Call: FP7-SEC-2013-1
Activity: SEC-2013.2.5-4: Protection systems for utility networks – Capability Project
Project Number: 608090

HyRiM

Hybrid Risk Management for Utility Networks

Collaborative Project

D2.1
Future trend SCADA-related attack, mitigation and prevention tools

Due date of deliverable: March 31 2015
Actual submission date: June 02 2015

Start date of project: April 1, 2014 Duration: 36 months

Organisation name of lead contractor for this deliverable
ETRA I+D

Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

HISTORY

Version	Date	Reason	Reviewed by
v.0.8	22-05-2015	First draft version	Ana María Arias (ETRA)
V0.9	29-05-2015	Complete version	All Authors

AUTHORS LIST

Organization	Name
ETRA I+D	Ana María Arias (amarias.etra-id@grupoetra.com; +34 96 313 40 82)
UNI PASSAU	Ali Alshawish (ali.alshawish@uni-passau.de;)
ULANC	Antonios Gouglidis (a.gouglidis@lancaster.ac.uk
AKH	Francesco Fileppo (francesco.fileppo@akhela.com; +39 011 7750904)
AIT	Paul Smith (Paul.Smith@ait.ac.at)
LINZ	Magdalena Roiser (ma.roiser@linzag.at)

Table of Contents

Index of Figures

Index of Tables

EXECUTIVE SUMMARY

This document is an extensive literature review based on previous research projects and scientific publications about cyber security in SCADA systems, including related attacks, mitigation techniques and prevention tools. It is worth mentioning that document points out 150 references, that gives an idea of the documents revised to produce this document (see section REFERENCES).

The document is built around four big building blocks:

- **Security Overview in SCADA networks**. Some general history about SCADA systems are given, and how this relates to security, in addition policy issues are taken into account.

- **SCADA cyber threats and vulnerabilities**. Extensive information about vulnerabilities and threats, categorising the vulnerabilities in different domains (architectural, software, communications, etc.), lessons learned in the past from these are compiled as well.

- **SCADA Cyber Attacks**. Cyber Attacks are studied in depth, we provide a taxonomy of challenges, and related attacks on hardware, software, communications and protocols, in addition attack sources and profile of attackers are detailed, and finally typical phases of an attack are described.

- **Improving cyber security of SCADA systems**. Finally some approaches, guidelines and advices based on previous experiences are given to deal with cyber-attacks in these kind of networks.

1 ABBREVIATIONS

Term	Meaning
ACL	Access Control List
API	Application Programming Interface
APT	Advanced Persistent Threats
ARP	Address Resolution Protocol
CERT	Computer Emergency Response Team
CIA	Confidentiality, integrity, and availability
CIP	Critical Infrastructure Protection
CSS	Cross Site Scripting
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DER	Distributed Energy Resources
DG	Distributed Generation
DMZ	Demilitarized zones
DNP	Distributed Network Protocol
DNS	Domain Name System
DoS	Denial-of Service
DSM	Demand Side Management
EMS	Energy Management System
ENISA	European Network and Information Security Agency
ESP	Electronic Security Perimeter
HIDS	Host Intrusion Detection Sensor
HMI	Human–machine interface
HTML	Hyper Text Markup Language
HVAC	Heating, ventilating, and air conditioning
ICCP	Inter-Control Center Communications Protocol
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDC	Internet Data Center
IDS	intrusion detection systems
IED	Intelligent Electronic Device
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPSec	Internet Protocol Security
ISO	International Standards Organization
ISRAM	Information Security Risk Analysis Method
IT	Information Technology
JSON	JavaScript Object Notation
LAN	Local area network
MAN	Metropolitan area network
MAP	Medium Access Control
MITM	Man-In-The-Middle technique
MMS	Manufacturing Message Specification
MSSP	Managed Security Service Provider
MTU	Master terminal unit
NERC	North American Electric Reliability Corporation
NIDS	Network Intrusion Detection Sensor
NTSB	National Transportation Safety Board
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OLE	Object Linking and Embedding
OPC	OLE for Process Control

OS	Operating System
OSI	Open Systems Interconnection
PCS	Process control system
PLC	Programmable logic controller
PLC	Programming Logic Circuit
PMU	Phaser Measurement Unit
RAT	Remote Access Trojan
REST	Representational State Transfer
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SG	Smart Grid
SQL	Structured Query Language
SSL	Secure socket layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTM	Unified Threat management
VNC	Virtual Network Computing
WAN	Wide area network
WDB	VxWorks Wind DeBug
XML	Extensible Markup Language

2 INTRODUCTION

SCADA systems control some of the world's most critical infrastructure including Nuclear power stations, electrical distribution stations, water distribution and waste treatment plants, oil and natural gas pipelines, chemical plants, and rail and other public transportation systems.

As stated in [1] loss of access to or misuse of these systems could result in severe physical damage, disruption and financial loss to a company. Therefore, security of these SCADA systems should be a high priority. Traditionally, SCADA networks have been segregated from other corporate networks to minimize exposure to unsecure areas, such as the Internet. Recently however, more organizations are connecting SCADA networks with other potentially unsecure networks in order to cut costs, share operational information, or distribute ordering/billing data. Even when connecting SCADA networks to other networks is prohibited by corporate policy, incorrectly installed systems can unintentionally bridge networks together - putting SCADA networks and the processes they control at risk.

Another studies like the Generic SCADA Risk Management Framework for Australian Critical Infrastructure [2] points out that business drivers for SCADA integration with enterprise management systems, load management and smart grid environments has meant that SCADA systems have become interconnected with corporate business networks, customer premises and directly or indirectly with the Internet. This, together with the rapid advancement of technology, shifting threat landscape and the changing business environment, is increasing the exposure of SCADA systems to network vulnerabilities and Internet security threats.

Often, as found in [1] security for SCADA systems consists of a basic password which is passed in plain text from the control system to the RTUs. These unprotected passwords can easily be intercepted by malware and packet sniffers. In many cases, these passwords remain set to the manufacturer's default value. Some corporate IT policies require password changes on a monthly basis. However, this safety measure is rarely applied to SCADA systems because of the resources needed to manually change passwords on potentially hundreds of devices, and the risk to the company should these devices become inaccessible.

SCADA systems have traditionally been viewed as being isolated and therefore 'safe' and less exposed to remote cyber-attacks. Risk assessment and management methodologies, correspondingly, have largely been directed at legacy SCADA systems in which underlying protocols were designed without modern security requirements in mind.

Recent incidents such as Aurora and Stuxnet demonstrate that a directed cyber-attack can cause physical harm to critical infrastructure. Traditional threat sources have evolved to now include focused foreign nation cyber-intrusions and industrial espionage capabilities [2].

The present document provides an overview of SCADA systems and its security issues including threats and vulnerabilities, a characterization of attacks specifically against SCADA networks, approaches for threat analysis and assessment of risks and preventative policies and solutions for improving security.

3 SCADA NETWORKS – SECURITY OVERVIEW

3.1 ICS PAST AND PRESENT

Industrial systems and critical infrastructures are often monitored and controlled by simple computers called Industrial Control Systems (ICS). ICS are based on standard embedded systems platforms and they often use commercial off-the-self software. ICS are used to control industrial processes such as manufacturing, product handling, production, and distribution. Well-known types of ICS include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLC). [3]

During the last decades the advantages offered by the Industrial Control Systems (ICS) have been focus on improve in the process within industrial environment, where the requirements of monitoring must be accurate. During the last years the use of SCADA systems have been improved too mixed to embedded systems platforms uses and commercial software; the results obtained have been focused in offer more precision in industrial process as manufacturing, product handling, production and distribution.

SCADA systems deploy largest subgroup of ICS systems and large scale processes ito multiple sites and large distances. In that sense the SCADA system will cover the monitoring procces of all interconnected equipment among industrial environments where the automatic process (as electricity power generation, transmission and distribution, Oil and gas refining and pipeline management, water treatment and distribution, chemical production and processing, rail systems and other mass transitare) are required [3].

Nowadays SCADA systems have been improved in order to gather remote data through unreliable or intermittent low-bandwidth or high-latency links. In terms of security information the SCADA systems must include improvements from software development to server deployment, . The information security has been achieved in the past 10 years to help secure them. SCADA deployment has consistently risen. Lack of information security implementation and advancements in SCADA technology have dramatically increased security risks worldwide with likely far-reaching consequences [4].

3.2 SCADA SYSTEM COMPONENTS AND OPERATIONAL PHYLOSOPHY

SCADA systems are specialized computer networks and devices that work in concert to monitor and control key processes involved in the management of machinery, equipment and facilities. SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in real time.
The SCADA system must be available to realise all the monitor and control key processes involved in machinery, equipment and facilities. All this process must be designed and sincronized in oder to to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in real time, mainly the SCADA system must be deployed in next areas [1]:

- ***Industrial process management:*** manufacturing, production, chemical processes, power generation, fabrication, and refining industries
- ***Infrastructure management:*** water treatment and distribution, waste water collection and treatment, oil and gas pipelines, electrical power transmission and distribution, large communication systems

Facility management: offices, data centers, airports, ships etc.; monitor and control HVAC, physical access, and energy consumption [6]

Nowadays SCADA System are improving the hardware and software componentsin order to made a efficient collection and feeds data into a computer with SCADA software installed, recording and logging all

events in a file that is stored in a hard disk or sending them to a printer [7]. The extraction process uses a great number of sensors (temperature, pressure, flow etc.) The SCADA system approach are used to make decisions based of measurements collected from its sensors. Precisely a typical SCADA system comprises of a hierarchy of Sensor Network, Remote Terminal Units, Master Terminal Units, and Corporate Network. Next paragraph will describe the main action by each one [5]:

- **Sensor Network:** This component has a direct interface with the utility system and it is responsible for data collection at consumer sites. Data collected may include parameters such as current, voltage, phase angle etc.

- **Remote Terminal Units (RTU):** As this component is connected to the sensor networks to process data collected by the sensors, the RTU store control parameters for local monitoring and could execute programs in order to manage the electricity parameters.
- **Master Terminal Units (MTU):** This component contains a software connected to many RTUs via communication channels (usually radio) to communicate with other peripheral devices in the facility like monitors, printers, the corporate network and other information systems. MTU polls the RTUs at regular intervals of time to read the data gathered by the RTU from the SCADA sensor network.
- **Corporate network:** The SCADA data historians, servers and databases are all a part of the corporate network which is connected to the internet.

Figure 1 shows a basic idea of use of SCADA system within industrial environment

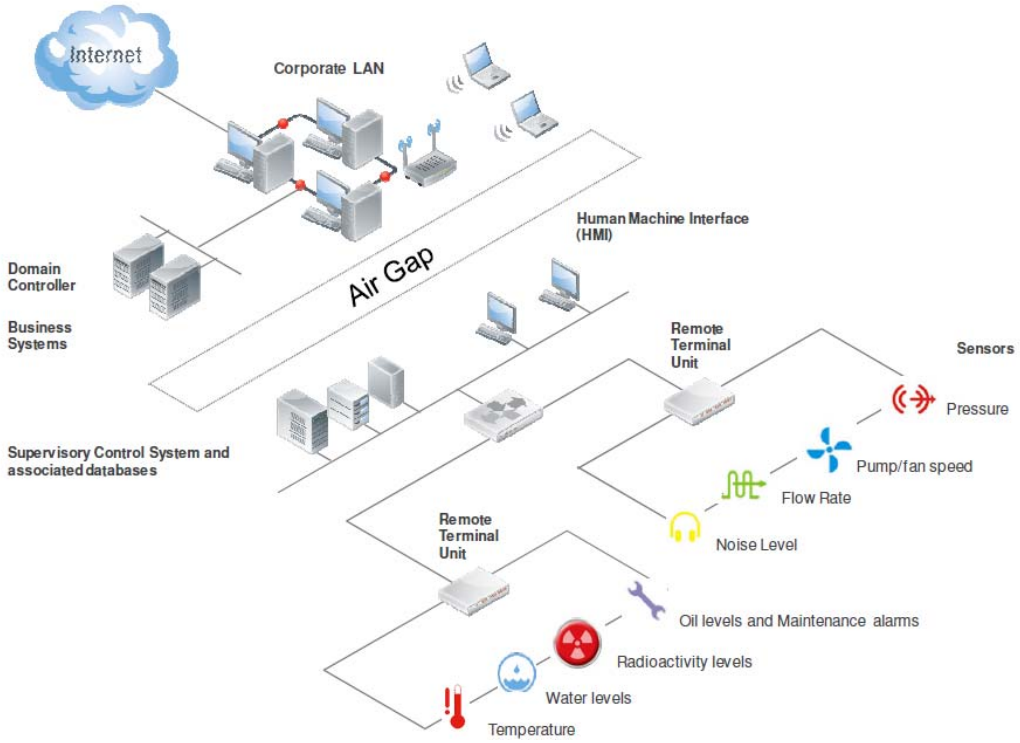

Figure 1. Industrial Control System with SCADA Network Architecture
Source: Securing SCADA Infrastructure-FORTINET White paper. 2010

SCADA field devices include RTUs, PLCs, and IEDs ; as the PLCs control system components used throughout DCS and SCADA systems can also be referred to as RTUs; and used in SCADA networks and not DCSs. The advantages of Data Historian records and logs gives real time information for operator via the HMIallowing the monitoring process applied to SCADA network and providing more information for

system implementation. Next figure will show an example of a SCADA system designed for a primary control center and three field sites [6].

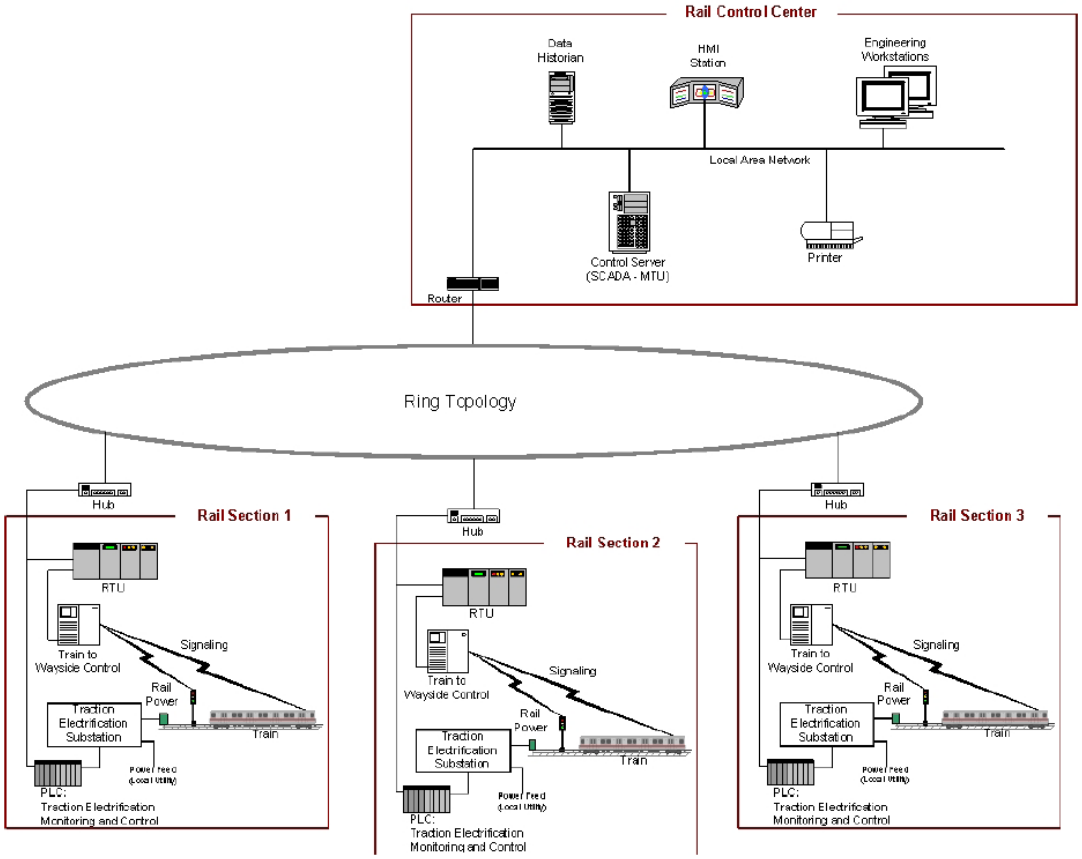

Figure 2. SCADA System Implementation Example (Rail Monitoring and Control)
Source: Guide to Industrial Control Systems (ICS) Security. NIST U.S Department of Commerce.

The modularity of SCADA architecture are interconnected among all levels in order to facilitate the monitoring task involving in industrial environments, for this reason any cyber-attack should be a disastrous to the whole SCADA network. As the Figure 2 shows any disaster or cyber attack will propagate all the way up to the corporate network level if not checked in time. In order to avoid this disaster the ciber-security system must be given high priority in all critical infrastructure industries [5].

SCADA Communication Protocols

Currently and according to the American Gas Association's AGA-12 standard, there are about 150–200 SCADA protocols. This protocols have been developed by individual companies, the current trend of standard protocol suggest the use of common open standard protocols. Next table shows the more popular and widely used protocols.

SCADA PROTOCOLS		
Protocol	**Organisation/standard**	**Main Features**
Ethernet/IP (Industrial Protocol)	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Object-oriented, protocol; provides interoperability over Ethernet and fieldbus networks
DeviceNet	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Belongs to the CIP (Control and Information Protocol) family; CAN protocol defines layers 1 & 2; the rest are defined by DeviceNet and CIP

ControlNet	ControlNet International (www.controlnet.org)	Belongs to the same CIP (Control and Information Protocol) family; new physical layer with higher speed, strict determinism and repeatability with greater range
PROFIBUS	Type 3 protocol of IEC Standard 11674 and 61158 (www.profibus.org)	3-layer OSI model; has extensions for safety features; ProfiNet version provides Ethernet compatibility
MODBUS TCP/IP	MODBUS-IDA (www.modbus.org)	Encapsulates fieldbus packets over TCP; attempting to become an IETF standard
DNP3	(IEC) Technical Committee 57, Working Group 03 standard	It is also a based on the 3-layer OSI model
Foundation Fieldbus	The Fieldbus Foundation/open standard protocol (www.fieldbus.org)	Incorporates many safety features that make it a good candidate for mission-critical applications

Table 1. SCADA Protocols Evolution

Protocol designs in SCADA are compact and are so designed as to send information to master station only in case the RTU is surveyed for information by the master station. Some Protocols as Modbus, RP570 and Conitel are the traditional vendor specific SCADA communication protocols. Standard communication protocols include IEC61850, DNP3, Profibus and IEC60870-5-101 or 104. All major SCADA vendors recognize these protocols. Communication protocols with extensions can operate in internet protocol TCP/IP. Modbus TCP/IP has now become standard for lot of hardware manufacturers and is a widely accepted communication protocol. Although for safety and security of SCADA system, it is advisable not to connect it to internet and expose it to risk, Ethernet TCP/IP has found its way into industrial automation breaking the barriers in majority of SCADA/HMI markets [7].

3.3 SCADA EVOLUTION AND SECURITY ISSUES

When SCADA protocols were first developed, the goal was to provide good performance and the emphasis was placed on providing features that would ensure that the task constraints on the network would be met. Until recently, the most common misconception regarding the security of SCADA networks was that these networks were electronically isolated from all other networks and hence attackers could not access them.

Three challenges must be addressed to strengthen SCADA networks. The first challenge is to improve the access controls to the SCADA networks. A solution will make it harder for an attacker to enter into the SCADA network. The second challenge is to improve security inside the SCADA network and to develop efficient security-monitoring tools. The security mechanisms developed to address this challenge will ensure that even if an attacker manages to enter the SCADA network, it will be difficult to carry out any sort of attack. The monitoring tools will help to detect intrusions and other suspicious activities on the network. The third challenge is to improve the security management of the SCADA network. The following sub-sections discuss each of these challenges in more detail.

Any mechanism designed to meet these challenges must also consider the limitations of fieldbus networks. Fieldbus network constraints typically include slow communication rates, small message packets, and real-time operating requirements. For example, according to the IEC standard specification IEC 61158, the PROFIBUS protocol has a data rate in synchronous transmission mode of only 3125 Kbps and most of the messages are only a few octets wide.

SCADA Evolution and main Issues solved	
Access control	The first task in securing any network is to ensure that unauthorized entities do not gain entry into the network. Therefore, it is crucial to improve the access control mechanisms of SCADA networks. The gateway provides protocol compatibility between the local SCADA network and the outside corporate network, but many gateways do not include security features. It is necessary to develop gateways that provide proper security mechanisms to ensure authentication, confidentiality, integrity, and privacy of data. These features must be flexible enough to support many different SCADA protocols.
Firewalls and intrusion detection systems	A basic function of a firewall is to block unauthorized traffic from entering the protected network. The firewall prevents the establishment of a direct connection from the outside Internet to the local SCADA network. Firewalls can be configured to recognize and allow only traffic belonging to certain protocols
Protocol vulnerability assessment	It is first necessary to analyse existing protocols and understand the vulnerabilities present in the protocols. This will help with the development of security mechanisms that can be incorporated into the protocol specifications. Current SCADA protocol specifications are well-established international standards governed by trade and professional organizations.
Cryptography and key management	SCADA protocols typically do not support any sort of cryptography, but this capability would be useful in securing these networks. The unique characteristics of SCADA networks make it difficult to adapt existing cryptographic techniques into these systems.
Device and OS security	The security of the SCADA network depends upon the security of the end devices on the network. Many nodes on SCADA networks are embedded computing devices that run real-time operating systems (RTOS) and other real-time control software.
Security Management	Over the last decade, many companies that rely heavily on Information Technology (IT) have developed good IT security practices. SCADA industries need to catch up with the rest of the IT world and improve their security management.

Table 2. SCADA security main challenges

Nowadays modern SCADA system (architecture) has been developed as corporate IT network providing "real-time" control information in order to detect and avoid any attack on such a system could have much more serious and widespread consequences (in terms of loss of life and physical damage) [8]. In the same line the current trends are using standards in order to exploit the use of open market technologies in control systems. Through complex software applications with the following characteristics: time critical, embedded, fault tolerant, distributed, intelligent, large, open, and heterogeneous. [12]

SCADA systems are exposed to the same cyberspace threats as any business system because they share the common vulnerabilities with the traditional Information Technology (IT) systems. Also, most SCADA systems are not protected with appropriate security safeguards. The operating personnel is lacking the security training and awareness. Threats against SCADA systems are ranked high in the list of government concerns, since terrorists have threatened to attack several SCADA systems of critical infrastructure and successfully launched near-disastrous attacks. [13]

In addition, recent attacks are becoming more sophisticated and the notion of what kind of vulnerabilities actually matter is constantly changing. For example, timing attacks are now common threats, whereas only a few years ago they were considered exotic. The threats are often poorly understood and ignored, and the vast majority of organizations lag in realizing secure infrastructures. [14]

In complexly interactive systems whose elements are tightly coupled, great accidents are inevitable. Vulnerabilities and attacks could be at different levels – software controlling or controlled device, application, storage, data access, LAN, enterprise, Internet, communications.

3.3.1 SCADA systems in Smart Grid

SCADA systems control, operate and monitor a huge portion of industrial facilities and critical infrastructures, which are often distributed over wide geographic areas. An example of SCADA application is the power generation and power distribution systems. The protection of the industrial control environments was earlier handled only by the use of proprietary protocols and separation. However, technologies, which make remote access more convenient, such as web interfaces and connections to the internet in general, were adapted to these industrial control systems. The increased rate of interconnections between control systems and utility networks delivers important benefits. However, these interconnections are tightly associated with security and safety implications because of the use of open protocols. Thus the control systems, such as SCADA, become more vulnerable to new vectors for attack. In fact, the changes in the design of the SCADA systems and the incorporation of such open technologies were performed without realizing the security consequences associated with such changes. Hence, new attacks, such cyber-attacks, are now possible from the outside. The standard SCADA systems are not prepared for such kind of attacks introduced by the modern technologies, which are already intensively used.

This realization is especially important in the context of the Smart Grid (SG), which is a new technique and philosophy for power systems, that blends the current power grid networks with modern information and communication technologies (ICT) to make power generation and distribution more efficient [9]. Aside from energy efficiency advantages, this new technology makes the power grid ready for an intelligent integration of renewable energies, self-healing through sophisticated partitioning, error finding capabilities and dynamic load balance due to constant feedback information based on two-way communications. The new philosophy introduced by Smart Grid addresses wide range of topics, such as efficiency, reliability, dependability, maintaining sufficient power quality, supporting distributed generation and distributed energy resources, and enhancing the demand side's role, as well as enabling decentralized decision and control. This paradigm plays an essential role in determining the characteristics and abilities of future SCADA systems, such as decentralized intelligence and decision abilities and context awareness [10]. Furthermore, the increasingly large number of involved and communicating entities emphasizes the need to scalable, effective and adaptive SCADA systems.

SCADA system is an important basic technology in the power generation and distribution sector and needs to fulfil a high security standard before it can be used in such interconnected and complex environment as the Smart Grid. The power supply represents an essential pillar of our modern society. Thus, the continuity of the society and economy is mainly dependent on the accurate and robust operation of the power system. Even small failures can lead to blackouts, which may have economically, ecologically and socially disastrous consequences and can even endanger human lives. With the increasing interconnection of communication technology and industrial control systems in the Smart Grid, the two systems become more and more dependent on each other. If one fails, the other one is very likely to collapse. Furthermore, SCADA systems become increasingly complex and interconnected to other networks since almost all other utility networks need electricity for their operation. These interconnections render SCADA systems, which previously have been completely isolated and relied on the practice of security through obscurity, more vulnerable to a wide variety of attacks associated with potentially catastrophic consequences.

A power distribution network, as an important part of the whole power grid, interconnects different subdomains of the power grid together, such transmission domain, customers and consumption metering points domain, distributed storage and distributed generation. Historically, the distribution systems were basically monitored and controlled by humans and rarely connected to SCADA. With advent of modern Smart Grid, a more advanced automation is expected in order to reach the envisioned improvement of

reliability, power quality and efficiency. This automation requires the use of robust SCADA systems. In this context, SCADA is combined with some additional, advanced and application-specific components, such as Energy Management System (EMS) and Phaser Measurement Units (PMU). SCADA/EMS is responsible for monitoring, controlling and optimizing the power generation, transmission and distribution. SCADA/PMU relies on sensors, which are widely dispersed throughout the entire power system, in order to collect high quality data. The collected data represents synchronized real time measurements of all remote points of the system. The benefits that this technology offers are various, such as enhancing the reliability of the system by detecting system anomalies and increasing power quality as well as enabling various load control techniques [11].

A reliable and safe SCADA system is actually inevitable need in the context of Smart Grid, in order to improve the controllability of the power system and to allow operations like separating and restoration to be performed dynamically and in real time [9]. At the core of smart grid is SCADA system, which monitors the system and makes decisions and adjustments to keep operation at the optimal level [12]. The first generation of SCADA relied on mainframe systems to process the data and the control system was fully isolated without any network connectivity to other systems. At those days, lack of duplex communication limited SCADA's ability to work fully in real time or even send and receive data simultaneously. Over decades, SCADA has evolved and proprietary LAN protocols have been employed in order to share the information and distribute the data processing among multiple connected stations. Thereafter, the next generation of SCADA, which represents the current SCADA, uses an increased number of connections between control system, business network and the internet. This interconnection made SCADA systems more vulnerable to cyberattacks that are previously only common in IT security. The next generation of SCADA will heavily depend on Internet of Thing technology and cloud computing in order to reduce the costs and to improve maintenance and integration. Furthermore, with advent of various integrated and robust cloud services, SCADA systems can heavily rely on cloud computing to solve critical issues related to the lack of computation and storage resources for the continuous data streams from hundreds of thousands of data sources on larger power grid. Cloud technology will allow increasing the capacity and adding capabilities on the fly without performing any changes in the infrastructure. However, migrating SCADA devices to the cloud is associated with several security concerns related to the nature of data, web application attacks, control, authentication, encryption, and logging. For example, confidential data is stored on external servers, where it cannot be assured that the attackers do not have access to. Therefore, the lack of encryption, authentication and the loss of control are important factors to consider when thinking of migrating to the cloud [13].

Since the power system operations relies on the use of SCADA systems, the inevitable combination of the old insecure SCADA systems and the modern intelligent power systems make the security of SCADA systems a critical concern. An observation extracted from interviews and surveys with a wide range of participating U.S. and Canadian electric utilities, conducted by Newton-Evans Research, was that SCADA market will be one of the fastest growing in the Smart Grid business between 2013 and 2015 and security concerns will become increasingly important [14].

3.4 SECURITY POLICY DEFINITION

In order to have an adequate security management it is required to have a clear administrative structure and an enforcement hierarchy. A security policy can be considered a root document, having various sections to cover the purpose, scope, etc., of the various security related subjects of a system. To ensure the protection of an IT system and information it is required to set an organization-wide security policy. The latter is meant to cover topics as the overall security risk management program, security goals and strategies, etc. Following, we refer in brief to an example of a SCADA specific security administration policy that is defined as [15]:

3.4.1 SCADA-Specific Security Administration

One of the most common problems seen in modern SCADA environments is the lack of a SCADA-specific security policy. SCADA systems need a separate, SCADA specific security administration structure to ensure that all the specialized features, needs, and implementation idiosyncrasies of the SCADA system are adequately covered. Acceptable use of SCADA should be narrower than IT systems due to its different mission, sensitivity of data, and heightened criticality. SCADA systems are oftentimes used to control time-critical functions. When time is an important factor, some standard IT security practices may not be appropriate for SCADA. For example, since anti-virus scanning can sometimes slow down a system, these may not be acceptable for some SCADA platforms. Therefore, the blanket recommendation in IT policy to include anti-virus scanning on every machine would not be appropriate for SCADA.

The mission in these automation systems may have safety-critical tasks which would preclude any significant downtime. While an IT system can at times allow down-time of hours, an electrical power plant cannot tolerate important safety functionality being lost for any period of time during operation. Also, since automation systems have more immediate physical consequences, interconnections between

- SCADA systems
- SCADA systems and other internal IT-systems
- SCADA systems from different companies
- SCADA systems and external public and private networks

must be better controlled, and interconnections between SCADA systems and external networks must be better controlled, and access must be more strictly enforced and monitored

Immediate adoption of security patches that are essential in IT may be impractical in SCADA. At times, vendor contracts preclude SCADA systems from installing patches that have not been approved and vetted by the vendor. Also, the possibility of a patch disrupting critical functionality is not tolerated in a SCADA system.

Finally, the data produced by a SCADA system may have different sensitivity than the data generated in the business side of the operation. SCADA data also has a different lifetime, so some SCADA data may only need protection for several minutes as opposed to days/months/years for personnel data residing on a business network.

Administration and enforcement is simpler with a separate policy. Trying to tailor a traditional IT policy to include SCADA may seem like a time saving effort, but in reality it is probably not. Trying to capture all the caveats needed for SCADA could be counterproductive and may produce a document which is not easily understandable. The resulting policy will often be so convoluted, watered down, inaccurate and vague that it is difficult to know what is and is not allowed. Since SCADA systems also have a small audience (including SCADA engineers, technicians, operators, and administrative personnel) the detail of the policy sections can be more precisely targeted. Finally, legislative requirements on automation systems are different than other IT systems.

Enforcement Hierarchy

Policy is the cornerstone of any sustainable security system. Systems without security policy and administration do not possess measurable, self-perpetuating security, and experience has shown that every ungoverned information network will eventually sprout vulnerabilities.

Business objectives are also a driving factor of policy. As a business, environments that use SCADA need to identify confidentiality, availability, and integrity requirements for the SCADA network and the data available from the SCADA system. These requirements will drive policy statements.

Risk assessment drives policy by identifying where the system is vulnerable to attack. The risk assessment process involves evaluation, reduction, transference, and mitigation. Security policy addresses the reduction, transference, and acceptance steps. Policy also details when, who, and how evaluations will be performed.

A defined policy is the first step in creating a security program which is self-sustaining and enforceable. Once a policy has been created, other specific security documents (including system security plans and implementation guidance) can be created to define the particular practices to be used within the SCADA environment.

3.4.2 Security policy concepts

Security policy for SCADA administration translates the *"desired security and reliability control objectives for the overall business into enforceable direction and behavior for the staff to ensure secure SCADA design, implementation, and operation."*

Policy Introduction and Background

An organization- wide security policy has the task of ensuring the

- confidentiality,
- integrity and
- availability

of information in an organization.

A security policy is a formal statement of what will and will not be done by persons and systems within an organization. The policy statements are derived from business goals and risk assessments. The Policy shall be appropriate to the purpose of the organization and has to include security objectives. The document shall also be communicated within the organization and has to be available to interested parties. Policy statements are rules – not suggestions or guidelines that users choose to follow. As rules, they require clear and consistent enforcement. Users must observe the mandatory rules within a company. Without consistency, it is very difficult to punish infractions. All employees must have knowledge of the main contents of the information security policy.

Policy must be vendor- and manufacturer-independent. As technologies change and new acquisitions occur, the policy must remain effective. When vendor- or technology-specific statements are used, the maintenance burden for the policy increases. Then, the policy must be changed any time there is a new purchase or an advance in technology. If the policy is not updated, the policies themselves become obsolete, which is not an acceptable situation.

Security policies do not include configuration rules, system setup guidelines, or specific security settings. These elements are important in any sustainable security program, but policy is not the proper place for this type of information. Security plans and implementation guidance is where these should go.

Important Policy Sections

According to [15] and LINZ security policy, a well written policy document must follow an easy-to-read and easily understandable format. Each policy should include:

- Purpose: The purpose section explains why this policy section exists.
- Management commitment: The management supports and promotes activities for information security management. The security policy contains an explicit statement of management's support of security goals.
- Scope: The scope specifies what is covered by the policy (for example, machines, people, and/or facilities).
- Policy: These are the actual statements of the organization's rules on the topic – what can and cannot be done by people, equipment, etc.
- Responsibilities: Who must do what in regards to this policy is specified here.
- References/Authorities: Here, the policy is tied back to other policies that must be followed due to the organizational structure. Also, external references to the policy are cited (for example, legal requirements). Compliance with all laws, contracts and regulations (Privacy Act, the Information Security Act , SLA - Service Level Agreements - and Standards)

- Revision History: This is a record of what changes were made, by whom, and when they were done.
- Enforcement: This specifies the consequences of not following the policy. This may be general and apply to all policies (i.e. subject to disciplinary action up to and including termination) or they may be specific (immediate dis-missal for knowingly and flagrantly disregarding a specific policy). Enforcement may also describe if legal action may be pursued.
- Exceptions: Exceptions might not be needed, but if they exist, each must be documented in the policy. This includes how to get an exception, who can approve it, and were the documentation will be stored. Also, the details about how often the exception must be re-approved are described.

Some of the preceding sections must be included for every part of the security policy that is written, such as policy and scope. Others can be stated once and that statement will apply to all policies (enforcement is a good example).

3.4.3 SCADA security policy framework

A SCADA policy framework as the "SCADA policy framework™", depicted in **Fehler! Verweisquelle konnte nicht gefunden werden.** and described in [15] is able to facilitate the development of SCADA security policies in a simple and easy way. The use of such a framework allows the author of policies to define them in a systematic approach, which ensures that the defined policies address all the critical topics in an adequate way. A virtue of that framework consists also the support of compartmentalizing the policies, i.e., allowing multiple authors to work at the same time with little or no overlap.

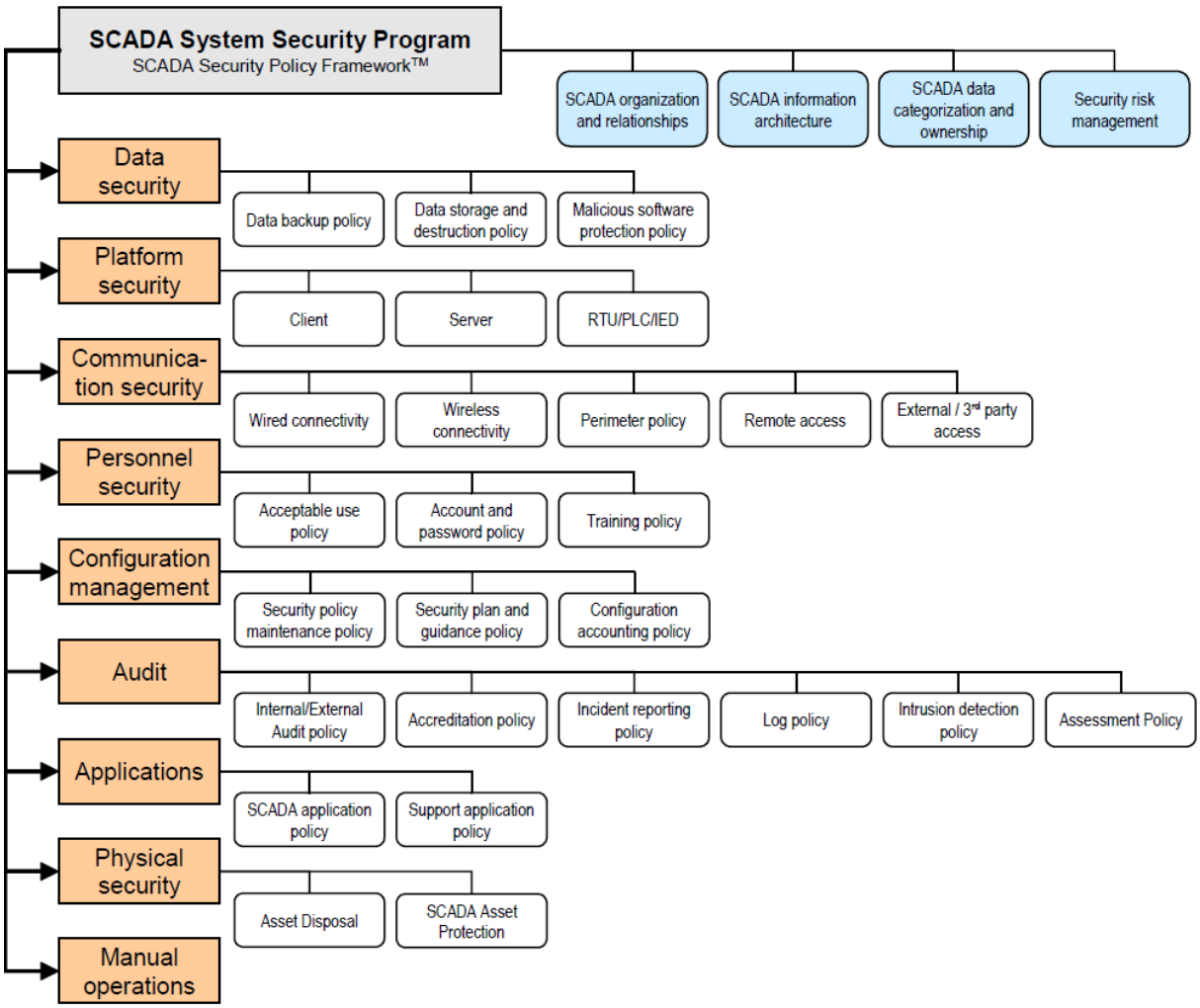

Figure 3. SCADA policy framework
Source: Sandia National Laboratories

Specifically, the writing of policies can start in isolation when then format of them as well as the identification of the most critical policies is completed. The hierarchical nature of the framework provides a great flexibility, and thus, supports the development of policies for various types of organisations. Following, we provide some brief information regarding the "SCADA policy framework™". More comprehensive information is available in [15].

The SCADA policy framework consists of ten main boxes, viz., the SCADA system security program; data security; platform security; communication security; personnel security; configuration management; audit; applications; physical security, and manual operations (depicted in **Fehler! Verweisquelle konnte nicht gefunden werden.**).

In more detail, the SCADA system security program operates as an introductory starting point for the target system, which also provides context for the rest of the policies, and includes valuable information as:

- The definition of the SCADA organisation and relationships since SCADA systems do not operate in isolation.
- Information on SCADA's architecture, providing a reference point for all the readers of the policies.
  A categorisation of the data contained, created, processed and used by the system and their ownership.
  A risk management programme.

A data security policy is capable of determining the treatment of the data categories defined in the security program. It includes a data backup policy, which defines the details with regards to what data and how frequently they should be backed up; a data storage and destruction policy, which describes the life cycle of data; and a malicious software protection policy, which set controls to prevent the installation of malicious software. .

In addition to the platform security policy, which identifies secure configuration defaults that are required within the SCADA system, a communication security policy is also set. The latter includes policies for wired and wireless connectivity; a perimeter policy; a remote access and external third party policy for connections.

The personnel security policy defines requirements, e.g., job or hiring ones. Such sub policies may include an acceptance use policy, which defines what users can and cannot do with equipment and network resources; an accounts and password policy that describes the proper care of passwords and accounts; and a training and awareness policy that copes with personnel and their awareness regarding security policies.

The configuration management policy ensures that a sustainable configuration management process is implemented, and the audit policy determines if protections are being correctly put into practice on the system. The latter includes an internal or external audit; accreditation; incident reporting; logging; intrusion detection; and assessments performed upon the system.

An application policy ensures that applications are configured and used in a manner commensurate with the security needs of the automation system. Such a policy defines policies for SCADA applications; support applications (e.g., databases); a physical security policy; a policy for the physical disposal of assets; and a SCADA protection of assets since SCADA equipment have different requirements than the standard office equipment used in the system. The "SCADA security policy framework™" is concluded with the definition of a policy regarding manual operations, required because of the critical nature of SCADA systems.

4 SCADA CYBER THREATS AND VULNERABILITIES

This project focuses on Hybrid Risk Management for Utility Networks (also known as Critical Infrastructures), and the research study is conducted through an analysis of those elements that may affect the regular functioning of CI. Thus it is important to evaluate and identify the potential critical events, such as malicious attacks on individual or network of critical infrastructures, or accident originated due to natural causes or internal faults.
Still, organizations employing SCADA systems are reluctant to admit that data acquisition and control networks are becoming attractive targets for malicious individuals, terrorist groups, hackers, and, perhaps, organization's competitors.

In fact, different studies [16] [17] [18] [19] [20] conducted on the security of SCADA systems have demonstrated that these systems cannot considered secure and safe.
Despite the awareness of security issues in critical infrastructure is significantly growing, there is not adequate information about SCADA incidents for different reasons. Firstly, companies are unwilling to release attack or incident data and furthermore, it is possible collect information but in most of cases the access to the database is not freely available, thus some sites provides paid subscriptions to access data [16].

This section identifies vulnerabilities, threats, and moreover, provides a list of major incidents in critical infrastructures. The study is conducted to identify all possible scenarios in order to avoid as many as possible incidents.

4.1 VULNERABILITIES

In this section, we provide information with regard to various types of vulnerabilities. We define the term of vulnerability as any type of weakness or flaw in any stage of a product's life cycle that when exercised will result in a security breach. Thus, having an understanding of how a system can be attacked would eventually result in being able to design potential countermeasures to avoid specific attacks

Since there is an increased number of attacks on SCADA based systems their security is required to be scrutinized. Specifically, the main issues that researchers are trying to address appear to be concerned with the following [7]:

- There is no great concern shown on the authentication processes, and /security of the SCADA networks regarding their design, operation and deployment.
- Security though obscurity approaches appear to be applied in SCADA systems, mostly via the use of specialized interfaces and proprietary protocols
- The existence of some physical security mistakenly provides a notion that SCADA systems are fully secure.
- Finally the absence of a linkage (in some cases) with the Internet mistakenly provides the notion of security in SCADA systems.
- It is also noteworthy, that the need for interconnections amongst various utility networks and their related enterprise systems, led to a widely use of mainstream operating systems (e.g., Microsoft Windows™ and UNIX/Linux based operating systems), public networks (e.g., Internet), and also general communication wired or wireless technologies.

Following, we briefly refer to a list of representative vulnerabilities that dwell in SCADA systems, as these are summarized in [21]:

- The existence of different vendors introduces many different characteristics.
- Existence of various protocols and operating systems.
- Management of networks is difficult because of the scattering of facilities over large areas.

- The installation of legacy equipment.
- Data simplicity imposes vulnerabilities because commands are simple and sequential.
- Real-time processing makes it difficult to insert security alarms since they will minimize the response time of the system.
- The linkage of SCADA systems with information systems (i.e., intra-network linkage).
- Use of generalized equipment, e.g., mainstream operating systems and protocols (e.g., TCP/IP)..
- The ubiquitous user since users want to interact with information and services from anywhere.
- The ubiquitous web that delivers and integrates information, services, and user data.
- The ubiquitous user agent, which run on a wide range of devices (e.g., desktop computers).
- Opportunistic scan of networks as the Internet by botnets, and attacks on poorly configured or insecure systems.
- The existence of zero-day exploits.
- Employees that can access the system might result in an insider attack.
- Existence of errors in new software products.

Being more specific, SCADA systems present vulnerabilities that can be classified according to this classification [22] [23] [24]: architectural vulnerabilities, security policy vulnerabilities, software vulnerabilities, communication protocol vulnerabilities and RTUs and SCADA Equipment Vulnerabilities.

4.1.1 Architectural vulnerabilities

This kind of vulnerabilities is strictly related to architecture adopted in SCADA systems. Current SCADA architectures are still substantially the same used in 1980s and 1990s and the reasons are various; firstly the development of a new architecture can bring high costs. Moreover, these architectures have been intensively used and, as result, they are stable and well-known.
After SCADA systems became open with the integration of Internet, they started to show several limits. Initially, process engineers tried to fix the emerging issues using IT past cyber-security situation, but SCADA systems showed more different physical security concerns.

Examples of some architectural vulnerabilities in SCADA systems are:

- Lack of barriers in the network between the **field network** composed by i.e. PLCs, and the **control network** which includes SCADA server and diagnostic servers. There is the firm belief it is improbable an attacker can reach the field network. Although different studies [25] [26] show that it is possible to access it easily;
- Lack of the **authentication** between physical components of the SCADA systems, such as actuators and SCADA servers, or actuators and PLCs. Until recently, in fact, the system has been electronically isolated; therefore it was not necessary to integrate a mechanism of authentication between components connected to the network. The focus was increasing physical security. Now, this vulnerability can be very dangerous because it can be used to perpetrate any sort of damage;
- Presence of **single points of failures**;
- Lack of **network load balancing** and **redundancy**.

The major issue of architectural vulnerabilities is that they are strictly connected to the architecture of the system. The modification of the architecture can affect the performance and the specific needs of the industrial system, furthermore it requires high costs.

4.1.2 Security Policy Vulnerabilities

In order to increase the system resilience to attacks, thus to have a system considered robust, it is necessary introduce security layers and implement policy security. Generally, SCADA systems use the typical security policies implemented in general purpose IT systems. The security policies used to access the physical SCADA components are well implemented, while the security policies related to IT in control

Network are usually not robust; moreover in different situation they are not best-suited for the Control Network and it could be not easy for the operator to recognize some problems related to them.
Common security policy vulnerabilities are:

- Lack of patching policies. Generally patches require the reboot of the system to become effective [22] and this fact may interfere with the production system.
- Antivirus updates policies. The updates need to grant the access of the process system to the Internet or to insert into the architecture a parent server able to dispatch the new signatures. It is generally preferred to update the signatures by hand, keeping the process network as isolated as possible [22] [23] In general, it is preferred to update the signatures by hand, keeping the process network as isolated as possible.
- Lack of consistent security policy guidelines. Access policies are badly implemented on the field, for example the classical post-it attached on a screen with password and login data.

4.1.3 Software vulnerabilities

A software vulnerability is defined as a flaw, weakness or even an error in the system (software or operating system) that can be exploited by an attacker in order to alter the normal behavior of the system.
SCADA systems are managed by software; therefore software vulnerabilities are extremely insidious since potentially they can allow an attacker to take full control of a part of system or all system.
Most of the known vulnerabilities are associated to an incorrect management of inputs by user of the system; if these inputs are not correctly processed before using them inside the program they can generate unexpected behavior of the system.
There are different software vulnerabilities, where the most known are:

- **Buffer overflow**: it occurs usually with fixed length buffers when some data is going to be written beyond the boundaries of the current defined capacity. The new data may corrupt the data of other buffers or processes. The buffer overflow can be used also to inject malicious code, and through the injected code it is possible take control of the system;
- **XSS or cross site scripting**: usually associated to web applications, consists in the injection of code in the pages accessed by other users. If exploited an attacker can bypass access controls, perform phishing [17], identity theft (i.e. gain unauthorized user credentials) or expose connections;
- **SQL injection**: it consists in the injection of code with in order to obtain the content of a database. Usually happens because the inputs are not managed correctly;
- **Format string bugs**: an external data is given to an output function as format string argument. An example of output function is "*printf*" used in C language; this function generates an output according to the specifications of the format string, and, some directives can write to memory locations. Through this function thus the attacker can write malicious code and change the control flow to execute it.

These vulnerabilities can be exploited because, generally, in SCADA the operating system is not patched to most recent version, thus exposing SCADA servers to threats nowadays considered obsolete [22].

Recently [18], Siemens has released software updates to address two critical vulnerabilities in its SIMATIC WinCC supervisory control and data acquisition (SCADA) system, one of which could be exploited remotely by an unauthenticated attacker. SIMATIC WinCC is used to monitor and control physical processes involved in industry and infrastructure, such as Oil & Gas sector. One of them would allow remote code execution for unauthenticated users if special packets are sent to the WinCC server. Both vulnerabilities can be exploited if the attacker has access to the network to the affected system.

There are several research and assessment activities to identify vulnerabilities, in particular different software are available to determine known vulnerabilities in traditional IT systems. For example, there are tools which are used to locate unpatched computers on a network, such as Nessus, FoundScan, etc.
Furthermore, there are a classes of vulnerabilities connected to PLC. Most part of PLCs use a simple

programming language called Ladder Logic to make it easier to program them. The simple nature of PLCs makes them exceptionally vulnerable to being exploited. Usually, the software logic of PLCs is not developed taking into account any kind of security issues [19]. PLCs being so close to the actuators they can be one of the most dangerous sources of threat, in fact by accessing the loaded libraries of the software that control, monitor, or program the PLCs it is possible to manipulate the physical state of anything connected to the PLC, such as the open/close state of valves, and also to suppress any notifications or alarms that are delivered or derived from the PLC.

4.1.4 Communication Protocol Vulnerabilities

A SCADA system consists of a number of remote terminal units (RTU/PLC/IED) collecting field data and sending that data back to a master station via a communications system. SCADA system's operation depends on the data received/sent between the SCADA components. It is important keep attention on communication protocol vulnerabilities because if an attacker gains access to the communication protocol it can generate dangerous situation. An example of exploitation of communication protocol vulnerability would allow forcing the opening or closing of a valve.

Protocols allow the SCADA units to communicate with each other. Nowadays, network architectures are based on ISO (International Standards Organization) standard seven layer OSI (Open Systems Interconnection) model as below:

- **Layer 7 - Application**. All network services provided to the user's application programs;
- **Layer 6 - Presentation**. Regards the data representation (including encryption);
- **Layer 5 - Session**. Control of the communications (sessions) between the users;
- **Layer 4 - Transport**. The management of the communications between the two end systems;
- **Layer 3 - Network**. It is responsible for the routing of messages;
- **Layer 2 - Data link**. It is responsible for assembling and sending a frame of data from one system to another;
- **Layer 1 - Physical**. It defines the electrical signals and mechanical connections at the physical level.

SCADA systems use different communication protocols; each one is positioned at a particular OSI layer. Examples of SCADA protocols are **Modbus**, **DNP3**, **IEC 60870-5**, **Profibus** (serial communication), etc. As remarkable examples, we take in account IEC 608-5 and Modbus protocols.

IEC 608-5-101 and **IEC 608-5-104** protocols are used in SCADA systems, in particular in power utilities sector. These protocols lack in the application layer and the data link layer security. Application layer security is necessary to protect the SCADA systems from Spoofing and Non-Repudiation attacks. Data link layer security is necessary to protect the systems from the Sniffing, Data modification and Replay attacks. A classification of attacks will be discussed in Section 5 (SCADA Cyber-attacks).

Modbus. It is an application layer messaging protocol, positioned at application layer, level 7 of the OSI model providing client/server communication between devices connected on different types of buses or networks [20], such as PLC devices. The devices to get interconnected can use either serial buses or TCP/IP-based communication channels. The Modbus operates according to a classical master/slave principle; the protocol allows one master to manage up to 247 slaves. Only the master initiates a transaction. Modbus protocol delivers messages using TCP/IP and there are some vulnerabilities:

- Lacks mechanisms for protecting confidentiality and for verifying the integrity of messages flowing between a master and slaves, for instance it is not possible to discover if the original message content has been modified by an "attacker";
- Lack of authentication between the master and slaves (i.e. a compromised device can declare to be the master and send commands to the slaves);
- Lack of incorporation of any anti-repudiation or anti-replay mechanisms.

ICCP. Another example of communication protocols, which can introduce wide range of vulnerabilities into the control system, is the Inter-Control Center Communication Protocol (ICCP). ICCP protocol is an international standard protocol used widely in electric utilities. It facilitates data exchange among utilities, control centers, such as SCADA/EMS systems, independent power generators, and others. These interconnections offer numerous benefits such as efficiency, stability and cost benefits. However, ICCP connections provide the attackers with different vulnerabilities, which can be readily exploited by an attacker in order to access and compromise SCADA networks. For example, this protocol transmits data in clear text which can offer an attacker the opportunity to intercept, understand and modify the communications in ways which fit closely his goals. Any credentials that are transmitted in clear text, can be sniffed and used by an attacker to gain increased privileges on the target system. Unfortunately, even encryption, which is not always feasible solution for such time-critical systems, cannot make ICCP connections trustworthy, since these connections are usually with outside entities [27].

4.1.5 Vulnerabilities of RTUs and SCADA Equipment

A great number of protocols and devices that are used in industrial systems are not designed with security in mind. What is usually done is that they rely on the principle of security through obscurity. It is worthy to note that some of the leading protocols for SCADA systems (e.g., DNP3 in North America and IEC-101 in Europe) [24] do not implement mechanisms for performing source authentication or validation of any of the received commands. As a proof of concept, in Project Aurora there was a demonstration of that vulnerability in 2007 at the Idaho National Laboratories. The demo presented a successful penetration of hackers in a mock substation, and caused a generator to self-destruct. Also, the STUXNET virus discovered in 2010, consisted of a virus able to exploit this vulnerability.

Furthermore, the lack of using open standards, and the application of proprietary solutions to RTUs and SCADA equipment also pose challenges. This persistence to proprietary solutions appears also to forbid utility operators from making modifications to SCADA systems. Such modifications would result in strengthening the overall security of systems since they are mainly considered with upgrading older-generation operating systems, or keeping them current with updated security patches. Thus, having a set of legacy hardware devices and software, which are not appropriately patched results in a highly vulnerable environment to attacks since many of their security holes may be public and well documented knowledge, and thus, easy to implement and exploit.

4.1.6 Vulnerabilities of public information availability

Another category of weaknesses which could adversely impact the operation of SCADA systems is publicly available information [27]. Wide range of information about utility companies and their control systems can be published and made publicly available. This information varies from general information about a utility company, such as company structure, employee names and email addresses to more specific information about used control system, such as operating systems, management applications, open devices, topology and even system configurations. Aside from the goal behind publishing of such information, attackers can use it in order to identify and select their target network and to start a more focused and devastating attack. The publishing of such information can inadvertently provide the foundation for performing successful social engineering tactics, which are used in acquiring as much information as possible about people, organizations and organizational operations. Websites and search engines often provide highly interesting information for attackers about product names, product versions, employee contact data and default usernames and passwords. For example, the search engine Shodan [28] can be used as an information gathering system for hacking attempts. Shodan can easily find and provide information about open SCADA devices that are connected to the internet. It support different search parameter such as country, operating system and port. Thereafter, the search results can be used to prepare and initiate successful attacks against targeted SCADA systems. The use of Domain Name Service (DNS) servers can sometimes represent another example of vulnerabilities related to open source information. Some

administrators of DNS servers use DNS zone transfer mechanism to replicate DNS databases across a set of servers. DNS zone can contain sensitive information about the control system, such IP addresses and server hostnames. Hence, such information, which was originally not publicly accessible, become available to unauthorized users because of performing a zone transfer. Another potential vulnerability associated with publicly available information is the use of default passwords from the manufacturer in the operational system. Default passwords can be assumed published information. Therefore, using such passwords can provide the best opportunity for the attacker to get access to the device that control the process. According to [29], there are a huge number of printers, servers and system control devices, which use the pair (“admin”,”1234”) as their (<user name>, <password>). This information was obtained through looking for “default password” using the aforementioned search engine, Shodan.

4.2 SECURITY THREATS

"Threat is that event with a potential negative effect on SCADA system. A threat is directed against the confidentiality, integrity, or availability of a SCADA system [22]". The threat can be seen as the exploitation of a SCADA vulnerability, in particular the occurrence of this event may have place through different means which permit to access the SCADA system [22].

Natural occurrence, malicious acts by individuals, accidents, improper procedures, or technical failures can be considered threats to SCADA systems. Nowadays, the most dangerous threats are the threats belonging to terroristic groups and hostile nation states [23]. These threats refer to organized group with a defined goal and deep knowledge of the company targeted for the attack. Another category of threat is that posed by internal sources, such as company's own employees, plant operators, or technical support staff. Company workers have access to internal controls and data, and they can originate a threat either by accident or malicious. Included are also threat posed by casual hackers, known as "script kiddies" [25].

Generally, threats are classified as follows [26]:

- Natural threat. Natural disasters not strictly controlled by human such as earthquakes, tornadoes, fires, thunderstorms, snow storms, hurricane, flood, lightening, hail, animal, etc.;
- Accidental threat. Failure of network devices and the wrong human decisions, such as human errors, operational fault, system equipment failure, accident due to the poor management, interruption of utilities or interference during normal execution of service utilities, maintenance services that causes plant shutdown and start-up, etc.;
- Malicious threat. Intentional actions undertaken by different agents (terrorist, criminal group, cyber-attackers, copper theft, vandal, psychotic, malware writer, etc.) by various means (explosives, malware, etc.);
- Emerging threat. The threat emerged with the evolution of utility network such as the integration of renewable energy and the interdependency between other networks.

Generally, natural threat and accidental threat are catalogued as conventional threat; and malicious threat and emerging threat are treated as unconventional threat.

In addition, regarding the Energy utility sector, Massoud Amin (EPRI - Electric Power Research Institute) defined three different kinds of threats related to power systems and the consequent attacks [30]:

- Attacks upon the power system. The primary target of the attack can be a single component of the critical infrastructure, such as a substation or transmission tower. Or there could be multiple attacks in order to bring down an entire area grid;
- Attacks by the power system. The target is the population. The attackers use the power plant to create damage and dangerous situation to the population, for example, to disperse chemical or biological agents.

- Attacks through the power system. The goal of the attacker is the civil infrastructure using the resources of the power plant, for instance they could shot down the telecommunication infrastructure through high voltage application.

The first threat is related to cyber security, while the other two are related to physical security.

4.2.1 General SCADA security threats

Following, we summarize a list of ten security threats in SCADA systems, as these are identified in [21] and [31] .

The process of standardization, i.e., the move from proprietary to standardized software has made systems more vulnerable. This holds since standards are well documented, and thus, it might be easier to find any existing vulnerability or weakness. In the past, SCADA systems were also partially benefited from the application of "security through obscurity", due to the use of proprietary solutions.

Shared networking is utilized to benefit from shared resources since a lot of organizations operate on the same network. Nevertheless, it may be the case that some of the nodes in that shared network is connected to widely used and public networks as the Internet. In this case, a malicious user (e.g., a hacker) might be in position to identify a potential point of entry for some of these organizations, and eventually leverage his/her access to a SCADA system.

The existence of low-speed connections with long polling cycles might provide to a hacker the potential to take advantage of this. More specifically, examples of technologies as the analog radio, which have minute-long polling cycles, may be taken into advantage by hackers in order to attack RTUs immediately after a communication is finished.

Alternative communication technologies might be used to maximize reliability. Such solutions provide a fail-safe way of communicating with a system, even in the case of a failure. An example of such a communication technology consists that of a dial-up telephone line.

Radio communications impose also a threat to many SCADA systems, e.g., omni-directional base station antennas and the employment of directional antennas by individual nodes. This will provide the potential to an attacker who is in the system's radius to intercept the base station's messages. Moreover, the attacker might be able to detect these nodes as well. Once both sides of the communication can be heard, it is not difficult to determine the protocol and the system setup, and to deploy a man-in-the-middle-attack.

In case an attacker is able to eavesdrop traffic, as in the previous case, he/she might also be in position to perform various adjustments without having to visit each node physically. This is feasible since various SCADA systems allow on-the-fly programming of RTUs through the same communications channel used for routine message passing. In turn, operations such as download, evaluation, and re-program of an RTU is considered to be feasible.

When an industrial control system is linked to an enterprise system, the latter might provide a point of entry for an attacker. For instance, when customers use the Internet to get information (e.g., account information) though a Web server, the internal systems may be under attack through the servers being exposed to the outside. A hacker or virus might have caused this. Even though security controls as IDSs, firewalls, and anti-virus applications may be in place, this may be of no use when it comes to protection against new attacks or vulnerabilities.

Similarly to the aforementioned type of threat, there may be also the possibility of having a remote intrusion in the control systems. This could be feasible via the use of utilities and tools made to connect with the ICS/SCADA. It is the case that when utilities or tools are used to directly control the control

systems, it is extremely hard for the placed security controls to detect and block intrusions, and to notify operators about that.

There are cases that vendors might place backdoors for connecting to services or ports to remotely access and support systems. Such a backdoor is considered as a possible point of entry to the internal system.. Therefore, after a system is constructed and delivered, sometimes such a backdoor remains enabled for remote access. In this case, intrusion incidents may occur.

- A similar threat to the previous may be considered to be that of accessing the servers placed in Internet Data Center or certain secure locations. Most managers do not work in front of their systems. Instead, they use remote management tools to manage and control their systems. Therefore, the existence of remote management tools (e.g., PC Anyware, Terminal Server and VNC (Virtual Network Computing) impose a great threat. The control of SCADA or DCS systems via a remote management tool may result in having direct attacks against them.

4.2.2 Advanced Persistent Threats

Advanced persistent threat (APT) is a term commonly used to refer to cyber threats, and usually refers to groups that have both the capability and intent to persistently and effectively target a specific entity. APT are used many times as a mean to perform espionage, and may utilize various attack vectors for its spread, including these of infecting a media; compromising the supply chain, or even apply social engineering approaches. Usually, APT are used to characterize threats that have a long-term pattern of sophisticated hacking attacks aimed at governments, companies, and political activists, and by extension, also to refer to the groups behind these attacks. Following, we refer to a definition of APT based on [21]:

Advanced: Operators of the threat have a full spectrum of intelligence-gathering techniques at their disposal. Such techniques include, computer intrusion technologies and techniques, telephone-interception technologies, satellite imaging, etc. The operators are in position to develop the advanced set of tools they require, and often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it.

Persistent: Operators give priority to specific tasks, rather than opportunistically seeking information for financial or other gain, and thus, imply that attackers may be guided by external entities. To achieve the defined objectives, continuous monitoring and interaction is conducted. One of the mains goals of the operator is to maintain a long-term access to the target. In case of loss of access to the target, they usually retry to access that, and usually succeed in that.

Threat: A main difference between an APT and other threats is that in the former cause the threat has both a capability and intent. Therefore, APT attacks are executed by coordinated human actions, and is quite unlikely to be executed by mindless and automated pieces of code. The people that operate an APT are known to be funded, and thus, have a specific objective. In overall, they could be characterized are highly skilled, motivated, and well-organized people.

Examples of the most powerful, systematic and popular APTs are: Stuxnet, DuQu and Night Dragon, which are described more in detail in section 4.4

4.3 THE BACK DOOR INTO THE CONTROL SYSTEM

Security through obscurity, disconnecting from the internet, isolating industrial control system and many other mechanisms, can readily reflect the fact that the industrial systems or at least important subsystems of these systems, such SCADA and control systems, are designed with the security as no matter of priority or even without any security in mind. The prevalent belief is that these systems are secure because they

are not connected to the internet. Actually, this security model has been long applied to protect critical industrial control systems that offer various public services, such as power, water, gas, and many others. However, taking the large number of viruses getting into these systems and associated security incidents can immediately lead to the twofold realization: first, this model is no more secure and not adequate at all in order to protect such critical infrastructure. Second, there are wide variety of remote points of entry and pathways to the control systems. One concrete example of existence of various remote entry points is Stuxnet. This malware has succeeded in getting into the disconnected Iranian nuclear facility and spreading indiscriminately. Then, it has caused a massive disruptive damage to the targeted industrial process, i.e. the Iranian nuclear enrichment program. Figure 4 depicts the results of a study conducted by a team of the Industrial Security Incident Database (ISID)[1] to identify the major categories for remote entry points into SCADA and industrial control systems. The study team has identified the following major categories [32]:

- Corporate Business LAN,
- Corporate WAN,
- Internet,
- Dial-up modem,
- Wireless system,
- Trusted Third Party,
- VPN connection, and
- Public Telecommunications Network.

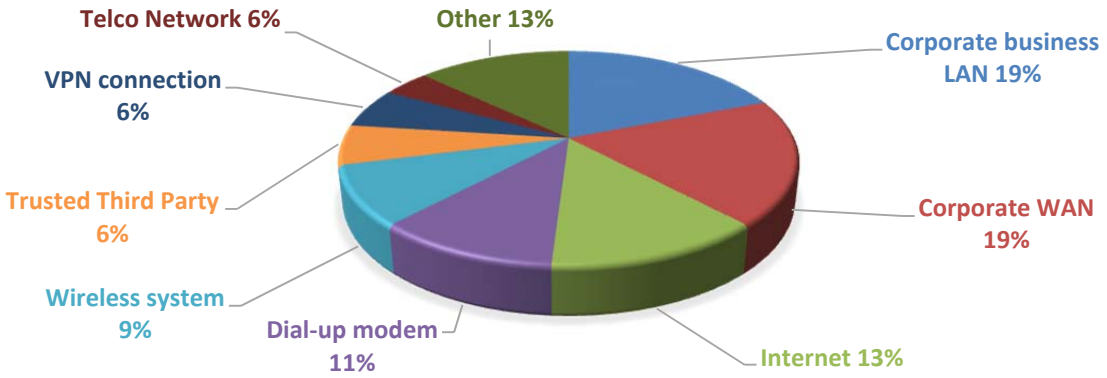

Figure 4. Remote points of entry charted as a percentage
Source: Industrial Security Incident Databse (ISID)

Moreover, the various infiltration opportunities in control systems are not only introduced by using old technologies such dial-up modems, but also by integrating modern technologies such as mobile devices and wireless technology. Dial-up modem is widely used to allow remote support of control systems located in remote locations. The main vulnerability of such devices is caused by using weak passwords or even no supporting for passwords at all. In contrast, new technologies, such as laptops and PDAs, support usually advanced security mechanisms and they are capable to be used in a variety of environments of different security policies, for example, plant and home environments. Hence, these devices create significant pathways for the attackers to get access into high secure environment, such as critical control systems through infecting their devices during the existence in less secure environments, such as home networks. Furthermore, the integration of some security solutions can create opportunities for malicious intrusion. For example, VPN provides secure communications into the control network across insecure public networks by using encryption technologies. However, VPN connections do not protect end-nodes or networks against data-driven attacks, such as viruses. Hence, VPN connections can easily bypass firewalls because the encrypted content cannot be checked and matched with the defined firewall rules. Therefore,

[1] ISID is intended to serve as an industrywide repository for collecting, analyzing, and sharing high-value information regarding cybersecurity incidents that directly affect SCADA, manufacturing, and process control systems.

VPN can limit or even disable the function of the Firewalls, which are set up to separate the control systems from the corporate business networks in order to prevent hacker and malwares from getting into critical networks as SCADA.

Therefore, it is important to emphasis the fact that for reason of convenience and efficiency most control networks are accessible from multiple pathways, not only from one. This issue can significantly complicate the task of securing the control network, whereas for attackers it increases the possibilities to get access into the control networks. Figure 5 can clearly show this issue and illustrate a few of the locations of possible infiltration paths in segregated control/SCADA networks.

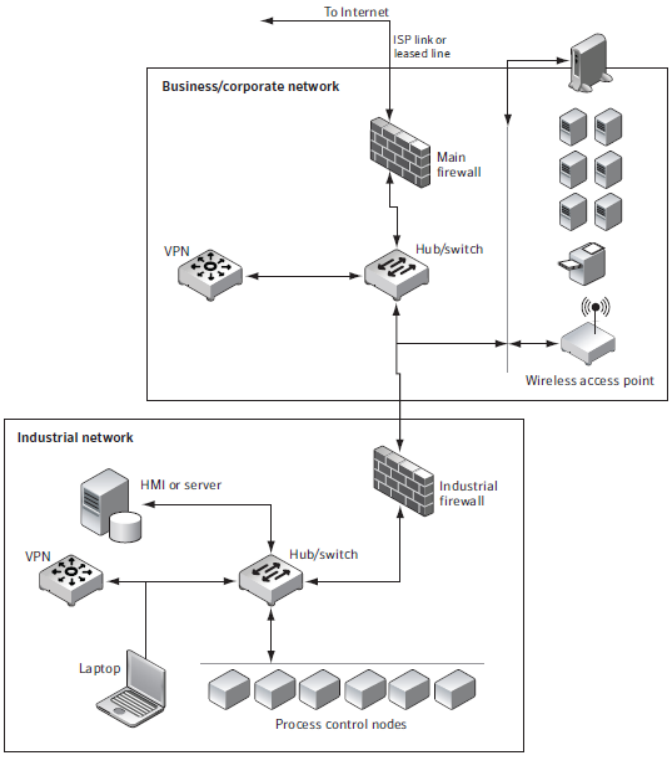

Figure 5. Typical entry points in control network structure
Source: Industrial Security Incident Database (ISID)

4.4 RECENT SECURITY INCIDENTS IN CRITICAL INFRASTRUCTURES

Critical Infrastructure Incidents

There are actually various factors that contribute to the increasing attractiveness of SCADA as a target of cyber-attacks. SCADA and ICS systems have been increasingly connected to business networks and to the internet without properly considering the fact that these systems are unready to confront the wide variety of potential attacks in cyberspace. Hence, this makes these systems an easy target for attackers even for amateur attackers, who may enjoy conducting serious attacks and causing a physical and real-world harm or disruption. The nature of SCADA systems and the critical services they control and operate can easily pave the way for granting the cyber-attacks the physical appearances in our real world. Therefore, it is of a vital importance to look at the reported historical attacks against critical infrastructures in order to understand how to defend against potential future incidents. The following are critical infrastructure security incidents that have occurred during the last years, presented in chronological order and pointing out different attack strategies and impacts [33]:

- **Siberian Pipeline Explosion (1982)** [34]**:** In this attack a "Trojan Horse" was introduced to the computer control systems, which control and operate the Trans-Serbian gas pipeline. The malware has manipulated the control system in such a way that the produced settings were far beyond the

acceptable limits and boundaries. This resulted in a tremendous explosion. In fact, this incident represents the first cyber-security incident involving industrial control systems.

- **Chevron Emergency Alert System (1992)** [35]**:** This attack has been conducted by a fired employee of Chevron's emergency alert network. The attacker has hacked computers in New York and San José, California and succeeded in bringing the alert system of the firm down. Due to the disabled alert system the Chevron refinery in Richmond, California, could not deliver an emergency notification of the release of a noxious substance. As a result, thousands of people were put at risk during a time period of 10 hours. [43]
- **Salt River Project (1994)** [36]**:** As explained in the section 4.3, dial-up modems represent a significant remote entry point category to gain unauthorized access into industrial control systems. In 1994, an attacker used this vulnerability by exploiting dial-up modem communications to get access to Salt River Project computer network. Then, he could have at least one 5-hour session on mission critical systems controlling a 131-mile water canal system used to transport water to customers in the Phoenix metropolitan area. During this attack, various types of data were captured, such as operational, financial and personal information. In addition, some data has been unauthorized modified, such as login and password files, log files, and root privileges. The estimated losses added up to $40,000, not including lost productivity due to the incident [43].
- **Worcester, MA Airport (1997):** In this attack, one teenager hacker has succeeded during two days in disabling two telephone company computers. The first result of this attack was cutting off the telephone service to different sectors of Worcester Airport in Massachusetts for six hours. The second impact of this attack was causing a power outage in the Rutland area, which in turn resulted in several negative consequences on the public health and public safety [43]]
- **Gazprom (1999)** [37]**:** In this attack, one teenager hacker has succeeded during two days in disabling two telephone company computers. The first result of this attack was cutting off the telephone service to different sectors of Worcester Airport in Massachusetts for six hours. The second impact of this attack was causing a power outage in the Rutland area, which in turn resulted in several negative consequences on the public health and public safety [43]
- **Bellingham, WA Gas Pipeline (1999)** [38]**:** This is a vital example of inadvertent incident involving critical infrastructure. On June 10, 1999, about 237,000 gallons of gasoline were released from a pipeline, which is owned by Olympic Pipe Line Company, into a creek flowing through Whatcom Falls Park in Bellingham, Washington. Then, the gasoline ignited and burned about 1 ½ mile along the creek. As a result of this accident, there were three deaths, eight documented injuries, and a total property damage accounted for $45 million. According to the results of Safety Board's investigation, one probable cause of the pipeline rupture was the company's practice of performing database development work on the SCADA system while the system was being used to operate the pipeline. This action has rendered the system non-responsive at a critical time during pipeline operations. The loss of human life in this incident can illustrate the high cost of failures in a critical infrastructure system and the potential immediate impact on public health and safety. [43]
- **Maroochy Water System (2000)** [39]**:** In Maroochy Shire, Queensland, Australia in 2000 a disgruntled ex-employee hacked into a sewage control system, which was controlling and operating 142 pumping stations. The attacker intercepted the communication between the control system and the pump stations. Hence, he succeeded in disabling the pumps and preventing the alarms from being reported to the control system. The attack resulted in significant environmental damage by flooding the grounds of a hotel, parks, and a nearby river with large amounts of sewage
- **California System Operator (2001):** In May 2001, Hackers broke into one of the computer networks at the California Independent System Operator (Cal-ISO). The Cal-ISO company has integrated a variety of operational systems that run the electricity grid of the state of California. The intent of the attack was unclear because of the lack of apparent damage. However, this attack represented a serious attempt to compromise the security of the company, in particular, because it remained undetected for a period of 17 days.
- **Davis-Besse Nuclear Power Plant (2003)** [37]**:** In January 2003, the SQL Slammer worm infected the private network of Davis Besse nuclear power plant in Ohio, USA. The worm caused a denial of

service on some hosts connected to the internet because of flooding routers with high network traffic. As a result of the worm's activity the plant's Safety Parameter Display System and Plant Process Computer were disabled for about five hours.

- **CSX Corporation (2003)** [40]**:** In 2003, train signaling systems in Florida were disabled by using a computer virus named Sobig. The trains were delayed as a major impact of this infection. The virus, which rapidly spread as an email attachment, was successful in shutting down several parts at CSX Corporation, such as signaling and dispatching systems.. [
- **Tehama Colusa Canal Authority (2007)** [37]**:** In a similar case to incidents of Gazproom and Maroochy Water System, also a disgruntled employee at Tehama Colusa Canal Authority (TCAA) installed unauthorized software on the TCAA's SCADA system. There were no technical reports or analysis having been publicly released of the caused damage.
- **Operation Aurora (2009)** [41]**:** Operation Aurora was a series of cyber-attacks conducted by advanced persistent threats such as the Elderwood Group based in Beijing, China, with ties to the People's Liberation Army. First publicly disclosed by Google on January 12, 2010, in a blog post, the attacks began in mid-2009 and continued through December 2009.

  The attack has been aimed at dozens of other organizations, of which Adobe Systems, Juniper Networks and Rackspace have publicly confirmed that they were targeted. According to media reports, Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical were also among the targets.

  As a result of the attack, Google stated in its blog that it plans to operate a completely uncensored version of its search engine in China "within the law, if at all", and acknowledged that if this is not possible it may leave China and close its Chinese offices. Official Chinese media responded stating that the incident is part of a U.S. government conspiracy.

  The attack was named "Operation Aurora" by Dmitri Alperovitch, Vice President of Threat Research at cyber-security company McAfee. Research by McAfee Labs discovered that "Aurora" was part of the file path on the attacker's machine that was included in two of the malware binaries McAfee said were associated with the attack. "We believe the name was the internal name the attacker(s) gave to this operation," McAfee Chief Technology Officer George Kurtz said in a blog post.

  According to McAfee, the primary goal of the attack was to gain access to and potentially modify source code repositories at these high tech, security and defense contractor companies. "Software configuration managements (SCMs) were wide open," says Alperovitch. "No one ever thought about securing them, yet these were the crown jewels of most of these companies in many ways — much more valuable than any financial or personally identifiable data that they may have and spend so much time and effort protecting."
- **Stuxnet (2010)** [42]**:** The Stuxnet malware worm has been called an incident "that marks a new age of cyber warfare". It was discovered in June 2010. Stuxnet Central provides a hub for the information that Byres Security has created regarding Stuxnet, along with links to key industry material. Stuxnet has infected at least 22 manufacturing sites, and it appears to have impacted its possible target - Iran's nuclear enrichment program. Using human vectors, local area network communications or infected project files, Stuxnet reached its PLC targets. Stuxnet digitally signed with two authentic stolen certificates, making it difficult to detect, and could be upgraded remotely via peer to peer networking. Stuxnet used Windows vulnerabilities as the vector for infection, comprising multiple computers in the network via the host operating system. Exploiting zero-day vulnerabilities makes the discovering of the malware extremely difficult. Stuxnet's target was disabling the centrifuges used at the infected facilities. To achieve this goal, Stuxnet changed the electrical current frequency to the frequency-converter drivers, which were used to power to the centrifuges. This led the drives to switch between high and low speeds at absolutely extraordinary rate, which in turn caused the centrifuges to fail. The Stuxnet worm is estimated to have taken several man years to develop and uses complex programming techniques, cryptography and a command and control structure.
- **Night Dragon (2011)** [37]**:** In February 2011 McAfee reported that five global oil, gas and other energy companies were targeted by a combination of attacks, called "Night Dragon". This attack

has combined a variety of hacking techniques with set of relatively unsophisticated attacking tools including social engineering, trojans and Windows-based exploits. The attackhas been confirmed to have been ongoing for at least two years. The complexity of the attacked corporate systems has made it difficult to link the various malicious activities together and hence discover the attack at an early stage. Due to usage of Chinese hacking tools, the attackis believed to have been of Chinese origin. However, the Chinese tools may simply be used by attackers in order to distract the eye away from their identity. While no SCADA systems were directly attacked, the corporate network segments belonging to companies that operate SCADA infrastructures were attacked. It is reported that attackers exfiltrated data such as operational blueprints.

- **DUQU (2011)** [43]**:** In September 2011, a new form of Malware was discovered. The malware is closely related to Stuxnet due to discovering several similarities, such as exploiting windows zero-day vulnerabilities and signing component with stolen digital keys. However, the new malware has completely different purposes. The malware has been dubbed Duqu. Duqu was not self-replicating and did not contain a payload. It appears to be designed to gather information about unknown industrial control systems in order to prepare for future attack scenarios.
- **Flame (2012)** [44]**:** Flame appears to be a carefully crafted attack toolkit for industrial or political espionage. Flame shares many characteristics with notorious cyber-weapons Duqu and Stuxnet: while its features are different, the geography and careful targeting of attacks coupled with the usage of specific software vulnerabilities seems to put it alongside those familiar 'super-weapons' currently deployed in the Middle East by unknown perpetrators. Flame can easily be described as one of the most complex threats ever discovered. It is big and incredibly sophisticated. It pretty much redefines the notion of cyberwar and cyberespionage. Currently there are three known classes of players who develop malware and spyware: hacktivists, cybercriminals and nation states. Flame is not designed to steal money from bank accounts. It is also different from rather simple hack tools and malware used by the hacktivists. So by excluding cybercriminals and hacktivists, it can be concluded that it most likely belongs to the third group. In addition, the geography of the targets (certain states are in the Middle East) and also the complexity of the threat leaves no doubt about it being a nation state that sponsored the research that went into it. From the initial analysis, it looks like the creators of Flame are simply looking for any kind of intelligence - e-mails, documents, messages, discussions inside sensitive locations, pretty much everything. Of course, such highly flexible malware can be used to deploy specific attack modules, which can target SCADA devices, ICS, critical infrastructure and so on.
- **Shamoon (2012):** also known as W23.Disttrack is a self-replicating destructive malware. Like Stuxnet, Duqu and Flame, the energy sector was also the target of this malicious software. Its attack against the energy infrastructure in the Middle East; namely against Saudi Aramco company, was announced in August 2012 by Symantec [45] and Seculert [46]. The malware with its extremely destructive potential corrupted the information on 30,000 to 55,000 workstations of the infected information network owned by the company and made them unusable [47]. The virus functions by targeting the information network of the attacked organisations, then destroying computers by deleting and overwriting the stored critical data, their master boot records (MBR) and the partition tables in order to completely disrupt their operations. Hence, Shamoon has been considered one of the most damaging malware against critical infrastructures' information network since discovering the sophisticated virus known as Stuxnet in 2010. Unlike Stuxnet, Flame and Duqu, which represent the most known and highly advanced attacks on the critical infrastructure, Shamoon seems to be designed neither to intentionally damage or disrupt the industrial process, nor to espionage.

  The malware has been introduced to the organization's network by an insider with some privileged access to the company network. An infected USB stick has been plugged in a computer of the local network. Then, the virus has spread by taking advantage of the network shares.

  According to Symantec, Shamoon consists of three different modules which act together to form the entire functionality of the malware [45]

  - Dropper: It represents the main module, which is responsible to create the botnet. It performs two main tasks after being introduced to the target network

- Dropping the other components (i.e. Wiper and Reporter) onto the compromised nodes.
- Infecting other nodes in the same network by exploiting the network shares.

▪ Wiper: This module represents the destructive functionality of the malware. It is responsible for compiling list of files on the infected workstations. Then, these files with the MBR and partition tables are deliberately overwritten with corrupted data so that the data will be rendered unrecoverable. In the case of no regular back up actions have been taken, all corrupted data will be lost forever.

▪ Reporter: this component sends information about the overwritten files back to the relevant botnet operator (i.e. command-and-control C&C server)

Based on the reporting and analysis of this virus, there is no direct evidence that Shamoon specifically targets SCADA or ICS components. According to the incident reports there were not any interruptions of the industrial process operation. Nevertheless, corrupting data on such large number of the workstations of the business and information network could hardly happen without any damage and any adverse impacts on the relevant critical infrastructure operations. Moreover, the increased rate of automation and interconnection of the utility networks increases the probability of negatively affecting the industrial control system or further other interconnected and dependent utility networks through such security incident in the business network of one of the interconnected utility networks.

Shamoon shows clearly the threats, which our contemporary networked world is facing, and especially, the SCADA and ICS components as a main part of this world, on the one hand, and as an integral part of the critical services, on the other hand. Additionally, this incident can actually make the utility providers realize the potential effective disruption, which could be caused by an insider attack even in the case of unsophisticated amateur malicious activity such as Shamoon. Hence, Shamoon-like attacks must put the utility provider on the alert and be carefully considered.

- **):** Symantec recently released a comprehensive Security Response [48] describing a 2013 cyber-attack on European and US energy infrastructures, called “Dragonfly” (also known as Energetic Bear) [49] [50] [51]. The security company F-Secure have been tracking one of the malware variants that were used as part of the attack, called Havex [49]. In a number of different stages, the attack used spear-phishing, water-holing and Remote Access Tools to compromise a number of important organizations in the United States, Spain, France, Italy, Germany, Turkey and Poland. Spear-phishing is a form of attack that targets individuals or organizations with, for example, targeted emails that redirect readers to malicious websites that contain viruses that infect the targets computers. Closely related to spear-phishing are water-holing attacks, whereby an attacker guesses the type of websites a set of target organizations typically visit, e.g., news sites for a specific sector, and aims to infect the site with malware that compromises the target’s computers. For Dragonfly, these targets included energy grid operators and electricity generation firms, as well as oil and gas infrastructure and industrial control system equipment manufacturers. It is understood that the attack was focused on exfiltrating data and authentication credentials, but also included infecting control system software packages with malware. Whilst the purpose of these attacks was the exfiltration of data from the targeted organizations, the infected control systems could have been used as a basis for an attack that sought to cause power outages, for example.

  Dragonfly represents the most recent and sophisticated attack targeting the industrial sector and critical infrastructure organizations. Unlike Stuxnet and Shamoon, which targeted mainly energy sector in the Middle East, the targets of this attack are located basically in US and Europe. The most malicious activities are in Spain, United States and followed by France, Italy, Germany, Turkey, Poland, Romania, Greece and Serbia with less number of detected infections [48].
- **Norwegian Oil and Gas Company (2014):** More than 50 Norwegian oil and energy companies have been hacked by unknown attackers. Furthermore, 250 additional companies have been warned by National Security Authority Norway. In 2011 a similar attack to oil, gas and defense sector firm were targeted by spear phishing e-mail attacks. Still, the methods and motives of the attack stay unknown.

4.5 WHAT CAN WE LEARN FROM SECURITY INCIDENTS?

Great concern has been expressed regarding the security of SCADA systems in the light of the breach that occurred in many critical infrastructures. The analysis of several incidents and the response to them can be useful to prevent or even deter from attacking the SCADA system. Therefore, the ability to respond to critical incidents and to analyse and learn from what happened is essential. Security of critical infrastructures is an urgent issue, in particular in EU where HyRiM project is focused. The European Union Agency for Network and Information Security (ENISA) organisation pointed out guidelines aimed at improving the security of a critical infrastructure and consequently its SCADA system, using as starting point the study of previous critical incidents. Therefore, firstly there is the phase where specialists (i.e. SCADA operators and security engineers) lead the ex post incident analysis in which helpful information regarding security are collected in order to have an in-depth knowledge of what happened.

In addition, the understanding of the circumstances under which a security incident occurred gives enough information in order to create a strategy to respond to changes of internal or external threats, and minimize the outages of critical infrastructure.
The collection of the evidences related to incidents permits to pinpoint the actions that took place during the incident and, perhaps the identity of the attacker. These evidences can be recovered through IT systems, such as network traffic and operating system (OS) log files. In particular, this analysis has the following aims [3]:

- Identifying the target of an attack;
- Deducing the attacker's actual goal (if possible);
- Identifying the vulnerabilities of the system on which the attack was based;
- Discovering a possible data theft and traces that can be used to reveal the source of the attack.

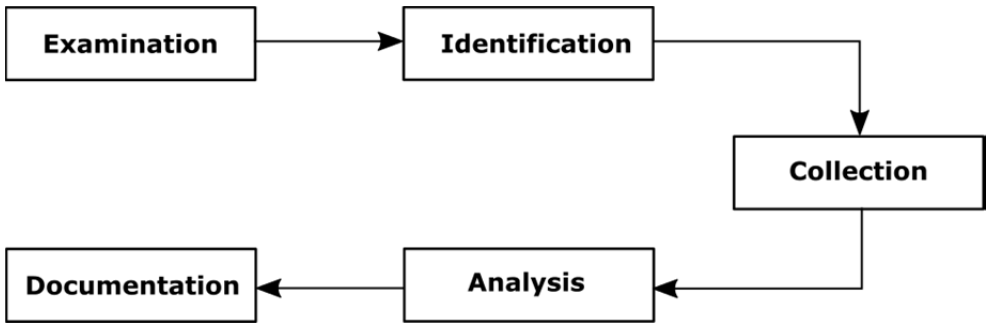

Figure 6. Schematic of incident analysis process.
Source: ENISA 2013

The incident analysis involves different phases as depicted in
Figure **6** and listed below:

- **Examination**: this phase involves the understanding of all the potential sources of evidence in a SCADA system and any other system related to them, such as access to the terminals, logging servers and routers.
- **Identification of evidence**: the first step of this phase is the identification of the type of system under investigation. Once the type of system has become known, the next step is to recognize the operating system used, specific types of PLCs, and the network design and implementation.
- **Collection of evidence**: i.e. the collection of data from all the systems with memory components that have been identified during identification of evidence.
- **Analysis of evidence**: the data collected are analysed and then identified as evidence.

- **Documentation of the process and results:** all the process involves the writing of comprehensive documentation, and each note has to be kept with records of time, date, and the person responsible plus other essential information**.**

As described above, during the post incident analysis there is the phase in which information are gathered. A description of types of data that can be extracted from the components of SCADA system, based on the underlying control technology and the acquisition tool used, is given in Table 3..

	Control Centre	Field Devices
Modern/Common Control Systems Technologies	• Network traffic capture. • Contact system administrator in case of modified OS on HMI (human machine interface).	• Device is off: Examination of device for possible evidence. • Device is on: Date and time, current active processes and current running processes.
Modern/Proprietary Control Systems Technologies	• Network traffic capture. • Interaction between the investigator and the vendor (mandatory).	• Network logs. • Control centre's logs regarding field devices. • Interaction between the investigator and the vendor (mandatory). • Embedded vendor-specific security mechanisms.
Legacy/ Proprietary Control Systems Technologies	• No logging functionality. • No longer supported by the vendor. • The owner of the equipment may provide some information. • Serial-based communications; network traffic cannot be captured.	• Serial-based communication; network traffic cannot be captured. • Rapid rate of sampling and data override • Rapid rate of sampling and data override. • Interaction with the vendor (mandatory).

Table 3. Types of data that can be extracted from the components of a SCADA system
(Based on the underlying control technology and the acquisition tools used)
Source: Symantec 2014

In general, the security community has focused much of its attention on security protection measures using a defense-in-depth strategy [53], with security controls such as firewalls and various authentication mechanisms, for example, being arranged in a layered manner. Whilst these activities are undoubtedly important for securing critical infrastructures, threats such as APTs make it clear they will inevitably be breached. Consequently, we can draw the following conclusions:

- ***The need for information sharing is paramount:*** the sharing of threat intelligence and incident information is important to support the prediction of sector-specific threats so that an organization's risk posture can be adapted, if necessary. Furthermore, shared incident information could lead to a reduced impact of an attack because an incident can be addressed more rapidly using the information.
- ***Incident response management is critical:*** Closely related to the sharing of incident is the development of suitable incident response strategies, such that the nature and impact (e.g., in terms of affected systems) of an attack can be rapidly ascertained, and appropriate responses can be initiated, such as informing customers about data breaches. The basis for this is an effective attack detection system.
- ***Personnel training is of paramount importance:*** Targeted attacks make significant use of social engineering to accomplish their objectives. Such approaches render many traditional security

mechanisms significantly less effective. Consequently, it is important that an organization's personnel receive adequate awareness-raising training to address these emerging threats.

4.6 THE CHANGING LANDSCAPE - THREATS TRENDS

SCADA systems is becoming increasingly computerized. Control Systems are used to ensure a reliable and effective operation of critical infrastructures. However, the enhancement of ICT in critical infrastructure makes control systems vulnerable to cyber-attacks. The main challenges threaten SCADA systems can be categorized into:

Equipment - Changing Scenario
Once industrial control systems are up and running, organizations are reluctant to patch their OS or applications [The SCADA threat Landscape], which gives an attacker great opportunity to exploit well-known vulnerabilities. SCADA systems and wireless networks that are set up for operators to access the SCADA systems are configured for convenience rather than security. Systems are accessible with no authentication and passwords cannot be changed and they are the same access multiple systems. Firewalls, an essential component for use authentication, usually introduce delays in real-time communication and need to be tailored to specific SCADA protocols and networks and need to be frequently updated. Moreover, the distributed nature of control systems gives an attacker great opportunity to break and interfere with the SCADA equipment with little fear of being caught and facilitate an intruder to physically access sensitive equipment.

Networks
Once industrial control systems are up and running, organizations are reluctant to patch their OS or applications [The SCADA threat Landscape], which gives an attacker great opportunity to exploit well-known vulnerabilities. SCADA systems and wireless networks that are set up for operators to access the SCADA systems are configured for convenience rather than security. Systems are accessible with no authentication and passwords cannot be changed and they are the same access multiple systems. Firewalls, an essential component for use authentication, usually introduce delays in real-time communication and need to be tailored to specific SCADA protocols and networks and need to be frequently updated. Moreover, the distributed nature of control systems gives an attacker great opportunity to break and interfere with the SCADA equipment with little fear of being caught and facilitate an intruder to physically access sensitive equipment.

Data Communications
Current SCADA networking practices are getting significant challenges from a new environment being evolved out of data communication networks. A demand for more information results in higher data rates through incorporating higher computer power in the SCADA systems. [7]

Protocols
More computer power and modern networks pose higher challenges for the SCADA equipment. The points of meeting these challenges are SCADA protocols. The new SCADA environment is Ethernet/IP protocols, higher speed and frame relay. Integrating these networks with SCADA is the important challenge. The dichotomy of industrial SCADA equipment and networking technology is that whereas the average lifespan of the former is more than ten years, the latter undergoes many changes during that period as technology changes faster. It is through network protocols that the SCADA protocols are transported. However the networks and their protocols pose limitation while interacting with the SCADA protocols. Delays and short gaps in data and absence of Data Carrier Detect (DCD) transitions are caused by the characteristics of different network protocols like Ethernet, IP, etc. These lead SCADA protocols to presume links errors. As a result of this deficiency in transition of control signal, microwave radio link cannot be keyed [7]

5 SCADA CYBER ATTACKS

Analysing the documented past attacks on SCADA systems, industrial control systems and critical infrastructures, it is possible to identify two main categories, viz., intentional and unintentional attacks. The latter category can be further divided into unintentional attacks as a result of a worm, virus, or failure of system's control; and unintentional attacks caused by the personnel or maintenance mechanisms (testing, configuration, etc.)three main categories of attacks [55]:

- Intentional targeted attacks (unauthorized access to computers within the network infrastructure, a Denial of Service (DoS) attack, or spoofing);
- Unintentional consequences due to worms, viruses or control system failures;
- Unintentional consequences caused by internal personnel or mechanisms (the testing of inappropriate software on operational systems or unauthorized system configuration changes).

Generally, the first category of attacks have a determined target and have a methodical organization, moreover are the least frequently occurring because such attack usually requires a deep knowledge of the system/infrastructure. In particular, this kind of attack belongs, principally, from an insider with personal complaint

Attackers of SCADA systems usually aim to compromise the SCADA networks' security parameters such as confidentiality, integrity, and availability (CIA) [Add citation here. See comment below]. The different assets of a SCADA system can be involved in these Cyber-Attacks, that lead to a worsening in functionalities with a resulting significant financial loss.

- **Attacks on SCADA Confidentiality**
  An attack to the SCADA network can be carried out by any outsider that gains unauthorized access to this network, or even an insider with required authorization (e.g. a disgruntled employee), and it could culminate even in a shut down the entire system, in spite of all monitoring and controlling facilities..
  An example of an attack on SCADA system confidentiality is eavesdropping on the data transmitted across the network, so that the main control commands can be learned and used for other attacks. As most of the SCADA communication protocols do not support any kind of cryptography, eavesdropping is easier than in the IT networks
- **Attacks on SCADA Integrity and Availability**
  The smart grid is totally dependent on the data flowing in the network, so the Integrity of data in the SCADA system is essential. There can be different kinds of data, raw data from the SCADA sensor network being sent to the RTUs, control data being sent from the MTUs to the RTUs or from the RTUs to sensor networks. The data stored in the memory of SCADA devices (sensor nodes, RTUs, MTUs) can be the target for attacks against integrity, like the Injection attack, where an attacker tamper with the stored data or data being transmitted over the network.
  Depending on the type of manipulated data, there are different kinds of effects: in the **Command Injection**, the control commands are changed to cause a device malfunction; in the **Response Injection**, are the responses to a certain command to be modified; in the **Stored-data Injection**, the device set-data points are manipulated in order to make the device function improperly or alarms to go off at wrong data values; the values displayed at the human machine interface are changed such that the human operator is unaware of the alert when an alarm signal goes off, causing a delay in human response to an emergency; in the **Routing Injection**, the routing data in the network protocol are changed to cause Denial-of-Service attacks (DoS).

Integrity attacks on SCADA networks mostly lead to Denial-of Service attacks Therefore, they can also be classified under attacks on availability.

After a general description of cyber-attacks, Table 4 lists some typical cyber-attacks which may

compromise SCADA systems in critical infrastructures.

Attacks		Consequences on SCADA
DoS/DDoS	*Crash services*	Disable the monitoring and control system. Loss of load and information.
	Flood services	
Intelligent Attacks	*Attack protective relay setting*	Set cascading effect which may cause power outage.
Intrusion	*IP scans*	The intruder can check the behavior of the system causing loss of load.
	Port scans	
Malicious Software	*Virus*	Compromise SCADA systems, e.g. slow down communication between substation and control centers.
	Worm	
	Trojan horses	
	Logic bombs	
	Backdoors	
Identity Spoofing	*Man-in-the-middle*	The attacker impersonate an authorized user so may cause safety issues.
	Message replays	
	Network spoofing	
Password Pilfering	*Social engineering*	Depending on the level of authority acquired the consequences can change.

Table 4. Cyber-attacks and consequences in SCADA systems [56]
Source: Man in the middle attack test bed (Y. Yang, K. McLaughlin, 2012)

5.1 TAXONOMY OF CYBER ATTACKS ON SCADA SYSTEMS

Within a study about security of SCADA systems, it is important to classify the different attacks. Through this classification one can get a better understanding on probable attacks. Different research studies [33] have been conducted, in particular, in HyRiM we will take in consideration the taxonomy presented below. This taxonomy is a modified version of that presented by [57]:

- **Source sectors, i.e. the source of incident**

A first classification includes the source of incident: commercial source (consumer product, industry, small business), local or national government, individual user, etc.

- **Method of Operation**

Here are listed some methods used by the intruder to carry out an attack:

- Misuse of Resources: Unauthorized use of IT resources (i.e. Storing unauthorized files on a server);
- User/Root Compromise: Unauthorized use of user/administrator privilege;
- Social Engineering: unauthorized access to privileged information through human interaction;
- Virus;
- Web Compromise: Using vulnerabilities in a website to further an attack;
- Trojan;
- Worm;
- Recon (*see section 5.3 Typical attack phases)*;
- Denial of Service.

- **Impact**

Every attack has different effects: disrupt (Access change, removal of access to victim or to information, and manipulate permissions, e.g. Denial of Service attack or Trojan Horse [13]), distort (modification of data within the file), destruct (File deletion, removal of information from victim), disclosure

(Unauthorized exposure of information, such as download of password file).

- **Target sectors**

The victim of the incidents can be commercial (consumer product, industry, small business, etc.), local or national government (including buildings/housing, emergency services, social services, etc.).

5.1.1 Taxonomy of challenges

Recent work from Çetinkaya and Sterbenz [48] aimed to develop taxonomy of *challenges* to communication networks. They define a challenge as a "characteristic or condition that may manifest as an adverse event or condition that impacts the normal operation [of a system]" [48]. Clearly, this is a broad definition that incorporates many issues beyond those of a cyber-attack. An overview of the proposed taxonomy is presented in Figure 7. Many of these relate to the communication networks that underpin SCADA systems.

Examining the taxonomy, one can see the classes of challenge that pertain specifically to cyber-attacks. Regarding the *cause* branch, the *human-made* sub-branch relates to attacks. Furthermore, challenges that are caused by a *dependency* can be indirectly related to an attack. For instance, the *lower level failure* sub-branch relates to failures of underlying communication levels, e.g., a challenge at the transport-level results because of a failure of the network-level of a communication infrastructure. Of particular interest to HyRiM are *cascading failures*, whereby failures, which could be caused by a cyber-attack, in other sub-systems or networks have an impact on those that depend on it. Similarly, challenges can have a *direct* impact on a target network, e.g., because of a targeted Distributed Denial of Service (DDoS) attack or they can suffer *collateral* damage, whereby there is damage caused to a network if the power infrastructure is targeted by an attacker, for example. Clearly, the *objective* of a cyber-attack is *malicious*; interestingly, the authors have a selfish category that aims to captures challenges such as flash crowd events – in practice, it may be difficult to differentiate these challenges from an attack.

A limitation of this taxonomy with respect to SCADA systems relates to the *scope* of a challenge, which describes its impact. The authors focus on different forms of network-related scope, such as *nodes*, *links*, and *geographical area.* SCADA systems are cyber-physical systems, resulting in the potential scope of a challenge being in the physical domain, e.g., in the physical plant of a factory.

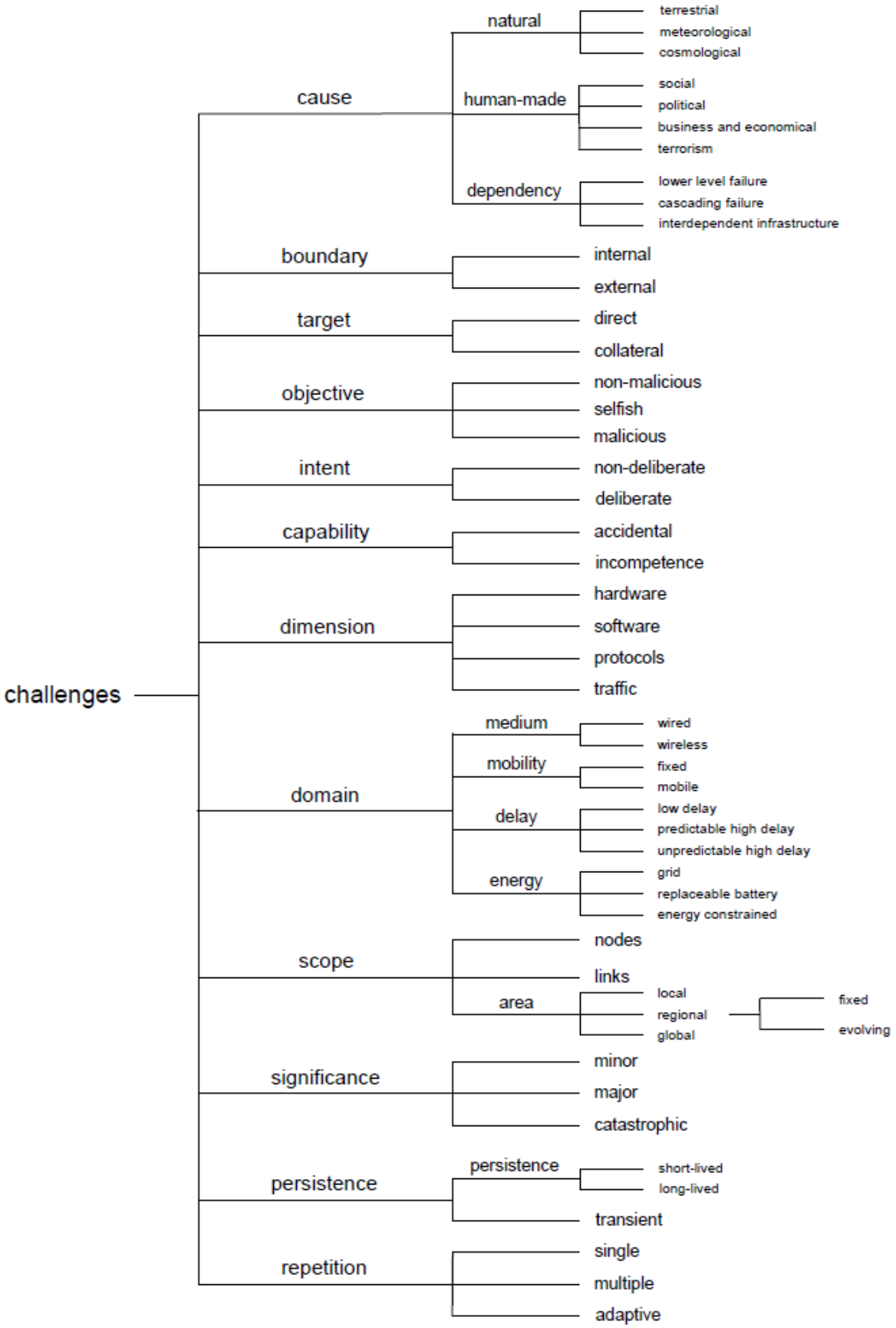

Figure 7. A taxonomy of challenges to communication networks (as proposed by Çetinkaya and Sterbenz)

Source: Symantec 2014

5.1.2 Attacks on hardware

The attacker wants to gain unauthenticated remote access to physical devices and control them, for instance components of SCADA field network (sensors, actuators, etc.). Once the attacker gains access to the device, he may change data set values, for example modifying a threshold values or set points for process control. The attacker could also manipulate the information shown to the operator through the HMI client, for example when an alarm goes OFF/ON. This causes delay to human response to an emergency which could take in danger the safety of people near the plant. To avoid such attacks it is very important to keep care to the access control security policies.

One of the representative attacks in this category is the doorknob-rattling attack. A very few common username and password combinations are performed on several computers resulting in very few failed login attempts. Unless the data related to login failures are collected from all the hosts and aggregated to check for this particular kind of attack from any remote destination, it can go undetected. [58]

5.1.3 Attacks on software

SCADA systems use a variety of software to furnish specific functionality. Furthermore, they utilize databases (i.e. data historians) that contain vital and potentially confidential process information [57]. These data are not only indispensable for technical reasons, such as that many control algorithms rely on past process data to make correct decisions, but also for business purposes, such as electricity pricing [57]. This kind of attack can be done by the exploitation of software vulnerabilities (*see section 4.1 vulnerabilities*), such as buffer overflow in order to affect the normal behavior of the program and also the execution of arbitrary code in the system. Another software vulnerability which can be exploited is SQL Injection.

Generally, SCADA systems present Web technology for the operational HMIs on their LAN. Furthermore, databases are used to interact with corporate Web servers that offer information within the corporate WAN and the Internet. Web server can support XML data exchanges with business-to-business (B2B) Web servers of principal customers, suppliers, and partners. Due to the fact Web sites interacts with back-end databases to obtain requested information, and check the user's ID and password for login purposes are vulnerable to SQL Injection which has a very strong implication on the security of SCADA systems. A specific text is put into data entry field on Web forms, in order that the logic behind the Web page is tricked revealing unauthorized data or gaining access as high level user. This special text can modify the query made to the relational database as consequence to look up user's ID and password, revelation of database tables, or extraction data from a table not accessible from external access [8].

5.1.4 Attacks on Communication Stack

These aims at hurting SCADA systems by attacking the network layer, transport layer, application layer and the implementation of protocols. For a full description of these attacks see [58]. An example of attack related to network layer is known as "Smurf ": is a type of address spoofing, in general, by sending a continuous stream of modified Internet Control message Protocol (ICMP) packets to the target network with the sending address is identical to one of the target computer addresses. In the context of SCADA systems, if a PLC acts on the modified message, it may either crash or dangerously send out wrong commands to actuators. Regarding application layer, the security control in protocols used in SCADA systems (i.e. Modbus) is not enough to avoid attacks. Generally, there is not authentication on source and data for those who have access to a device through a SCADA protocol, and they can both read and write. The write access and diagnostic functions of these protocols are particular vulnerable to cyber and cyber-induced physical attacks [58]. A probable attack is known as DNS forgery and consists to send a fake DNS reply with a matching source IP, destination port, request ID, and fake information inside; so that the fake reply is processed by the client before the real reply is received from the real DNS server.

In the following, two exemplary attacks on communication stack are described briefly, which are Denial of Service and Man in the middle Attacks.

Man-in-the-Middle Attack (MITM)

The Attacker with access to the communication traffic can intercept different transmitted packages, modify them and then send them forward to their original destinations. In the context of control systems, the attacker can initiate this form of active eavesdropping attack on the target system after collecting enough information regarding the system and knowing the used protocols. AS a consequence, the attacker can exploit the weaknesses of the communication protocol to invisibly capture the transmitted data, alter the messages and then relay them between the communicating entities. In this way, the communicating entities will believe that they are directly communicating over private channel. But the fact is that there are two independent connections and the attacker has the control of both channels. Therefore, the entire communication is routed and controlled through the attacker [59]. By conducting successful MITM attack, i.e. by capturing and modifying the data, the attacker can obtain the operator-level awareness and further control of the system, as well as can perform successful spoofing of the system state. Furthermore, many SCADA systems have easily programmable devices, such as RTUs. This vulnerability give an attacker the opportunity to reprogram the devices on-the-fly through the communication channel, whereas the operator, at the control center, is deceived with fake data about the system state. The following list contains some vulnerabilities that can be exploited to launch successful MITM attack [27]:

- Standard IT protocol with weak encryption
- Standard IT protocol with clear text authentication
- Control system protocol with weak or no authentication
- Control system protocol with weak integrity checks for detecting bad data
- Improper security implementation and configuration, such as sharing passwords among users.
- Non-usage of long and complex passwords

Denial of Service Attack (DoS)

ICS systems are often resource-constrained systems. Their individual devices are typically designed to support intended process. These devices with their limited processing capabilities represent an attractive and easy goal for attacker in order to cause damage in the entire system. Denial of Service (DoS) attack is widely used by malicious adversary to cause serious damage to potentially large part of the target system. By initiating a successful DoS attack on a control system, the attacker can prevent the system from performing its legitimate operations. DoS attacks mainly target the availability of a control system, which refers to the ability of all components of being accessible. Wide range of scenarios can be utilized by adversary in order to launch DoS, such as jamming communication links, compromising devices, manipulating routing protocols or even flooding the communication network and the devices with a huge amount of requests or useless traffic [60]. A successful DoS attack against typical computer networks can result in disruption of communications across the network. Furthermore, it can potentially make the situation worse by shutdown the affected computers. However, the implications of a successful DoS attack on a control system, as a core of numerous critical infrastructures, have completely different sense in comparison with the consequences on typical computer networks. The adverse effects can range from slowing down control system operations, which are usually time-critical, to completely shut down or compromising major facilities in utility network, such as nuclear power plant [61]. There are various vulnerabilities, which can be exploited to launch a DoS attack against SCADA network, such as vulnerabilities inherited from TCP/IP networks and inadequate access control mechanisms, as well as insufficient implementation or misconfiguration of security mechanisms. In the context of Smart Grid (SG), such interruption of SCADA communications could disrupt the key features of SG, such as grid stability, Distribute Generation (DG) and Distributed Energy Resource (DER), as well as Demand Sid Management (DSM).

5.1.5 Attacks on Implementation of Protocols

The exploitation of vulnerabilities in protocols (segmentation faults, stack, heap or buffer overflow) can result in the failure of protocol implementation. It is stated that SCADA implementation vulnerabilities are more prone to infrastructure failures than lack of security controls in SCADA protocols [62]. Table XX gives an overview of protocols in SCADA systems, as well as their vulnerabilities and potential attack scenarios [62].

Name	Vulnerabilities	Potential attack scenarios	Remarks
TCP/IP	• Out-dated patches • Poor software design/ Coding practices	One company's network is compromised and a polymorphic worm takes down most servers and any unpatched SCADA servers running Windows	
OPC	The item write function: the server maps handles to memory addresses and fails to validate a client-provided handle	• Collateral damage by OPC-unaware Malware • Opportunistic OPC Denial of Service Attack • Intelligent, aggressive attack against OPC hosts through a man-in-the-middle technique	
ICCP	Heap-based buffer overflow	Sending a specially crafted packet to a vulnerable LiveData RFC 1006 implementation, a remote attacker may be able to trigger the overflow to execute arbitrary code or crash a LiveData ICCP Server to cause a denial of service.	Used to exchange information between the corporate network and control center network
MMS	Improperly actions towards malformed RFC 1006 packet	Denial-of-service attack	

Table 5. Vulnerabilities and attackers on protocol implementation

5.2 ATTACK SOURCES AND ATTACKER PROFILES

5.2.1 Cyber-Attack sources

Threats to SCADA systems may arise from two different sources, mainly internal employees and external attackers. The threat from internal employees is real but not very likely as it would be easier to identify the attacker in most cases and the fear of the consequences would in itself reduce the likelihood of such attacks. On the other hand, it is easier for external attackers to launch cyber-attacks and the attack could go undetected, thereby making the SCADA systems more vulnerable. [21]

Essentially two basic sources of attacks can be distinguished:

- Internal
  - Non malicious: employees or contractors causing unintentional damage.
  - Malicious: system users with extensive internal knowledge of the system who intentionally cause damage.
- External
  - Opportunistic: hackers seeking a challenge
  - Deliberate: malicious, well-funded political activists, organized crime groups, or nation states.

5.2.2 Attacker profiles and typical goals

There are many attacker profiles [63]:

- **The lone individual *(coder/hacker) or small group of individuals***.. Every human who has access to a computer and the internet can be potentially a cyber-attacker. Depending on the skills, different kinds of lone individuals can be identified:
  A highly skilled coder able to find unique vulnerabilities in existing software and create working exploit codes. Owner of an undergraduate degree in computer science (or equivalent) with a certain expertize on the systems area, a deep understanding of the TCP/IP protocol as well as network and security protocols in general, and a basic knowledge of operating systems concepts. Probably needs several years of hands-on experience in an IT environment to perform host platform vulnerability assessments and learn hardening standards and methodologies. Most of them are not malicious, some are actively involved in developing technologies that can be used to improve overall computer and network security
  The *low skill coder*, the most common type of hacker. Often called the "script kiddie", cause generally relies on previously coded scripts and pre-packaged hacking tools downloaded from the Internet, is challenged by the notion of gaining unauthorized access and is open to using untested pieces of code without knowing their consequences. If a low skill coder with malicious intent penetrates a corporate network, he could go ahead damaging until detected; it normally happen quickly because he is not able to cover his tracks
  Coders can work also by means of a network of hacking teams that run exploits from different locations, making it harder to trace the activities back to their source. These teams can grow up in Internet Relay Chat (IRC) channels, in conferences such as DefCon, or in small groups of computer geek friends. Often the program created by a coder is run against target networks by other members of the team. This creates a reputation for the group rather than a single individual
- **The Insider(s).** The disgruntled employee is one of the main roots of computer crime, since his knowledge of a target system often allows him to gain unrestricted access to cause damage to the system or to steal system data. The threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems. Insiders may be also contractors, or business partners.
- **Criminal Groups.** The primary goal of a criminal group carrying out a cyber-attack on a SCADA facility would be extortion. An attack to a power system could cause a power outage that affects extended urban areas
- **Terrorist Group.** Terrorist Group. Critical infrastructures are not the best target of terrorist groups that more likely prefer higher-impact ones. Most terrorist groups seek higher-impact targets than bringing down a critical infrastructure, even one in the USA. However, a group with a long enough time horizon and enough financial backing may develop capabilities on par with nation-states.
- **Nation-States.** A nation state, or highly motivated terrorist group, most likely could develop the capabilities to bring down a SCADA system, or even a network of facilities, by the means of:
  - recruiting highly-skilled coders, control system engineers and bribe insiders
  - obtaining the source code for proprietary software to identify vulnerabilities unknown to the general public
  - persuading vendors or their employees to intentionally insert "backdoors" or other zero-day vulnerabilities(security breaches not yet discovered) into their software code or hardware devices
  - buying the system of interest in order figure out what are its operational strengths and weaknesses as well as its vulnerabilities.

An attacker can penetrate the SCADA system potentially causing very dangerous situation because he may gain some level of control of the SCADA system components. A list of **malicious goals of an attacker** on SCADA system is listed below [22]:

- Access to the SCADA master control station;
- Compromise the correct working operation of RTU or local PLCs;

- Compromise the SCADA master control station;
- Obtain SCADA system passwords from master control station;
- Obtain access to RTUs or local PLCs;
- Spoof RTU and send incorrect data to master control station;
- Spoof master control station and send incorrect data to RTU;
- Shut down the master control station;
- Shut down local control RTUs;
- Interrupt communications between SCADA master control station and RTUs:
- Modify RTU control program.

5.3 TYPICAL ATTACK PHASES

In order to protect a critical infrastructure it is important the knowledge of how an attacker may approach a critical infrastructure, or in particular access to SCADA system of the CI, gain access, and finally take control of it. As discussed previously, SCADA system is a very important part of the critical infrastructure, and the major part of attacks are directed to it. Different steps are involved during the attack process.

5.3.1 Essential phases of an attack

This section provides information based on [64] with regards to the first phases during an attack on systems that are connected with public networks as the Internet. Despite the fact that these attack phases apply mostly to IT systems, it appears to be also applicable to SCADA since lately there is an integration of IT into ICS. Hence, this information will result in examining the exposure of SCADA systems connected with public networks as the Internet, and also in assessing the difficulty or easiness of deploying attacks against them.

In order for an attacker to gain access to an on-line system, the former focuses on three essential phases i.e., foot-printing, scanning and enumeration of the target system. A successful attack eventually provides to an attacker access to the target system. In Figure 8 , we illustrate the order of these initial phases, which when followed might lead to a successful attack (i.e., gaining access to the target system). In the case of an attacker has successfully penetrated the target system, the attack can be leveraged to another level. This includes an effort from the attacker to escalate his/her privileges; identify mechanisms to gain access to trusted systems; cover the tracks of the attack and ensure that privileged access will be easily regained in the future at the will of the attacker. Despite the importance of the latter phases, we further elaborate on the first ones. Covering of attack trails and ensuing future access to SCADA systems are considered to be out of this report's scope.

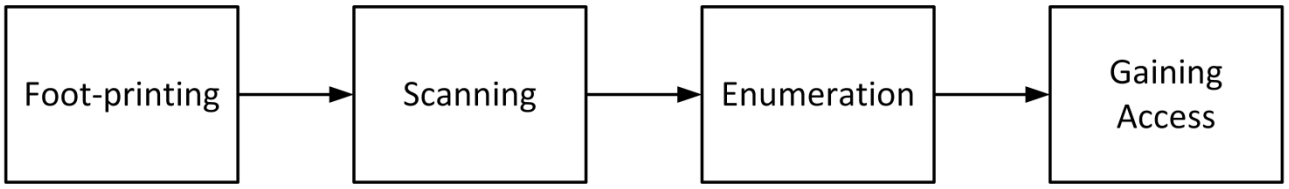

Figure 8. The essential phases of an attack
Source: *Hacking Exposed 7 (Mcclure, S, 2012)*
An effective attack method based on information exposed by search engines (Gouglidis, A, 2012)

Foot-printing helps an attacker in creating a complete profile of an organization's security posture. This is feasible through the use of a number of tools and techniques. The purpose of this step is for the attacker to take an unknown entity and reduce it to a specific range of domain names, network blocks, and individual IP addresses of systems directly connected with public networks, as well as many other details pertaining to its security posture. Although there are many types of foot-printing techniques, they are primarily aimed at discovering information related to the following environments: Internet, intranet, remote access, and extranet. In the case of SCADA systems, it is also possible for an attacker to perform foot-printing on the

physical infrastructure. Similarly to digital foot-printing, this will lead an attacker to collect information about the type of equipment used in a utility infrastructure.

After successfully foot-printing a system, the next step of **scanning** includes the determination of what systems are listening for inbound network traffic, and whenever these are reachable from public networks using a variety of tools and techniques such as ping sweeps, port scans, and automated discovery tools. In more detail, the main purpose of this step is to test a potential target system to see if it's alive and what ports are listening on it, if any. For the mapping of a network, a ping sweep on a range of IP addresses and network blocks can be performed to determine if individual devices or systems are alive. Port scanning is the process of connecting to TCP and UDP ports on the target system to determine what services are running or are in a LISTENING state. Identifying listening ports is critical to determining the services running, and consequently the vulnerabilities present from remote. Additional information that can be determined includes the type and version of the operating system and applications in use. Therefore, it can be seen that the information collected thus far is notable critical to perform a focused attack.

The scanning step can be done by dedicated tools, such as Nmap scanner, a tool that combines functions as indicated below:

- Ping computers and displays those alive;
- Detection hardware MAC-addresses, even across routes;
- Detection internal and external IP addresses;
- Scanning to listen TCP ports, UDP and SNMP services;
- Recovery currently logged-on users, configured user accounts, uptime, etc;
- Mount and exploration of network resources;
- Launch of external third party applications;
- Exportation of the collected information to HTML, XML, CSV and TXT;
- Remote shutdown and sending network messages;
- Recovery any system information via WMI;
- Recovery information from remote register, file system and service manager.

During the **enumeration** phase an attacker continues to further probe the successfully identified live hosts and running services for known weaknesses. The key difference between previously discussed information-gathering techniques and enumeration is in the level of intrusiveness. Enumeration involves active connections to systems and directed queries. Hence, this step in most cases will be logged or otherwise noticed. Much of the information gathered through enumeration may appear harmless at first glance. However, such leaking information can be disastrous since it can be used to compromise a system. In general, the information attackers will seek via enumeration includes user account names, misconfigured shared resources, and older software versions with known security vulnerabilities. Once one of these openings is enumerated, it's usually only a matter of time before the intruder compromises the system in question to some degree, if not completely. A fundamental enumeration technique consists of banner grabbing. Banner grabbing can be simply defined as connecting to remote applications and observing the output. At the very least, they may have identified the make and model of the running service, which in many cases is enough to set the vulnerability research process in motion.

An attacker after successfully fulfilling the objectives of the aforementioned attacking phases has enough data gathered in order to make an informed attempt to **access the target system**. This depends on the type of the system or service being attacked.

5.3.2 Automated attacks against SCADA systems

In this section, we further elaborate on an automated attacked method proposed in [65], which appears to be applicable in the case of attacking SCADA systems through public networks. The proposed automated attack method was mostly targeted to web applications. Specifically, the automated attack against web

applications included three phases. The first phase included information gathering using a web search engine. This could be accomplished through the use of advance operators that exist in most web search engines. The latter is a technique also known as 'Google Hacking' when the Google search engine is used. The described attack method proposed that queries do not need to be performed to the web site of the search engine. The reason is that most of them make use of Web 2.0 technologies, and therefore, they provide a series of services to consumers for information retrieval. For instance, it is possible to use the REST (Representational State Transfer) approach for getting information content from search engines web sites by reading a designated web page that contains HTML, XML or JSON information. Most search engine APIs, viz. Google Custom Search API [66] and Bing Search API [67] support the JSON (JavaScript Object Notation) data-interchange format. Hence, in during the first phase, a specially crafted search query is required in order to successfully identify potential target systems. The results include information about the systems that were described in the search query. In contrast to the manual attack, this single phase is equivalent to the first three manual phases. Figure 9 depicts the comparison between the manual and automated phases of an attack. Additionally, the advantage of the automated approach is that the attacker is not being noticed to do any illegal actions. However, this is opposed to the phases of 'Scanning' and 'Enumeration' that take place during a non-automated attack against a system. Furthermore, in the case of attacking SCADA systems it is worthy to refer to the Shodan search engine [68]. Shodan consists of a search engine that is capable of retrieving information regarding online devices. A case of constructing simple queries would include the name of a device e.g., 'Siemens S7-300'. The latter will result into a list of systems that are identified to use the requested PLC. However, there is support for more operators that can help in the refinement of results.

During the second phase of the automated attack it is possible to process the information extracted from the previous step. This is mainly required to determine some more concrete and meaningful information that could be used for an attack as the target device's IP, port number etc. The last step includes the deployment of an exploit. Having all the adequate information, it is possible to use it as an input to an application that deploys an attack against the target device. This last step is equivalent to the step of 'Gaining access' in the aforementioned methodology.

As stated above, in the case of SCADA systems the use of Shodan might lead to the identification of several devices that are known to have vulnerabilities. Additionally, Shodan provides an API for accessing Shodan's data including access to search features, and allowing to get the requested information. The API is provided for a list of common programming languages (i.e., Python, Ruby and NodeJS). This could be perceived as the first phase of the automated attack method. When having the information, an attacker can use only the required information from the set of identified devices e.g., IP address and port number. Furthermore, using Python is also feasible to communicate with Metasploit [69]. Therefore, an attack to SCADA systems using the Shodan search engine, Python and Metasploit could be fully automated to attack devices with known vulnerabilities.

Lastly, it is worthy to refer to two dangers that are posed by the aforementioned automated attack. Firstly, the attack cannot be noticed by the target system before the deployment of the exploit (i.e., the last phase of the attack). This holds since an attacker doesn't probe the actual system for devices and running services. Instead the attacker requests this information from a search engine, which in the case of SCADA systems can be Shodan. Secondly, the attack can be deployed against multiple systems due to its automation. Thus, in the case of zero day attacks this may lead to catastrophic results.

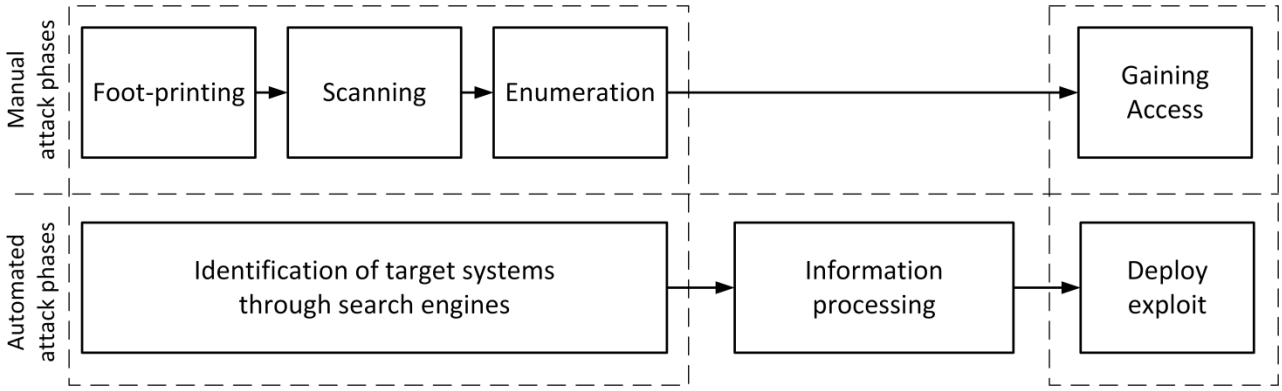

Figure 9. Manual vs. automated attack phases

Source: *An effective attack method based on information exposed by search engines (Gouglidis, A, 2012)*

5.3.3 Stages of an Advanced Persistent Threat

ATPs attacks are characterised as being executed over extended periods of time, e.g., potentially over several months, implementing a number of attack stages, and are realised in a particularly stealthy manner, with attackers using advanced technical measures in order to avoid detection. Figure 10 shows the stages of an APT, and contrasts them to other types of threats (e.g., commodity and hacktivist threats) with respect to the stages that are typically realised.

Figure 10. The stages of an Advanced Persistent Threat

Source: Dell Secureworks – Understand the threat.

In what follows, we briefly highlight some of the interesting aspects of an APT:

1. *Define target:* initially a target is defined by the group that is carrying out the attack. Depending on the desired outcome of the attack, a target could be a specific organisation, e.g., a bank or a utility company, or governmental organisations.

2. *Find and organize accomplices:* the implementation of contemporary attacks and APTS, in particular, can involve a number of skilled individuals that need to be organized. For example, such individuals could include programmers, social engineering experts, and money launderers (if this is the purpose of the attack). For an APT that targets a specific organisation or sector, e.g., the energy sector, individuals with knowledge in that domain will also be required, potentially including insiders. Perhaps unique to an APT are the (financial) resources that are available to gather and fund such a collection of often highly-skilled individuals.

3. *Build or acquire tools:* to implement an attack a variety of software is required, such as a Remote Access Trojan (RAT) that allows an attacker to remotely observe and control an infected computer, effectively giving them full-control of a target machine. These can either be purchased (and modified, if necessary) or built from scratch – again, unique to an APT is the availability of resources to develop specific software for an attack, making them difficult to detect. Another important item to be acquired is software vulnerabilities that can be exploited in later attack stages. APTs typically make use of so-called zero-day vulnerabilities – those which have not been previously announced and consequently for which patches do not exist. Markets exist where these vulnerabilities can be purchased.

4. *Research target infrastructure/employees:* an important stage for an APT involves carrying out reconnaissance of the target, both from a technical and organisational perspective. Technically, this can involve remotely probing the target infrastructure, in order to understand the nature of the systems that are in-place. This information can be useful for identifying technical vulnerabilities in systems, including those used to secure it, that can later be exploited. Furthermore, information about the organisation itself and the personnel will be collected, which could form part of a social engineering attack, such as a targeted email spear phishing campaign.

5. *Test for detection:* these preparatory activities may be detected by a target organisation. Consequently, an attacker will take steps to determine whether they have been detected by the organisation itself or third parties, such as security companies or law enforcement authorities.

6. *Deployment and initial intrusion:* having prepared to attack a target organisation, the necessary infrastructure for their attack will be deployed, such as malicious websites or the registration of social media accounts that can be used for command and control activities. With these items in place, the next stage is to carry out an initial intrusion. Commonly, this is achieved using an email spear phishing campaign – for example, a targeted email that is sent to key individuals in an organisation that directs them to a malicious website. Malicious content on the website is used to exploit the target's computer, thus giving an attacker access to the systems within an organisation. As part of this initial intrusion, a RAT (or other remote access capability) can be installed to give the attacker access to the computer that has been compromised.

7. *Outbound connection initiated:* having successfully completed the initial intrusion, the software that is installed will attempt to make a connection back to a remote control server. In contrast to other malicious activity, such as a botnet, this endpoint will likely be closely monitored by a human operator. With this connection enabled, the remote attacker can then use this compromised machine to expand their operations within the target infrastructure.

8. *Expand access and obtain credentials and Strengthen foothold:* in these phases of an APT, the attacker will aim to compromise further systems in the infrastructure, in order to support their nefarious objective. For example, in the case of the Stuxnet malware, the attackers compromised a number of computers that resulted in them being able to access the target Siemens equipment. Furthermore, a number of computers will be compromised as a form of redundancy, in case malware is detected and sanitized on the computer that is primarily being used to execute the attack.

9. *Exfiltrate data:* finally, the target data, such as organization's intellectual property, will be transmitted to the attacker. Attempts will be made to ensure this activity is not readily detectable, for example, by using steganography [70] – embedding the data to be exfiltrated in apparently benign data transfers, such as images [71].

10. *Cover tracks and remain undetected:* in order to make it difficult for a victim to detect and understand the potential impact of an attack, in a final phase an attacker may take measures to hide their activity, e.g., by manipulating log files that show activity and removing malware.

It can be seen from this short description that an APT involves persistence and significant resources to implement on the behalf of the attacker.

5.3.4 Attacks on the Siemens S7 PLCs series

Following, we briefly elaborate on the vulnerabilities and attacks that can be performed to Siemens SIMATIC S7 Programmable Logic Controllers (PLCs). Specifically, we refer to the S7-300, S7-400, and S7-1200 series that have proven to be vulnerable, as presented in [72], and to the SIMATIC S7-315 and S7-417 PLCs. In Figure 11, we depict a low cost basic controller, i.e., the Siemens SIMATIC S7-1200 PLC.

Figure 11 Siemens SIMATIC S7-1200 [73]
Source: Siemens 2014

The Siemens SIMATIC S7 consists of a product line and software for programming it, including also the network protocol. The aforementioned PLCs rely on the PROFINET protocol, which uses the IEEE 802.3 Ethernet standard [74]. PROFINET consists of a standard that can be used in industrial networks for the networking of equipment and production assets, and supports three protocols, i.e., standard TCP/IP, Real Time (PROFINET RT), and Isochronous Real Time (PROFINET IRT) [75]. The attacks that are referred in the following, assumes the use of the PROFINET over TCP/IP. Although the attacks are not targeting the PROFINET protocol, the latter can be used to connect to the SIMATIC S7 PLCs. S7 is a proprietary application layer protocol used by Siemens, and it is used on top of ISO-TSAP protocol [76]. The latter is a transport layer, TCP protocol, with no encryption support, and inveterate shortcomings [77]. SIMATIC STEP 7 is the software that is used for user configuration, program, test and diagnose of all SIMATIC controllers [78]. To communicate with each other, STEP 7 and the controllers are using the ISO-TSAP protocol.

The existing attacks dissect the original ISO-TSAP packets that are send over a TCP stream to the PLCs, with maliciously crafted packets, and are send back to them. As stated before since the traffic is not encrypted it becomes easy to replicate packets. Through this procedure, an attacker can perform tasks that could normally be done only by the STEP 7 management software. This includes, but not limited to, turning off the PLC's CPU, changing the PLC's logic, etc. Particularly, bellow we list a set of potential attacks to the S7 PLC's, as these were presented in [72]:

- TCP replay over ISO-TSAP attack, which can lead to CPU stop and start attacks;
- Memory read and write logic attack;
- S7 authentication bypass;
- Decryption of Siemens SIMATIC firmware; and
- Accessing a shell on the PLC.

The aforementioned vulnerabilities were partially utilised in cases as the Stuxnet worm, which was targeting the SIMATIC S7-300 PLCs [8], and the S7-315 and S7-417 PLCs. It is also worth mentioning the fact that a set of implemented Metasploit modules currently exist, which automate the aforementioned attacks. Implementations are provided in [42]. The latter facilitates even more the identification and exploitation of vulnerable PLCs, even by less experienced attackers.

6 IMPROVING CYBER SECURITY OF SCADA SYSTEMS

6.1 EXISTING STANDARDS AND GUIDELINES

In this section, we present a summary of existing standards and guidelines for information security and critical infrastructure risk assessment and management. .

The canonical information security standards are the ISO 27000 series that target information security management, risk management and security controls. In total, there are six standards that are part of this series. The first, ISO 27001, outlines a number of stages of information security management, from initial establishment, through to implementation and finally improvement of an Information Security Management System (ISMS)[2]. The standards make use of the so-called *Plan-Do-Check-Act* (PDCA) model to structure the improvement process. Building on this initial standard, ISO 27002 describes a code of practice for information security, which outlines controls and control mechanisms that may be implemented according to the guidance that is provided within ISO 27001. Meanwhile, ISO 27003 focuses on providing help and guidance for the implementation of an Information Security Management System (ISMS). The next standard in the series, ISO 27004, provides guidance on the development and use of measures and measurement for the assessment of the effectiveness of an implemented information security management system and controls, as specified in ISO 27001. ISO 27005 addresses topics that are related to information security risk management. Finally, ISO 27006 offers guidelines for accreditation – an important aspect, as many organizations seek to acquire ISO 27000 certification.

The National Institute of Standards and Technology (NIST) SP800-53 document [79] is similar in nature to the ISO 27000 standards and lists and classifies security control requirements. The controls should be used to extract a baseline for security implementation for US Federal Information Systems and Organizations. Furthermore, SP800-53 provides fundamentals on the risk management process, specifying all activities for the selection of security controls to their application through to an organization's information systems. Meanwhile, ISO 31000 is a broad set of standards that provides fundamental guidelines on the principles, a framework and a process for managing risk[3].

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) method [81] can be used for identifying and managing information security risks. It contains methods, techniques and tools for an *asset-driven* evaluation approach. The OCTAVE method is intended to be driven by the organization under scrutiny, and provides specific guidelines and forms for its implementation. In a similar fashion to OCTAVE, Magerit is a risk analysis and management methodology that has been widely applied in Spain [85]. Like OCTAVE, it is driven by an analysis of the assets that are associated with an organization. The Magerit methodology formed the basis of an information security management method that was developed as part of the EU-funded PRECYSE project[4], which is focused on industrial control system security.

Specific to industrial control systems are the ISA99 [53] (also known as ISA/IEC 62443), the NERC CIP [86], and the NIST SP800-82 [6] standards. Forming the basis for ISA/IEC 62443, ISA99 proposes an approach that starts from the confidentiality, integrity and availability objectives for information security, taking into account the specific priorities characterizing automation systems with respect to standard IT infrastructures. The NERC CIP standards are published by the North American Electric Reliability Corporation. These standards contain best practices for securing power systems. Finally, NIST SP800-82 provides best practices on architecture design and security controls for SCADA and industrial control systems.

[2] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[3] http://www.iso.org/iso/home/standards/iso31000.htm

For a catalogue of risk assessment methods and tools, we direct the reader to a repository maintained by the European Network and Information Security Agency (ENISA) [84]. According to a recent ENISA study [87], ISO 27002 for information security management is the most adopted standard, followed by NERC-CIP, NIST SP 800-82, and finally ISA99. In a paper that provides a survey of risk assessment approaches, Behnia *et al.* [80] outline the range of differences between security analysis methodologies, including OCTAVE [81], ISRAM [82], and CORAS [83], amongst others.

6.2 CYBER SECURITY AND RISK MANAGEMENT APPROACHES

Several tactics have been employed to mitigate the vulnerabilities of operational networks. The current approaches vary, but tend to focus on the IT nature of the network [24].

6.2.1 Perimeter Protection

The first set of defences aims to separate the power operational network from any outside contact. Perimeter defences include:

- **Network Firewalls** – Designed to regulate the exchange of information by only allowing contact between approved entities, network firewalls can approve or reject connection requests as well as check remote users for credentials. They are limited in effectiveness, however, since once they permit a connection, they have no notion of the data that passes through. As such, malware or invalid data can potentially penetrate.
- **One-Way Network Firewalls** – These appliances are designed to provide a "physical" separation of the operational network from user monitoring requests. They allow only a one-way flow of information – from the operational network outward – and minimize the exposure of mission critical components to possible outward control.
- **Encrypted VPNs** – This measure is typically used in conjunction with network firewalls and allows secure communications between different elements of the Electronic Security Perimeter (ESP). In essence, it prevents "Man in the Middle" attacks and compromises of control information.
  The majority of security measures today are derived from the concept of perimeter protection. The limitations of such defenses are typically tied to the ease of physical security breaches. While some networks (e.g. carrier networks) house their equipment in well-protected locations such as central offices, the communications equipment relied upon by utilities often resides in unmanned, lightly protected locations. Here, it's relatively easy to breach physical security and circumvent all of the network's perimeter security. In such cases, it's essential to contain and mitigate the break-in. This is where additional security measures are required.

6.2.2 Network Protection

The underlying architecture and protocols for interconnection of locations in the communications network are also a source for potential vulnerabilities to the power utility network. While often not considered, the underlying network technology that's selected can have wide ranging implications on the stability and susceptibility of the network to cyber-attacks.
As outlined above, there are several ways to breach network security, including attacks to both the control plane and the data plane. There are also several ways in which such threats could be mitigated or limited in a way that would improve security and resiliency, yet not impact network performance.

6.2.3 Minimizing Control Plane Attacks

One of the more dangerous types of attacks is one on the control plane, where the attacker either corrupts or crashes it. In either case, the ultimate result is the complete collapse of the network. This type of attack is especially alarming because the breach of just a single location has potential to crash the entire network.

Essentially, the entire network is only as secure as its weakest link, and power utility networks are at the mercy of their least protected substation.

Network designs that include a control plane or signalling protocol are therefore highly susceptible to these types of attacks. These include MPLS and IP type networks. Control plane vulnerabilities have been demonstrated multiple times in both standardization bodies (see IETF's RFCs 4272, 5920 and 6941) and hacker conferences. In fact, a technique to bring down an MPLS network via the control plane was demonstrated live at the 2011 Black Hat conference.

While mitigation is possible to an extent, the threat of danger remains as long as control planes exist. Networks that are based on technology devoid of a control plane will always be much more secure. These include SONET/SDH and Carrier Ethernet networks. Neither SONET/SDH nor Carrier Ethernet offers a means to attack their signaling plane, and both require a management station to provision them. Once that management station is secured, no control plane attacks are possible.

6.2.4 Minimizing Data Plane Attacks

Attacks on the data plane are also a potential source of peril. Although these tend to be more focused (e.g. DoS attacks focus on a particular host), the potential loss of connectivity between the HMI station and RTUs can interrupt control of the electrical grid. As with attacks that are centered on the control plane, data plane attacks can be mitigated as a result of design decisions relating to the operational network.
In scenarios where rigid connectivity is forced (as with SONET/SDH or Carrier Ethernet), it is much more difficult for an attacker to gain visibility into network elements outside of their direct connection. Such data plane rigidity serves to only expose the minimum necessary parts of each host to the network, and shield other parts that may be more vulnerable. In cases where a routed network exists (such as MPLS and IP), an attacker can first collect information by snooping and scouting the network from an unsecured location, and then use spoofed addresses to perpetrate an attack.

Another way to increase security and avoid masquerading or spoofing is through the use of source authentication protocols. The most prominent of these is the Ethernet-based 802.1X, which validates each newly inserted device through a centrally managed database. It uses encryption to verify the identity and ensure the new device is not masquerading as a valid network device. This ensures all devices connected to the network are indeed valid authentic network devices and not hacker-inserted ones.

6.2.5 Internal Application Protection (Malware Protection)

Among the most difficult attacks to detect are those that originate from elements inside the network. Insider attacks pose hazards from a number of perspectives.
First, it is extremely challenging to make a determination as to whether a particular command is valid or malicious. Some commands (e.g. decommissioning of an old RTU) may have a valid use when issued by authorized personnel, but can be harmful when initiated by others without permission.
Second, since attacks travel through diverse paths, a system that's omnipresent and able to track all possible paths is necessary to secure the entire network. Some utilities use a location firewall to mitigate the risk of one site controlling another, as well as to contain cyber-threats at their general point of origin. Still, this can cause a wider than desired blockage or outage, and the larger the substation, the greater the risk of damage.

Finally, it is tough for standard "firewall" equipment to inspect commands. While standard DPI-enabled firewalls with can check software payload to determine if a previously isolated "signature" is present, and flag potential matches it has no way to evaluate whether a particular command is valid or malicious.
All of these limitations present a seemingly insurmountable obstacle when it comes to internal threats. The problem is, NERC CIP expects power utilities to deal with them. Specifically, NERC CIP expects power

companies to detect and block occurrences where malware has taken over a piece of equipment – whether it be an RTU or control console – and be able to stop it from performing its malicious task.

In order for a network to cope with all the limitations posed by internal threats, a few deductions must be made. The distributed nature of possible attacks renders a centralized or transitional solution inadequate. In addition, solutions must "understand" the ICS protocol and make an intelligent determination of whether a particular command is valid or out of bounds.

Hence, the ideal solution must be a distributed ICS-aware firewall. This type of solution can be omnipresent, as it is integrated into the fabric of the network (made part of the network switching equipment). Plus, the ability of an ICS-aware firewall to determine the validity of different SCADA commands can be used to block and detect insider threats or threats stemming from the introduction of malware to the network.

Two primary elements of this solution, omnipresence and application awareness, derive from the inherent characteristics of attacks. The distributed nature of power utility networks, plus the fact that most elements of the network can be placed in areas that are not highly secure – makes an omnipresent distributed approach preferable to a central solution. The only way of implementing this without having all traffic home-runned to the central gateway and incurring excessive delay, is by distributing the intelligence.

Application awareness as a requirement stems from the difficulty associated with detecting malware attacks. Malware typically piggybacks on real control stations and verifiable hosts, and only changes the content of control messages. In order to detect this type of tampering, an external unaffected element must then verify the content of those communications. The intelligence to read and verify each command is required to enable this functionality, necessitating the use of application aware equipment.

6.3 ICS SECURITY SOLUTIONS

Most organizations leveraging contemporary ICT are familiar with cyber-security issues and what is required to protect critical information assets. According to [21] common ICT and ICS security elements include:

6.3.1 Policies

The foundation of any effective cyber-security program is the cyber-security policy. Although, they can range in size and style, there are usually several themes that are always present. Contents in a standard cyber-security policy can include [88]: Policy upkeep, refinement of policy, and compliance.

- Cyber-security countermeasures
- Cyber-security technologies
- Incident response
- Forensics
- Access control
- Physical security
- Patches and upgrading [94]

6.3.2 Antivirus / antimalware

Contemporary ICT security systems are often deployed with countermeasures to mitigate virus, malicious software, and other types of malicious code have some sort of transport capability of are used specifically to increase an attacker's level of compromise. Implementing antivirus and malware protection on critical systems can help detecting and defeating such attempts, not only for viruses, malware and worms but also for malicious activity as well, being able to detect hacking tools. Any notification of these products must be

logged to a centralized sever, with notifications being sent to administrators. There is a concern about the way anti-virus might affect the real-time performance of critical control systems (such as Master stations). As individual mileage may vary, a previous assessment of the antivirus or malware protection performance overhead may be advisable.

6.3.3 Firewalls and Intrusion Detection System (IDS)

Firewalls are probably the most common security technology found within ICT environments. Most people understand the principle of the firewall and how they provide security. Firewalls work in much the same way that burglar alarms or anti-tamper technology can be used to detect and thwart attack attempts. Intrusion detection and intrusion prevention (IDS and IPS) are used as alarm mechanisms to indicate possible malicious activity, technically, are two different security solutions.

Since the most important threat to the SCADA network may come from malicious attackers via the Internet, it is necessary to monitor the traffic flows from the Internet (IP network) to the SCADA network. Generally, firewalls and other Intrusion Detection Systems (IDS) are installed at the various ingress points (gateways) of the SCADA network to identify malicious traffic before it is allowed to enter. Although this would help to filter out some attacks, it may still be an inadequate defence action against attacks. Viruses and worms could swamp the systems with huge volumes of attack traffic. Hence, having only firewalls and IDS at entry points may not suffice. This leads to the concept of the electronic perimeter.

- **Electronic Perimeter**

The extended perimeter can be formed by multiple IDS devices across a wide area. Huge volumes of traffic can be handled by an extended perimeter as it would be possible to stop the attacks further away from the SCADA network. In addition, the IDS devices along the electronic perimeter could form an overlay network (i.e., a virtual private network over the Internet) and function in a distributed and collaborative fashion, supporting one another in tackling the attacks more effectively. The setup can be viewed as an electronic fence or protective perimeter barrier that allows only legitimate traffic to reach the gateway of the SCADA network.

- **IDS systems**

Intrusion Detection Systems (IDSs) provide an add level of security for networks and systems, by providing critical information about attacks. In general, they do not actively block attacks or prevent exploits from being successful, a task that falls into the scope of Intrusion Prevention Systems (IPSs). IDSs fall into three main categories: Host IDS (HIDS), Network IDS (NIDS) and Hybrid IDS (which share the characteristics of NIDS and HIDS)

- **Domain specific IDS**

Signature-based NIDS (the most common type) are mostly effective to detect attack patterns such as network scans or malformed packets. However, the lack of AAA mechanisms in SCADA systems enables an intruder to easily perform an attack by simply forging network streams which are sent to target devices on the control network. Therefore, the NIDS must have some sort of context-specific information to deal with SCADA systems.

However, typical SCADA networks have specific characteristics that can be used to provide the IDS with a more complete knowledge of the environment it is working on. Relatively static topologies and control flows enable the use of mapping the possible connections between different equipment, in terms of protocols, ports and direction of the communication flows. The figure below shows an example of this approach, where a compromised HMI tries to communicate directly with a slave on the control network (something it's not supposed to do). For such abnormal situations, the IDS could be configured to provide alerts.

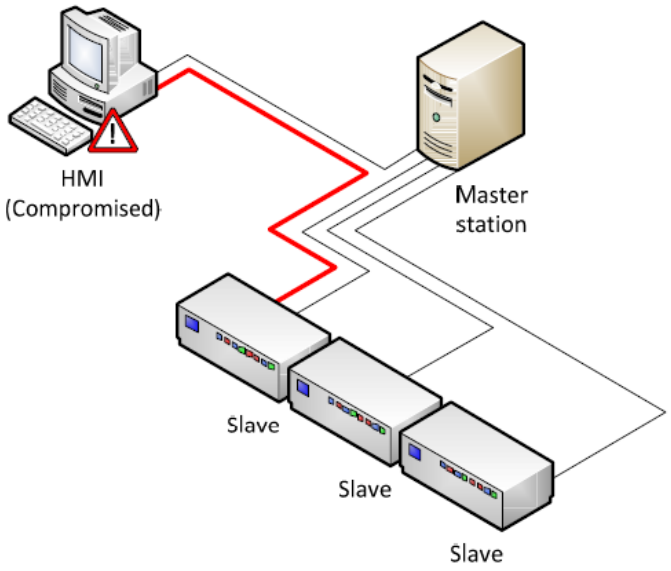

Figure 12. Incorrect communication flow in a SCADA system
Source: Cockpit Project. FP7-SEC-2011-1 Project 285647

Another example has to do with SCADA protocol characteristics. For instance, Modbus frames cannot exceed a maximum size of 256 bytes. As such, it would be relatively easy to an attacker to forge packets to cause a buffer overflow in a slave. Since this is possible to achieve while maintaining a correct framing structure for the protocols of the network layer, conventional IDS are not able to detect such attacks. Moreover, if the control protocol frames are correctly forged, an attacker can induce deviant behavior on the control systems. To overcome these problems, an IDS might be able to assess if a given command makes sense from an inference database with actions and transitions states for the system].

6.3.4 Unified Threat management (UTM)

Often, Unified Threat management is referred to by many different names but the essence of the solution remain the same. UTM is about collecting security information from across the ICT architecture and analyzing it at a single location. Operators and security administrators can obtain a common operating picture as it relates to the cyber-security of their network. UTM is deployed to include information collected from firewalls, routers, remote access points, wireless access points, IDS, IPS, data flow analysis, and in the security log files, collected from any number of serves in the operational environment.

6.3.5 Online Vulnerability Map Tool

It is also useful a vulnerability analysis tool to test whether the servers, hosts, routers, and devices that are part of the SCADA network are vulnerable to known attacks. This tool performs host/network vulnerability analysis periodically (through port scanning and other mechanisms) and provides a visual map of the vulnerability that alerts the operators/engineers to take appropriate remedial actions. The tool has to be flexible so that new attacks can be added to the repertoire any time. The tool acts as a security management technique, and complements the IDS techniques. Examples of such tools are the Nessus[5], Metasploit[6], Core Impact[7] and Canvas[8] [186] modular penetration-testing frameworks for which SCADA modules are available.

5 http://www.tenable.com/products/nessus
6 http://www.metasploit.com/
7 http://www.coresecurity.com
8 http://www.immunitysec.com

6.3.6 Honeypots and Honeynets

A Honeypot is a decoy or dummy target set up to attract and detect/observe attacks. By being exposed to probing and attack, its purpose is to lure and track intruders as they advance. Deploying and running a honeypot infrastructure requires a careful approach: defenses have to be planned in advance so that the infrastructure itself cannot be used to increase the attack surface, while keeping a low profile.

A Honeypot can be implemented in a different fashion, depending on its operation scope: in the operations network a honeypot might simulate the operation of a network server (e.g., Master Station), while in the field network a honeypot could be implemented using a system capable of simulating the operation of an RTU (e.g., a Modbus emulator).

Honeypots can be classified in two groups: research and production – the first are used to obtain intelligence information about attack methods, while the latter is used to implicitly protect and ICT infrastructure by providing advance warning of attacks against the production infrastructure.]

Honeynets extend the concept of Honeypots in a distributed fashion, by deploying several honeypot instances on a production network. This requires at least two components: a Honeywall and Honeypot hosts. In these situations, an attacker has access to a high interaction Honeypot (with a full-fledged OS) – however, in order to limit the possibility of an attack, the Honeywall (which also maintains an internal IDS to monitor an track suspicious activity) acts as firewall (ideally operating in bridging mode, without having an IP on the network, apart from the management interface), limiting outbound connections or even using a “bait-and-switch” technique to reroute traffic to another host.

6.3.7 ICS security zones

ICS security zones are used to distinguish components, in a large and complex network, at which are required and applied different requirements of security. Particularly, a security zone is a logical grouping of physical, informational, and application assets sharing common security requirements. This concept applies to the electronic environment where some systems are included in the security zone and all others are outside the zone. There can also be zones within zones, or subzones, that provide layered security, giving defense in depth and addressing multiple levels of security requirements. Defense in depth can also be accomplished by assigning different properties to security zones. A security zone has a border, which is the boundary between included and excluded elements. The concept of a zone also implies the need to access the assets in a zone from both within and without. This defines the communication and access required to allow information and people to move within and between the security zones. Zones may be considered to be trusted or untrusted.

When defining a security zone, an organization must first assess the security goals and then determine whether a particular asset should be considered within the zone or outside the zone. The security goals can be broken down in: Communications Access, Physical Access and Proximity, Conduits and Channels.

6.4 MODELLING TECHNIQUES AND TOOLS

Cyber security methodologies, models and tools are fundamentally based on identification of attacker profiles, attack objectives, attack steps characterization, spreading throughout ICS network and consequences on CI customers.

At the state of the art, no single modelling technique has the modelling power and the analytical tractability to adequately deal with the modelling and early prediction of Quality of Service (QoS) of SCADA system facing adverse events, such as cyber-attacks, and accounting cyber-interdependency along CI ICT backbone. According to [21], the following models are distinguished:

6.4.1 Stochastic approaches

A stochastic model is a model that involves probabilities, or randomness, associated with time and events. When using such a model, a stochastic process will represent the system behavior. The stochastic model can be depicted as a state transition diagram, which describes all relevant operational system states and the possible transitions between these states. To describe time aspects between events, a rate matrix has to be specified. One usually assumes that the event that will occur next, as well as the time until the next event, is random. Hence, the behavior of the system is a stochastic process. The main advantage of this modelling approach is that it captures the dynamic system behavior, i.e., the sequence and time aspects of events, such as failures and repairs. The stochastic process can then be used as a basis for quantitative analysis of the modelled system. By using mathematical analysis techniques, closed-form solutions may be obtained, which describe how the failure and repair rates affects the expected system dependability in terms of its reliability, availability and so forth. In many cases, the stochastic modelling approach is the most appropriate system evaluation method when quantitative dependability measures are needed.

According to the definition of dependability provided by A. Avizienis, et al (2004), dependability comprises several system properties, amongst them also the Confidentiality, Integrity, Availability (CIA), typically, security attributes. One would therefore expect that security can be modelled and analyzed by the same methodologies as the other dependability properties. However, it turns out that this is not the case. The main reason is that malicious behavior is rarely considered as a possible fault source when evaluating system dependability.

This means that the stochastic modelling approach that is so useful when analyzing systems to obtain quantitative measures cannot be applied as it is to evaluate security properties. At the state of the art different approaches try to overcome this problem by proposing methodologies that makes it possible to incorporate attacker behaviour into the transition rates of a stochastic model, so that a comprehensive system evaluation can be performed.

6.4.2 Game theory

Game theory has been perceived as natural way of modelling cyber-security. Indeed, a game is a description of the strategic interaction between opposing, or co-operating, interests where the constraints and payoff for actions are taken into consideration. Depending on the nature and amount of information held by each player locked in a play, a game can be perfect or imperfect, complete or incomplete, static or dynamic.

A Markov game approach to the assessment of risks is proposed by of Xiaolin et al. (2008). The authors argued that a comprehensive assessment of risk in network information systems should account of, not only the current, but also the future risks. The work is based on the extension of the relationship between threat, vulnerability and asset commonly used in the determination of a risk level. They noted that a vulnerability that remains unpatched can help in the spread of risk, while a risk can be considerably reduced if a prompt and decisive action is taken by the administrator. Subsequently, they proposed a game of where the threat and the vulnerability agents are represented as the players. Thus the threat agent increases the risk by through the action “threat spreading” and the vulnerability agent decreases the risk by through the action “system administrator’s repairing the vulnerability”. The ultimate aim of the game is to get a more comprehensive value of risk as well as giving enabling the system administrator to select the best system repair scheme.

6.4.3 Attack Trees

Attack trees were introduced by Schneier[9] as a way of formally analyzing the security of systems and subsystems based on varying attacks. This is basically FTA with the attack goal in place of a fault and basic event probabilities are not failure rates. Schneier's work is notable because it was the first to apply this approach to the area of information security. The attack goal is the root of the tree and the different ways of accomplishing the attack are the leaves, with connections via AND and OR nodes.

Recently, attack trees have been applied to a SCADA communication system. Eleven attacker goals and associated security vulnerabilities in the specifications and development of typical SCADA systems have been identified:

1. Gain SCADA System Access
2. Identify MODBUS Device
3. Disrupt Master-Slave Communications
4. Disable Slave
5. Read Data from Slave
6. Write Data to Slave
7. Program Slave
8. Compromise Slave
9. Disable Master
10. Write Data to Master
11. Compromise Master

A related approach that arose in the computer and information security literature is vulnerability tree analysis. Vulnerability trees are hierarchy trees constructed as a result of the relationship between one vulnerability and another as well as the steps that a threat agent has to carry out to reach the top of the tree. Vulnerability trees help security analysts understand and analyze different attack scenarios that a threat agent might follow to exploit a vulnerability. With this understanding, countermeasures can be taken. The top of the tree is known as the top vulnerability or the parent vulnerability. There is a large number of ways that such a top vulnerability can be exploited. Each of these ways will constitute a branch of the tree. The branches will be constructed by child vulnerabilities. Consequently the child vulnerabilities can be exploited by steps that the threat agent will have to perform in order to get to the parent. Each vulnerability will have to be broken down in a similar way. Normally this will end up in more than one levels of decomposition. When the point is reached where the branches contain only steps, and no child vulnerabilities, then we know that we have reach the lowest level of decomposition (the "step-only" level).

Several tools are available even on the commercial site to implement attack trees. A short description of the attack tree provided by *Isograph*, named AttackTree+, follows:
AttackTree+, through the use of attack tree models, allows the user to model the probability that different attacks will succeed. AttackTree+ also allows users to define indicators that quantify the cost of an attack, the operational difficulty in mounting the attack and any other relevant quantifiable measure that may be of interest. In AttackTree+, different categories and levels of consequence may also be assigned to nodes in the attack tree. A successful attack may have financial, political, operational and safety consequences. A partially successful attack may have a different level of consequence to a totally successful attack. All these types of consequence measure may be modeled in AttackTree+.

[9] https://www.schneier.com/

6.4.4 Petri nets

Petri nets (PN), in their various shapes and sizes, have been used for the study of the qualitative properties of systems exhibiting concurrency and synchronization characteristics.

The use of PN-based techniques for the quantitative analysis of systems requires the introduction of temporal specifications in the basic, untimed models. This fact has been recognized since a fairly long time, and several different proposals for the introduction of temporal specifications in PN have appeared in the literature.

- **PENET tool**

Among tools based on Petri nets, PENET tool introduces concepts such as the dynamic nature of attacks, the reparability of a system, and the existence of reoccurring attacks.

It attempts to find a balance between ease of use and representation power by providing a set of constructs, parameters, performance metrics, and a time domain analysis of attacks. Particularly, users can draw model diagrams of a given system throughout an intuitive user interface, perform time-domain simulations and carry out security evaluations. Time-domain analysis produces outputs such as “time to reach the main goal” and the “path taken” by the attacker.

The main contribution of the tool is to extend modelling capabilities of attack trees by using Petri net constructs in order to significantly improve the analytical capabilities of attack trees, specifically by:

- Addressing existing issues in attack trees such as limited representation power, imprecision, and lack of defined defense modelling.
- Introducing concepts of recurring attacks, defense modelling, and dynamic constructs.
- Introducing an analysis approach that follows attack execution in time domain.
- Providing means to evaluate system survivability and defense strategies.

Primary audience of this tool is individuals and organizations who want to use such a tool in vulnerability evaluation of cyber-attacks and developing defense strategies for their systems. Secondary audience is research community desiring to learn more about attacker behaviour modelling and PENET approach.

- **Stochastic Petri Net Package**

Since attacks occur randomly, a stochastic process can be used for the model. In some studies, the intrusion and cyber-net are modelled by a generalized stochastic Petri net (GSPN) model. The states of the stochastic process are the status of intrusions to a network that are inferred from the abnormal activities. These include malicious packets flowing through pre-defined firewall rules and failed logon password on the computer system. Transition probabilities are obtained from the abnormal activity data in the system.

A GSPN consists of two different transition classes: immediate and timed transitions. SCADA systems typically have specially designed firewall rules and password policies to achieve a high level of computer security. A firewall is a technology of cyber security defense that regulates the packets flowing between two networks. As there may be different security trust levels between networks, a set of firewall rules is configured to filter out unnecessary traffic. These rules are written with the following criteria for acceptance or rejection:

- Type of protocols
- Incoming and outgoing traffic
- Specific port service or a port service range
- Specific IP address or an IP address range

6.4.5 SIR Model of Epidemics

SIR is an epidemics based model that may be used in cyber-security to study how a malware infection spread among different machines. SIR stands for Susceptible, Infected, Recovered. SIR model represents a disease spread where individuals are susceptible to a disease, potentially contract the disease, recover and become immune to future infections after recovery. There is also a variant of SIR called Susceptible, Infected, Removed that allow infected individuals to die due to the disease and thus leave the considered population. An individual potentially moves from the susceptible to the infected group when s/he comes in contact with an infected individual.

Given specific assumptions on the average number of spread transmission possible from a given infected individual in each period and on the recovering rate of each individual, there are specific algorithms that show the result of spread transmission.

There are several analogies between the malware and the epidemics affecting the animal word. Cyber-security domain considers each individual as a machine that may be infected by a malware and a recover capability as the action of antivirus software that are in place to remove the infections. Dying individuals represent the machines that have been fatally compromised.

The Susceptible, Infected and Resistant (SIR) model was originally developed to study the evolution of a disease over a population, where each individual could be susceptible to the infection, having contracted the infection, or be immune/resistant. The similarity with malwares is very high but some ICT models got the problem that model variables have different values depending on the cyber-security solution adopted for each kind of node.

6.5 STEPS TO IMPROVE CYBER SECURITY OF SCADA NETWORKS

According to the U.S Department of Energy, the following steps focus on actions that should be taken to increase the security of SCADA networks [89]:

6.5.1 Specific actions

- **Identify all connections to SCADA networks.**

Conduct a thorough risk analysis to assess the risk and necessity of each connection to the SCADA network. Develop a comprehensive understanding of all connections to the SCADA network, and how well these connections are protected. Identify and evaluate the following types of connections:

- Internal local area and wide area networks, including business networks
- The Internet
- Wireless network devices, including satellite uplinks
- Modem or dial-up connections
- Connections to business partners, vendors or regulatory agencies

- **Disconnect unnecessary connections to the SCADA network.**

To ensure the highest degree of security of SCADA systems, isolate the SCADA network from other network connections to as great a degree as possible. Any connection to another network introduces security risks, particularly if the connection creates a pathway from or to the Internet. Although direct connections with other networks may allow important information to be passed efficiently and conveniently, insecure connections are simply not worth the risk; isolation of the SCADA network must be a primary goal to provide needed protection.

Strategies such as utilization of “demilitarized zones” (DMZs) and data warehousing can facilitate the secure transfer of data from the SCADA network to business networks. However, they must be designed and implemented properly to avoid introduction of additional risk through improper configuration.

- **Evaluate and strengthen the security of any remaining connections to the SCADA network.**

Conduct penetration testing or vulnerability analysis of any remaining connections to the SCADA network to evaluate the protection posture associated with these pathways. Use this information in conjunction with risk management processes to develop a robust protection strategy for any pathways to the SCADA network. Since the SCADA network is only as secure as its weakest connecting point, it is essential to implement firewalls, intrusion detection systems (IDSs), and other appropriate security measures at each point of entry. Configure firewall rules to prohibit access from and to the SCADA network, and be as specific as possible when permitting approved connections. For example, an Independent System Operator (ISO) should not be granted "blanket" network access simply because there is a need for a connection to certain components of the SCADA system.

Strategically place IDSs at each entry point to alert security personnel of potential breaches of network security. Organization management must understand and accept responsibility for risks associated with any connection to the SCADA network.

- **Harden SCADA networks by removing or disabling unnecessary services.**

SCADA control servers built on commercial or open-source operating systems can be exposed to attack through default network services. To the greatest degree possible, remove or disable unused services and network daemons to reduce the risk of direct attack. This is particularly important when SCADA networks are interconnected with other networks. Do not permit a service or feature on a SCADA network unless a thorough risk assessment of the consequences of allowing the service/feature shows that the benefits of the service/feature far outweigh the potential for vulnerability exploitation. Examples of services to remove from SCADA networks include automated meter reading/remote billing systems, email services, and Internet access. An example of a feature to disable is remote maintenance. Numerous secure configuration guidelines for both commercial and open source operating systems are in the public domain, such as the National Security Agency's series of security guides. Additionally, work closely with SCADA vendors to identify secure configurations and coordinate any and all changes to operational systems to ensure that removing or disabling services does not cause downtime, interruption of service, or loss of support.

- **Do not rely on proprietary protocols to protect your system.**

Some SCADA systems use unique, proprietary protocols for communications between field devices and servers. Often the security of SCADA systems is based solely on the secrecy of these protocols. Unfortunately, obscure protocols provide very little "real" security. Do not rely on proprietary protocols or factory default configuration settings to protect your system. Additionally, demand that vendors disclose any backdoors or vendor interfaces to your SCADA systems, and expect them to provide systems that are capable of being secured.

- **Implement the security features provided by device and system vendors.**

Most older SCADA systems (most systems in use) have no security features whatsoever. SCADA system owners must insist that their system vendor implement security features in the form of product patches or upgrades. Some newer SCADA devices are shipped with basic security features, but these are usually disabled to ensure ease of installation. Analyze each SCADA device to determine whether security features are present. Additionally, factory default security settings (such as in computer network firewalls) are often set to provide maximum usability, but minimal security. Set all security features to provide the maximum level of security. Allow settings below maximum security only after a thorough risk assessment of the consequences of reducing the security level.

- **Establish strong controls over any medium that is used as a backdoor into the SCADA network.**

Where backdoors or vendor connections do exist in SCADA systems, strong authentication must be implemented to ensure secure communications. Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the SCADA network and remote sites. Successful "war dialing" or "war driving" attacks could allow an attacker to bypass all other controls and have direct access to the SCADA network or resources. To minimize the risk of such attacks, disable inbound access and replace it with some type of callback system.

- **Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring.**

To be able to effectively respond to cyber-attacks, establish an intrusion detection strategy that includes alerting network administrators of malicious network activity originating from internal or external sources. Intrusion detection system monitoring is essential 24 hours a day; this capability can be easily set up through a pager. Additionally, incident response procedures must be in place to allow an effective response to any attack. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.

- **Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.**

Technical audits of SCADA devices and networks are critical to ongoing security effectiveness. Many commercial and open-source security tools are available that allow system administrators to conduct audits of their systems/networks to identify active services, patch level, and common vulnerabilities. The use of these tools will not solve systemic problems, but will eliminate the "paths of least resistance" that an attacker could exploit. Analyze identified vulnerabilities to determine their significance, and take corrective actions as appropriate. Track corrective actions and analyze this information to identify trends. Additionally, retest systems after corrective actions have been taken to ensure that vulnerabilities were actually eliminated. Scan non-production environments actively to identify and address potential problems.

- **Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.**

Any location that has a connection to the SCADA network is a target, especially unmanned or unguarded remote sites. Conduct a physical security survey and inventory access points at each facility that has a connection to the SCADA system. Identify and assess any source of information including remote telephone/computer network/ fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Identify and eliminate single points of failure. The security of the site must be adequate to detect or prevent unauthorized access. Do not allow "live" network access points at remote, unguarded sites simply for convenience.

- **Establish SCADA "Red Teams" to identify and evaluate possible attack scenarios.**

Establish a "Red Team" to identify potential attack scenarios and evaluate potential system vulnerabilities. Use a variety of people who can provide insight into weaknesses of the overall network, SCADA systems, physical systems, and security controls. People who work on the system every day have great insight into the vulnerabilities of your SCADA network and should be consulted when identifying potential attack scenarios and possible consequences. Also, ensure that the risk from a malicious insider is fully evaluated, given that this represents one of the greatest threats to an organization. Feed information resulting from the "Red Team" evaluation into risk management processes to assess the information and establish appropriate protection strategies.

6.5.2 Management actions

- **Clearly define cyber-security roles, responsibilities, and authorities for managers, system administrators, and users.**

Organization personnel need to understand the specific expectations associated with protecting information technology resources through the definition of clear and logical roles and responsibilities. In addition, key personnel need to be given sufficient authority to carry out their assigned responsibilities. Too often, good cyber-security is left up to the initiative of the individual, which usually leads to inconsistent implementations and ineffective security. Establish a cyber-security organizational structure that defines roles and responsibilities and clearly identifies how cyber-security issues are escalated and who is notified in an emergency.

- **Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.**

Develop and document robust information security architecture as part of a process to establish an effective protection strategy. It is essential that organizations design their networks with security in mind and continue to have a strong understanding of their network architecture throughout its lifecycle. Of particular importance, an in-depth understanding of the functions that the systems perform and the sensitivity of the stored information is required. Without this understanding, risk cannot be properly assessed and protection strategies may not be sufficient. Documenting the information security architecture and its components is critical to understanding the overall protection strategy, and identifying single points of failure.

- **Establish a rigorous, ongoing risk management process.**

A thorough understanding of the risks to network computing resources from denial-of-service attacks and the vulnerability of sensitive information to compromise is essential to an effective cyber-security program. Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Initially, perform a baseline risk analysis based on a current threat assessment to use for developing a network protection strategy. Due to rapidly changing technology and the emergence of new threats on a daily basis, an ongoing risk assessment process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective. Fundamental to risk management is identification of residual risk with a network protection strategy in place and acceptance of that risk by management.

- **Establish a network protection strategy based on the principle of defense-in-depth.**

A fundamental principle that must be part of any network protection strategy is defense-in-depth. Defense in-depth must be considered early in the design phase of the development process, and must be an integral consideration in all technical decision-making associated with the network. Utilize technical and administrative controls to mitigate threats from identified risks to as great a degree as possible at all levels of the network. Single points of failure must be avoided, and cyber-security defense must be layered to limit and contain the impact of any security incidents. Additionally, each layer must be protected against other systems at the same layer. For example, to protect against the insider threat, restrict users to access only those resources necessary to perform their job functions.

- **Clearly identify cyber-security requirements.**

Organizations and companies need structured security programs with mandated requirements to establish expectations and allow personnel to be held accountable. Formalized policies and procedures are typically used to establish and institutionalize a cyber-security program. A formal program is essential for establishing a consistent, standards-based approach to cyber security throughout an organization and eliminates sole dependence on individual initiative. Policies and procedures also inform employees of their specific cyber-security responsibilities and the consequences of failing to meet those responsibilities. They also provide guidance regarding actions to be taken during a cyber-security incident and promote efficient and effective actions during a time of crisis. As part of identifying cyber-security requirements, include user agreements and notification and warning banners. Establish requirements to minimize the threat from malicious insiders, including the need for conducting background checks and limiting network privileges to those absolutely necessary.

- **Establish effective configuration management processes.**

A fundamental management process needed to maintain a secure network is configuration management.
Configuration management needs to cover both hardware configurations and software configurations. Changes to hardware or software can easily introduce vulnerabilities that undermine network security. Processes are required to evaluate and control any change to ensure that the network remains secure. Configuration management begins with well-tested and documented security baselines for your various systems.

- **Conduct routine self-assessments.**

Robust performance evaluation processes are needed to provide organizations with feedback on the effectiveness of cyber security policy and technical implementation. A sign of a mature organization is one that is able to self-identity issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems. Self-assessment processes that are normally part of an effective cyber-security program include routine scanning for vulnerabilities, automated auditing of the network, and self-assessments of organizational and individual performance.

- **Establish system backups and disaster recovery plans.**

Establish a disaster recovery plan that allows for rapid recovery from any emergency (including a cyber-attack). System backups are an essential part of any plan and allow rapid reconstruction of the network. Routinely exercise disaster recovery plans to ensure that they work and that personnel are familiar with them. Make appropriate changes to disaster recovery plans based on lessons learned from exercises.

- **Senior organizational leadership should establish expectations for cyber-security performance and hold individuals accountable for their performance.**

Effective cyber-security performance requires commitment and leadership from senior managers in the organization. It is essential that senior management establish an expectation for strong cyber-security and communicate this to their subordinate managers throughout the organization. It is also essential that senior organizational leadership establish a structure for implementation of a cyber-security program. This structure will promote consistent implementation and the ability to sustain a strong cyber-security program. It is then important for individuals to be held accountable for their performance as it relates to cyber security. This includes managers, system administrators, technicians, and users/operators.

- **Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.**

Release data related to the SCADA network only on a strict, need-to-know basis, and only to persons explicitly authorized to receive such information. “Social engineering,” the gathering of information about a computer or computer network via questions to naive users, is often the first step in a malicious attack on computer networks. The more information revealed about a computer or computer network, the more vulnerable the computer/ network is. Never divulge data related to a SCADA network, including the names and contact information about the system operators/administrators, computer operating systems, and/or physical and logical locations of computers and network systems over telephones or to personnel unless they are explicitly authorized to receive such information. Any requests for information by unknown persons need to be sent to a central network security location for verification and fulfillment. People can be a weak link in an otherwise secure network. Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords.

CONCLUSIONS

In this deliverable, we examined SCADA-related attacks and how these could be prevented or mitigated. Through a security review, we provided information regarding the past and present of SCADA systems by referring to information on the implementation of industrial control systems in the past; how these were evolved, and the security issues imposed by that evolution. By presenting an existing security policy framework, we pinpointed the need for having adequate security management, and showed how this can be done using a systematic approach.

A comprehensive reference to existing cyber threats and vulnerabilities that dwell in SCADA systems was used to landscape them, and thus, resulting in offering an adequate level of awareness against threats and vulnerability. Cyber attacks on SCADA systems were also examined in a comprehensive way by providing a taxonomy of them; a description of the attack sources and profiles of attackers, and last but not least, the typical attack phases of such an attack. Regarding the latter, we also described how some type of attacks could be easily automated, something that might result in attacking multiple systems in an efficient way.

Having discussed all the aforementioned, we conclude the report with the presentation of a set of existing approaches, guidelines and tools that when applied would result in the improvement of the overall security level of SCADA systems.

REFERENCES

[1] Fortinet, "Securing SCADA Infrastructure - White Paper," 2010.

[2] I. -. I. S. E. A. Group, "Generic SCADA Risk Management Framework For Australian Critical Infrastructure," Saltbush Group, 2012.

[3] K. M. M. L. D. J. M. a. D. T. T. Adrian Pauna, "Can we learn from SCADA security incidents?," ENISA, 2013.

[4] K. Wilhoit, " The SCADA That Didn't Cry Wolf," A Trend Micro Research Paper, 2013.

[5] B. Sudeeptha Rudrapattana, "Cyber-Security Analysis in Smart Grid SCADA Systems : A Game Theoretic Approach," Texas Tech University, 2013.

[6] J. F. a. K. S. K. Stouffer, "Guide to Industrial Control Systems (ICS) Security," June 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

[7] scadaworld.net, 2013. [Online]. Available: http://www.scadaworld.net/communication-infrastructure.html.

[8] W. T. Shaw, Cybersecurity for SCADA Systems, PennWell Books, 2006.

[9] S. Iyer, ""Cyber Security for Smart Grid, Cryptography, and Privacy"," *International Journal of Digital Multimedia Broadcasting,* vol. vol. 2011.

[10] Z. Vale, H. Morais, M. Silva and C. Ramos, ""Towards a future SCADA,"," in *Power & Energy Society General Meeting*, 26-30 July 2009.

[11] ENISA, "Smart Grid Security Recommendations," Jul 10, 2012.

[12] S. Zajkowski, " SCADA – The Brain of the Smart Grid," *Remote Magazine,* January 14, 2014.

[13] K. Wilhoit, "Scada in the cloud - a security conundrum?," *Technical report, Trend Micro Incorporated,* 2013.

[14] N.-E. Research, "Release of North American 2013-2015 EMS, SCADA, DMS and OMS Report.," January 25, 2013.

[15] D. S. J. Kilman, "Framework for SCADA Security Policy. Sandia National Laboratories," 2005.

[16] "http://www.risidata.com/," [Online].

[17] "http://en.wikipedia.org/wiki/Phishing," [Online].

[18] "http://www.securityweek.com/siemens-fixes-critical-vulnerabilities-wincc-scada-products," [Online].

[19] M. M. L. G. a. G. C. Igor Nai Fovino, "An Experimental Platform for Assessing SCADA Vulnerabilities and Countermeasures in Power Plant," 2010.

[20] K. M. Konstantinos Markantonakis, Secure Smart Embedded Devices, Platforms and Applications, Springer, 2014, pp. 451-469.

[21] A. D. P. M. M. e. a. E. Ciancamerla, "D2.1-Overview of modelling techniques and tools for SCADA systems under cyber attacks," Cockpit CI Project. FP7-SEC-2011-1, 2012.

[22] R. L. Krutz, "Securing SCADA systems," Wiley, 2006.

[23] J.-J. L. S.-J. K. a. J.-H. P. Dong-Joo Kang, "Analysis on Cyber Threats to SCADA systems," 2009.

[24] M. Anavi, "Cyber Security for Power Utilities: A defense primer for the operational network - White Paper," RAD Data Communications, 2013.

[25] "http://en.wikipedia.org/wiki/Script_kiddie," [Online].

[26] T. H. Y. W. M. C. Ettore Bompard, "Classification and trend analysis of threats origins to the security of power systems," *Elsevier,* no. 50, pp. 50-64, 2013.

[27] I. N. Program, "Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program," November 2008.

[28] "Shodan search engine," [Online]. Available: http://www.shodanhq.com. [Accessed January 2015].

[29] D. Goldman, "Shodan: The scariest search engine on the Internet.," April 8, 2013.

[30] A. Massoud, "Security Challenges for the Electricity Infrastructure," *Special Issue of the IEEE Computer Magazine on Security and Privacy,* pp. 8-10, 2002.

[31] G. T. D. a. B. T. Francia III, "Cyberattacks on SCADA Systems. Proceedings of the 16th Colloquium for Information Systems Security Education Lake Buena Vista," Jacksonville State University, Florida June 11 - 13, 2012.

[32] E. L. D. K. M. Byers, "Security incidents and trends in SCADA and process industries".*Industrial Ethernet Book.*

[33] B. R. D. Miller, "A Survey of SCADA and Critical Infrastructure Incidents," New York, 2012.

[34] S. a. C. W. T. S. P. Explosion, "http://defsecnet.com/software-and-cold-war-the-siberian-pipeline-explosion/," [Online].

[35] D. Denning, "Cyberterrorism: The Logic Bomb Versus Truck Bomb," *Global Dialogue,* vol. 2, no. 4, 2000.

[36] R. Turk, " Cyber Incidents Involving Control Systems," *Contract,* 2005.

[37] E. b. D. e. a. Remenyi, "Proceedings of the 5th European Conference on Information Warfare and Security," 2006.

[38] "Pipeline Rupture and Subsequent Fire in Bellingham," Washington, 2002.

[39] S. Mustard, "Security of distributed control systems: the concern increases," *Computing & Control Engineering Journal,* 2005.

[40] A. e. a. Nicholson, " SCADA Security in the light of Cyber-Walfare," *Computers & Security,* vol. 31, no. 4, 2012.

[41] Wikipedia, "Operation Aurora," 2014. [Online]. Available: http://en.wikipedia.org/wiki/Operation_Aurora.

[42] "http://en.wikipedia.org/wiki/Stuxnet," [Online].

[43] K. Zetter, "Son of Stuxnet Found in the Wild on Systems in Europe," *Wired,* 2011.

[44] "http://abcnews.go.com/Blotter/flame-cyber-attack-israel-largest-cyber-spy-weapon/story?id=16449339," [Online].

[45] Symantec, "The Shamoon Attacks," 16 August 2012.

[46] Seculert, "Shamoon, a two-stage targeted attack," 16 August 2012.

[47] Shamoon Malware and SCADA Security, "What are the Impacts?," Tofinosecurity, 25 October 2012 .

[48] Symantec, "Dragonfly: Cyberespionage Attacks Against Energy Suppliers," July 2014. [Online].

[49] F. Secure, "Havex Hunts For ICS/SCADA Systems," June 2014. [Online]. Available: https://www.f-secure.com/weblog/archives/00002718.html.

[50] Kaspersky, "Lab Research on Energetic Bear," 01 July 2014.

[51] Symantec, "Dragonfly: Western Energy Companies Under Sabotage Threat," 30 June 2014.

[52] Tofinosecurity., "Dragonfly Malware Targets ICS Systems," 08 August 2014 .

[53] International Society of Automation (ISA), "ISA99, Industrial Automation and Control Systems Security," [Online]. Available: http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821, 2013.

[54] R. S. &. e. management, "Protecting Critical Infrastructure – Understanding the Threat to SCADA Networks," Oct 7, 2014.

[55] R. Tsang, "Cyberthreats, Vulnerabilities and Attacks on SCADA Networks".

[56] K. M. T. L. S. S. E. G. I. Z. Q. Y. B. P. H. F. W. Y. Yang, "Man in the middle attack test bed investigating cyber security vulnerabilities in smart grid SCADA systems," 2012.

[57] M. Kjaerland, "A taxonomy and comparison of computer security incidents from the commercial and government sectors," vol. 25, no. 7, pp. 522-538, 2006.

[58] A. J. S. S. Bonnie Zhu, "A Taxonomy of Cyber Attacks on SCADA Systems," *IEEE,* pp. 384-387, 2011.

[59] C. Sanders, "Understanding Man-in-the-Middle-Attacks," 17 March 2010. [Online]. Available: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html. [Accessed 28 January 2015].

[60] S. A. A. C. a. S. S. S. Amin, *"Safe and secure networked control systems under denial-of-service attacks." Hybrid Systems: Computation and Control,* Springer Berlin Heidelberg, . , 2009, pp. 31-45.

[61] C. Joe Weiss PE, *assuring industrial control system (ICS) cyber security, Applied Control Solutions, LLC,* 25 Aug 2008.

[62] B. X. Zhu, "Resilient Control and Intrusion Detection for SCADA," Electrical Engineering and Computer Sciences. University of California at Berkeley, 2014.

[63] R. Tsang, "Cyberthreats, vulnerability and attack on SCADA network".

[64] S. S. J. &. K. G. Mcclure, " Hacking Exposed 7, Network Security Secreats & Solutions," , 2012.

[65] A. Gouglidis, "An effective attack method based on information exposed by search engines," Kaspersky, IT Security for the Next Generation, European Cup, 2012.

[66] Google, Custom Search 2014. [Online]. Available: https://developers.google.com/custom-search/.

[67] Microsoft, Bing Search API 2014. [Online]. Available: https://datamarket.azure.com/dataset/5BA839F1-12CE-4CCE-BF57-A49D98D29A44 2014.

[68] SHODAN, "Shodan Search Engine," 2014. [Online]. Available: http://www.shodanhq.com.

[69] RAPID7, "Metasploit," 2014. [Online]. Available: http://www.metasploit.com.

[70] C. E. B. a. C. S. S. Cabuk, "IP covert timing channels: design and detection," in proceedings of the 11th ACM conference on Computer and communications security (CCS '04), 2004.

[71] a. S. J. N.F. Johnson, "Steganalysis of images created using current steganography software," David Aucsmith (Ed.): Information Hiding, LNCS 1525, pp. 32-47, Springer-Verlag Berlin Heidelberg, 1998.

[72] D. Beresford, "Exploiting Siements Simatic S7 PLCs," 2011.

[73] Siemens, 2014. [Online]. Available: http://w3.siemens.com/mcms/programmable-logic-controller/en/basic-controller/Pages/Default.aspx. [Accessed 2014].

[74] IEEE, 2012. [Online]. Available: http://standards.ieee.org/about/get/802/802.3.html. [Accessed 2014].

[75] PI, 2006. [Online]. Available: http://us.profinet.com/technology/profinet/. [Accessed 2014].

[76] T. L. Group, 2011. [Online]. Available: http://www.langner.com/en/2011/08/20/ics-cert-on-beresford-vulns-flawed-analysis-misleading-advice/. [Accessed 2014].

[77] R. Graham, 2011. [Online]. Available: http://blog.erratasec.com/2011/08/what-heck-is-iso-tsap.html. [Accessed 2014].

[78] Siemens, 2012. [Online]. Available: http://www.automation.siemens.com/salesmaterial-as/brochure/en/brochure_simatic-step7_tia-portal_en.pdf. [Accessed 2014].

[79] J. T. F. T. Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[80] R. R. a. J. C. A. Behnia, "A Survey of Information Security Risk Analysis Methods," Smart Computing Review, 2(1), , February, 2012.

[81] Software Engineering Institute Carnegie Mellon, "OCTAVE Information Security Risk Evaluation," 2013. [Online]. Available: http://www.cert.org/octave/.

[82] B. K. a. I. Sogukpinar, "ISRAM: information security risk analysis method," Computers & Security, 24(2):147–159, 2005.

[83] T. D. B. G. M. L. K. S. a. J. A. F. den Braber, "The CORAS methodology: model-based risk assessment using UML and UP," UML and the Unified Process, pages 332–357, 2003.

[84] ENISA, "Inventory of risk management/risk assessment methods and tools," 2013. [Online]. Available: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory.

[85] M. A. G. a. J. C. F.L. Crespo, "MAGERIT – version 2 Methodology for Information Systems Risk Analysis and Management Book I – The Method," Ministerio de administraciones públicas, 2006.

[86] North American Electric Reliability Corporation (NERC), "CIP Standards," 2013. [Online]. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[87] E. E. L. T. V. V. R. E. a. J. A. R. Leszczyna, "Protecting Industrial Control Systems Recommendations for Europe and Member States," ENISA Whitepaper 2011. [Online]. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems-recommendations-for-europe-and-member-states/at_download/fullReport.

[88] D. o. H. S. F. C. i. F. Cybersecurity, "Critical infrastructure protection report," May 2005.

[89] U.S Department of Energy, "21 Steps to Improve Cyber Security of SCADA Network," Office of Electricity Delivery & Energy Reliability, 2007.

[90] P. F. José Cecílio, Wireless Sensors in Industrial Time-Critical Environments, Springer, 2014.

[91] G. C. a. S. Kim, "Towards Improving SCADA Control Systems Security with Vulnerability Analysis," in *Parallel and Distributed Computing and Networks*, 2010.

[92] L. N. a. B. Huba, "Top ten differences between ICS and IT cybersecurity," May-June 2014.

[93] W. D. K. L. H. Owens, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Research Council of the National Academies, The National Academies Press, 2009.

[94] L. S. A. a. W. R. D. Igure V. M., "Security issues in SCADA networks," vol. 25, no. 7, 2006.

[95] R. Leszczyna, I. Nai Fovino and M. Masera, "Security Evaluation of IT Systems Underlying Critical Networked Infrastructures," 2008.

[96] A. Carcano, I. Nai Fovino and N. a. T. A. Masera, "Scada Malware, a proof of Concept.," Rome, 2008.

[97] J. Weiss, Protecting Industrial Control Systems from Electronic Threats, Momentum Press, 2010.

[98] Y. c. N. O. C. L. Fujiyama, "Process for fluid catalytic cracking of oils". 2001.

[99] Homeland Security, "Partnering for Critical Infrastructure Secure and Resilience," 2013.

[100] J. Hyne, Nontechnical Guide to Petroleum Geology, Exploration, Drilling, and Production, PennWell Books, 2012.

[101] M. M. a. S. P. E. Ciancamerla, "Modeling cyber attacks on a critical infrastructure scenario," 2013.

[102] T. A.-N. S. Chen, "Lessons from Stuxnet," vol. 44, no. 4, pp. 91-93, 2011.

[103] T. T. J. T. Spyridopoulos, "Incident Analysis & Digital Forensics in SCADA and Industrial Control Systems," vol. 2013, 2013.

[104] "https://www.schneier.com/crypto-gram-0005.html," [Online].

[105] "https://www.princeton.edu/~ota/disk3/1983/8312/831208.PDF," [Online].

[106] "https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf," 2013. [Online].

[107] "http://www.washingtonpost.com/wp-dyn/content/article/2005/08/26/AR2005082601201.html," [Online].

[108] "http://www.isa-95.com/," [Online].

[109] "http://www.gao.gov," [Online].

[110] A. Hopkins, "http://www.futuremedia.com.au/docs/Lessons%20from%20Longford%20by%20Hopkins.PDF," [Online].

[111] U. E. I. A. ". E. O. r. EIA, 2010. [Online].

[112] "http://pipelineandgasjournal.com/hacking-industrial-scada-network?page=show," [Online].

[113] S. C. R. Holditch, "Factors That Will Influence Oil and Gas Supply and Demand in the 21st Century," *MRS Bulletin,* vol. 33, 2008.

[114] R. C. M. Kozik, "Current cyber security threats and challenges in critical infrastructures protection," 2013.

[115] M. M. W. A.V. Gheorghe, Critical Infrastructures at Risk: Securing the european Electric Power System, Springer, 2006.

[116] R. S. S. D. Javier L., Critical Infrastructure Protection, Springer, 2012.

[117] C. Alcaraz and S. Zeadally, "Critical Control System Protection in the 21st Century," vol. 46, no. 10, 2013.

[118] S. K. Suad Ibrahimkadic, "Characteristics of modern industrial control systems," *IEEE,* 2011.

[119] T. Reed, At the Abyss: An Insider's History of the Cold War, 2004.

[120] R. H. Simon Hansman, A taxonomy of network and computer attacks, Computer & Security, 2004.

[121] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Nai Fovino and A. Trombetta, "A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems," vol. 7, 2011.

[122] N. T. S. B. NTSB, "'"Safety Study – Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines," Washington, , 2005.

[123] G. Cagalaban, T. KIM and S. KIM, " Improving SCADA Control Systems Security with Software Vulnerability Analysis," 2010.

[124] K. F. J. K. K. Stoufer, " Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial control Systems Security," National Institute of Standards and Technology, Maryland, 2008.

[125] G. Dondossola, M. Masera, I. Nai Fovino and J. Szanto, " Effects of intentional threats to power

substation control systems.," vol. 4, 2008.

[126] S. Melito, "http://defsecnet.com/software-and-cold-war-the-siberian-pipeline-explosion/," [Online].

[127] Z. K., "“Flame” spyware infiltrating Iranian computers," *Wired,* 2012.

[128] "https://www.jivesoftware.com," [Online].

[129] "http://www.advanced-ip-scanner.com/," [Online].

[130] "http://www.advanced-ip-scanner.com/," [Online].

[131] B. Robert-son, "Integrating Security into SCADA Solutions," PA Consulting Group, NISCC SCADA Security Conference, 2003.

[132] J. C. P. D. J. D. J. a. Y. W. Stamp, "Sustainable Security for Infrastructure SCADA," Sandia National Laboratories report SAND2003-4670C, Albuquerque, New Mexico, 2003.

[133] I. S. S. IBM, "A Strategic Approach to Protecting SCADA and Process Control Systems - White Paper," 2007.

[134] B. J. A. S. S. Zhu, "A Taxonomy of Cyber Attacks on SCADA Systems," Department of Electrical Engineering and Computer Sciences. University of California , Berkeley, CA.

[135] R. D. Larkin, "Evaluation of Traditional Security Solutions in the SCADA Environment," Air force institute of technology. Wright-Patterson air force base, Ohio, 2012.

[136] J. G. Y. E. Fiaidhi, "SCADA Cyber Attacks and Security Vulnerabilities," Department of Computer Science, Lakehead University, Hannam University, Korea.

[137] R. G. e. al., "A Review of Cyber Security Techniques for Critical Infrastructure Protection.," International Journal of Computer Science & Engineering Technology (IJCSET)., 2014.

[138] E. L. D. K. N. Byres, "Security Incidents and Trends in the SCADA and Process Industries. A statistical review of the Industrial Security Incident Database (ISID)," Symantec, 2007.

[139] J. C. L. B. R. a. C. L. A. Avizienis, "Basic concepts and taxonomy of dependable and secure computing.," IEEE Transactions on Dependable and Secure Computing, 2004.

[140] T. X. Z. Y. a. X. H. Xiaolin, "A markov game theory-based risk assessment model for network information systems," International conference on computer science and software engineering, 2008.

[141] M. Hentea, "Improving Security for SCADA Control Systems.," Interdisciplinary Journal of Information, Knowledge, and Management. Excelsior College, Albany, NY, USA., 2008.

[142] ISA99/IEC, "Security for Industrial Automation and Control Systems," Models and Concepts (ISA-99.00.01/ IEC-TS62443-1-1), 2007.

[143] E. K. Ç. a. J. P. Sterbenz, "A Taxonomy of Network Challenges," in 9th IEEE/IFIP International Conference on Design of Reliable Communication Networks (DRCN). pp. 322–330., Budapest, Hungary, March 2013.

[144] A. J. S. S. B. Zhu, "A Taxonomy of Cyber Attacks on SCADA Systems," in Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing. pp.380–388, 19-22 Oct. 2011.

[145] C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network Security, vol. 2011, no. 8, pp. 16–19, 2011.

[146] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," IEEE Security & Privacy, vol. 9, no. 3, pp. 49–51, 2011.

[147] D. SecureWorks, "Understand the Threat," [Online]. Available: http://www.secureworks.com/cyber-

threat-intelligence/advanced-persistent-threat/understand-the-threat/.
[148] Blenden, "Shamoon: Malicious Malware Harms 30,000+ Computers," 29 October, 2012.
[149] Blenden, "How Dragonfly Hackers and RAT Malware Threaten ICS Security," 15 September 2014.
[150] Kaspersky Lab Reports, "First Victims of the Stuxnet Worm Revealed," 11 November 2014.