
- Team members involved in remediation of the cyber security incident
- Policies that will be revised as a result of the incident resolution

6. Monitor for Possible Future Occurrences

After incident resolution is complete, and operations has returned to normal, monitoring the system at a higher level for a period of time, to insure no residual effects remain in the system, and that the corrective actions to not introduce any unintended consequences is required

6.2 Dealing With Cyber Vulnerability: Industry Efforts

In this age of ubiquitous digitization, cyber security becomes a hot issue. Government, EPRI and other leading industry organizations are continuing to develop and deploy new cyber security initiatives and technologies [40].

Growing concern over the possibility of computer-based security breaches led to

development of EPRI's Energy Information Security (EIS) program in 2000. EIS was designed to provide tools that individual utilities could use to enhance their own security programs, including cyber security awareness training, information sharing, approaches to assessing control system vulnerability, and risk management protocols.

EPRI's Infrastructure Security Initiative (ISI) was designed to develop both prevention countermeasures and enhanced recovery capabilities. As part of the work to provide utilities with immediately useful countermeasures, ISI has documented lessons learned from actual terrorist attacks and other catastrophic events at utilities around the world. One of the highlights of this effort came in 2004 with a report from Israel Electric Corporation (IEC) on the best practices they developed to defend their grid against terrorist attacks. The key conclusions stated in this "countermeasures" IEC report are as follows:

- There is no simple, single checklist for action that is appropriate to all possible emergencies.
- Be prepared for anything, i.e., any scenario you can think of, based on local/national information and past experience.
- Successful defence is based on three elements: people-related work efforts; procedures-related work efforts and technology/spare equipment-related work efforts.

The "countermeasures" project is also providing utilities with information on new ways to protect grid facilities, including an artificial intelligence technology that can automatically analyze the streaming video from large sets of multiple cameras in remote locations.

High-voltage transformers represent a critical vulnerability among potential infrastructure targets that are attractive to terrorists. In response to this threat, ISI came up with the concept and developed preliminary designs for a new type of so-called recovery transformer that can be easily stored, transported, and installed for emergency use.

Much progress has been made through the ISI and EIS programs. Considering the complexity of the nation's power infrastructure, the ever increasing capability of cyber attackers, and the diverse nature of current security efforts, an industry-wide highly coordinated cyber security program was developed by EPRI in cooperation with several industry organizations. As a result, an alliance has been formed to create the *PowerSec Initiative*, which brings together EPRI staff, a variety of industry organizations, and several industry experts to address the cyber threat issue as it could impact electric utility operational and control equipment.

One of the objectives for the PowerSec Initiative is to develop an overview of the electric power industry's current cyber security posture by consolidating and leveraging ongoing and completed cyber security work from utilities, government, regulatory agencies, and others. The PowerSec Initiative will focus first on electric utility SCADA systems and EMS, both of which have been identified by experts as critical cyber systems to secure. Information gleaned from the PowerSec cyber vulnerability assessment process is intended to complement ongoing security standards developed by NERC and the FERC.

Whereas PowerSec reducing the probable success of attacks, another industry-wide initiative — EPRI's IntelliGrid Consortium features limiting the scope of their effects by working on adaptive, self-healing technologies that can be built into the nation's power delivery system to increase overall system resiliency [63].

6.3 National security approaches

6.3.1 United States of America

In the following we will discuss some efforts in the United States, as the most representative of the worldwide initiatives in the field. Moreover, the US approaches also serve as guidance to other national initiatives.

i. DHS – The National Strategy to Secure Cyberspace

One of the components of the U.S. National Strategy for Homeland Security, The National Strategy to Secure Cyberspace [7] offers suggestions, to business, academic, and individual users of cyberspace to secure computer systems and networks. The document was prepared after a year of research by businesses, universities, and government, and after five months of public comment.

The document identifies three strategic objectives: (1) Prevent cyber attacks against America's critical infrastructures; (2) Reduce national vulnerability to cyber attacks; and (3) Minimize damage and recovery time from cyber attacks that do occur. To meet these objectives, the National Strategy outlines five national priorities:

1. National Cyberspace Security Response System: focuses on improving the government's response to cyberspace security incidents and reducing the potential damage from such events.
2. National Cyberspace Security Threat and Vulnerability Reduction Program

3. National Cyberspace Security Awareness and Training Program
4. Securing Governments' Cyberspace aim to reduce threats from, and vulnerabilities to, cyber attacks.
5. Establishment of a system of National Security and International Cyberspace Security Cooperation: intends to prevent cyber attacks that could impact national security assets and to improve the international management of and response to such attacks.

ii. DHS - Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts integrated threat analysis for all Critical Infrastructures/Key Resources (CI/KR) sectors. HITRAC brings together intelligence and infrastructure specialists to ensure a comprehensive understanding of the risks to U.S. CI/KR. HITRAC works in partnership with the U.S. Intelligence Community and national law enforcement (to integrate and analyze intelligence and law enforcement information on the threat) and with the sector-specific agencies (SSAs) and owners and operators (to ensure that their expertise on infrastructure operations is integrated into threat analysis).

HITRAC develops analytical products by combining intelligence expertise based on all-source information, threat assessments, and trend analysis with practical business and CI/KR operational expertise informed by current infrastructure status and operations information. The analysis is intended to provide an understanding of the threat, CI/KR vulnerabilities, the potential consequences of attacks, and the effects of risk-mitigation actions on not only the threat, but also on business and operations. This combination of intelligence and practical knowledge allows HITRAC to provide CI/KR risk assessment products that contain strategically relevant and actionable information. It also allows HITRAC to identify intelligence collection requirements in conjunction with owners and operators so that the intelligence community can provide the type of information necessary to support the CI/KR protection mission.

Based on HITRAC analysis, DHS produces two classes of information, addressing both the emergency preparedness and response capabilities and the long-term, strategic policies for enhancing the protection of US CI/KR.

ii.1 HITRAC functions

The following functions are supported by HITRAC [64]:

Threat and Incident Information:

DHS handles intelligence and operations monitoring and reporting from multiple sources to provide analysis that is based on the most current information available on threats, incidents, and infrastructure status. Real-time analysis of threat, situation, and CI/KR status information provided by DHS helps in determining if changes are needed in CI/KR risk management measures.

Specialized products include incident reports and threat warnings. These results are made available to appropriate security partners.

Incident Reports:

DHS monitors information on incidents to provide reports that CI/KR owners and operators and other decision-makers can use with confidence when considering how evolving incidents might affect their security posture. The information gathering is a common effort between government and private sector operations and watch centers.

Threat Warnings:

DHS combines all-source information to provide analysis of emergent threats on a timely basis. Many of the indicators that are reported by intelligence or law enforcement are not associated with an incident in progress, but are the product of intelligence collection. Such indicators also may be of significance only when interpreted in the context of infrastructure operational or status information. DHS monitors the flows of intelligence, law enforcement, and private sector security information on a 24/7 basis in light of the business, operational, and status expertise provided by its owner and operator security partners to produce relevant threat warnings for CI/KR protection. This analysis clarifies the implications of intelligence reporting about targeted locations or sectors, potential attack methods and timing, or the specific nature of an emerging threat.

Strategic Planning Information:

HITRAC analyzes information about terrorist goals, objectives, and attack capabilities to assess the potential terrorist attack profiles that might be used against each CI/KR sector. This provides the estimate of the potential threat, and is used as a supplement to, or in the absence of, specific intelligence and warnings regarding particular targets, attack vectors, or timing. This analysis provides decision-makers with the broad, analytically based information on the threat that is necessary to inform investment priorities and program design in conjunction with strategic planning. It also provides the overarching analytic foundation for

incident reports and threat warnings produced by DHS and other Federal partners.

The specialized products developed by HITRAC for strategic planning include a terrorist target selection matrix, which outlines plausible means of attack for each of the CI/KR sectors, a catalog of attack-specific scenarios, and a sector-specific threat report that provides detailed information on the estimated threat facing each sector. In addition to these HITRAC produces special, longer term strategic assessments and trends analyses that help define the evolving threat to the CI/KR.

Terrorist Target Selection Matrix:

DHS provides threat assessments to SSAs, CI/KR owners and operators, and other security partners who require them. It uses the Terrorist Target Selection Matrix produced by HITRAC as an analytical tool for identifying which sectors are potentially prone to different terrorist attack modalities.

The matrix maps terrorist goals and objectives against an array of possible attack modalities on a sector-by-sector basis. The attacks are classified as 'unlikely', 'modestly attractive' or 'attractive' based on the number of objectives of the criminal act accomplished by producing the attack.

Attack-Specific Threat Scenarios:

Attack-Specific Threat Scenarios are detailed vignettes of the specific methods, techniques, and actions terrorists are likely to use to attack specific types of U.S. CI/KR. The scenarios are based on HITRAC analysis of known terrorist capabilities or on their stated intent as derived from intelligence and the study of terrorist tactics, techniques, and capabilities. Threat scenarios are specific enough to be used by corporate or facility-level security officers to support operational security planning.

According to HITRAC 'this product supports facility-level threat surveillance by security forces, owner and operator requests for intelligence information, and risk management action planning. It also provides detailed threat information for the sector-specific threat assessment described below'.

Sector-Specific Threat Assessment:

DHS uses the information developed for the Terrorist Target Selection Matrix and the Attack-Specific Threat Scenarios to produce Sector-Specific Threat Assessments that provide an overall assessment of the potential terrorist threats posed to each of the CI/KR sectors, as well as an analysis of how these threats relate to sector vulnerabilities and consequences.

These assessments include known specific and general terrorist threat information for each sector, as well as relevant background information such as terrorist objectives and motives as they apply to the sector. Each sector-specific report includes the Terrorist Target Selection Matrix for the sector and specifies those Attack-Specific Threat Scenarios that may be relevant to the sector. The assessments are updated on a routine basis to include the most current intelligence findings and operational trends analyses. HITRAC works with each sector to develop and provide threat products that are tailored to meet sector-specific and subsector information needs.

This product is used to support detailed sector-level planning, including SSP development and implementation, and also to provide the detailed threat information necessary for additional security-related planning.

ii.2 Threat Assessment (Energy Sector)

The following types of threat products provided by HITRAC for the Energy Sector [65]:

- *Common Threat Scenarios*, which present methods and tactics that could be employed in attacks against the U.S. infrastructure;
- *General Threat Environment Assessments*, which are sector-specific threat products that include known terrorist threat information and long-term strategic assessments and trend analyses of the evolving threats to the sector's critical infrastructure; and
- *Specific Threat Information*, which is critical infrastructure-specific information based on real-time intelligence, and that will drive short-term measures to mitigate risk.

The Energy Sector also benefits from the continuation of [65]:

- Periodic conference calls with asset owners and operators to relay recently reported suspicious activities near energy facilities and other pertinent unclassified threat-related information;
- Reports analyzing suspicious activities said to have occurred near energy facilities;
- Classified threat briefings for representatives of the energy industry. Various Federal agencies would use these briefings to inform industry representatives about general and specific threats associated with the Energy Sector, as well as the overall threat of terrorism to the Nation. Such briefings should include representatives of intelligence community members, as appropriate;

- Improved communications and increased participation with regional, State, and local joint terrorism task forces and organizations; and
- Interagency forums and workgroups, such as the Forum for Infrastructure Protection, Pacific Northwest Economic Region (PNWER), and other State and local information-sharing, emergency-planning, and exercise efforts that benefit the Energy Sector as well as other participating sectors.

These forums and materials provide insights to sector security partners regarding the overall threat to the energy industry. More specifically, they help energy facilities, local law enforcement, and others to be more aware of potential indicators of terrorist and/or criminal activity.

iii. DHS Protective Programs

DHS also sponsors a variety of protective programs:

Control Systems Security:

DHS coordinates efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all CI/KR sectors.

Federal agencies and the law enforcement community provide information-sharing services and programs that support CI/KR protection information sharing. These include:

DHS Homeland Security Information Network:

HSIN is a national, Web-based communications platform that allows government entities and security partners to obtain, analyze, and share information based on a common operating picture of strategic risk and the evolving incident landscape. The network is designed to provide a robust, dynamic information-sharing capability that supports both steady-state CI/KR protection and incident management activities.

FBI's InfraGard:

InfraGard is an information-sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence related to the protection of U.S.

CI/KR from both physical and cyber threats. InfraGard chapters are geographically linked with FBI Field Office territories. Each InfraGard chapter has an FBI Special Agent Coordinator who works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters.

Interagency Cyber Security Efforts:

Interagency cooperation and information sharing target to improving national counterintelligence and law enforcement capabilities in terms of cyber security. The intelligence and law enforcement communities have various official and unofficial information-sharing mechanisms in place. Among these:

U.S. Secret Service's Electronic Crimes Task Forces (ECTFs): provide interagency coordination on cyber-based attacks and intrusions. As of 2010, 15 ECTFs are in operation, with an expansion planned.

FBI's Inter-Agency Coordination Cell: multi-agency group focused on sharing law enforcement information on cyber-related investigations.

Computer Crime and Intellectual Property Section: DOJ, Criminal Division, Computer Crime and Intellectual Property Section is responsible for prosecuting nationally significant cases of cyber crime and intellectual property crime. In addition to its direct litigation responsibilities, the division formulates and implements criminal enforcement policy and provides advice and assistance.

Cybercop Portal: DHS-sponsored, Cybercop portal is a secure Internet-based information-sharing mechanism that connects more than 5,300 members of the law enforcement community worldwide (including bank investigators and the network security community) involved in electronic crimes investigations.

Law Enforcement Online (LEO):

The FBI provides LEO as national focal point for electronic communications, education, and information sharing for the law enforcement community. The system is intended to provide a communications mechanism to link all levels of law enforcement throughout the United States.

Regional Information Sharing Systems:

The RISS Program is a federally funded program administered by DOJ, Office of Justice Programs, and Bureau of Justice Assistance. The program is comprised of six regional

centers that share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Typical targets of RISS activities are terrorism, drug trafficking, violent crime, cyber crime, gang activity, and organized criminal activities. The majority of the member agencies are at the municipal and county levels; however, more than 485 State agencies and more than 920 Federal agencies also participate.

Sharing National Security Information:

The ability to share relevant classified information poses a number of challenges, particularly when the majority of industry facilities are neither designed for nor accredited to receive, store, and dispose of these materials. Ultimately, HSIN may be used to more efficiently share appropriate classified national security information with cleared private sector owners and operators during incidents, times of heightened threat, or on an as-needed basis. While supporting technologies and policies are identified to satisfy this requirement, DHS will continue to expand its initiative to sponsor security clearances for designated private sector owners and operators, sharing classified information using currently available methods.

6.3.2 United Kingdom

i. Centre for the Protection of National Infrastructure (CPNI)

CPNI addresses the security of process control and SCADA systems in a series of nine nine good practice guidance documents [66] . In the context of the aforementioned documents, Good Practice is defined as '*The best of industry practices such as strategies, activities, or approaches, which have been shown to be effective through research and evaluation.* '[67].

The documents set covers a framework proposed for securing the process control systems from electronic attack. The framework – based on industry good practice from process control and IT security – focuses on seven key themes:

- Understand the business risks
- Implement secure architecture
- Establish response capabilities
- Improve awareness and skills
- Manage third party risks
- Engage projects
- Establish ongoing governance.

The guiding principles at the base of developing the documents are [67]:

1. **Protect** (deploy specific protection measures to prevent and discourage electronic attack against the process control systems) **Detect** (establish mechanisms for rapidly identifying actual or suspected electronic attacks) and **Respond** (undertake appropriate action in response to confirmed security incidents).

2. **Defense in depth**

3. **Technical, Procedural and Managerial protection measurements**

The very first step in risk assessment is 'Understand the business risks'. According to [67] 'before embarking on a programme to improve security, an organization must first understand the risk to the business from potential compromises to process control systems. (…) Only with a good knowledge of the business risk can an organization make informed decisions on appropriate levels of security and required improvements to working practices.'

The business risk is a function of *threats*, *impacts* and *vulnerabilities*.

The report [68] states that 'organizations need to understand the risk that their businesses are facing in order to determine what an appropriate risk appetite (risk level) is, and what security improvements are required in order to reduce the level of risk exposure to align with the risk appetite.' Definitions of the key notions are given in the sequel:

Risk – Possibility of an event occurring that will have a negative impact on the control system. The event may be the result of one threat or a combination of threats.

Risk appetite – The level of risk, used to determine what an acceptable risk is.

Threat – Any circumstance or event with the potential to harm an process control and SCADA system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Likelihood – The probability of a specified outcome.

Impact – The consequences of a threat taking place.

Vulnerability – The degree to which a software system or component is open to unauthorized access, change, or disclosure of information and is susceptible to interference or disruption of system services.

The good practice principles in undertaking a risk assessment of the process control systems are [68]:

Understand the systems – by conducting a formal inventory audit and evaluation of the process control systems. The inventory should contain among others information on the existence, location, role, business and safety criticalities of different components (sub-systems) of the assessed system. In addition the owner, the management, support provider and 'how the systems interact' should be provided for each of the identified components.

Understand the threats – by first identifying and evaluating the threats facing the process control systems. The assessment should be performed threat source – threat manner. Among the threat sources that should be considered are:

- Hackers
- Internal attackers
- Criminals
- Illegal information brokers
- Disgruntled staff
- Staff undertaking unauthorized actions (e.g. accessing the Internet)
- Corporate intelligence
- Contractors
- Foreign intelligence services
- Organized crime
- Terrorists
- Protesters and activists (e.g. environmental, political, animal rights).

The types of threat that should be considered include:

- Worms (generic, targeted)
- Hackers (internal, external, external with insider knowledge)
- Viruses
- Trojans or backdoors
- Bots and spyware
- Loss of integrity
- Loss of availability (denial of service)
- Loss of confidentiality
- Unauthorized control.

The report [68] specifies that 'these threats are somewhat generic so it is useful to consider these into example scenarios so that the impacts and any related vulnerabilities can be considered more specifically, care needs to be taken to ensure that the scenarios chosen are

wider enough to consider all threats.'

Example consequences scenarios include:

- Systemic loss of all machines based on a particular operating system
- Systemic loss of Ethernet/IP networking technologies
- Loss (or reduction) of functionality of process control systems
- Loss of connectivity between the process control systems and
- Corporate networks
- Other systems (e.g. supply chain, laboratory systems or other companies)
- Remote field devices
- Unauthorized change of setpoints or configuration by malicious or inadvertent actions
- Accidental change of system configuration by an authorized user

Understand the impacts – by identifying potential impacts and consequences to the process control systems should a threat be realized, based on the scenarios defined in the previous step. In this phase, each scenario for each site, system or sub system should be assessed by considering what the real life impacts might be, not only on that system, but also for any system that it is dependent upon.

Due to the intrinsic differences between the regular engineering systems and the IT systems, a 'traditional' quantifying the consequences in monetary terms might not be feasible. Thus, the following are provided as examples of possible 'real life' impact descriptions:

Safety, Health and Environmental event or damage to plant: an event that results in harm to individuals, the environment or damage to the plant.

Non-compliance with regulatory requirements or minor Safety, Health and Environmental event: an event that results in the site being non-compliant with regulatory requirements.

Forced controlled shutdown of operations: an event that results in the emergency shutdown system being automatically invoked with no human intervention.

Elected controlled shutdown of operations: an event that results in the site electing to shutdown its operations.

Reduction in operating efficiency: an event that would result in the plant continuing its operations in a less efficient or profitable manner or result in reduced production.

No Impact: no impact on operations.

Other impacts that should be considered are:

- loss of confidential information
- damage to Critical National Infrastructure
- loss of business continuity
- reputation
- value or supply chain.

Time variance of impact: when considering the impact of a particular threat then it is important to consider how that threat might vary with time.

Successive impacts: the effect of coincident or successive impacts should be considered, this is especially important where a common cause failure could be responsible

Understand the vulnerabilities

Understanding vulnerabilities involves a detailed review of all the system elements, (e.g. servers, workstations, network infrastructure etc.) to determine any vulnerability that might exist. Examples of common vulnerability areas include:

- Connections to other systems
- Remote access
- Physical security
- Anti-virus protection
- Access control
- Passwords and accounts
- Security patching
- System monitoring
- System resilience and continuity
- Third parties who produce code for plant systems

i.1 Outputs of understanding the business risk

The key outputs from this are inventory, prioritized sites and systems, list of key threats based on impact assessment, prioritized vulnerabilities.

A different layer assessment approach is proposed for applying this risk assessment methodology [68]. In order to overcome the complexity of large organizations one should first perform a ‘high level risk assessment’, followed by a low-level site/system assessment.

Regarding phase 1, [68] states that ’The first iteration of the risk assessment provides an

enterprise level view of the process control security risk. It will provide an indication of the security gaps with the greatest impact to the enterprise by considering the 'value chain', interdependencies and impacts that have enterprise level significance. The analysis will provide the enterprise with both the priority security issues and the sites that should be addressed first.'

The results of the assessment may be very well suited for being represented in a Boston Grid (risk matrix). This approach eases the priority order identification. Moreover, it is recommended that the risk parameters be plotted in a Site Risk Table (Threat, Attractiveness, and Vulnerability).

Phase 1 plays a key role in Individual sites/systems risk assessment. The low-level assessment builds on the key risk areas prior identified. On this, [68] states that '(…) After selecting the initial site priority for the organization, the same process can be used at a site level to help each site determine their priorities. Each site creates a more detailed inventory and then assesses the individual assets in terms of threats, impacts and vulnerabilities. This way a site can prioritize which assets or services should be tackled first.'

Once an enterprise risk assessment has been carried out a similar process of understanding the systems, threats, impacts and vulnerabilities, should be followed at a site, system and asset level to understand the business risk relating to that level

6.3.3 The Netherlands

i. National Advisory Centre on Critical Infrastructure (NAVI)

In the Netherlands, The National Advisory Centre on Critical Infrastructure (NAVI) has been created as a public-private joint-venture, in order to connect government and business in the protection of the critical physical and digital infrastructure.

According to [69], 'NAVI is intended for anyone with a responsibility for critical infrastructure. As a public-private joint venture, it works with both government and business parties. NAVI targets specific actors:

- managers, including security managers, in business enterprises in the critical sectors;
- representatives of professional associations and industry organizations;
- policy officers at government levels.'

In its security management development mission, NAVI focuses of four core activities:

Advice on security protection to the owners and managers of critical infrastructure in the Netherlands. It conducts risk analyses, issues second opinions on existing security protection plans, evaluates risk analyses of existing and proposed security measures. The service is provided in response to client need.

Knowledge and information exchange on security protection

'NAVI ensures that parties working in the critical sectors in the Netherlands can share knowledge and information.' Contacts with government bodies and business enterprises operating in the critical sectors and with relevant contacts and organizations abroad are established maintained.

Knowledge and information is available by organizing meetings, communicating via NAVI website, and providing access to its knowledge bank.

Product development

NAVI develops products (manuals, solutions) that can be used within entire sectors or even multiple sectors. For instance, it is currently developing a series of manuals on various aspects of security protection.

Networking

NAVI maintains and develops a wide network of contacts among security professionals, and it serves as a meeting point for critical infrastructure parties in government, research and business at home as well as abroad.

NAVI is a product of the National Security Strategy, subject of the next section.

ii. National Security Strategy

In the Netherlands, an 'all risk' approach is taken to tackle the National security. The Ministry of the Interior and Kingdom Relations is in charge with National Security Strategy. The strategy targets the protection of 'society and citizens within Dutch territory against internal and external threats' [70].

The referenced document states that the National security is endangered whenever 'vital interests of our state and/or our society are threatened to such an extent that it might lead to societal disruption.' Moreover, '(…) national security encompasses both breach of security by intentional human actions (security) and breach due to disasters, system or process faults,

human failure or natural anomalies such as extreme weather (safety)'.

The strategy focuses on five facets of security: territorial, economic, ecological, physical, and social and political stability. All of these facets are explicitly used in the recommended risk assessment method.

The document sketches a three stage working method for reinforcing national security [70]:

Stage 1: Analysis of threats and assessment of risks

The analysis and the assessment of the threats in terms of risks to vital interests and a pair-wise weighing of these risks is performed in this phase. The assessed risks are then prioritized for follow-up in the next stage.

The analysis is based on three time-horizons: long term (from approx. 5 years), mid term (up to approx. 5 years) and short term (up to approx. 6 months). This changes the perspective of the analyses from exploratory (long term), to policy-based (mid term) and action-oriented (short term) [70]. The existing sector-oriented procedures are used in analysis and risk assessment; however, the procedures are merged to enable an integral approach.

Stage 2: Strategic planning

In this stage the government determines which capabilities it would require to deal with the prioritized risks and which capabilities it already possesses and/or can expect from external parties such as the business community, social organizations and international organizations.

The strategic planning relies on a capabilities-based approach (capabilities based planning – CBP). According to [70], 'this approach is not geared towards one specific threat or risk. Rather it focuses on what is necessary to prevent the consequences of threats or risks as much as possible (prevention) and/or to be prepared (preparation and response)'.

Stage 3: Follow-up

The political-administrative choices (e.g., policy, legislation and concrete measures) are developed at this level.

For supporting the risk assessment at a national level (Stage 1), the Ministry of the Interior and Kingdom Relations provides methodological guidance in National Risk Assessment Method Guide [71], subject of the next section.

iii. National Risk Assessment Method Guide

This document adopts an all hazard approach for risk assessment. 'Scenarios for floods,

pandemics and long-term failures of utility supplies, for example, and for terrorist attacks are described in an unambiguous manner, backed up by figures, and aggregated.' [71] The advantage of this approach is that the assessment results of intrinsic different systems are rendered comparable, thus making, for instance, prioritizing actions possible.

[71] states that the national security is endangered whenever 'vital interests of the Dutch state and/or society are threatened in such a way that there is a question of - potential - social disruption.' The vital interests are defined as: territorial security, physical safety (public health), economic (undisrupted working of the economy), environmental security and social and political stability.

The suggested risk methodology takes as read that *threats* are described in the form of *scenarios*. According to the referenced document, 'this is the most important information for the application of the methodology; requirements are set for those scenarios.'

Other characteristics of this method are given in the sequel [71]:

- despite the 'all hazard' approach, some distinctions must be made between *natural threats (hazards*, in the form of flooding, for example) and those triggered by humans, *malicious threats* (*threats,* in the form of terrorist attacks, for example);
- the method is scientifically sound, and consists of a combination of existing, proven parts of methodologies, as well as new elements that have been developed to meet the requirements of the national risk assessment;
- the method is as transparent as possible, seeking a balance between comprehensibility and simplicity on the one hand, and on the other hand the capability to facilitate what is, in itself, a complex assessment;
- the method offers the ingredients and the methodology to rank scenarios from a multidisciplinary perspective by risk, leaving scope for administrative input about what is considered more or less important and for other aspects of policy judgment;
- an analysis of the sensitivity of the results to changes in seriousness and importance judgments is part of the NRA.

Risk is defined as a composition of the *impact* (total of the consequences of the incident scenario) and *likelihood* (a forecast about the occurrence of the incident scenario).

The risk is computed based on an Incident scenario. A scenario should fulfill the following requirements: plausibility, relevancy, consistency, usable, time related. Thus, a scenario:

- must be a plausible story, with factual supporting information; or, put another way, a report on events that may occur in the (near) future;
- must be relevant to the objective of the scenario analysis and representative for one of the security topics selected;
- must be consistent and logically structured;
- is mentally usable and therefore can be explained to and is acceptable to others;
- includes the time horizon and the policy field or security topic to which it relates, including specific questions that are on the agenda.

In the national risk assessment context, a scenario is a description of [71]:

- (the nature and scale of) one or more related events (incidents) which have
- consequences for national security;
- the lead-up to the incident, consisting of the (underlying) cause and the *trigger* which actually brings about the incident;
- the context of the events, indicating the general circumstances and the degree of vulnerability and resistance of people, object and society, where relevant to the incident described;
- the consequences of the incident, indicating the nature and scale;
- the effects of the incident on the continuity of critical infrastructure.

More specifically, each scenario must contain information about:

- pressure on the physical environment;
- pressure on (critical) infrastructure;
- the pressure on people and society with particular attention to aspects of trust by the population, foreknowledge by the population about risk and institutional embedding;
- pressure on institutions and government.

A list of different impact criteria is also provided in the referenced document [71] for guidance purposes. Once the scenario set is ready, the assessment methodology goes as follows [71]:

Step1 – Check on completeness of the scenario description.

The scenario must contain the information enabling assessment of the impact and the

likelihood.

Step 2 – Assess the impact of the scenario.

Each scenario is analyzed and assessed impact criteria. The impact criteria are directly related to the five vital security interests. The individual impact scores are merged into a (qualitative and quantitative) final score per scenario. The multi-criteria analysis that is necessary for this step does, in itself, require that a number of steps be gone through.

Step 3 – Assess *the likelihood of the scenario*.

Each scenario is analyzed and assessed on the likelihood of it occurring. In doing so, a distinction is made between scenarios describing a natural form of hazard (and where it is plausible that historic data is available to some extent), and scenarios describing a threat caused deliberately (and where it is plausible that an assessment of likelihood must be based mainly on intelligence and forecasts). The likelihood is expressed at least qualitatively and wherever possibly quantitatively.

Step 4 – Assess the risk of the scenario.

A risk matrix is proposed for this task. Assessments of the impact and likelihood of all scenarios are brought together in a two-dimensional risk diagram. Based on this diagram, a clustering by priority can be shown. For the impact assessment, in particular, sensitivity analyses are used because there is a high level of subjectivity in assessing the degree of impact and relative importance of the various types of impact.

Step 5 – Presentation of the analysis result.

Despite the aggregated character of the risk, and the associated classification into priority clusters, attention must also be paid to the underlying findings. These include, in any case, mentioning the most basic “impact drivers” per scenario and indicating the robustness of the final score on impact.

The end product of the risk assessment is a report to the Cabinet. This report contains the following sections:

- a description of the scenarios used;
- a description of the methodology used;
- a report on the findings, including the scenario assessment and scores;
- a recommendation to the Cabinet about capabilities that should be incorporated into

the strategic planning as a priority (put on the agenda);

The report meets the following quality requirements [71]:

- the incident scenarios are described uniformly (according to a format), they are possible, and can vary in seriousness from fairly serious to the worst imaginable;
- the incident scenarios are practical, to the extent that it is possible to derive planning assumptions for the strategic planning. This means that based on the scenario, it is clear which capabilities will have to be used;
- the guide gives an accessible, transparent description of the methodology; • the methodology maintains a good balance between transparency, practical usability and scientific substantiation;
- the methodology must be suitable to compare incident scenarios (as a translation of the risks) against each other, based on criteria derived from the vital interests of national security;
- the method indicates how the criteria can be made operational.

6.3.4 Sweden

In Sweden, risk and vulnerability analyses must be conducted by all governmental agencies. The assessment must be carried out in accordance to the ordinance on emergency preparedness and heightened state of alert [71].

According to section 9 of the Emergency Preparedness Ordinance [71], governmental agencies shall – for the purpose of strengthening both their own and society's emergency preparedness – conduct annual analyses of whether vulnerabilities, or threats and risks, exist within their areas of responsibility that could severely degrade operational capabilities. In conducting this analysis, special consideration shall be taken to:

- situations that arise quickly, unexpectedly and without warning, or a situation in which there is a threat or a risk that such a situation can arise.
- situations that require rapid decisions and co-ordination with other parties.
- that the most necessary critical societal functions can be maintained.
- the capability to deal with very serious situations within the agency's area of responsibility.

The document mainly deals with governmental agencies being able to guarantee that they

can maintain functions that are needed to uphold emergency preparedness capabilities, even when exceptional events occur. Both cases, ordinary operations and exceptional events should be taken into account when dealing to risk assessment [72]. According to [72], '…this can entail that requirements that are sufficient for ordinary operations are not sufficient when exceptional events occur, and that the agencies therefore require enhanced capabilities, such as expanded command and information capacities.'

[72] also states that '(…)To improve society's collective capabilities to prevent or reduce the effects of exceptional events, it is important that we have knowledge of what the threats and risks are, and where society is vulnerable.'

The purpose of the assessment is to enhance Sweden's capabilities in emergency preparedness and response.

The agency level assessments are compiled and analyzed by the Swedish Emergency Management Agency (SEMA). SEMA also provides 'Risk and vulnerability analyses' [72] as a guide for assessment methodology to be used at agency level.

We list in the sequel the definition of the key notions addressed by the aforementioned document. The relevance of those is to express the position Sweden takes towards the considered issues. Thus,

Exceptional event is an event that deviates from the norm, which entails serious disruptions or impending risks for serious disruptions to critical societal functions, and that requires prompt responses.

Capability in this context refers to the robustness and capacity that is needed to avoid and deal with serious emergencies.

Crisis management capability refers to an organization's capability during serious disruptions to lead its own operations, to make decisions within its area of operations or responsibility, to quickly distribute correct and reliable information, and when necessary, to be able to co-ordinate with other parties and their actions.

Operative capability refers to the capability that entities deployed "in the field" need to initiate and conduct the measures required to assist, protect and lessen the effects of that which has occurred as quickly as possible.

The capability in critical societal functions to resist serious disruptions refers to the capability needed for operations to be conducted at such a level that society – despite a

serious disruption – can still function and ensure fundamental service, security and care.

Threat embraces an entity's capacity and intention to conduct destructive actions. A threat can even consist of an event or phenomenon that in itself produces danger to something or someone without there being entities with the capacity and intention to cause damage in the context.

Critical dependency is defined as a relationship in which the dependent organization is quickly and lastingly affected by a substantial decline in function during a reduction or severe disruption in the providing organization. Conditions for critical dependencies are:

- the providing organization cannot be easily replaced with another organization
- the societal consequences of the dependent organization's functional reduction become sufficiently serious that the current emergency cannot be dealt with in an acceptable manner.

Risk can on a purely technical plane refer to a weighing of the probability that an event will occur and the (negative) consequences that this event can produce. In relation to threats, a risk is to be viewed as a more concrete effect of various occurrences. Climatic changes (threat) can, for example, entail an increased probability for, and greater consequences of, for widespread flooding (risk).

Risk analysis can be described as a systematic method of identifying risks and evaluating them with regard to probability and consequences.

Vulnerability denotes how much and how seriously a society or parts of a society are influenced by an event. The consequences that an entity or society – despite certain capabilities – does not manage to foresee, handle, resist or recover from indicates the degree of vulnerability.

Vulnerability analysis can be described as a systematic method of evaluating and determining vulnerability.

SEMA's proposes a 4 steps approach to enhancing the nation's emergency preparedness:

- Identification of threats and risks
- Evaluation
- Capability assessment
- Results and reporting

- Identification of threats and risks

Identification is to be based on a governmental agency's area of responsibility. It is important to identify threats and risk within the agency's area of responsibility that other entities are expected to deal with. In a corresponding manner, it is important to include threats and risks beyond the area of responsibility but that can nonetheless affect the agency's function.

According to [72] the objective of identifying threats and risks are:

- increase a governmental agency's knowledge and awareness for the purpose of strengthening its own and society's emergency preparedness;
- find the reasons and conditions that permit an event to escalate into a situation that seriously degrades the capacity for operations in an area;
- discover critical dependencies within and between sectors and geographic areas.

Evaluation of threats and risks

The process in this step follows the 'classic' approach of risk assessment: evaluate the frequency and the consequences of a disruptive event, and then aggregate the results to obtain the risk in a quantitative or qualitative manner.

The frequencies may be evaluated both by quantitative and qualitative approaches. The quantitative approach should be used when empirical estimates (based on, for example, statistical material) are available. On the quantitative assessment [72] states that '(…) In many cases, expert assessments must be used to estimate probability, either to complement empirical data or as the sole relevant source. Probability is assessed based on the subjective estimates of persons with good knowledge of the pertinent conditions.'

Assessing consequences concerns predicting the direct and indirect (negative) effects that can arise based on certain given conditions [72]. There are cases when qualitative descriptions of the consequence are sufficient. However, in some other cases, quantitative consequences in regard to, for example, number, scope or size is required for a sustainable assessment. SEMA proposes a 5 levels scale for qualitative consequence characterization, as follows:

Level 1 – Very limited consequences

Minor direct health effects, very limited disruptions to societal functionality, passing distrust of single societal institution.

Level 2 – Limited

Moderate direct health effects, limited disruptions to societal functionality, passing distrust of several societal institutions.

Level 3 – Serious

Significant direct or moderate indirect health effects, serious disruptions to societal functionality, enduring distrust of several societal institutions or changed behavior.

Level 4 – Very serious

Major direct or significant indirect health effects, very serious disruptions to societal functionality, enduring distrust of several societal institutions or changed behavior.

Level 5 – Catastrophic

Catastrophic direct or major indirect health effects, extreme disruptions to societal functionality, firmly rooted distrust of societal institutions and general instability.

Risk evaluation is intended to rank the threats and risks that have been assessed based on probability and consequence. To make an evaluation more easy to survey, [72] uses classes in which both the probability and the consequence are assessed on a scale from one (very low probability) to five (very high probability).

According to [72], '(…) By presenting the results in a matrix, we show how risks relate to one another in an easy-to-grasp manner. This facilitates matters for other entities in easily utilizing the results of a governmental agency's evaluation.'

Capability assessment and analysis of vulnerability

'That an agency assesses its capability is thus a central aspect in a risk and vulnerability analysis. By taking measures to improve its capability, an agency can consequently contribute to reducing society's degree of vulnerability' [72]

The capability that is needed to avoid and deal with emergency preparedness capability consists of three components:

- crisis management capability;
- operative capability;
- capability to resist serious disruptions in critical societal functions.

The governmental agencies should assess these three capabilities for all identified risks. The method proposed is based on indicator sets. [72] proposes three sets of indicator for *Crisis*

management capability, *Operative capability*, and *Capability to resist serious disruptions* in critical societal functions

The main advantage of using the same indicator sets is – according to SEMA – that it makes it easier to compare agencies' capability assessments with one another and over time, even thou the relevance of individual indicators vary from agency to agency and from scenario to scenario.

In SEMA approach, after relevant indicators have been selected for a particular situation, the next step is to "rate" the capability. The recommended procedure is to use a four level capability assessment scale. The agency capability is thus classified as [72]:

Level 1 – Capability is good

Level 2 – capability is primarily good, but has some deficiencies

Level 3 – There is a certain capability, but it is insufficient

Level 4 – There is no or insufficient capability.

The assessment resulting data is used by SEMA to compile a comprehensive picture of how capabilities can be developed within various areas from year to year, to make comparisons between different agencies and sectors, and to weigh together the various agencies' assessments into a collective assessment of society's capability.

7 COUNTERMEASURES

In light of what presented in the previous section, it is evident that Power Systems need to be protected against potential cyberattacks. In this section we identified a set of security countermeasures for each class of vulnerabilities described in the previous section.

7.1 Communications protocols countermeasures

Communication protocols are the core of every ICT infrastructure. They are the means for providing distributed services, remote management services, data sharing etc. Unfortunately, as describe in the previous section, can be, and indeed are, used as target of attacks or as vehicle put under attack a third target. Several of the traditional ICT countermeasures involve the enforcement of the communication protocols. Taking as example the attacks presented in section 4, several of them would be seriously limited by introducing in the used protocols some “integrity, confidentiality and authentication” mechanisms. Unfortunately in the context of Power Systems and especially for process networks/SCADA systems, these mechanisms are not always easy to be deployed for several reasons:

- *Real-Time constraints*: the use of encryption mechanisms introduces delays in the communication channel; such delays, in strong real-time environments might not be well tolerated
- *Computational Constraints*: signature/verification operations are usually computationally demanding. Devices as PLCs traditionally have low power computation, making hardly feasible the use of traditional encryption schemas such us RSA.
- *Key management*: the management of the encryption keys (from the distribution to the revocation), and the use of Key Management Systems not trivial in a fully distributed infrastructure as the network of PLCs of an Energy Grid. Again here also the computational constraints play a relevant role.
- *Integration in the existing infrastructure*: the integration of these new mechanisms into the existing infrastructure is not trivial, implying systems stops, reconfigurations etc. impacting heavily on the economical aspects of the management of the Energy System.

In the following we present an overview of the different countermeasures related to the communication protocol vulnerabilities

7.1.1 TCP/IP countermeasures

TCP/IP protocols are quite vulnerable to classic attacks, such as man-in-the-middle, replay etc. This is due to the intrinsic lack of authentication mechanisms embedded into the protocol itself. These vulnerabilities are obviously not acceptable in SCADA systems, which need to be secure. Luckily there exists a huge scientific and technical literature about the protection of TCP/IP flows from these vulnerabilities. These protection techniques are part of the encryption tunneling family. In other words, in order to protect a network flow, it is sufficient to insert it into an encryption tunnel between the sender and the receiver. In this way: (a) only the receiver will be able to understand the contents of the flow, (b) nobody will be able to modify the packets sent, and (c) nobody will be able to reuse packets (is the encrypted tunnel include also time-stamp mechanisms).

In the case of a typical energy system architecture, as will be showed in the following section on Filtering, this kind of solution is usually applied in order to create secure channels between the PC of operators located in the intranet and the process network firewall, and between a remote site and the local intranet of a plant hosting a SCADA system.

These secure channels are also known as point-to-point (or Site-to-Site) Virtual Private Networks. They can be built adopting several techniques. IPv6 supports these mechanisms, but the same performance can be used adopting IPsec (an extension of IPv4). Alternatively a cheaper, but less efficient (in terms of performance) solution could be built creating a VPN based on SSL/TSL [89] [90] channels. For a full reference about the TCP/IP cryptographic based enforcing mechanisms, we point the reader to [91] below.

The use of secure mechanisms for protecting TCP/IP flows is a quite well established practice; however, as claimed in the introduction of this section, these mechanisms are conceived for general purpose ICT systems. In other words, while they are normally applied in the upper ICT layers of the Power Energy Infrastructure, they can be hardly used, as they are, in the lower layers (e.g. the SCADA network and the field network).

7.1.2 SCADA protocol countermeasures

In the last years the scientific community finally acknowledged the need for more secure SCADA protocols. Several variations of the classical SCADA protocols embedding security features have been recently proposed:

- Secure DNP3 [92] below
- DNP3Sec [93] below
- AGA12 [94] below
- Secure Modbus [95] below

As described in the introduction of this section, a not negligible problem is related to the key management system (KMS)
Some initiatives related to the KMS infrastructures exist in the Energy Field:

- Working Group 15 of Technical Committee 57 of the International Electrotechnical Commission (IEC) presented a standard for the cyber-security of the electric system [102] below. The document do not indicates explicitly a KMS architecture, but defines some key design aspect related with it.
- The IEEE PESS Committee presented a draft for the “Trial Use Standard for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access”. The document describes some KMS functional requirements [88] below.

The use of these secure protocols would make harder the successful attack of SCADA systems, i.e. the lower e most vulnerable levels of the Power System. However, it has to be remarked that the integration of the new secure protocols into existing architectures is not painless and in several cases would not be possible at all, requiring a complete re-engineering of the process system. Challenges in this field might be identified in the development of light-weight secure mechanisms limiting as much as possible the impact of the additional cryptographic layer on the performances of the SCADA system.

7.2 Filtering Countermeasures

A quite common security arrangement for ICT based industrial systems is to isolate the different logical area by means for dedicated firewalls. This approach is not effective for the industrial part of power systems, since modern firewalls are not able at the moment to analyze in deep SCADA protocols.
Thus, from a theoretical point of view, a SCADA system should be a closed system controlled only by trusted elements. Unfortunately, as described in [96] below for maintenance purposes the process network might need to be accessed from external elements (e.g. remote operators, vendor support services etc.). That means that the process network and the

external network are in some way connected, i.e. there exists, even if limited, a communication channel between the SCADA system and a potentially hostile environment. A firewall, or a firewalling architecture, is then needed to create filtering between the external network and the process network. In the literature some guidelines for configuring firewall in SCADA environments have been released in the past, for example the *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks* [97] below and the *NIST Guide to Industrial Control Systems (ICS) Security* [98] below. Both documents provide overviews of the typical infrastructures of a Process Control Network, presenting a set of traditional firewall best practices adapted to those particular infrastructures.

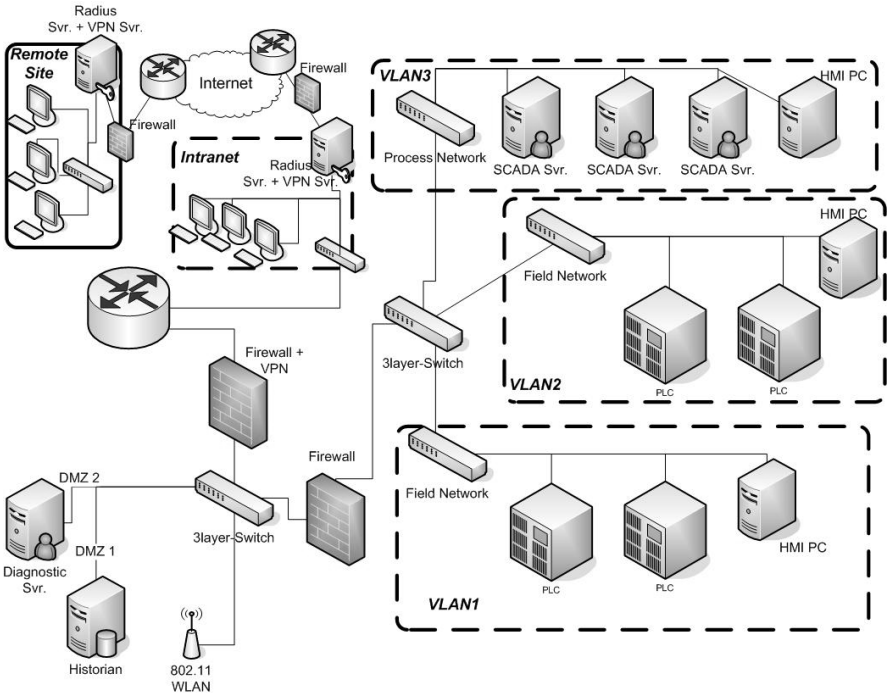


Fig 6. - Firewalling Architecture

Figure 6 shows and example of firewalling architecture for Industrial Systems. As it is possible to see, operators hosted in a remote site can connect to the local Intranet through a site-to-site VPN, showing their credentials to a Radius authentication server. Moreover, also in order to access the plant networks (DMZs, process and field networks), the operators hosted in the Intranet, will need to authenticate themselves to the VPN-firewall, which will also permit the creation of a host-to site VPN connection between the PC of the operator and the firewall. In this way the access to the plant networks is indeed extremely hardened.

While modern firewalls are extremely advanced when analyzing traditional ICT traffic, they are not able to analyze in depth SCADA protocols. In this field Byres proposed a solution [99]

below aiming at enforcing the SCADA architecture by filtering at low level each single packet sent to a target PLC/RTU. This approach can provide a good low-level of protection; however, still an open issue remains related to more complex and subtle attacks. In order to better understand the problem, let's consider the following example: we have a system with a pipe in which flows high-pressure steam. Two valves (1 and 2) regulate the pressure. An attacker connected to the process network sends a DNP3 packet to the PLC controlling valve 1 in order to force its complete closure and a command to the PLC controlling valve 2 in order to maximize the incoming steam. It is evident how such commands, when considered locally, will result perfectly legitimate, while jointly will bring the system to a critical state. In order to mitigate this risk, it is necessary to provide the firewall with a detailed, explicit knowledge of the SCADA system under analysis (components, commands and critical states). The area of industrial processes, although extremely complex from an architectural point of view, has the advantage to be extremely structured and well defined. Nai et al [95] below, present an innovative filtering technique for industrial protocols based on the state analysis of the system being monitored. Since this approach focus its attention on the system behavior rather than on modeling the behavior of the possible attackers, this approach enables the detection of previously unknown attacks This kind of approach seems to promise good results in fighting against SCADA ICT attacks.

7.3 Monitoring

Firewalls are powerful security protections, but the way in which they work is quite invasive (they have to stay physically in the middle of a communication channel in order to be effective). In some places, for example in the field network, and in some particular situations, the delays introduced by the presence of firewalls, especially in real-time networks, might create unwanted problems. For that reason in the last ten years firewall architectures have been combined with Intrusion Detection Architectures (IDS).

IDS techniques have as main characteristic that of being passive, i.e. they analyze the behavior of networks or of PCs in a silent way, without excessively interfering with the environment under control.

Traditionally, IDS techniques can be classified in two families on the basis of the source of information to be analyzed:

- Network IDS: sensors analyzing network flows in search of attack proofs
- Host IDS: sensors installed on a target server, which analyze the operation it performs in

search of malicious behaviors.

Unfortunately, host based IDS are quite invasive since they need to be hosted by the same system being monitored. For that reason, for SCADA systems, one should prefer to use NIDS (with obviously exceptions in particular cases).

IDS can be also classified according to the techniques used to identify the threats:

- Signature based IDS, which compare the information gathered with signatures which characterize the target attacks
- Anomaly based IDS, which compare the actual behavior of the system with a “behavioral template” in search of deviations from the normal profile, i.e. in search of anomalies.

Both techniques can be used in power systems, the first in order to quickly identify known attacks, limiting the risk of false positives; the second in order to identify unknown attacks.

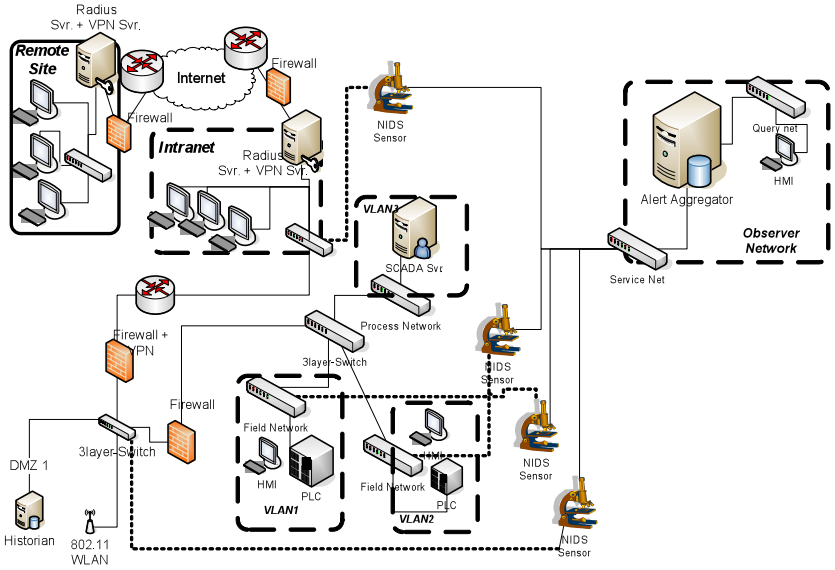


Figure 7. Monitored Architecture

Figure 7 "Monitored Architecture” shows a networked architecture for SCADA systems integrating Intrusion Detection Sensors.

Ideally, the Observer Network interconnects the different sub-networks of the system with the sensors and with the Alert Aggregator. Roughly speaking, that means to connect the switches, the sensors, and the database.

Modern Intrusion Detection systems are quite mature regarding the detection of traditional ICT threats and attacks; unfortunately, they are generally unable to analyze SCADA protocols (e.g. Modbus, Profibus, DNP3 etc.). For that reason some attack profiles, properly crafted in order to take advantage of the vulnerabilities of those industrial communication

protocols, cannot be easily detected. For example, if a malicious user, able in some way to have access to the process network, starts sending legitimate Modbus packets to a pool of slaves (i.e. PLCs) attempting to change the state of the system, a traditional IDS will not be able to detect it since the Modbus packets, (contained into the payload of a TCP packet) are just “meaningless payload” for that IDS.

Only recently some extensions, for example for Snort (a well known IDS), have been developed in order to allow IDSs to analyze single packets [100] below. However, also in this case, more complex and articulated attacks, will not be understandable for those IDS, that cannot decipher that a chain of legitimate commands would drive the system into a critical state. In other words, not knowing what is the current state of the monitored system, and IDS will hardly able to understand if an apparently licit command can, indeed, be considered, under particular system conditions, dangerous. In order to solve this problem, Nai et al. have developed a State Based Intrusion Detection System for SCADA systems, which can identify, by analyzing chains of SCADA commands, whether a system is maliciously evolving from a safe state to a critical state. This approach permits to detect new and unknown attacks, since the attention is given not to the way in which the attack is conducted but to the state in which the system is evolving [101] below.

As described in the previous sections, Energy Systems are quite complex, distributed and composed by a huge amount of heterogeneous elements. Traditionally all these properties are also those considered the most undesirable from an IDS perspective. In fact, the more the system is huge and heterogeneous, the higher is generally the probability of making the IDS generate false positives and generally speaking “alert noise”. In order to make IDSs effective in protecting this kind of systems, it is then needed a set of multilayer aggregation features to correlate events generated from different sources (e.g. correlating events coming from the process network of a remote transmission substation with events coming from the office network of a control center) in order to detect large scale complex attacks. This probably represents the next research challenge in this field.

7.4 Software Management and Update Mechanisms

Several attacks exploit known vulnerabilities and bugs of software. For this reason, software management and update procedures are necessary to avoid or recover from security problems. The proactive management of vulnerabilities and related patches aimed at

reducing or preventing their exploitation. This management should be more effective, requiring less time and effort than recovering the system and responding after some exploitation has been performed.

Organizations should provide documentation providing the software patching and hardening policy for theirs systems. The policy should be reviewed every year in order to address new threats and discovered vulnerabilities. The policy has to be consistent, for example software patching cannot reinstall software removed for hardening the system, or change security setting, and so on.

A typical model of systematic software patching is based on a pattern cycling through four phases:

- Assessment and Inventory, aimed at identifying, classifying and assessing the software components of the system, possible security threats and vulnerabilities, and determining the most appropriate policy the organization can apply for software update and vulnerabilities discovery.
- Patch Identification, for identifying software updates available, understanding their relevancy and effectiveness, and determining the urgency of updates (i.e. response to security emergency or normal software update).
- Evaluation, Planning and Testing, aimed at i) deciding which patches are to be deployed in the operational environment, ii) planning when and how to perform software updates, and ensuring that the software update fulfills the system requirements, without compromising its business and operational aspects; and finally iii) testing the proposed patches in a realistic setting for verifying the potential negative effects onto the system.
- Development, aimed at actually carrying out the software updates in the operational environment, minimizing the impact on the system.

A rigorous qualification of the software used, as well as its security conformity certification (performed by third party certification laboratories and authorities) might also be considered a way for enforcing the security of the Power System. In the same way, the adoption of an Information Security Management System (ISMS) such as the standard ISO 21001, can help in adopting a systematic approach to the management of the cyber security of Energy Systems.

8 Cybersecurity scenarios

The following four sub-sections detail potential attacks to generic power systems. They are based on past cases and knowledge developed by the JRC in its Testbed for Industrial Networking Security (TINS), in its Ispra site.

8.1 Attack Scenario 1 –Master Emulation

Scope:

To damage the electrical power transportation system, interacting with PLC of the field network controlling the dispatch of the energy.

Prerequisites:

1. Access to the process/field network of one of the transmission stations
2. Knowledge of technical aspects of networking, hacking and Process Engineering.

Tools required:

1. ARP Poisoning tool (e.g ettercap)
2. SCADA protocol sniffer (e.g. CS-IDS)
3. PLC software simulator
4. Scada Master software emulator

Attack Description

In the following, we describe the relevant steps of the attack evolution:

1. The attacker gets access to the process network or the field network of a transmission center (i.e. one of the control centers managing the physical devices – such as substations, switches, etc. – that maintain in a working state the power transmission grid). The access can be obtained in different ways, for example:

    a. The attacker obtains, using a set of social engineering techniques, the credentials of some operator having access to a machine on this network.
    b. The attacker breaks the security of a machine on this network (e.g. if having physical access, using live CDs for mounting another operating system on the

target machine, and from this environment stealing the user credentials or directly mounting the attack)

c. The attacker obtains access to one of the network switches and connects directly to this machine its own pc (notebook/chip PC etc.)

2. The attacker installs an ARP poisoning tool on the exploited machine, and starts to poison the ARP tables in order to receive the traffic sent by the Master. If the Attacker has adopted the technique 1.c, he can try to obtain the administrative credentials of the switch and configure one of its ports as Mirror port, to receive directly all the traffic flowing through the network in a completely seamless way.

3. The attacker captures a portion of traffic flowing through the network and then stops the ARP attack.

4. The attacker analyzes the traffic and reconstructs the field network topology and the functionalities provided by the field devices (this point can be skipped if the attacker, being an insider, already know these details)

5. The attacker installs the PLC simulators on the machine and configures them according to what discovered from the previous analysis.

6. The attacker installs on the machine the SCADA Master emulator and configures it in order to be able to interact with the real PLCs on the network.

7. The attacker run the ARP poisoning attack, launching it in between the SCADA master and the slaves. More in detail, the following example the steps required for this attack. Let's assume that the situation, before the attack, form a network point of view is the following:

   a. Attacker: IP = 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
   b. Master: IP = 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
   c. Slave: IP = 192.168.1.88, MAC = 00:00:00:LL:LL:LL

   The ARP caches in each host before the attack are the following:

a. For the attacker:
    i. 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
    ii. 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
    iii. 192.168.1.88, MAC = 00:00:00:LL:LL:LL
b. For the Master:
    i. 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
    ii. 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
    iii. 192.168.1.88, MAC = 00:00:00:LL:LL:LL
c. For the slave:
    i. 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
    ii. 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
    iii. 192.168.1.88, MAC = 00:00:00:LL:LL:LL

To perform the ARP poisoning, the attacker will send a set of ad-hoc forged ARP reply packets: to the Master it will send a reply containing the IP address of the slave (192.168.1.88) but having the MAC of the attacker (00:00:00:ZZ:ZZ:ZZ); and to the slave, it will send a reply with the IP address of the Master, but, again with its own MAC address (00:00:00:ZZ:ZZ:ZZ). In this way, the attacker will be able to receive the packets sent by Master and slave, and impersonate the slave in front of the Master and the Master in front of the Slave. Obviously, since on average every 10 seconds the cache is cleaned, the attacker should send multiple packets of this type to the victims in order to keep the cache poisoned. In summary, after the attack, the ARP caches on each machine will be the following:

a. For the attacker:
    i. 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
    ii. 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
    iii. 192.168.1.88, MAC = 00:00:00:LL:LL:LL
b. For the Master:
    i. 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
    ii. 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
    iii. 192.168.1.88, MAC = 00:00:00:ZZ:ZZ:ZZ
c. For the slave:

iv. 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
v. 192.168.1.13, MAC = 00:00:00:ZZ:ZZ:ZZ
vi. 192.168.1.88, MAC = 00:00:00:LL:LL:LL

8. The PLC simulator start to answer to the requests of the Master, providing false information about the state of the system

9. The Master Emulator starts to send commands to the real PLCs. In this way, it will cause a direct effect on the activity of the field network. In this scenario, the attacker would be able to send extremely dangerous commands to the PLCs, which can for example disconnect a line of the transmission grid, or introduce oscillations on the power line. These actions can in some cases trigger some protection mechanisms that might, for safety reasons, disconnect a certain line. This might be a safe state in reality, but the PLC emulator could present it to the Master as highly damaged, provoking a wrong reaction by the operators of the system.

Considerations

This scenario shows how it is possible to have direct access to field devices. SCADA technologies are extremely weak from the security viewpoint. SCADA protocols (DNP3, Modbus, Profibus, OPC, IEC 60870-5/6 etc.) are used by field RTUs and PLCs to remotely exchange data and commands with the supervisory system. They constitute the “backbone” of every industrial system; in fact, it can be said that the “last mile” of the control flow in Power Systems is embedded into a SCADA protocol flow. The porting of SCADA protocols over TCP/IP has obviously introduced new layers of complexity for reliably managing the delivery of control packets in an environment with strong real-time constraints.

In addition, it has opened new possibilities to attackers motivated to cause damage to target industrial systems. In particular, those protocols in their original formulation:

- Do not apply any mechanism for checking the integrity of the command packets sent by a Master to a Slave and vice-versa.
- Do not perform any authentication mechanism between Master and Slaves, i.e. every item could claim to be the Master and send commands to the Slaves.
- Do not apply any anti-repudiation or anti-replay mechanisms.

These security shortcomings can be used by malicious users for attempting to carry out

different kinds of attacks.

In a smart grid context, these attacks can have devastating effects, not just impacting onto the industrial actor directly hit, but also across the whole set of interconnected actors due to cascading effects. In addition, considering that in smart grids, loads and prices will be affected by real-time issues, event the minor attack could also disturb the running of the related markets. Most worrying is the fact that different operators use the same technology. In this way, the attack can be replicated in similar systems, which by definition will have similar protection levels.

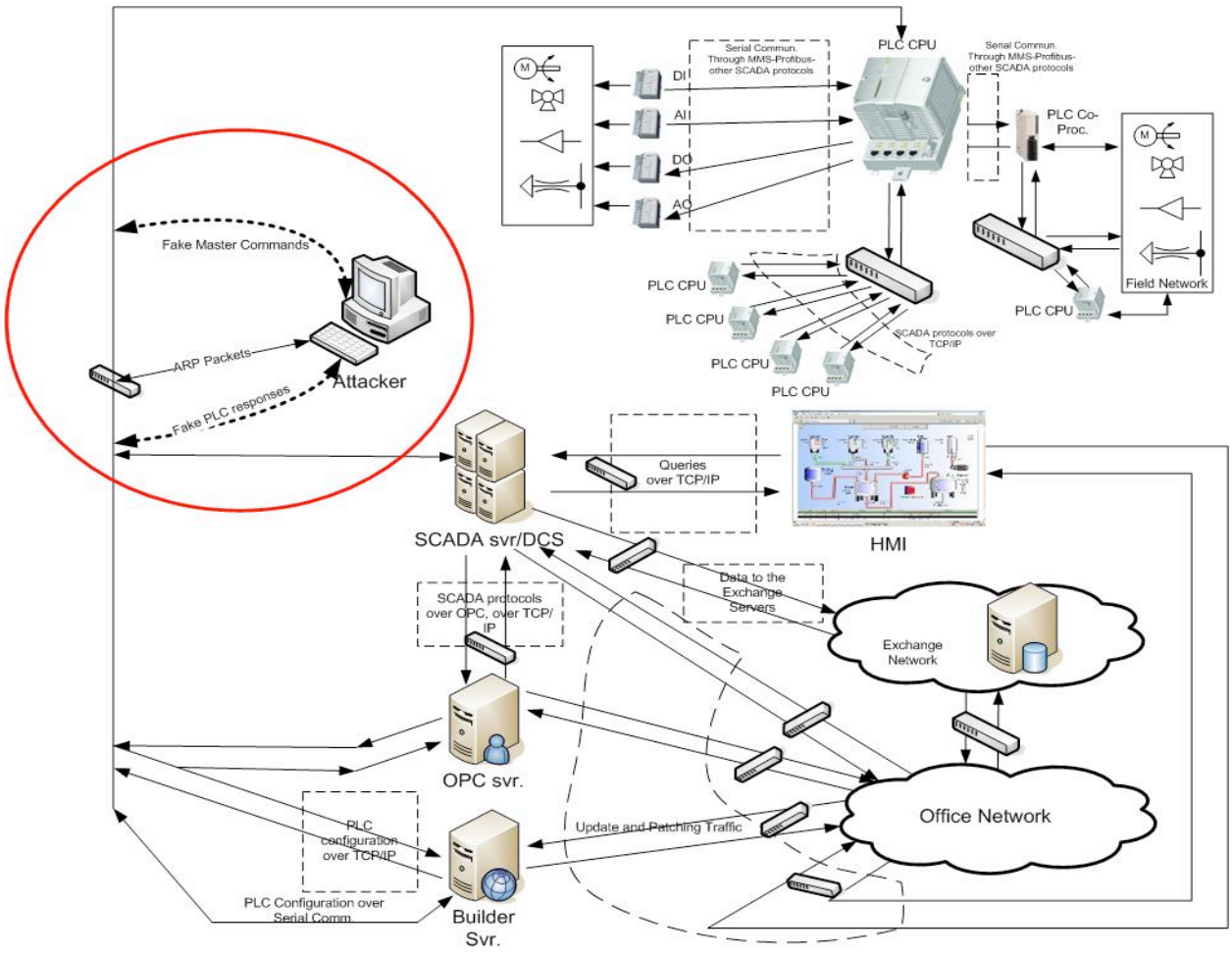


Figure 8 - Attack scenario 1

8.2 Attack Scenario 2 – Protection PLC Corruption

Scope:
To change the configuration of the field devices protecting the dispatch of the energy.

Prerequisites:

1. Access to the field network of one of the transmission stations
2. Knowledge of technical aspects of networking, hacking and Process Engineering.

Tools required:

1. Builder Server emulator

Attack Description

This attack is a variation of the attack scenario n. 1. Also in this case, it is required to gain access to the field network. Moreover it is needed to have some knowledge of the system configuration. This knowledge can be obtained as described in the previous section, or it can be already in possession of the attacker (considering that he might be an insider).

The field network is composed of PLCs and RTUs. These devices usually contain a set of pre-installed programs, which how the device should behave/react to some events (e.g. if the digital input has a certain value -i.e. a switch is opened- and another indicate a value bigger than 25 -i.e. the temperature of a line is higher than X- then write 0 on the digital output 5 (i.e. close the switch-). This type of "programs" is usually written off-line on a "Builder server" (for example through a Ladder Logic, or a block diagram program) and then, through a point-to-point Ethernet connection (or serial connection), downloaded on the PLCs. In this attack scenario, the attacker has the knowledge and resources for writing his own "PLC programs", and then, having access to the field network, he is able to download the new PLC configuration on the target PLCs.

This kind of attack requires a deep knowledge of the target field network, and the technical skill for programming the PLCs. However, on the other side, it is extremely difficult to detect it. The new code inserted into the PLC behaves as the original one. It can stay latent for a long time, and then, may be in correlation with some external trigger (a certain value of power

needed on the grid or some kind of similar trigger), behave in a completely unpredictable (for the operators) manner. This is the most typical case of “byzantine failure” applied to power grid ICT control systems.

An example of the criticality of this attack could be the following:

1. The attacker in a first stage accesses the field network of a crucial node of the transmission system, and, by using a builder server emulator, copies the code installed on the PLCs responsible for the control of the grid protection mechanisms. These, for instance, are the protection devices in charge of taking the proper actions to protect the network from the effects of energy peaks.

2. The attacker modifies off-line the code of these PLCs, with new instructions that can disable the protection routines, or trigger an incorrect behavior.

3. The attacker access for the second time the field network, and installs the new code in the PLCs.

The PLCs will behave as usual in normal conditions, but at the first occurrence of the critical state for which they should activate the protection routines, they will react according to the new incorrect logic. This might drive the power transmission system into an unstable state.

When the corrupted PLC protects a critical sector of the power system, the effects can be extremely dangerous,. Moreover, this attack scenario could be seen as a component of a more complex attack, where several protection, automation and control PLCs have been corrupted, and concurrently triggered at some particular state of the system.

Considerations

This scenario shows how some sophisticated attackers with knowledge of the system can affect their same protection. This situation is directly related to safety and reliability considerations, with potential serious economic impact for the operator of the installation.

Compromising the Process network enables the attacker to potentially take full control of one (or more) portions of the Power System. From there, all types of malicious actions are possible.

In consideration of smart grids, one has to consider that in their multi-tier architecture the malfunctioning of one system can escalate to the whole tier and onto the whole grid. More importantly, the compromise of one node that receives sensitive information from other nodes might have serious implications beyond the disturbance of the operations. Also here, common vulnerabilities should be a main concern.

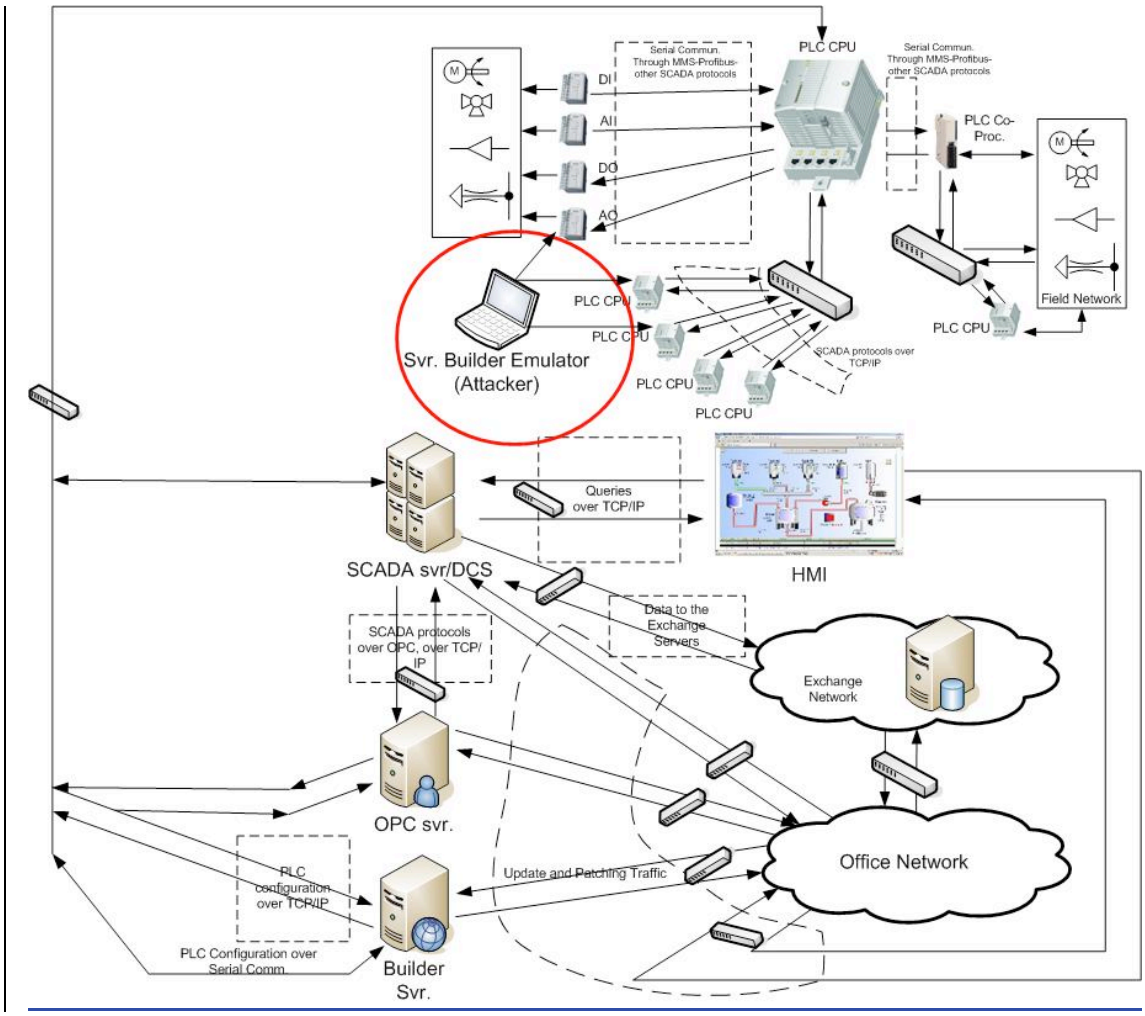


Fig. 9 - Attack Scenario 2

8.3 Attack Scenario 3 –SCADA Protocol-based Denial of Service

Scope:
To disrupt the communication between Master and Slaves in the Power Transmission Control Center.

Prerequisites:

1. Knowledge of Malware design techniques
2. Knowledge of technical aspects of Process Engineering and SCADA protocols

Tools required:

1. Software Development environment

Attack Description

The goal of the DoS attack is to desynchronize the communication between Master and Slave and, if possible, completely inhibit the communication stream between Master and Slaves.

Modern SCADA control systems largely use TCP/IP SCADA communication protocols. Examples of these protocols are TCP/IP Modbus and DNP3. In this scenario, we assume that in the transmission control station of a node (e.g. substation) of the power grid, the Master of the field network controlling the connection between multiple links of the grid, uses one of these protocols (e.g. DNP3). In the field network, we assume to have a number of Windows machines not patched against well-known viruses (e.g. Slammer), but all mounting an antivirus with the signature of this virus (the fact that the machines are un-patched is quite common, since some patches are extremely invasive and the process engineer prefer to protect the perimeter of the network instead to put at risk the stability of the systems involved in the control of the field network).

In the following we provide the description of the attack:

1. The attacker, after having reverse-engineered Slammer, selects from the obtained code only the infection engine (the information for carrying out this tasks is ready

available on the Web).

2. The attacker builds a new function which forges DNP3 packets containing the function code link “reset link (0x00)” (which prevents any “data communication” until the link status is not reset). Moreover, the new code, taking as “IP generation base” the address of the infected machine, generates random IP addresses to which send the crafted malicious DNP3 packets.

3. The attacker merges together the infection engine of Slammer and the new code, obtaining a completely different virus for which there is no signature yet.

4. The attacker adopts two alternative strategies:
    a. If he has direct access to one PC into the local network of the Node transmission control station, he injects the new virus directly into the process network.
    b. If not, through a mix of social-engineering and phishing stratagems, he deceives an authorized operator into downloading the malware (e.g. through a pdf document appearing to be a licit manual from a PLC vendor).

5. The malware starts to send the malicious DNP3 packets to all the probable IP addresses of the PLCs, making impossible any type of communication between master and slaves.

The net effect of this attack is the complete isolation of the field network. In the proposed scenario, this attack happens just few minutes before the peak of power usually happening in the evening, when the energy consumption augments. In this case, the SCADA master, with the logic required to smoothly manage this variation, cannot send to the PLCs the proper commands. The grid will then not be able to reconfigure itself to face the changes occurring on the generation and load edges of the transmission system, causing instabilities in the network.

Considerations

This scenario shows how a control center can lose the command of some technical system. In these cases there is always the opportunity to go directly to the field to actuate commands, but this might imply first to identify what is happening and where, and then to reach the lost

systems. This can have safety, environmental and reliability consequences, with financial implications for the system operator.

In a smart grid scenario this kind of situations might result in diminished services, which can be countered by the use of other power sources or transmission/distribution lines. An efficient management of these issues will require the design and deployment of an intelligent monitoring system able to detect any local attack, with fast reaction mechanisms. In some forward-looking smart grid roadmaps, this ability has been mentioned as the capacity to heal itself. With the current state of technologies, this feature appears to be a futuristic capability that will require a different approach to the architecture and control of systems.

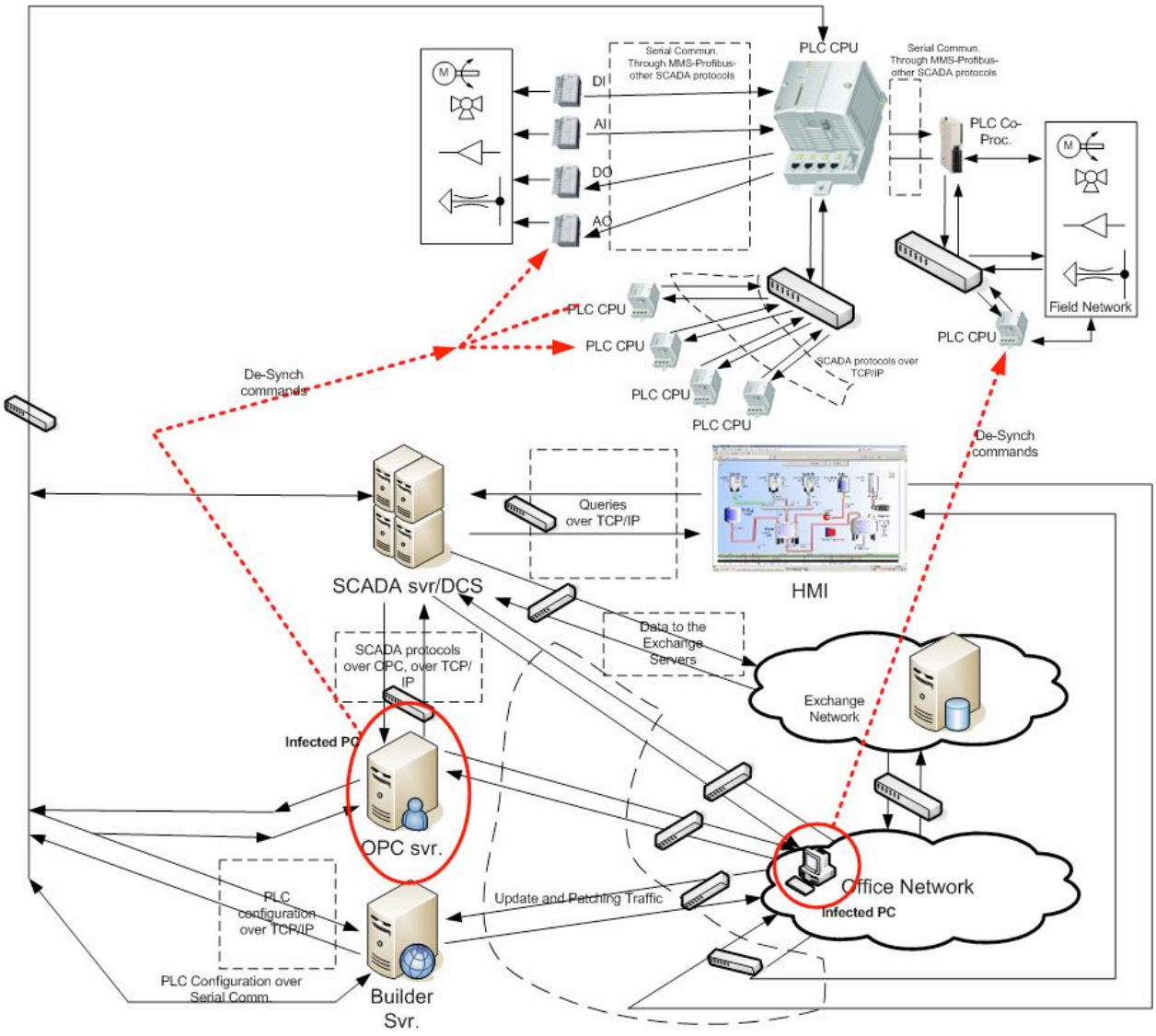


Fig. 10 - Attack scenario 3

8.4 Attack Scenario 4 –SCADA Protocol-based Coordinated Attack

Scope:

To disconnect as much grid lines as possible.

Prerequisites:

1. Knowledge of Malware design techniques
2. Knowledge of technical aspects of Process Engineering and SCADA protocols

Tools required:

1. Software Development environment

Attack Description

This attack scenario is based on the same concepts used in the previous one; however, although the vulnerabilities related to the different SCADA protocols are quite similar, we will assume in this scenario that the field network is controlled using Modbus. Moreover in this scenario, the attacker wants to hit the power grid simultaneously in different points.

In the following we provide the description of the attack:

1. The attacker collects as much information as possible about the ICT network structure of the power grid he wants to attack. Key information is the set of public IP addresses of the systems that provide the interface between the internal network of each control station and the external corporate network of the transmission system operators. This information will be used to improve the effectiveness of the attack by better identifying the targets. Nevertheless, the attack would work also without this kind of information.

2. As in the previous scenario, the attacker, after having reverse-engineered Slammer, selects from the obtained code only the infection engine.

3. The attacker builds a new function that forges Modbus packets containing the function code “write discrete output register” (which basically sends a command to a field device like a switch, or a digital instrument). The payload of this function will tell the

PLC to write the specified value into all the output discrete registers available.

4. On the basis of the information gathered by the attacker in the previous phase, the value to be written in the register should be the one that, if written on a register that corresponds to a field device that controls the “node connection”, causes its disconnection.

5. The new malicious code will have a delayed activation after the infection of the target machines: it will launch the malicious packets after a certain data, by checking the local clock. This will enable a coordinated attack by all copies of the malware.

6. The attacker merges together the infection engine of Slammer and the new code, obtaining a completely different virus for which there is no signature yet.

7. The attacker creates two versions of the malware: one will target the IP addresses retrieved during the first phase of the attack, and another will use a random address generator. In this way, also systems of which the attacker was unaware will possibly be infected.

8. The attacker releases the two versions of the malware “in the wild” (meaning in the corporate network for a targeted attack against a company – on the condition that the attacker has access to it -, or in the Internet, in a general attack against operators using that technology).

9. The malware will start to spread until reaching a target machine. Every time it reaches a new system, it starts to infect other systems in the neighborhood, and then silently puts itself in a dormant situation.

10. When the pre-defined data occurs, each piece of the malware resident in different machines or systems will wake-up and start to send the malicious Modbus packets against every possible IP address, starting from the ones in the same subnets, then proceeding with the ones in the nearest subnets and so on.

11. In a few minutes, entire lines of the grid will start to be disconnected by the PLCs

executing the command received by the malware, and causing a coordinated loss of power cuts.

Considerations

This scenario shows how a catastrophic situation. This shows how the existence of common vulnerabilities in different components of the power grid can be the cause of extremely dangerous events. In additions, it shows how the protection of the grid should incorporate security mechanisms in the communications network.

In a smart grid scenario, it will be normal to find the same software and hardware components repeatedly use in many systems. One recurring vulnerability will be exploitable with the same mechanisms, over and over again. This example shows how there is going to be the need for governance mechanisms for the patching and handling of vulnerabilities, linking vendors and users of technologies. This, in essence, will have an international flavour as the same technologies will be used worldwide.

Fig. 11: Malware Coordinated attack (red circles represent the infected field networks of the transmission grid of a country

9 Concluding remarks

This report presents four scenarios of potential cyberattacks to power grids. For the sensitivity of the subject, the power grid and the related technologies are generic, without any reference to specific real systems.

These scenarios show how it is possible to disrupt power systems, and how vulnerable they are due to the intensive use of ICT. The power grid is a typical target used for damaging society (as it can be seen in many conflicts around the world), as it is an essential service for all societal and economic activities. While managing the physical vulnerability is a mature discipline, the cyber aspects have not been adequately tackled yet.

In light of the many proposals for the development of advance and more efficient power systems (e.g. smart grids), which are going to be based on the extreme use of digital technologies, two-way communications, reaching all over society, it would be necessary to pay due consideration to cybersecurity.

The malware Stuxnet has shown that industrial control is not immune to threats. Therefore the question is not whether there is going to be some cyber offence to power systems, but when it is going to happen. The best way for being prepared for such event, it is do develop solid and rigorous cybersecurity studies, both theoretical and practical, and to disseminate the results to all the stakeholders that should know about the problem (end users, technology providers and integrators, authorities).

10 List of Acronyms

ANSI	Americal National Standards Institute
AP	Attack Potential
CBP	Capabilities Based Planning
CC	Common Criteria
CESI	Centro Elettrotecnico Sperimentale Italiano
CI	Critical Infrastructures
CPNI	Centre for the Protection of National Critical Infrastructure
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DOE	Department of Energy
DOJ	(U.S.) Department of Justice
DoS	Denial-of-Service
DSL	Digital Subscriber Line
EC	European Commission
ECTF	Electronic Crimes Task Force
EH	Electronic Highway
EIS	EPRI's Energy Information Security
EMS	Energy Management Systems
EPRI	Electric Power Research Institute
ESISAC	Electricity Sector – Information Sharing and Analysis Centre
FBI	Federal Bureau of Investigations
FedCIRC	Federal Computer Incident Response Centre
FERC	Federal Energy Regulatory Commission
FERC	Fereral Energy Regulatory Commission
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HMI	Human Machine Interface
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
IEC	International Electro-technical Commission
IEC	Israel Electric Corporation
IEC	International Electrotechnical Commission
ISA	Instrumentation, Systems, and Automation Society
ISACs	Information Sharing and Analysis Centres
ISI	EPRI's Infrastructure Security Initiative
ISMS	Information Security Management System
ISP	Internet Service Provider
KR	Key Resources

LEO	Law Enforcement Online
NAVI	National Advisory Centre on Critical Infrastructure
NERC	North American Energy Reliability Council
NIPP	National Infrastructures Protection Plan
NIST	US National Institute of Standards and Technology
NRA	National Risk Assessment
PDCA	"Plan-Do-Check-Act" model
PLC	Programmable Logic Controllers
PNWER	Pacific Northwest Economic Region
RCMP	Royal Canadian Mounted Police
SCADA	Supervisory Control and Data Acquisition
SDLC	System Development Life Cycle
SEMA	Swedish Emergency Management Agency
SSA	Sector Specific Agency
SSP	Sector Specific Plan
ST	Security Target
TOE	Target of Evaluation
TSO	Transmission System Operator
UCTE	Union for the Coordination of Transmission of Electricity
WG	Working Group

11 List of Figures

12 List of Tables

References

[1] Introduzione alla protezione di reti e di sistemi di controllo e automazione, Enzo M. Tieghi, Quaderni Clusit n. 007

[2] IT Security for Industrial Control Systems: Requirements Specification and Performance Testing, Joseph Falco, James Gilsinn, Keith Stouffer, NDIA Homeland Security Symposium & Exhibition, Crystal City, Virginia, May 25-27, 2004

[3] ISA99, Industrial Automation and Control System Security, (http://www.isa.org)

[4] The Analysis and Design of Network and Information Security of Electric Power System, Yongli Zhu; Baoyi Wang; Shaomin Zhang, Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES 2005, pp.1-6

[5] Analysis of Electric Grid Security under Terrorist Threat, Javier Salmeron, Kevin Wood, Ross Baldick, IEEE Trans. Power Syst., vol. 19, no. 2, pp 905–912, May 2004.

[6] On The Solution Of The Bilevel Programming Formulation Of The Terrorist Threat Problem, J. M. Arroyo, F. D. Galiana, IEEE Trans. Power Syst., vol. 20, no. 2, pp. 789-797, May 2005.

[7] National Strategy to Secure Cyberspace, (http://www.whitehouse.gov/pcipb*)*

[8] Common vulnerabilities in critical infrastructure control systems. Jason Stamp, John Dillinger, William Young and Jennifer DePoy. SANDIA Corporation, 2003.

[9] Information Impact on the Risk Analysis of the Malicious Attack against Power System, Ettore Bompard, Ciwei Gao, Roberto Napoli, 2007 iREP Symposium- Bulk Power System Dynamics, August 19-24, 2007, Charleston, SC, USA

[10] Attack and Fault Identification in Electric Power Control Systems: An Approach to Improve the Security, Coutinho, M.P.; Lambert-Torres, G.; da Silva, L.E.B.; da Silva, J.G.B.; Neto, J.C.; da Costa Bortoni, E.; Lazarek, H, Power Tech, 2007 IEEE Lausanne 1-5 July 2007 pp. 103-107

[11] Tutorial: Security in Electric Utility Control Systems, Hurd, S.; Smith, R.; Leischner, G., Protective Relay Engineers, 2008 61st Annual Conference for 1-3 April 2008 pp. 304-309

[12] The Next Threat to Grid Reliability-Data Security, Jones, D.A.; Skelton, R.L, Spectrum, IEEE Vol. 36, Issue 6, June 1999 pp.46-48

[13] Confronting the Risks of Terrorism: Making the Right Decisions, John Garrick, B. Hall, James E, Kilger, Max, Reliability Engineering and System Safety, 2004, 86(2), pp.129-176

[14] Guide to ISO/BS 17799 - Risk Assessment and Risk Management, BSI, PD 3002:2002.

[15] Common Criteria for Information Technology Security Evaluation. CC version 2.1, August 1999 (aligned with ISO 15408:1999). Common Criteria project Sponsoring Organizations.

[16] Emerging Standards and Methodological Issues for the Security Analysis of Power System Information Infrastructures, G. Dondossola; O. Lamquet; M. Masera, Secruing Critical Infrastructures, Grenoble, October, 2004

[17] Threat Alert System and Physical Response Guidelines for the Electricity Sector (V2.0), NERC,

Oct. 8, 2002. http://www.esisac.com/publicdocs/tas_physical_V2.pdf

[18] Threat Alert System and Cyber Response Guidelines for the Electricity Sector (V2.0), NERC, Oct. 8, 2002. http://www.esisac.com/publicdocs/tas_cyber_V2.pdf

[19] Security Challenges for the Electricity Infrastructure, Massoud Amin, Computer, vol. 35, no.4, pp. 8-10, Apr., 2002

[20] 2000 Information Technology—Code of Practice for Information Security Management. ISO IEC 17 799.

[21] Critical Infrastructure Protection in the Fight against Terrorism, EC, Brussels, 20.10.2004

[22] On A European Programme For Critical Infrastructure Protection, EC, Brussels, 17.11.2005, COM(2005) 576 final

[23] The European Programme for Critical Infrastructure Protection (EPCIP), EC, MEMO/06/477, Brussels, 12 December 2006

[24] Analyzing the Vulnerability of Critical Infrastructure to Attack, and Planning Defenses, Gerald Brown; Matthew Carlyle; Javier Salmerón; Kevin Wood, Tutorials in Operations Research, INFORMS, ISBN-1-877640-21-2 pp.102-123.

[25] Attack Vulnerability of Scale-Free Networks Due to Cascading Breakdown, Liang Zhao, Kwangho Park, and Ying-Cheng Lai, Phys. Rev. E 70, 035101 (2004)

[26] Fusion of intelligence information: a Bayesian Approach. Paté-Cornell E., Risk Anal 2001, Vol. 22, Issue 3, pp. 445-454

[27] Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. Paté-Cornell E, Guikema S., Oper. Res., vol. 7, no. 4, pp. 5-20, 2002

[28] Cybersecurity for Electric Power Control and Automation Systems, Chee-Wooi Ten; Govindarasu, M.; Chen-Ching Liu, Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference on 7-10 Oct. 2007 pp. 29-34

[29] Correlating Multi-Step Attack and Constructing Attack Scenarios Based on Attack Pattern Modeling, Zhijie Liu; Chongjun Wang; Shifu Chen, Information Security and Assurance, 2008. ISA 2008. International Conference on 24-26 April 2008, pp. 214-219

[30] Electric System Vulnerabilities: Lessons from Recent Blackouts and the Role of ICT, Alberto Stefanini, 2005

[31] Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage, OTA-E-453. U.S. Congress Office of Technology Assessment, 1990

[32] Vulnerability Assessment Activities (for Electric Utilities), Jeff Dagle, IEEE PES Winter Power Meeting in Columbus, Ohio, Vol. 1, pp.108-113,Jan.-Feb. 2001

[33] Network Security Vulnerabilities in SCADA and EMS, Amanullah, M.T.O.; Kalam, A.; Zayegh, A,Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES 2005 pp. 1-6

[34] Cyber Security Vulnerability Assessment of Power Industry, Jiaxi, Yu; Anjia, Mao; Zhizhong, Guo, TENCON 2006. 2006 IEEE Region 10 Conference 14-17 Nov. 2006 pp. 1-4

[35] Vulnerability Assessment of Cyber Security in Power Industry, Yu Jiaxi; Mao Anjia; Guo

Zhizhong, Power Systems Conference and Exposition, 2006. PSCE '06. 2006 IEEE PES Oct. 29 2006-Nov. 1 2006 pp.2200-2205

[36] Vulnerability Assessment of Power System Using Various Vulnerability Indices, Haidar, Ahmed M. A.; Mohamed, Azah; Hussain, Aini, Research and Development, 2006. SCOReD 2006. 4th Student Conference on 27-28 June 2006 pp.224-229

[37] Modeling Complex Control Systems to Identify Remotely Accessible Devices Vulnerable to Cyber Attack, Daniel Conte de Leon, Jim Alves-Foss, Axel Krings, Paul Oman

[38] The Use of Game Theory to Measure the Vulnerability of Stochastic Networks, M. G. H. Bell, IEEE Trans. Reliab., vol. 52, no. 1, pp. 63-68, Mar. 2003

[39] Counter Terrorism- A Game Theoretic Analysis, Daniel G. Arce M. Todd Sandler, Journal of Conflict Resolution. 2005, 49(2), pp.183-200

[40] Electric Utility Responses to Grid Security Issues, Robert Schainker; John Douglas; Thomas Kropp, Power and Energy Magazine, IEEE Vol. 4, Iss. 2, March-April 2006 pp. 30-37

[41] Power System Control and Associated Communications – Data and Communication Security, Technical Report, IEC TR 62210, First edition 2003-05

[42] Instrumentation, Systems, and Automation Society (ISA) SP99. Available: http://www.isa.org

[43] Security Technologies for Manufacturing and Control System. ISA-TR99.00.01-2004, Instrumentation, Systems, and Automation Society (ISA).

[44] Integrating Security into the Manufacturing and Control Systems Environment. ISA-TR99.00.02-2004, Instrumentation, Systems, and Automation Society (ISA).

[45] The NERC Program for the Electricity Sector Critical Infrastructure Protection, Lou Leffler, Power Engineering Society Winter Meeting, 2001. IEEE Vol.1, 28 Jan.-1 Feb. 2001 pp.95-97

[46] Guidelines for Responding to NERC (Technical report), EPRI, Oct., 2004

[47] Security Vulnerability Self-Assessment Guidelines for the Electric Power Industry, EPRI Report 1001639, 2002

[48] Guidelines for Detecting and Mitigating Cyber Attacks on Electric Power Companies, EPRI Report1008396, 2004.

[49] (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1, NERC, 2007

[50] Information Security Management. Part 2: Specification for Management Systems, 1999. British Standard, BS 7799.

[51] Information Security Management Systems—Specifications with Guidance for Use. BS 7799-2:2002.

[52] Management Of Information Security for an Electric Power Utility-On Security Domains and Use of ISO/IEC17799 standard, *Göran N. Ericsson; Åge Torkilseng; Power Delivery, IEEE Transactions on Vol. 20, Iss. 2, Part 1, April 2005 pp. 683-690*

[53] Toward a Framework for Managing Information Security for an Electric Power Utility—CIGRÉ Experiences, Ericsson, *G.N, Power Delivery, IEEE Transactions on Vol. 22, Issue 3, July 2007 pp. 1461-1469*

[54] Operation Handbook, UCTE, 2004

[55] North American Electricity Infrastructure. Are We Ready For More Perfect Storms*, Massoud Amin, IEEE Security and Privacy magazine,* 2003, 1(5), pp.19-25

[56] North American Electricity Infrastructure: System Security, Quality, Reliability, Availability, and Efficiency Challenges and their Societal Impacts, *Massoud Amin, Chapter 2 in the National Science Foundation (NSF) report on "Continuing Crises in National Transmission Infrastructure: Impacts and Options for Modernization,"* June 2004

[57] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model. September 2006 Version 3.1 Revision 1 CCMB-2006-09-001 http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf

[58] Common Methodology for Information Technology Security Evaluation - Evaluation methodology. September 2007 Version 3.1 Revision 2 CCMB-2007-09-004

[59] ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models

[60] ANSI/ISA-TR99.00.01-2007, Security Technologies for Industrial Automation and Control Systems

[61] ISO/IEC 27001, Information Technology - Security techniques - Information security management systems - Requirements.

[62] ISO/IEC 27002, Information Technology - Security techniques – Code of practice for information security management.

[63] Increasing Robustness, Resilience, and Security of the Energy Infrastructure, *EPRI Author-D. Sobajic, Electricity Technology Roadmap Limiting Challenge*, Final Report, Dec. 2003

[64] National Infrastructure Protection Plan. *U.S. Department of Homeland Security*. 2006

[65] Energy Critical Infrastructures and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan. *U.S. Department of Homeland Security and U.S. Department of Energy*. 2007

[66] CPNI – SCADA. http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

[67] Good Practice Guide Process Control and SCADA Security. *Centre for the Protection of National Infrastructure – CPNI*

[68] Good Practice Guide Process Control and SCADA Security. Guide 1. UNDERSTAND THE BUSINESS RISK. *Centre for the Protection of National Infrastructure – CPNI*

[69] National Advisory Centre on Critical Infrastructure http://www.minbzk.nl/bzk2006uk/subjects/public-safety/national-security/protection-of#blw_Whatiscriticalinfrastructure

[70] National Security – Strategy and Work programme 2007 – 2008, *Ministry of the Interior and Kingdom* Relations, ISBN 978-90-5414-19-8, May 2007

[71] National Security – National Risk Assessment Method Guide 2008, Ministry of the Interior and Kingdom Relations, ISBN 978.90.5414.155.6, June 2008

[72] Förordning (2006:942) om krisberedskap och höjd beredskap.

http://www.notisum.se/rnp/sls/lag/20060942.htm

[73] Risk and vulnerability analyses. Guide for governmental agencies. Swedish Emergency Agency (SEMA), Stockholm, 2008

[74] Critical Infrastructures at Risk; Securing the European Electric Power System. Series: Topics in Safety, Risk, Reliability and Quality, Vol. 9. Gheorghe, A.V., Masera, M., Weijnen, M., De Vries, L.J., 2006, XXIX, 371 p., Hardcover. ISBN: 978-1-4020-4306-2

[75] Guidelines for Smart Grid Cyber Security, NIST, August 2010. Available at http://nist.gov/smartgrid/

[76] Siemens. Information concerning malware. Available at http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&=en&objid=43876783&caller=view

[77] “Experimental Proof of Malware Attacks on SCADA Systems”. I. Nai Fovino, A. Carcano, M. Masera, A. Trombetta. International Journal of Critical Infrastructure Protection. Ed. Sujeet Shenoi. Vol. 2, Issue 4, pp. 135-144, 2009, Elsevier.

[78] “Effects of intentional threats to power substation control systems”, G. Dondossola, M. Masera, I. Nai Fovino, J. Szanto. International Journal of Critical Infrastructure, (IJCIS), Vol. 4, No. 1/2, 2008

[79] "ICT Security Assessment of a Power Plant, a Case Study", Igor Nai Fovino, Marcelo Masera, Rafal Leszczyna. In Proceeding of the Second Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, George Manson University, Arlington, USA, March 2008

[80] Creery, A., Byres, E.: Industrial Cybersecurity for power system and SCADA networks. IEEE Industry Apllication Magazine (July-August 2007)

[81] Chandia, R., Gonzalez, J., Kilpatrick, T., Papa, M., Shenoi, S.: Security Strategies for Scada Networks. In: Proceeding of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, USA, March 19-21 (2007).

[82] “Towards a Taxonomy of Attacks Against Energy Control Systems”. T. Fleury, H. Khurana and V. Welch.. In Critical Infrastructure Protection II, IFIP International Federation for Information Processing, 2009, Springer Boston, pp. 71- 85.

[83] “A Taxonomy of Attacks on the DNP3 Protocol”. S. East, J. Butts, M. Papa and S. Shenoi. In Critical infrastructure protection III, ed. C. Palmer and S. Shenoi, pp.67-82, Springer, 2009

[84] “Assessing the Integrity of Field Devices in Modbus Networks”. R. Shayto, B. Porter, R. Chandia, M. Papa and S. Shenoi. In Critical Infrastructure Protection II, IFIP International Federation for Information Processing, 2008, Springer Boston, pp 115-128

[85] “Security Analysis of Multilayer SCADA protocols”. J. Edmonds, M. Papa and S. Shenoi. In Critical Infrastructure Protection, IFIP International Federation for Information Processing, 2007, Springer Boston, pp 205-222

[86] W32.Stuxnet Dossier, Version 1.3 (November 2010), Nicolas Falliere, Liam O Murchu, and Eric Chien, Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[87] “MPLS and label switching networks”. Michael H. Behringer and Monique J. Morrow. Cisco Press; illustrated edition edition (June 18, 2005).

[88] IEEE (Institute of Electrical and Electronics Engineers), Trial Use Std. for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access, P1689, Draft, 2007.

[89] The TLS Proposal, Network Working Group, January 1999, Version 1, Internet Engineering Task Force (IETF) TLS rfc2246. Available at: http://www.ietf.org/rfc/rfc2246.txt

[90] “The SSL Protocol: Version 3.0”. A. Freirer, P. Kariton and P. Kocher, Netscaper Communications, Inc. Mountain View, CA (Mar. 1996).

[91] “Computer Security, Art and Science”. Matt Bishop, ISBN 0-201-44099-7; Publisher Addison Wesley Professional; Copyright 2003; Format Cloth; 1136 pp.; Library of Congress Number QA76.9.A25 B56 2002.

[92] Secure DNP3. Last access June 1, 2010. http://www.digitalbond.com/wiki/index.php/Secure_DNP3

[93] “DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework”, M. Majdalawieh. In Proceedings of ACSAC 2005 Tech-Blitz.

[94] Cryptographic Protection of SCADA Communications, AGA Report N. 12.

[95] “Secure Modbus Protocol, a proof of concept”. I. Nai Fovino, A. Carcano and M. Masera: In Proc. of the 3rd IFIP Int. Conf. on Critical Infrastructure Protection, Hanover, NH, USA, 2009.

[96] “ICT Security Assessment of a Power Plant, a Case Study”. I. Nai Fovino, M. Masera, R. Leszczyna. In Proceeding of the Second Int. Conference on Critical Infrastructure Protection, Arlington, USA, March 2008

[97] NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks: www.cpni.gov.uk/docs/re-20050223-00157.pdf

[98] Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology Special Publication 800-82 Natl. Inst. Stand. Technol. Spec. Publ. 800-82, 156 pages (September 2008)

[99] Tofino Security. Description available at http://www.tofinosecurity.com. Last access November 1, 2010

[100] SCADA IDS preprocessors. Last access 12 November 2010 http://www.digitalbond.com/index.php/research/scada-idsips/scada-ids-preprocessors

[101] “Modbus/DNP3 State-based Intrusion Detection System”. Igor Nai Fovino, Andrea Carcano, Marcelo Masera, Alberto Trombetta, Thibault Delacheze-Murel. In Proceedings of the 24th International Conference on Advanced Information Networking and Applications, Perth, Australia, 20-23 April 2010.

[102] IEC (International Electrotechnical Commission), Power system control & associated communications - Data & communication security, IEC62351 part 1 to 7, Technical Specification, 2007.

European Commission

EUR 24721 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: ICT aspects of power systems andICT aspects of power systems and their securitytheir security
Author(s): Marcelo Masera, Igor Nai Fovino, Bogdan Vamanu
Luxembourg: Publications Office of the European Union
2011 – 127 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-19282-1
doi:10.2788/46277

Abstract
This report provides a deep description of four complex Attack Scenarios that have as final goal to produce damage to the Electric Power Transmission System. The details about protocols used, vulnerabilities, devices etc. have been for obvious reasons hidden , and the ones presented have to be understood as mere (even if realistic) simplified versions of possible power systems.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

LB-NA-24721-EN-C

Publications Office

ISBN 978-92-79-19282-1