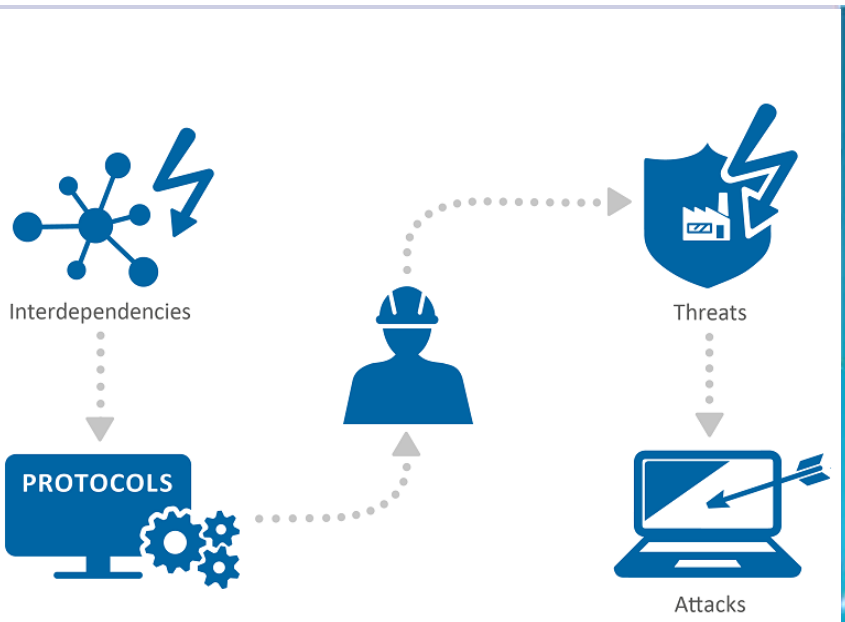


Communication network dependencies for ICS/SCADA Systems

DECEMBER 2016

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

Over the course of this study, we have received valuable input and feedback from:
Aurelio Blanquet, Edp Distribuiçao
Vytautas Butrimas, Ministry Of National Defense, Republic Of Lituania
Bart De Wijs, Abb
Brice Copy, Cern
Christopher Johnson, Glasgow Ac
Eduardo Di Monte, Agbar
Gitta Bengkrut, Eon
Ignacio Paredes, Booz Allen Hamilton
Jos Menting, Engie Lab Laborelec
Konstantin Rogalas, Honeywell
Leire Rodríguez, Gas Natural Fenosa
Luís Parrondo, London Underground
Michael Weires, Covestro
Pablo Barreiro, Gas Natural Fenosa
Paul Bremen, Watercompany Groningen
Stefano Bracco, Agency For The Cooperation Of Energy Regulators
Tomi Pitkanen, Neste
Ignacio Paredes, Booz Allen Hamilton
Jean-Charles Tournier, Cern
Swiss Federal Office For Civil Protection Focp
Symantec Corporation
Finally, we thank the experts of the ENISA ICS Stakeholder Group, EuroSCSIE and all participants to the ENISA open sessions held in Frankenthal in September 2016 and in Stockholm in October 2016 in providing us with useful feedback during discussions and interviews.

ISBN: 978-92-9204-192-2, doi: 10.2824/397676

Table of Contents

Executive Summary

The use of long-range communication networks, and specially the Internet, has revolutionised ICS/SCADA systems and architectures. The use of network communication in these systems has proven to be an effective way of gaining a means for remotely operating and maintaining these infrastructures in real-time. Therefore, they have become vital assets that provide a functionality otherwise impossible.

However, this also opens up the way for new threat vectors that can potentially compromise the efficient and secure operation of these systems. These threats are not necessarily new; many are inherited from the use of networking technologies (in use in IT areas for a long time now), which leads to the fact that there are already countermeasures available to mitigate or even eliminate them.

For this reason, ENISA is continuing the work on communication network dependencies in industrial infrastructures, focusing in this case on ICS/SCADA systems and networks. The main objective is to provide insight into the communication network interdependencies currently present in industrial infrastructures and environments, mapping critical assets, assessing possible attacks and identifying potential good practices and security measures to apply.

In order to properly map the critical assets in these network infrastructures, the layers from ISA95 [1] have been given as a guideline. The main reason to choose it (as opposed to other alternatives such as ISA99) is the fact that it focuses mainly on the network connection between the different assets in play in the network, providing a perfect means for identifying and classifying them.

The experts contacted and interviewed also provided their views and concerns regarding the need for security and the main obstacles and issues that they were facing. The consolidation of the feedback obtained provided the three most worrying potential attack scenarios, considering their potential impact and the assets that could be affected. These scenarios are:

- A compromise of the SCADA systems where an attacker took control of one or multiple assets within the network and as a result, the attacker would have been able to manipulate them at will, affecting, corrupting and even making them crash. This requires the compromised system to be accessible through the Internet, even if it is not directly connected (for example, behind a security perimeter). In a worst-case scenario, this compromise could impede operations, causing blackouts or service cuts, and directly affecting the population.
- A situation where an internal user (employee, contractor or third-party staff) is disgruntled with the organisation was also discussed as a risk scenario. The reason is that these users have in-depth knowledge of the internal workings of the organisation, infrastructure, network, operations and procedures. In the unlikely event that they decide to cause havoc, they would have the means to do so and it would be up to the security measures in place (such as authentication processes or unauthorised behaviour/intrusion detection systems) to stop them.
- The infection of the ICS/SCADA systems during maintenance and upgrade processes is also of high concern. The risk of these systems becoming infected, either by malware transmitted via the technicians' laptop, or via an infected firmware or update package represents a considerable issue; maintenance is a process in which the security measures in place often do not apply, as a direct connection with the SCADA.
- Website where the update files and firmware are located.

To promote solutions to these issues and concerns, it is vital to achieve a higher level of interaction between the different actors that participate throughout the whole lifecycle of the ICS/SCADA assets.

In conclusion, after taking into consideration the views expressed by the experts interviewed, the available standards, good practices and security measures, a series of recommendations has been developed. They are focused on the operators and asset owners mainly and are in the benefit of their CISOs, in order to help them determine how to face the new challenges that have appeared and reduce the threats that put their infrastructures and organisations at risk:

- Recommendation 1: Include security as a main consideration during the design phase of ICS/SCADA systems. Traditionally, only safety is included as one of the main considerations during the design of the ICS/SCADA systems, infrastructures or assets (alongside efficiency, real-time constraints, etc.), but security was usually omitted. The objective is to ensure that security is included as one of these main considerations not only during the design phase but also during the update of the systems.
- Recommendation 2: Identify and establish roles of people operating in ICS/SCADA systems. The management of the access privileges of users in ICS/SCADA systems is a critical process. The objective is to improve this process to ensure that the privilege assignation is adequately controlled and unauthorised access to systems, either intentional or accidental, is reduced to a minimum.
- Recommendation 3: Define network communication technologies and architecture with interoperability in mind. As ICS/SCADA systems are becoming more interconnected with other systems, not only from the same organisation but also with external ones, interconnectivity and compatibility become critical factors. The objective is to focus on promoting the use of common protocols and technologies that are compatible across different devices from multiple manufacturers, avoiding locked proprietary protocols and technologies.
- Recommendation 4: Establish brainstorming and communication channels for the different participants in the lifecycle of the devices to exchange needs and solutions. Another point of concern is that there is usually a lack of communication between the different actors involved across the lifecycle of the ICS/SCADA assets and devices. The need to improve between all these parties involved is a factor that would definitely improve the security of the systems, as needs and solutions would be shared across all.
- Recommendation 5: Include the periodic ICS/SCADA device update process as part of the main operations of the systems. The process of updating the software and firmware of ICS/SCADA devices is a relatively new process, and a very delicate one. Traditionally, this was not needed as there was no interconnection and the threats were limited to physical tampering. Nowadays, the update process needs to be added as part of the lifecycle of the devices, including periodical update processes, to ensure that they are protected against the threats they are exposed to.
- Recommendation 6: Establish periodic ICS/SCADA security training and awareness campaign within the organisation. The concept of cyber-security is relatively new in ICS/SCADA environments, as it was not needed traditionally. Therefore, there is a need to ensure that the staff is aware of the threats that they are exposed to on a daily basis, both in their operations and in the systems they operate with.
- Recommendation 7: Promote increased collaboration amongst policy decision makers, manufacturers and operators at an EU Level. nowadays, critical infrastructures have become linked with the cyberspace, taking advantage of the functionality and benefits it offers. However, this brings about the need to make critical systems and infrastructures safer and more reliable, in order to protect them from the new threats that have arisen from this new interconnectivity level. This also needs to be addressed by policy makers, manufacturers and operators in order to ensure that they are aligned with this objective.
- Recommendation 8: Define guidelines for the establishment of reliable and appropriate cybersecurity insurance requirements. The critical infrastructures of the organisations are now more exposed than ever to threats and attackers worldwide due the use of network communications and the Internet. This leads

to the appearance of insurance solutions to protect the assets in case of an incident. For this purpose, it is recommended to establish guidelines on proper insurance coverage to help both organisations and companies in providing and making use of these services.

Glossary

ACL	Access Control List
APT	Advanced Persistent Threat
BI	Business Intelligence
BSS	Business Support Systems
CIM	Common Information Model
CISO	Chief Information Security Officer
CRM	Control Room Management
CSP	Communication Service Provider
DCS	Distributed Control System
DMZ	Demilitarized Zone
DNP	Distributed Network Protocol
DoS/DDoS	Denial of Service/Distributed Denial of Service
DRP	Disaster Recovery Plan
EAP	Extensible Authentication Protocol
ERP	Enterprise Resource Planning
HMI	Human-Machine Interface
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IED	Intelligent Electronic Device
IoT	Internet of Things
ISP	Internet Service Provider
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MES	Manufacturing Execution System
MITM	Man-In-The-Middle
MMI	Man-Machine Interface
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NFC	Near-Field Communication
OSS	Operation Support Systems
PEAP	Protected Extensible Authentication Protocol
PLC	Programmable Logic Controller
RBAC	Role-Based Access Control
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SSH	Secure Shell
SSL/TLS	Secure Socket Layer/Transport Layer Security
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WAN	Wide Area Network

1. Introduction

Industrial Control Systems (ICS) are command and control systems designed to support industrial processes. These systems are responsible for monitoring and controlling a variety of processes and operations such as gas and electricity distribution, water treatment, oil refining or railway transportation. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems.

ICS/SCADA nowadays are standard technologies, sometimes highly interconnected with other corporate networks and the Internet.

On the one hand, there are many benefits obtained from the implementation and development of ICS/SCADA communications (e.g. remote access, increased automation, improved supervision, etc.). On the other hand, this increased level of communications also exposes SCADA systems to new and traditional threats (already existing in other intercommunicated systems), and this is something that has to be taken into account. Furthermore, as many of these systems are related to critical infrastructures, attacks against them are likely to increase in the future [2].

This report focuses on the aspects related to the communication networks and the intercommunications between ICS/SCADA, identifying vulnerabilities, risks, threats and safety implications caused by cyber-physical systems controlled by ICS. This report also provides a series of recommendations to mitigate the risks identified.

1.1 Objectives and Scope

ENISA, in 2016, is continuing its work on communication network dependencies in critical infrastructures with a study on network attacks against ICS/SCADA systems.

The key outcome of the study is a list of good practices and guidelines in order to limit, as far as possible, the attack surface of ICS/SCADA systems. The main objective of the study is to provide insight into the communication network dependencies in ICS/SCADA systems, mapping assets critical for security and safety and looking into realistic attack scenarios and threats against the communication networks.

1.2 Methodology

This study was carried out using a seven-step methodology (depicted in Figure 1) which begins with a brainstorming session over the phone with the ENISA ICS Security Stakeholder Group (EICS) and European SCADA and Control Systems Information Exchange (EuroSCSIE) experts groups. Then, it moves on to the initial stage of information gathering, drawing from official sources and experts in the field. Ultimately, the study ends with the development of a report summarising the findings and the recommendations to the target audience.

Figure 1: Methodology used to carry out the study.

1. **Brainstorming call:** The first step was to conduct a brainstorming session with the EICS and EuroSCSIE expert groups, to discuss the structure, objectives and focus of the project.

2. **Identification of experts:** The following step was to identify the experts in the field of ICS/SCADA security. In order to obtain varied and well-balanced results, experts from industrial, academic and governmental sectors were contacted. The main target audience is asset owners and more specifically, operators of electricity, oil, gas, transport, health, water supply, and the manufacturing industry.

3. **Desktop Research:** Initial desktop research of already published documents in order to get as much information as possible about communication dependencies was conducted for developing at a later stage a questionnaire to achieve the project objectives.

4. **Collecting Experts' and Stakeholders' point of view:** During this step, a questionnaire was used internally to guide the interviews with experts. These interviews were carried out during an eight-week period in order to obtain experts' and stakeholders' point of view. Interviews with experts from the field were conducted in order to:

    - Map the critical assets for security and safety.

- Determine the most commonly used protocols and their weaknesses.
- Identify attacks scenarios against assets and most worrying threats.

5. **Analysis:** The fifth step was to analyse all the data obtained, including the results of the interviews, to gather initial conclusions and develop three attack scenarios and mitigation actions as a proof of concept.
6. **Conclusions and recommendations:** The sixth step was to further analyse the gaps from the security perspective and propose guidelines for minimising the success possibility of malicious activities against ICS/SCADA.
7. **Stakeholders validation:** the findings of the study were presented and discussed with the participants in order to further refine the results and recommendations during:
   - ENISA session "Network Attacks against ICS/SCADA" at IMI 2016 – IT meets Industry[1].
   - Open ENISA session at 4SICS[2].
   - EICS and EUROSCSIE members and participants of the study review and comment of the final draft.

1.3 Target audience

This report provides information about the communication networks and the interconnections between them in ICS/SCADA systems, aiming at helping operators-asset owners and manufacturers to better understand them and be prepared to mitigate possible security risks.

The primary target audience is **SCADA operators and asset owners** within the following sectors:

- Electricity
- Oil
- Gas
- Transport
- Health
- Water
- Manufacturing industry
- Pharmaceutical sector

[1] https://www.enisa.europa.eu/events/enisa-session-network-attacks-to-ics-scada-imi-2016-2013-it-meets-industry
[2] https://www.enisa.europa.eu/events/open-enisa-session-4sics

1.4 Structure of this document

The report is structured as follows:

- **Introduction:** Briefly presents the study, listing the objectives that have been set and describing the methodology followed.

- **Key aspects of communication networks in ICS/SCADA Systems:** Study of the state of the art of communication networks and intercommunications in the different domains of ICS/SCADA, detailing the most commonly used architectures and technologies in each one, as well as the critical assets affected and protocols used in ICS/SCADA systems.
- **Interdependencies in ICS/SCADA Systems:** Evaluates the interdependencies that can be found in ICS/SCADA networks and their relationship with telecommunication providers and the Internet.
- **Threat and risk analysis on communication networks in ICS/SCADA Systems:** Presents the security threats, vulnerabilities, incidents and attacks affecting communication networks in ICS/SCADA systems, focusing on those that might derive in cascading effects.
- **Attack scenarios in ICS/SCADA Systems communication networks:** Analysis and development of three use cases including the most worrisome threats and possible mitigation solutions derived from good practices.
- **Constraints and gap analysis:** Presents a gap analysis to determine which areas require further revisions, as well as to detect those constraints and incentives for applying security measures.
- **Security good practices in communication networks for ICS/SCADA Systems:** Having taken into account relevant international standards and good practices, a list of good practices for securing ICS/SCADA systems and their communications is summarized.
- **High-level recommendations for manufacturers, operators and security experts to improve the security and resilience of ICS/SCADA Systems:** Contains a series of recommendations to improve the security level of the communication networks used for intercommunications in ICS/SCADA systems.

2. Key aspects of communication networks in ICS

A major part of Europe's Critical Infrastructures is managed and controlled by ICS/SCADA systems. These systems are evolving and have increased their connectivity capabilities using both private and public communication networks, which in turn results in a larger attack surface, which means that they are exposed to more risks.

As ICS are usually controlling critical and sensitive installations (such as those from utilities or energy sectors), they have become very attractive targets for attackers, due to the potential impact that a successful attack can have, as well as due to cascade effects affecting different areas and even countries. These systems usually interact with the following:

- **PLC** (Programmable Logic Controller): the devices in charge of carrying out the physical interaction with the system components (e.g. actuators).
- **Data Concentrators**: an electronic device that interfaces with the sensors and transmits the obtained data to other system components. This includes process automation controllers and the more power-oriented RTU (Remote Terminal Unit) devices.
- **Historian**: it is a high-capacity system designed to collect and store the logs generated by the readings and operations of the sensors, assets, alarms and other events generated by plant devices, part of the network.
- **HMI** (Human-Machine Interface): a component responsible for the presentation of the data to human operators, usually including a console capable of monitoring and controlling the status of the operations.
- **DCS** (Distributed Control System) **central server**: in charge of the data acquisition and control activities of the processes and operations. It may include monitoring, analytical instrumentation.
- **Communication infrastructure**: can make use of traditional and specific network equipment in order to enable the intercommunication of the different devices of the system.

ICS systems were designed, from a general point of view, to cover a series of characteristics that are needed in order to properly carry out their functions:

- **Availability**: ensures that the systems and information contained within them are available to authorised users. This is especially important for industrial systems and critical infrastructures where access to the data is paramount to maintain proper operations.
- **Fault-tolerance**: ensures that the systems are robust and can continue operating at a reasonable level in the event of a failure.
- **Performance**: ensures that the system is efficient and can carry out its intended tasks timely and correctly.
- **Safety**: systems must be able to detect unsafe conditions and trigger actions to reduce unsafe conditions to safe ones. In most safety-critical operations, human oversight and control of a potentially dangerous process is an essential part of the safety system [3].

Nowadays, there is an inherent need to define additional characteristics to comply with the new needs and requirements:

- **Maintainability**: it is highly recommended for the system to have adequate diagnosis and control functionalities to allow correct maintainability.
- **Openness**: makes use of open standards and technologies in order to increase interoperability between devices and assets from different systems and infrastructures.
- **Security**: guarantees that the systems are protected, at least, against the most common threats that they face (such as unauthorised access or data manipulation), taking into consideration not only Availability, Integrity and Confidentiality security tenets, but also the Safety needs as they are cyber-physical devices.

- **Usability**: the ease-of-use and proper functionality of the systems and related tools and devices.

When designing a network architecture for an ICS/SCADA deployment, one of the main recommendations that should be taken into account is to ensure its segregation from existing corporate or traditional networks, in order to reduce the attack surface.

As this study focuses on the network communication in ICS/SCADA systems located in different areas and sections of an ICS infrastructure, it was necessary to choose a standard to be based upon and better present the findings.

The main options were between ISA95 [4] and ISA99 [5] [6] with each one focusing on different aspects and bringing different benefits. ISA95 focuses on the interconnection between assets and systems, sorting them into layers depending on the communications and activities carried out by each asset/device. On the other hand, ISA99 focuses on sorting these assets/systems into zones depending on their activities/operations, and it does not focus on communications as they are emphasised by ISA95.

As a result, for this study the ISA95 standard was selected, ensuring that the focus remains on the interconnection of these systems.

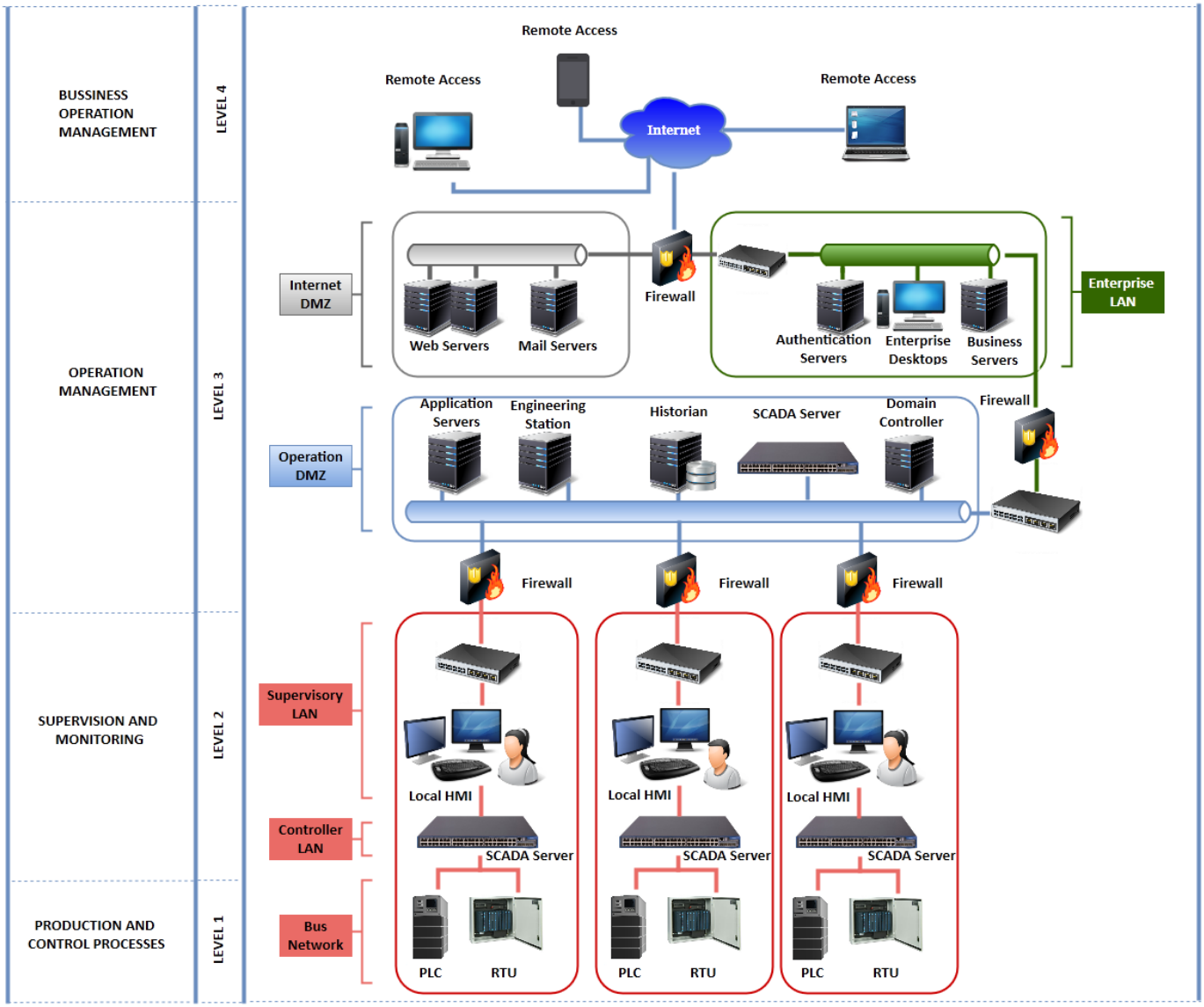
In more detail, the ISA95 standard focuses on the integration of control systems within a company, establishing different levels that range from the basic industrial processes up to the higher management ones, such as accounting systems, in order to fully map the application hierarchy in use within the company [7] [8]. The following sections will provide a brief insight into the different levels, processes and ICS/SCADA architectures in relation to the ISA95 levels, including different technologies that can be used in each one (hardware, software and protocols).

Finally, in order to summarise the information provided, a review of the communication between the levels previously defined will be presented, including both the channels in use and the data types that can be transmitted over them.

2.1 Architectures and technologies

The ISA95 standard separates the processes, activities, systems and devices of an industrial network architecture into four levels (see **Figure 2**): production and control process, supervision and monitoring, operation management and business operation management.

Figure 2: ISA95 levels applied to a SCADA architecture.



A detailed summary of the hardware and software used in the four ISA levels is provided in the Annex – "ISA95 levels overview".

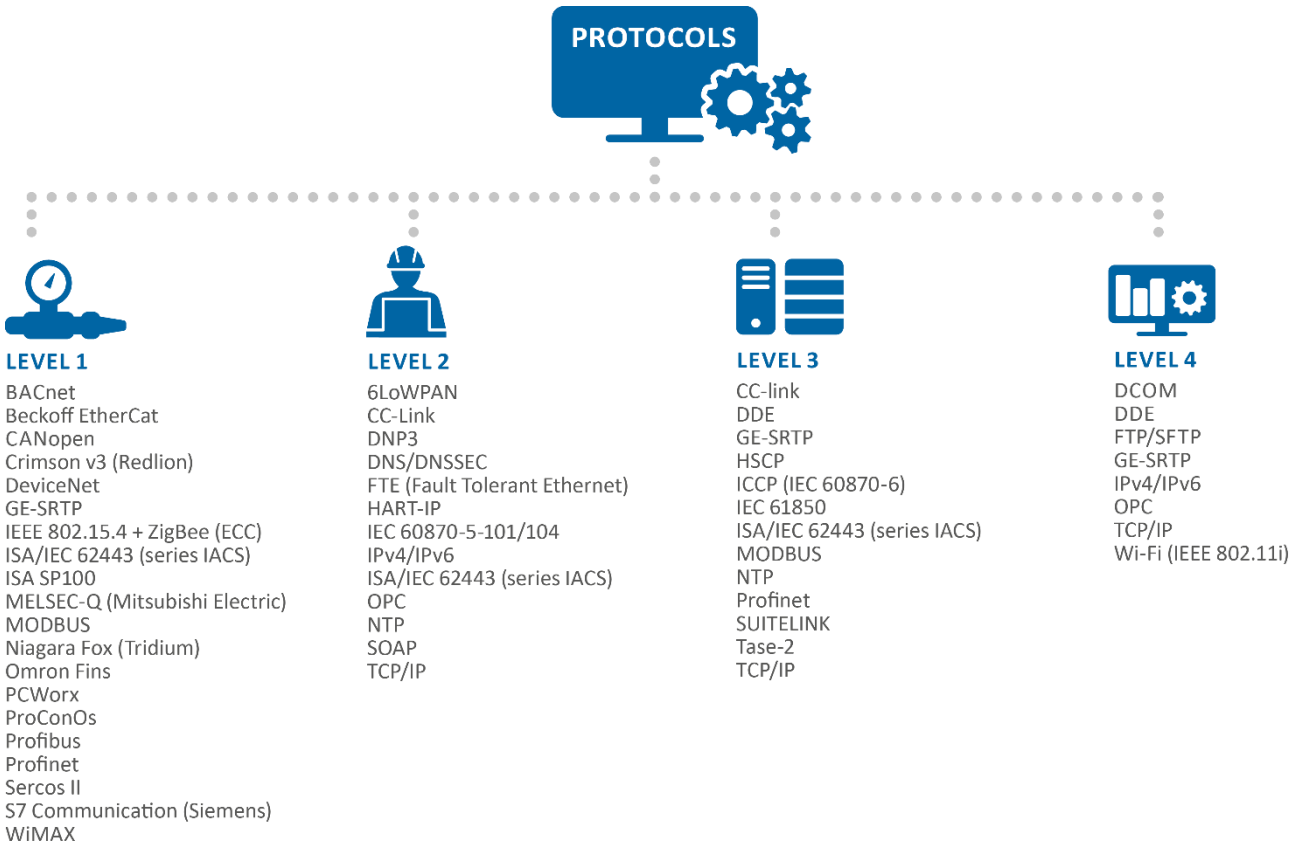
2.1.1 Protocols in use within and between levels

The following protocols are in use in each one of the four ISA levels. In order to properly display them, the following mind-map (see **Figure 3**) has been developed to list some of the most commonly used protocols like:

- **DNP3:** a communication protocol used to interconnect components within process automation systems, mostly in utilities like water and energy.
- **IEC 60870** (including ICCP): provides a set of standards and protocols to cover ICS/SCADA communication needs in power system automation.

- **OPC**: a set of client/server protocols designed for the communication of real-time data between data acquisition devices (e.g. PLCs) and interface devices (e.g. HMIs).
- **MODBUS**: an application-layer communication protocol designed to provide client/server communications between assets connected to different bus and network variants.

Figure 3: Protocols (ISA 95 levels).



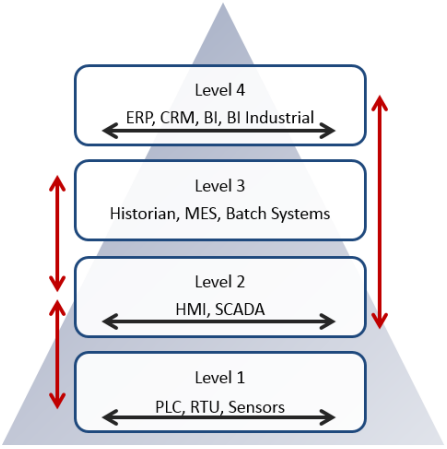
2.1.2 Communications between levels

The intercommunication between the devices, as well as the communications between levels are of high importance and relevance. Two main groups of intercommunications can be defined as:

- **Horizontal communications**: all the data exchanges that occur between devices and systems located within the same level.
- **Vertical Communications**: all the data exchanges that occur between devices and systems that are located in different levels.

This leads to a series of well-defined communication 'channels' [1] (or ways) between levels and within levels (see Figure 4).

Figure 4: Relation of the communication between the different levels of ISA95.



The vertical communications occur between all levels and are:

1. **Between level one and two** (bi-directional): exchange of information between the sensors, or field devices, and the systems in charge of interpreting and processing the readings of these devices. Output is usually numerical, controlling operational functions (e.g. closing valves).
2. **Between level two and three** (bi-directional): information exchange between supervisory and operation management systems; the interpreted information (originated from level one and processed in level 2) is communicated to the higher level systems to register (Data Historian), verify (MES) and transfer to other processes (Batch) if needed.
3. **Between level two and four**: information exchange between operation management systems and the ERP or BI systems, regarding mostly the operational status, progress and evolution as to aid on manufacture planning or resource needs.

The horizontal communications (within the same level) related to SCADA and ICS systems specifically occur in levels one and two:

4. **Within level one**: numerical values are commonly exchanged between field devices as sensors, PLCs, or RTUs, among others. The information is exchanged among devices within the same level, but only the one that acts as the master can command the others.
5. **Within level two**: the interchanged information or actions acquired or sent by SCADA systems are notified to the HMI system for a more understandable visualization on the part of the user. These communications must be realised in real time.
6. **Within level four**: standard IT communications between the CRM and ERP systems (among others) in order to exchange needed information for customer-related, invoice and billing processes. If BI systems are in place, additional interactions may be created to fulfil the needs of the information.

3. Interdependencies in ICS/SCADA Systems

ICS systems can span large geographical areas and be located in multiple remote field sites that can be interconnected to one or several centre locations, which at the same time may also be sharing communication data amongst each other and other operational sites.

This leads to the need to use WAN (Wide Area Network) technologies for the communication exchanges, which is usually covered by using part of the infrastructure provided by a Telecommunication Services Provider company. This results in a scenario in which the external service provider is in charge of protecting the network against the threats that put them at risk. However, some companies use their own network infrastructure (cables, network equipment, architecture), transferring the risks associated with the network to them (as there are no external providers).

According to NIST SP 800-82, SCADA systems are not the only ones to make use of third-party ICT communication infrastructures; SCADA systems and DCS systems are often networked together, such as in the cases of (electric power distribution) electric power control and electric power generation facilities [9].

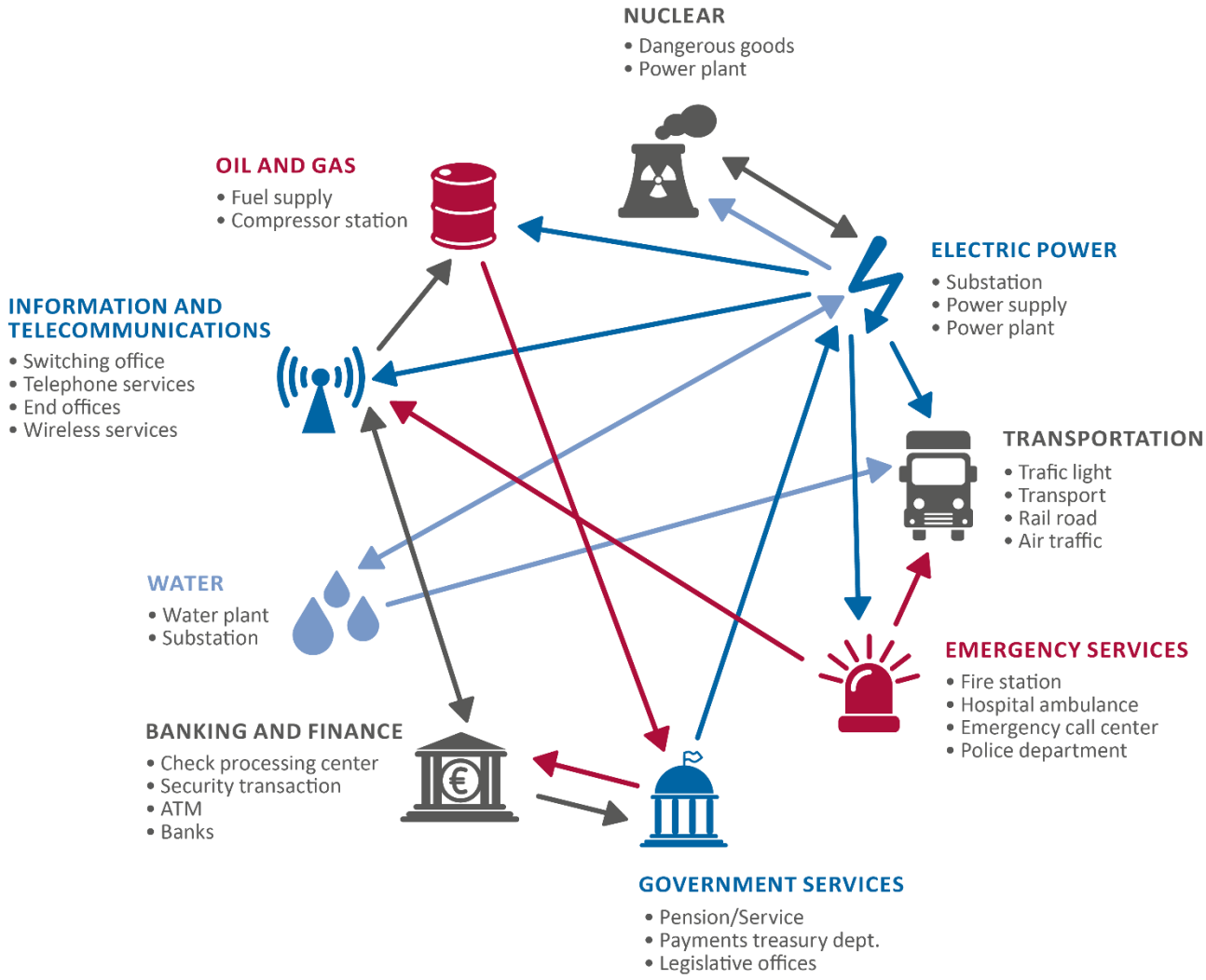
ICS are dependent on communication infrastructures and in many cases these are not under the control of the same organisation. It is important to highlight that the dependencies of ICS on the underlying ICT communication infrastructure are just one example of the multiple interdependencies that can arise when addressing the security of Critical Infrastructures.

There are four distinguishable types of interdependencies [10]:

- **Physical:** Two infrastructures are physically dependent when each requires a physical product from the other (e.g. a physical product from one infrastructure is a physical input for the other).
- **Geographical:** Infrastructures are geographically dependent if a local environmental event can cause a change in their state.
- **Cyber:** When the state of an infrastructure is conditioned upon information broadcast through the information or communications infrastructure (e.g. production of electricity is conditioned, among other things, on information transmitted about the consumers' consumption of electricity).
- **Logical:** Two infrastructures are logically dependent when the state of one infrastructure depends on the state of the other through some mechanism that is not a physical, geographical, or a computer linked (e.g. this type of dependency is created through decision-making processes made by the human factor).

Figure 5 provides a depiction of some of the most relevant interdependencies among the main critical infrastructures considered. These interdependencies are, in most cases bidirectional. Energy is one of the most important infrastructures, given that it establishes dependencies with many other infrastructures [10] [11] [12].

Figure 5: Concept of the interdependencies of each Critical Infrastructure.



It is very important for inter-operators of critical infrastructures among Member States to become aware and take into consideration the risks they are exposed to by the existence of interdependencies in ICS/SCADA system communication networks.

This is needed in order to prevent the possibility of an incident or event evolving and leading to a cascading effect that could ultimately lead to catastrophic consequences in one or more infrastructures , potentially affecting the population (e.g. blackouts affecting large areas, distribution issues, etc.).

3.1 Dependencies between operator of CIs & telco providers

In industrial environments, it is common for asset owners to rely on telecommunication services providers for their connectivity, either to public networks or private networks. As a result, each operator has additional responsibilities to secure these communications, as they ensure their successful operation.

A trend has already appeared with regard to communication services and their relation with third-party communication service providers. It is aimed at reducing costs, and it is not dependent on only one provider. As far as security is concerned, there are some points to consider regarding operators and Communication Service Providers (CSPs) / Internet Service Providers (ISPs). The operators who hire these types of services

become dependent on them in order to carry out their work functions. For this reason, it is recommended not to depend on a single CSP/ISP, and to use several ones instead. The following recommendations to mitigate the possible risk posed to the communications should also be taken into consideration:

- **Risk Management diversification**: having more than one CSP/ISP is a means to minimize the potential risks posed to the communications in the event of a failure or attack that affects the main CSP/ISP that provides the infrastructure intercommunications.

- **Technology variety**: by using devices and systems that make use of different technologies, the risk of a total failure is mitigated, as the vulnerabilities that could be exploited in one of them do not apply to the others. In case of an attack it would only affect a part of the devices.

- **Geographical location**: another advantage of having several CPSs/ISPs is that you can choose the most expert service depending on the technologies and the local features required.

- **Traffic isolation**: it is a mechanism to protect the information according to data needs and to the sensitivity.

However, there are also several disadvantages of using multiple CSPs/ISPs that must be taken also into consideration.

- **Security Management** (Lower Integrity): such as the encryption and redundancy of the customer data, or the locations where it is stored (third-party information systems).

- **Operational Cost**: the use of several CSPs/ISPs is significantly more expensive that using just one.

- **Information Access** (Confidentiality): the likelihood of suffering a confidential information leakage increases exponentially with each additional CSP/ISP.

Therefore, a good diversification of the communications with an implementation of appropriate security measures is in order. This would help to mitigate the possible disadvantages previously explained to ensure proper functioning of the communications between operators.

These communications must comply with a set of specific characteristics and interdependencies in order to respond to the needs of real-time data exchange. Another option would be to operate the communications at certain intervals, where the data necessary for the processes are obtained and executed, leading to a discontinuous communication scenario. In addition, they must be resilient in order to resist hostile environments; for example, situations or environments where there is a large amount of electromagnetic noise or adverse conditions that could affect data transmission. Some points to be taken into consideration in order for them to be resilient are the following:

- **Use of secure protocols** and associated specifications (improved versions of traditional protocols such as DNP3 secure or OPC UA).
- Use of **Multiprotocol Label Switching** (MPLS); it provides high-performance communications as it uses short labels to direct data from one node to another instead of the traditional long network addresses. This results in shorter and simplified network routing tables, and is compatible with most common communication technologies including DLS, ATM and Frame Relay. Due to these features, it can be highly efficient on engineering and SCADA-based networks.

- Incorporation of **specific technologies** that provide security for insecure protocols (e.g. data diodes, Protocols Whitelisting, VPN) and encryption and authentication protocols.
- Deployment of redundant architectures for communication servers.

3.2 Inter-Member State communication infrastructures

The Inter-Member State infrastructures that support the communication networks are another important factor that has to be taken into account. ICS are no longer confined to a single country and can span over several Member States.

These systems have intercommunications between Member States, allowing the provision of services to neighbouring countries. This also exposes them to the risk of an incident on one country affecting another one, potentially leading to a cascade effect which could affect even the general population.

As an example of the interdependencies and the possible cascading effects that can result in by an attack scenario, Figure 6 shows the interdependencies of the oil and gas pipelines within Europe.

Figure 6: Europe oil and gas pipelines map (*source*: [13]).

More importantly, while there is a large number of interdependencies among organisations, both from the same country and from different ones, the risk posed by cascade effects is not usually considered. While co-operation is usually done de-facto in some aspects, the possibility that one incident in one organisation may directly affect another in a critical way is not often considered.

Recently, a sophisticated attack against energy control centres within Ukraine left over 230,000 people without access to electricity for a period of six hours and over thirty substation and two power supply centres

where taken offline by the attackers. Due to the fact that the organization affected had a high level of security and logging systems in place (according to SANS [2]), investigators were able to determine the process that has occurred.

The reason why the recovery took six hours was due to the fact that the firmware of multiple SCADA and control systems was replaced by the attackers, disabling remote control, and requiring operators to manually control each substation. Regarding the control centres, the attackers compromised and disabled backup uninterruptible power supply (UPS) devices to ensure that the operators were also unable to be aware of what was happening on the substations once the main power was out. All of this was explained on a detailed step-by-step reconstruction in [2] and [14].

In conclusion, taking advantage of an entry point from a control centre, one substation after another was compromised, into an attack that could have potentially led to a cascade effect affecting other countries.

3.3 The role of the Internet in ICS/SCADA Systems

Nowadays, most industrial companies design their own control systems to manage their operations using interconnected SCADA systems and devices. Since these systems are no longer isolated and have become interconnected with many others, e.g. vendors, both locally and remotely, it has become necessary to establish a set of security measures. Firstly, it is imperative to develop a network segmentation model to allow the separation of the different zones depending on their purpose and criticality, and secondly, establish a set of security measures to protect the interconnection between each zone, with a special emphasis on connections made to any public networks or remote connections (e.g. VPN). While the first point (network segmentation) is something that is done in most cases, as observed from the feedback obtained from the contributors of this study, the second factor, according to the feedback from the interviews, is somewhat lacking and needs a further push.

In general, these infrastructures have different layers set up in their technical automation systems. The top layer operates the general systems (business operation management), a lower layer covers the operations management (including WLAN and Internet connections), a deeper layer covers the supervision and monitoring of the systems (covering as well the remote control or remote communications in place) and finally the production and control layer covers the communications between the assets themselves (such as between sensors and actuators). The remote connection needs depend on specific scenario, as well as on the severity and sensitivity of the data to be transferred.

A SCADA station is usually connected to local controller stations through a hardwired network or to remote controller stations through a communication network that may be connected through the Internet, a public switched telephone network (PSTN), a LAN, a wireless network or a VPN, all of which introduce factors that contribute to the escalation of risks in these control systems.

Therefore, the asset owners and operators from the companies within the sectors in scope of this study were in charge of every aspect of their own systems and from a security point of view their main concern was initially the physical protection of their assets and facilities.

For this reason, in the past communications used to be limited and not exposed to external shared networks, even less to the Internet, thus avoiding threats and the risk that they entail. However, the widespread use of the Internet gives rise to new security threats and reliability problems in the system, such as the disruption of services, information theft or data alteration, among others, which might be intercepted through

communication channels. Later, in chapter 4 we will analyse the threats and risks to communication networks [12].

One way of protecting the communication channels is to add an encryption layer (SSL/TLS) over the TCP/IP standard, the use of hard cryptographic primitives and hash functions on the authentication mechanisms, and the use of Intrusion Detection/Prevention Systems (IDS/IPS), firewalls and proxies. Furthermore, the use of VPNs might be considered a cost-effective, high-speed communication solution between the SCADA systems [15]. It is also necessary to configure authentication mechanisms to verify the authorised access to resources and services in the system through this communication channel, as well as to create privileged and standard accounts on these systems and to ensure that default passwords are changed in all cases. These solutions, while improving security, can also potentially introduce latency, which could be an issue for real-time operations, as latency would put them at risk.

3.3.1 Internet intercommunication architectures

The Internet has become the network of networks, a massive grid that connects the whole world together; communications from one side of the world to the other take less than a second. To maintain such large infrastructures, it has become necessary to adapt the traditional infrastructures in order to integrate the connections to the Internet, use wireless connections (when needed), and ensure interoperability with other systems and networks from other companies or infrastructures.

The architecture of the Internet follows a distributed and redundant paradigm. There are no established hard point-to-point lines; connections are established using the most efficient path, and so connections to the same destination can make use of different intermediate devices and communication lines each time, or even within the same communication.

There is a wide range of common and proprietary protocols that can be used on these networks. However, not all of them support security measures by default, and as such it becomes necessary to use additional compensating measures in order to protect them, especially when communicating over public networks such as the Internet.

Communications over the Internet are possible using both wired and wireless networks, and the protocol support on them does not vary a lot, as they are simply different ways of transmitting the communications. However, there is a big difference in the exposure that wireless networks inherently suffer; while a wired communication requires an attacker, or third-party, to directly connect via cable to the network and intercept communications, wireless communications can be intercepted simply by being in the range of the network wireless emitter.

Focusing on Wireless communications, it is undeniable that they can be of great use for automation and control processes communications (see references [12], [16], [17] and [18]), they provide in this aspect:

- Same control options as a wired infrastructure but with a low installation and maintenance cost.
- Mobility and connectivity with other control components independently of the environmental conditions or restrictions.

The vast majority of wireless technologies, such as Bluetooth, Wi-Fi, Mobile technology, Satellite, GPS, or Wireless Sensor Networks, among others, have already been proposed to be included in industrial control networks. Furthermore, wireless communications have recently been standardised to ensure the secure control and coexistence with other ICT systems and the reliability of the communications. Examples of used wireless standards are the following: ZigBee PRO, Wireless HART,ISA 100.11a, IEEE 802.11, WiMAX [19], NFC [20].

3.3.2 Security groups and tools for SCADA systems

The Internet has become a highly helpful communication channel for industrial sectors and organizations alike. This has given rise to multiple projects and initiatives focusing on ICS/SCADA systems, as well as the appearance of multiple open communities and information exchange groups, such as ScadaBR [21], IGSS FREE50 by Schneider Electric [22], IndigoSCADA [23], Scadastrangelove.org [24] and TeslaMultiSCADA [25].

Figure 7 shows an overview of the ICS/SCADA systems that are connected to the Internet:

Figure 7: ICS/SCADA systems connected to the Internet (EU overview) [26]

There are multiple related projects being carried out, such as Redpoint [27] and SCADAPASS [28] (both hosted in the open-source development site, *Github.com*), as well as SCADA-specific tools (*SCADA Hackers' Toolset* [29]). These projects and initiatives focus mainly on the security point of view of ICS/SCADA systems, and are providing multiple solutions that will be very helpful in identifying, testing and even preventing attacks and security incidents in the future.

Below there is a short list of tools and platforms that can be used to evaluate the security of SCADA systems:

- **SHODAN.IO search engine**: it is a free, widely available service capable of searching computer systems connected to the internet, with a special focus on smart devices comprising Internet of Things [30]. It is capable of detecting and listing SCADA devices that are directly connected to the Internet with no security whatsoever.

- **Censys.io**: is a public search engine that enables researchers to quickly ask questions about the hosts and networks that compose the Internet [26]. Figure 7 above has obtained data provided by this search Engine.

- **Scanner - BACnet.nse** (nmap extension): it is designed to discover and enumerate BACNet Devices and collect information about them [31].

- **IoTivity**: a project that aims to establish a common framework of services that will manage the interconnection of the billions of Internet of Things (IoT) devices that will come online during the

next decade [32]. It will also provide multiple standard specifications and implementation references.

- **Threat Assessment framework for Critical Infrastrucutres proTection (TACIT)**: a simulation environment that allows the design and evaluation of SCADA networks, covering a wide range of devices and assets from multiple manufacturers [33]. It provides a testing environment capable of testing any designed SCADA network in order to evaluate the behaviour of an infection or attack.

- **Civil Infrastructure Platform (CIP)**: an open-source collaborative project focused on establishing a base layer of industrial grade software; this would allow the use of any implementation of software "building blocks" when developing new infrastructure projects [34].

4. Threat and risk analysis on communication networks in ICS/SCADA Systems

The main focus of this chapter is to determine and list the main security threats, risk factors and attack scenarios that affect ICS/SCADA systems, as well as the different level of importance and criticality that the interviewed experts consider for each threat, risk and attack scenario.

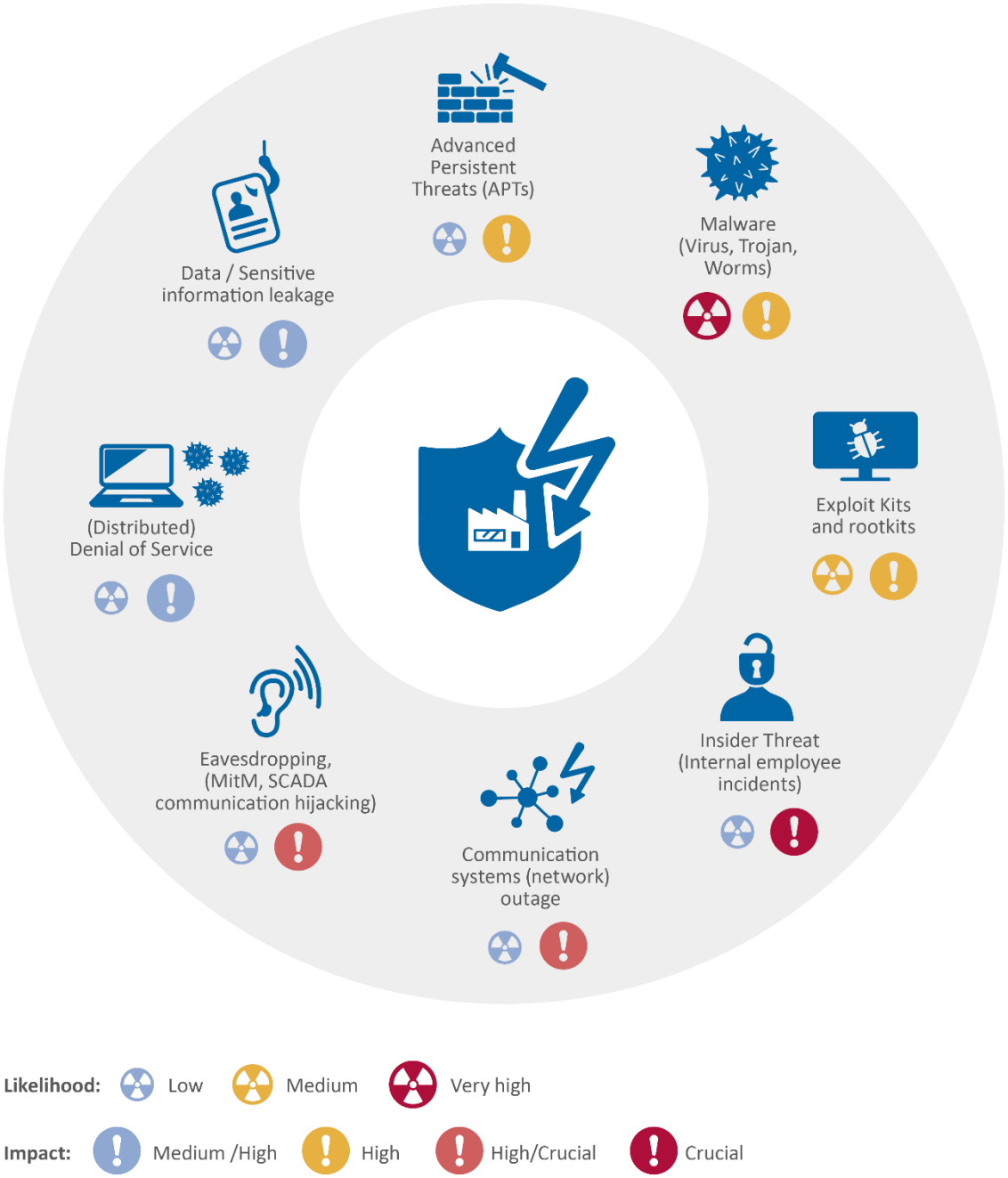
4.1 Threat analysis

The number of cyber incidents targeting ICS/SCADA systems has increased dramatically in recent years. This is also due to their increased intercommunication and their exposure to private and public networks. The number of ICS vulnerabilities increased tremendously in 2015. According to Symantec in 2015, there were at least **135 public vulnerabilities** reported, a significant increase considering that in 2014 only 35 ICS-related vulnerabilities were disclosed [35]. Furthermore, a study conducted in 2015 by Kaspersky Lab [36] showed that the most vulnerable ICS components were HMI, electric devices and SCADA systems. More seriously, not all vulnerabilities have been addressed; while 85% of them have been fixed via patches or new firmware versions, there are still 15% partially fixed or without a fix, although some of them being of a critical severity.

The following table, shows the most common threats and the level of importance indicated by the experts. The threats have been organised according to the frequency with which they occur. In some cases the level of importance depends on the type of asset affected and the impact. Most of the experts agree that one of the most affected asset is HMI.

The likelihood value range (*Low*, *Medium*, *High* and *Very High*) represent the probability of the attack ever happening on an infrastructure. These values were obtained as an average of the feedback provided by the interviewees regarding this factor. For the importance values (*Low*, *Medium*, *High* and *Crucial*), the same process was followed regarding threats' impact. The results shown below are a conclusion drawn from the interviewees' feedback.

Table 1: Threats affecting ICS/SCADA systems



4.2 Common Vulnerabilities

The next step is to enumerate vulnerabilities, weaknesses that ICS/SCADA systems may have, based on the knowledge provided by the experts consulted.

The following table shows a list of vulnerabilities with their respective descriptions; these are general vulnerabilities that communications of ICS/SCADA systems have to address (descriptions based [37] [38] [39] [40]).

Table 2: Vulnerabilities

VULNERABILITIES	DESCRIPTION
Non-existent monitoring process	Without active network monitoring, it is very difficult to detect suspicious activity, identify potential threats, and quickly react to cyber-attacks. The use of Intrusion Detection Systems (IDS) is not as common as in common IT networks. Furthermore, even if they are in-place they may not be able to fully understand ICS protocols. This can be partially addressed by implementing anomaly detection systems. Firewalls and antivirus are more common, but it is not a universal solution and does not cover all the risks.
Deficient traffic content understanding	Managers need to know what type of traffic is going through their networks in order to be able to make informed decisions on how to respond to potential threats and on which kinds of traffic to allow and which to filter. This also helps to establish proper segregation and network segmentation.
Deficient traffic content understanding	Managers need to know what type of traffic is going through their networks in order to be able to make informed decisions on how to respond to potential threats and on which kinds of traffic to allow and which to filter. This also helps to establish proper segregation and network segmentation.
Staff inexperienced in cyber-security related topics	SCADA system staff and operators are familiar with keeping control systems running. The normal goals of reliability and availability can initially feel in conflict with security efforts. With a bent for engineering and technical solutions to problems, the important role of developing security policies can be a foreign concept to typical SCADA staff. Furthermore, SCADA staff may not be receptive to IT staff recommendations.
Operating System Vulnerabilities	The whole host of normal IT operating system vulnerabilities are present in SCADA systems. The difference from an IT system is that patching may be performed less rigorously. It is usual for a SCADA system operator to have a running system that is expected to perform without interruptions.
Slow / lack of updates	Maintaining ICS/SCADA firmware and software up-to-date is not easy, and it can be very complex for critical infrastructure systems, as an update error could cause severe issues on the whole system [41] [42]. Cyber fragility results from applying a change to the system without having tested it beforehand and having foreseen its effects.
Remote Processor operations	Certain classes of remote processors have known security vulnerabilities. In this case the difficulty is two-fold: First the computation power and memory resources of the processors are modest and not suitable for security upgrades. Second, once they are installed they typically stay in place for ten years or more. The result is vulnerable equipment that stays vulnerable for a long time.
SCADA Software features	SCADA applications and software usually provides basic and modest security features, however these are not always enabled by default, and could act as additional weaknesses if operators are unaware of the need of enabling these features.
Inappropriate applications installed on critical SCADA host computers	Because very few security measures are used in SCADA host computers; this leads to an operator or administrator inadvertently installing an inappropriate application on a critical system network device.
Lack of knowledge regarding the devices	Since most SCADA systems have been developed gradually over time, it's not uncommon to see technology that's a couple of years old working alongside an industrial network environment. Knowledge transfer regarding functioning and maintenance of ageing devices should be ensured.

Authentication weaknesses	Authentication solutions are designed to keep unauthorized people away from accessing the SCADA systems. However, this can easily be defeated if the solution is not properly implemented (e.g. allowing weak passwords, hard-wired passwords, user credential sharing, no user logging…), or in the case of older devices, which make use of weaker, more primitive authentication methods. In some cases moving to two-factor authentication is limited by work conditions that may impede iris scans or fingerprint scans because of dirty hands or the wearing of safety goggles. Confidentiality and authentication is often compromised by the use of clear text transmissions. This weakness **eliminates authentication and accountability validity**.
Unauthenticated PLC / RTU network connections	Older SCADA systems lack basic security features, so it is imperative for organizations that own such systems to insist on vendors to provide security measures in the form of product patches and upgrades which can protect the system from unauthenticated PLC/RTU network connections.
Remote access supervision	Because of economics for staffing control centres around the clock, it is not uncommon for SCADA systems to be configured with remote access. This can include dial-up access or VPN access over the Internet. These scenarios should be controlled and monitored, and should include, at least, the same security measures as internal connections.
Interconnection management	The more connections, the more exposure a SCADA system has. Economic and enterprise pressures often result in the existence of internal connections between the SCADA network and the business network in order to allow remote access, control and/or maintenance.
Wireless connections	SCADA systems often use microwave, data radios and cellular packet services for communications. Depending on the implementation, these forms of communication can be vulnerable to certain types of attacks.
Available public information	In the past it was not unusual for SCADA system owners to publish information on the design of their systems, as security was not a top concern and most devices where not interconnected, required physical access. It is also fairly common for consultants/contractors to advertise past experience including information regarding the systems they have worked on. Both these scenarios can result in the exposure of system vulnerabilities which is more serious as these systems have now become interconnected.
The wrong belief that SCADA systems have the benefit of security through obscurity	The use of closed-source proprietary protocols does not provide security, and it can be counterproductive. Security by obscurity is not a good practice, and usually gives users a false sense of security, while in fact they are at greater risk.
The wrong belief that SCADA systems are isolated	Just because a SCADA network is not connected to the internet does not make it secure. Physical access is still possible, and regardless of the network size, all connection points should be always controlled and monitored. For maintenance and support reasons devices belonging to segmented networks are sometimes exposed to Internet through VPNs or remote access connections. These connections should be controlled, and be enabled on-demand only when required.
Physical security	SCADA systems are usually distributed over large distances with multiple unstaffed locations. The physical protection of SCADA devices becomes important in these cases. But, as pin tumbler locks, master keys and cylinder locks all have reported weaknesses it is important to be realistic about the level of protection they provide and take it into account when protecting physical locations.

4.3 Sample attack scenarios

The previously listed threats and vulnerabilities could be used by attackers and could cause different levels of damage and cascade effects in the infrastructures. The attack scenarios and the level of importance of each attack have been gathered from the information provided by experts, who contributed to the study (Table 3).

As an important note, the attacks take place in the whole process. The impact that attacks may have on specific part of the whole process has been analysed.

The importance level value provided for each sample attack scenario ranges from *Low*, *Medium* and *High* to *Crucial* representing the negative impact level that these attack scenarios could have on a real-life incident, as provided by the interviewed experts.

Table 3: Sample Attack Scenarios

SAMPLE ATTACK SCENARIOS	IMPORTANCE LEVEL
1. Against the administration systems of SCADA	**Crucial**
2. Against actuators	**High** / **Crucial**
3. Against the network link between sensors/actuators and HMI or controller	**High**
4. Against sensors	**Medium** / **Crucial**
5. Against the information transiting the network	**Medium** / **Crucial**
6. Compromised ICT components as backdoors	**Medium** / **Crucial**
7. Exploit Protocol vulnerabilities	**Medium** / **High**
8. Against Control Data Historians, Local HMIs or controllers	**Medium**

Sample Attack scenario details

For these scenarios, additional feedback was received which is relevant for this study. The details of each one are listed in the following points:

1. **Against the administration systems of SCADA**

   Consider a scenario where a centralized SCADA system or management system (such as operator centres or control stations) is attacked. This can be achieved via staged attacks on these systems, which can include one or several of the following related attacks: *Exploits against the control system/installed software/operating system*, *Trojans*, *Malware* and *Spyware*.

   - **Details**: If an attacker gains full control over the SCADA systems or communication networks, he could potentially compromise the whole chain, hindering greatly the recovery process.
   - **Impact**: The compromise, manipulation or interruption of the SCADA systems could affect many people, cause environmental issues, electrical/water outages, and even extend to other systems, affecting their communications or even disabling them (cascade effects).
   - **Likelihood**: This type of attack is not very likely, as usually other security measures are already in place.

2. Against actuators modifying or sabotaging their normal settings

Manipulation of the actuators' configuration or parameters in order to impede their standard operation, or by sabotaging their normal operation settings.

- **Details**: The attacker modifies the actuators in order to make them use wrong configuration, thresholds or data, affecting the production process and interfering with the reporting process of the SCADA systems. Therefore, the risk posed is high as the SCADA control systems will send the right commands but the actuators will react as expected but according to their modified configuration.
- **Impact**: The impact level ranges depending on the actuators affected, it could simply affect or stop production processes or, in a worst-case scenario, cause the loss of equipment, installations, and even loss of lives.
- **Likelihood:** The probability of this type of attack happening is low as other systems in the network need to be compromised first, and there are many different models of actuators using different formats, protocols and internal software.

3. Against network link between sensors/actuators and HMI or controller

Unauthorized eavesdropping of the data transferred between sensors (or actuators) and the HMI in order to obtain sensitive and operational information. This includes data such as ID, address, action to carry out, value, and timestamp.

- **Details**: Eavesdropping is another feared threat, as it allows an attacker to extract sensitive and operational information that can be used for multiple malicious activities, including its use on later attacks against systems or the SCADA network devices themselves. In APT attacks, eavesdropping and information gathering is one of the first stages carried out in order to identify weak spots and potential entry/attack points.
- **Impact**: Usually the main effect is the leakage of data; depending on the environment the severity can be lower or greater, but it is also a sign of a possible larger attack in progress.
- **Likelihood:** There are no known cases of an attack affecting the links between the sensors and other SCADA devices.

4. Against sensors modifying their threshold values and settings

Manipulation of the thresholds established on the sensors, allowing for higher/lower values to be accepted when they should not, posing a severe threat to critical systems.

- **Details**: The attacker modifies the configuration of the sensors, changing the threshold values to allow readings that should be out of range, and which can put the systems and installation in danger. As larger installations usually have multiple and redundant sensors, the attacker would have to compromise multiple sensors in order for the attack to be

efficient; if only one was compromised, the readings would be compensated with the rest of the sensors.

- **Impact**: By allowing the sensors to report and accept incorrect values, the whole installation and SCADA systems are put at risk; a voltage sensor that malfunctions may allow a power spike to go through, or not report it, physically damaging the systems.
- **Likelihood:** There are no known cases of an attack affecting the configured values and thresholds of sensors and actuators. This kind of attack is complex and could easily be detected if there were redundant/secondary sensors controlling these values.

5. Against the information transiting the network

By blocking or modifying the information transiting the network, an attacker can hope to impede the normal operation of the system and eventually to compromise it, if critical systems are isolated (e.g. temperature sensors).

- **Details**: The manipulation, or blockage, of the information that usually travels over a SCADA network can cause alerts or mask legitimate commands being sent by attackers. Also by manipulating the contents of the communications, the SCADA control systems would not be aware that the other systems are acting on wrong instructions.
- **Impact**: This attack can have a direct impact on the production, as it can impede or completely stop it depending on the systems affected. This attack is difficult to be detected if there is a lack of security devices in the network, as the control systems send the correct instructions, but the end devices either receive it manipulated or they do not receive it at all.
- **Likelihood:** This attack encompasses a set of common variants that can negatively affect the network, and which are reasonably likely to happen. The probability is set at medium as these attacks can not only be intentional, but also accidental if wrong configurations are set on internal network devices.

6. Compromised ICT components as backdoors

This could act as an entry or staging point for other attacks, including APTs, information theft/leakage or even terrorist attacks.

- **Details**: By compromising a system/software with a backdoor, an attacker is able to install an entry point (or backdoor) into the system, allowing its remote control, or to act as a staging point for further attacks.
- **Impact**: On itself, the backdoor only compromises the system creating an entry point for the attacker. However, this is never used alone; it is always part of a larger attack being carried out or espionage process.

- **Likelihood:** The probability of this type of attack happening is high, but there are mechanisms related to the security of supply chain that can be set in place to detect and prevent it.

7. Exploit Protocol vulnerabilities

This type of attack could provide a means for an attacker to develop other attacks against SCADA systems or communications (*IP, Ethernet and Modbus*).

- **Details**: Similarly to backdoors, exploits are used to gain privileged, unauthorized access to a system, which can lead to the installation of other malicious content or backdoors. It is used as part of an attack, regardless of if the target is a single system/device or a whole network. Even more, the exploits themselves are complex to be detected, and it is rather easier to detect the actions carried out after the exploit has been successful.

  One of the most common exploit variants takes advantage of improperly managed string or integer entry functions in order to carry out unexpected or unauthorised functions. Other common attacks such as DNS Forgery can also affect SCADA devices. Most importantly, there are already specific attacks for SCADA protocols, such as:

  - *DNP3*: no security measures implemented by default, therefore instructions received are not validated. If an attacker sends a command, it will be carried out by the system (e.g. the code 0x0D causes a power-cycle reset, or the x013 forces the load of new configuration parameters) [43].
  - *ICCP (part of the IEC 60870 standard)*: the Livedata ICCP default server implementation suffers from a widely known buffer overflow that could result in the execution of arbitrary code [43].
  - *Modbus*: as no encryption or validation is done, instructions received are processed without question (e.g. the code 0x05 can enable/disable remote outputs, or the 0x08 which enables diagnostics, that alongside code 0x01 can restart devices and reset event counters) [43].
  - *OPC*: the IO interface write function that it provides can be used to write any value virtually to any memory address, which could potentially allow the execution of arbitrary code on the system.

- **Impact**: If successful, the exploit may create an entry point to a system, in some cases with elevated privileges or the system is likely to crash or become unstable. This attack is usually used as part of a larger attack, which could be a simple data theft attack or a complex APT one. On the other hand, protocol and software vulnerabilities are published in ICS-CERTs advisories and they are in the interest of suppliers and operators.

- **Likelihood:** The vulnerabilities affecting these protocols are known and public, and for some of them there are already exploits published. Therefore, if not properly mitigated, there is a high chance of this attack happening, although it requires the attacker to directly connect, or compromise a device in the network.

8. Against control Data Historians, Local HMIs or controllers

To compromise these assets in order to manipulate, control, or put at risk SCADA systems. It includes cases such as obtaining what is stored in the memory and control functionality of these systems.

- **Details**: It does not affect the production process directly, but the data leaked by this server could be used at a later stage for a more sophisticated attack. The modification of the HMI configuration and/or parameters, as their main functionality has to do with the provision of information regarding the process of the systems it controls.

  If this information is modified, or inaccurate, it could cause a chain effect to the whole system, making the operators believe the system is working fine when it does not, or that it requires extreme adjustments when in fact it is running fine. It could potentially cause the whole process to crash.

- **Impact**: Malfunction of the production process, but depending on the process can damage either the environment or human health. This manipulation would render the HMI device useless, as it would be unable to carry out its main function.

- **Likelihood:** There are few known cases of attacks against these systems, and their value may vary from one system to another, therefore having a low probability.

5. Attacks scenarios in ICS/SCADA Systems communication networks

During the interviews with experts and relevant stakeholders, multiple attack scenarios regarding ICS/SCADA systems and networks were described and discussed. From the scenarios discussed during the interviews, including those presented in point 4.3, several were identified as being of particular concern. Three scenarios have been further developed in this chapter, as a proof of concept to better understand their risk, their impact and possible countermeasures to reduce and mitigate these threats.

The selected scenarios are:

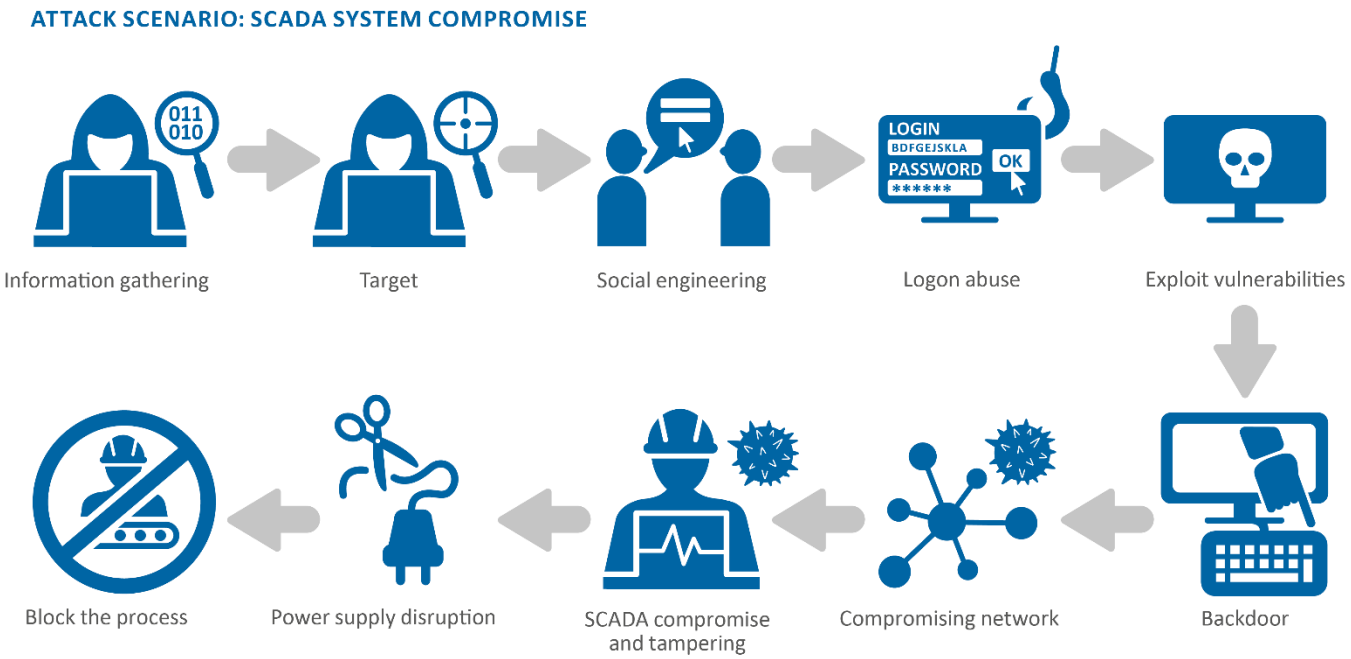
- SCADA system compromise.
- Insider threat/data manipulation.
- Malware infection

The following sections detail each one of these scenarios, including likelihood, impact, stakeholders involved, cascade effect risk, gap and technical details. These values were defined during the interviews with the stakeholders, and are scaled **compared to other threats and risks** that have been considered and/or analysed in this study.

5.1 Attack scenario 1: SCADA system compromise

This attack covers an infection designed to take control of one or multiple SCADA assets within a network in order to be able to manipulate or crash them at will (e.g. modifying values, changing functions or denying access).

This can cause undesired effects including asset malfunction, asset corruption or asset physical damage; as well as the risk of the impact expanding to other assets and systems within the infrastructure (or other infrastructures), potentially causing a cascade effect (e.g. blackouts).



SCADA SYSTEM COMPROMISE

IMPACT	LIKELIHOOD
Critical: The compromise of SCADA systems can cause them to malfunction or cease operating, directly affecting the related production processes and potentially causing physical or infrastructure damage.	**Low-Medium**: SCADA systems and assets are becoming more interconnected and exposed to the Internet and other networks. This adds a new attack layer that did not apply in the past to these devices, increasing the number of potential attacks against them.
EASE OF DETECTION	**CASCADE EFFECT RISK**
Medium: The changes made on SCADA systems can be detected by security control systems and sensors, as long as those are not compromised as well. Having redundant or secondary control systems would allow better detection.	**Low**: The compromise of these systems can result in their manipulation, compromise or interruption, which can directly affect other interconnected systems (other companies, sectors, etc.), and even translate to direct effects on the population (e.g. blackouts, floods, etc.).

ASSETS AFFECTED	STAKEHOLDERS
SCADA systems, HMI (Human-Machine Interfaces), Centralised Control System	CISOs and security officers SCADA operators Operators and technical staff

ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)

1. The attacker gathers information on the target organization.
2. A relevant control centre is targeted.
3. Information is gathered regarding the operators and staff of the control centre, a social-engineering campaign is launched against the staff of that control centre to gain an entry point into the corporate network.
4. An internal users' credentials are stolen and used to gain access to a computer inside the corporate network; a staging area has been stablished.
5. The attacker carries out further information gathering to identify vulnerable systems.
6. A vulnerable computer is found and an exploit is launched against it to gain access.
7. A backdoor is installed in order to maintain access to that system.
8. If that system does not have access to the SCADA network (direct or remote) more systems keep being compromised.
9. Once a system with access to the SCADA network is found, this attack phase stops.
10. The attacker uses the compromised system to attack the SCADA systems.
11. The SCADA systems are "updated" with modified firmware that grants exclusive access to the attacker and restricts other remote accesses.
12. The SCADA assets are reconfigured to cause the whole system to fail.
13. The corporate local power supply and backup supply systems are compromised to disable them.
14. Finally, the SCADA system fails, the operations stop and the control centre is unable to act, as their corporate systems are disabled and erased. Furthermore, the local power and backup systems are compromised, stopping the operators from being aware of what is going on the operation facilities.

RECOVERY TIME / EFFORT	CHALLENGES AND GAPS
Medium: Depends on the area where the assets are compromised and the number of assets that are infected. It can range from a few hours and **up to several days** if critical systems are compromised (e.g. nuclear sectors).	Need for restricting physical access to SCADA networks components in order to reduce the risk of unauthorized access to them. The use of anomalous behaviour detection systems and active system monitoring and logging are good protection measures for this attack.

COUNTERMEASURES

- ✓ Ensure that SCADA assets are not directly connected to the Internet.
- ✓ Ensure that patches have been approved and deployed to SCADA systems.
- ✓ Anomaly detection systems to identify unexpected and/or unauthorised behaviors.
- ✓ Elaborate a role and permission matrix (RACI) and include intelligence (control location and activity hours).

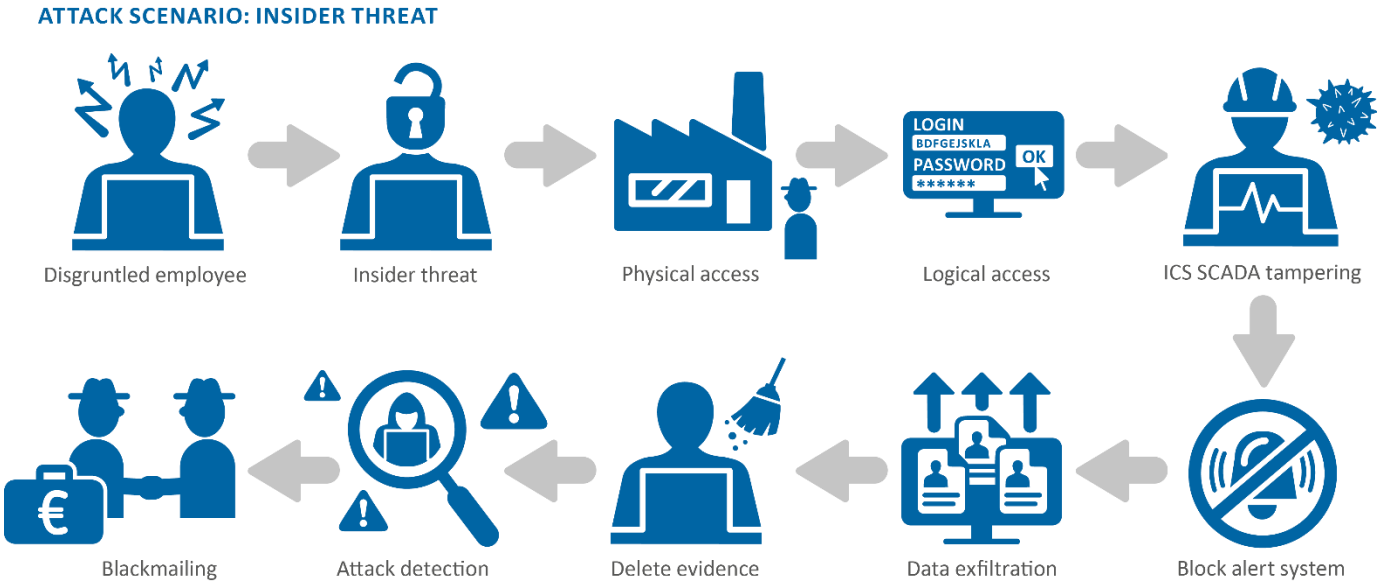
- ✓ Users with access (direct or remote) must be controlled and validated.
- ✓ Implement adequate authentication measures (e.g. pre-shared keys, tokens, one-time passwords, etc.).
- ✓ Communications and transmissions should be protected (e.g. using SSL/TLS encryption).
- ✓ Log alerts should be reviewed daily.
- ✓ Logs should be generated and kept for a reasonable amount of time to serve as an aid to incident investigations.
- ✓ Change the default passwords in all devices and apply configuration hardening
- ✓ Periodic system auditing and risk assessment.
- ✓ Apply network segmentation.

5.2 Attack scenario 2: Insider threat

Internal users (employees, contractors and third-party staff) have direct knowledge and experience in a variety of internal systems, on corporate systems and even in physical and logical SCADA network and installation details.

Therefore, a disgruntled employee can take advantage of this knowledge, as well as the privileged physical and logical access to the organization's systems, to carry out malicious activities with a lesser effort than an external attacker and with a much reduced chance of being detected in the short run.

This makes them very dangerous, and for this reason the internal users' accesses and activities need to be restricted on a need-to-know and the least privilege principles and monitored when accessing sensitive or critical systems, as well as providing employee awareness and training to allow them to detect unauthorized behaviours.



INSIDER THREAT/DATA MANIPULATION

IMPACT	LIKELIHOOD
Critical: Depends on the privileges of the user and their objective; it could range from *low* (information leakage) to *very high* (actuator or sensor data manipulation).	**Medium**: Depends on the number of users and external staff, but due to the privileges and knowledge they are more common than other attacks.
EASE OF DETECTION	**CASCADE EFFECT RISK**
Hard: Due to the internal knowledge these users have, these attacks tend to be hard to detect and identify the source, which allows them to pass undetected for long periods of time and are also complex to investigate and recover from.	**Medium**: Internal staff and contractors have access to internal systems (including critical infrastructures), and have the potential of causing changes that affect the whole system expanding to other environments and/or sectors and directly affecting the population, either by the malfunction of the operations or their cease.

ASSETS AFFECTED	STAKEHOLDERS
Human Machine Interfaces, PLCs and sensors, Data Historian	General Staff and operators Security Officer and CISO

ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)

1. A disgruntled employee is angry at the organization.
2. This employee has knowledge and access to internal systems and areas.
    a. Physical access to a control centre and installations.
    b. Knowledge on how the network and systems are set up.
    c. Maintenance credentials to several SCADA systems and assets.
3. The employee becomes aware that is going to be fired.
4. The employee decides to cause havoc on the organization by stealing sensitive information and/or compromising the operational facilities (causing reputational damage and financial loss).
5. The employee physically access the installations.
6. The employee accesses several control systems with his/her credentials to connect to several SCADA systems remotely.
7. Once connected to them, he/she changes several voltage thresholds in several actuators and sensors so the next power spike will not be detected.
8. Then he/she moves to a control centre and accesses the control systems and disables the alert mechanisms and recovery systems.
9. Finally, he/she accesses the client database on their corporate network (via the user interface, with his/her credentials), and downloads a large number of private and contact data. This data will be sold to the competition.
10. Once all these changes are done, using the administration credentials, he/she deletes logs and other traces from the systems (as these are not remotely collected).
11. The employee leaves the company, and the attack is discovered some time after, as the changes were almost undetectable until a power spike occurred on the system.
12. As a final action, the now ex-employee sells the stolen data to the black market (or competition).

RECOVERY TIME / EFFORT	CHALLENGES AND GAPS
High: The main issue is the time taken to detect the data or system that has been manipulated, which can be **several days/weeks** or even months in extreme cases. Also, as the potential access that these employees can have, both logical and physical, the damage may be greater and difficult to recover from, potentially requiring system reboots, resets **several days** or replacements. This could take, in average, to return to standard operations.	Need to harden applications, systems and equipment; restrict access to only what is needed, implement access and activity logging controls.

COUNTERMEASURES
✓ Separation of duties. Application of the "need to know" principle, employees should only have access to the knowledge and access privileges for their daily work. ✓ Apply the least-privilege principle to ensure that employees only have access to the systems they are supposed to. ✓ Users must have unique access credentials for the systems to ensure traceability on a need to know basis. The use of shared or functional accounts should be avoided, if possible. If functional/shared accounts are needed, additional traceability controls should be placed in order to control user actions. ✓ Use training courses and awareness campaigns to provide good practices to employees and teach them to detect anomalous behaviors or unauthorized actions. ✓ Provide periodic good practice posters and triptychs. ✓ Consider providing periodic security webinars to train users in the secure usage of the installations and systems. ✓ Limit the freely available internal information within the organization in order to avoid information leakage or theft (e.g. shared folders, databases, etc.). ✓ Carry out internal audits to evaluate the security level and any previously undetected issues. ✓ Definition of standardized recruitment and background check process both for potential employees and third-party contractors. This also includes living process and confidentiality agreements. ✓ Automatic system monitoring and log review processes to detect anomalous behaviors.

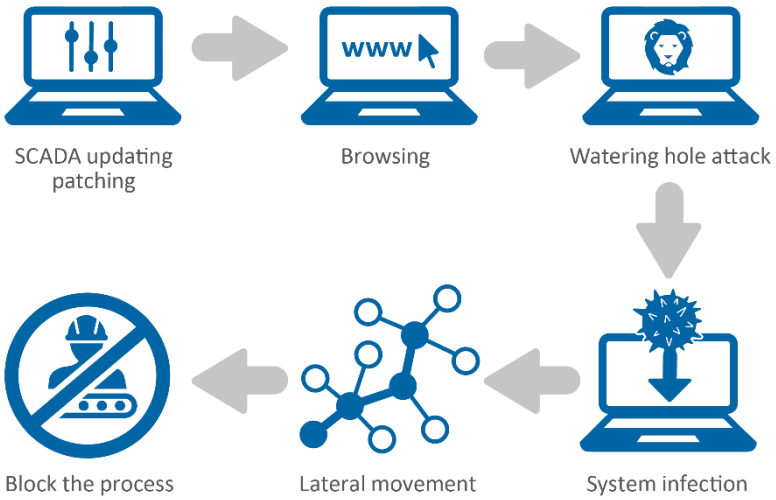
5.3 Attack scenario 3: Malware infection

SCADA systems and devices, as well as any other IT-based system, requires periodic maintenance, as well as upgrading (via patches, features updates and security fixes) to ensure the most secure and efficient operation possible.

Therefore, this is a critical phase, as the technicians need to directly connect to the devices, and the risk of a malware infecting the devices at this point, or the installation of an infected firmware, are increased tenfold. This puts further risks by the fact that most technicians use their standard corporate laptop to carry out these tasks, which is later used for other functions such as working with documents, receiving e-mails or browsing over the Internet.

Another key issue that should be taken into consideration is the source of updates and patches; if the manufacturer/vendor sites are not properly secured, or if the technicians' laptop is compromised, he/she could download an infected file instead and inadvertently infect the SCADA devices.

ATTACK SCENARIO: MALWARE INFECTION



MALWARE INFECTION

IMPACT	LIKELIHOOD
Critical: Due to the maintenance, connections usually are directly done with the SCADA systems and devices (either locally or through a VPN), therefore the malware or infection can be carried out easily.	**Medium/high:** Maintenance is done on a regular basis in order to ensure the proper operation of the systems; therefore each time an external system is connected, the network and systems are at risk.
EASE OF DETECTION	**CASCADE EFFECT RISK**
Easy/medium: Detection will greatly depend on the security measures in place, as this will determine the chance of detection. Perimeter and network security measures (such as antivirus or IDS) may be able to detect these threats.	**Low/Medium**: Maintenance operations are usually done internally, connecting directly to the systems and bypassing intranet a locally implemented security measures. This leads to the risk of infecting the internal systems and aiding on their expansion, potentially extending to other environments and sectors.

ASSETS AFFECTED	STAKEHOLDERS
SCADA assets, HMI, data historian, PLCs, Common systems	CISOs and chief security officers Technicians and maintainers Vendors and manufacturers

ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)

1. Technician has a portable computer that is used to connect and update SCADA devices.
2. This computer is also used to carry out other tasks such as viewing e-mails and browsing the Internet.
3. Attackers direct an attack against a vendors' website.
4. The vendors' website does not require authentication for downloading firmware updates and related files; which have been previously compromised by the attackers.
5. The technician is unaware that the vendors' website has been infected, and downloads a firmware file that in reality contains a remote access Trojan horse (RAT) attached to it.
6. Through this malware, several actions are made on the victims' computer:
    a. Connects to a C&C server to allow remote access to the attackers.

b. Extract and access information from the infected computer in order to find other potential victims, steal internal business information or even act as a staging point for the infection of other systems.
c. Intercept and modify connections to steal private and sensitive information.

7. The technician uses the downloaded patches and firmware files to update the ICS/SCADA devices under maintenance and, unknowingly, installs an infected version.
8. The infection is then inside the network, and the malware can now be executed from the SCADA devices causing malfunctions, creating backdoors, or carrying out other malicious activities.
9. From this point onward, the infected SCADA systems spread the infection to other devices and modify/corrupt other devices and systems connected, leading to a crash of the whole system and a full operations halt.

RECOVERY TIME / EFFORT	CHALLENGES AND GAPS
High: For advanced malware versions, it can take weeks before it is discovered. Furthermore, the recovery of the devices can be complex if the maintenance systems have also been compromised, and a complete clean-up may take **several days** .	It is necessary for the whole chain (from manufacturers and up to the final operators) to understand the security threats they are exposed to, and how they can become an unwilling means of distribution if they do not control their systems and secure their maintenance and operation procedures.

COUNTERMEASURES

- ✓ Implement network segregation depending on the sensibility and purpose of each network.
- ✓ Isolate, whenever possible, critical infrastructure network segments.
- ✓ Include 'traditional' perimeter safeguards (e.g. firewalls, antivirus or IDS/IPS).
- ✓ Systems under maintenance should be disconnected from the rest of the system.
- ✓ Only use dedicated systems and computers to carry out the updates.
- ✓ Remote access must only be enabled for the duration of the purpose it was enabled for, and only used by internal personnel (or with the supervision of internal personnel).
- ✓ Carry out periodic risk analysis.
- ✓ Implement configuration management in order to secure your system.
- ✓ Log monitoring to detect anomalous or unexpected connections and/or traffic.

6. Constraints and gap analysis

This chapter deeps into constraints and impairments that could affect the security of ICS/SCADA systems' communication networks and a gap analysis that evaluates which areas require further review. Finally, we provide an overview of common applicable security practices and available communication security guidelines.

6.1 Constraints analysis

There are multiple constraints that impede the deployment of security measures in ICS networks

One of the main issues that has to be considered and understood is the fact that the IT and OT environments follow two distinct focuses:

- **IT environments:** the main focus is on ***Security***, as users are already accustomed to the threats faced from intercommunications, having the following three principles as pillars: confidentiality, integrity and availability.
- **ICS/SCADA environments:** on the other hand, the focus on these environments is on ***Safety***; only encompassing availability and integrity (the system works as expected).

This leads to a possible conflict of concepts: **Security** vs **Safety**. This conflict is heightened by the fact that security maturity in ICS is still low, as people responsible in ICS are more concerned in safety than security (usually due to economic or complexity issues). This trend, however, is slowly changing as the need for security is becoming a common concern in ICS areas and these areas are becoming part of the security strategy of the organizations (traditionally CISOs only covered IT systems, a trend that is also changing).

Another factor that constraints the development and application of security measures is the misconceptions that usually happen within these environments:

- **ICS systems are not connected**: just because they are not connected to the Internet or the internal business network does not mean that a malicious user, or disgruntled employee, may not decide to access this 'isolated' network from an uncontrolled access point or maintenance terminal. Controls should always be put in place against both internal and external threats.
- **Security through obscurity**: the concept of security through obscurity does not provide security, and the use of proprietary protocols may leave the systems exposed due to the lack of security features or to the existence of vulnerabilities or weaknesses on the implementation.
- **The vendor devices are secure**: vendor devices do not necessarily implement security measures if not requested by the clients, and in many cases the implementation may be partial or incomplete if there are other objectives with a higher preference such as efficiency, low memory consumption, data transmission limitations, etc.
- **Safety systems already in place**: as mentioned before, safety is not the equivalent of security, and while it may cover some common points, it is not enough.

Apart from the points already covered, there are also several factors that slow down the implementation and deployment of security features and measures on SCADA systems and networks. These are constraints/impairments and incentives, which are grouped into [44]:

6.1.1 Common constraints

The most relevant and common barriers that have been identified, and validated during the interviews conducted with the experts and stakeholders from the different sectors are:

- **Cost associated with the implementation of security measures**: the costs related to the application of security measures is one of the main constraints observed.
- **Difficulty to justify the investment in cybersecurity**: as the exposure of ICS/SCADA systems to private network (and the Internet in some cases), there is a false sense of lack of risk in these environments. So far, the number of incidents has been relatively small, but their potential and likelihood increases as more and more systems become interconnected.
- **Device lifecycle**: the ICS/SCADA devices are designed to last many years, and they are rarely replaced, except when required due to new features needed or to device failure. This complicates the implementation of security measures that requires many devices to adapt to them (e.g. understand encrypted communications, authentication processes, data validation…).
- **Device replacement**: this process can also be a weakness if it has not been considered during the initial design phase and testing phase. In some cases it is not perceived feasible to replace a device since the result of the integration of a new component may put the system at risk and lead to an increased risk for the overall system operation.
- **Lack of awareness**: there is a general lack of knowledge amongst SCADA operators and asset owners regarding the threats that could put the ICS/SCADA devices at risk, especially those related to network communications, Internet exposure and remote access.
- **Lack of risk awareness among the top management**: it is also common for the top management not to be aware of the new threats that their systems are facing, due to their interconnection to internal networks (or the Internet in some cases). This leads to a lack of investment in security measures to mitigate these threats.
- **Lack of good practices regarding security of ICS systems**: there are quite a few good practice guides available, however their application is not common in many sectors.

6.1.2 Technical constraints and incentives

There are several technical constraints that restrict the proper application of security measures, or make them hard to manage. As a summary, the most relevant ones (some of which have been already mentioned on previous chapters) are:

- **Use of proprietary systems**: the use of proprietary OS or applications makes it more difficult for operators or asset owners to secure their devices and systems.
- **Complex/non-existent patching process**: most ICS/SCADA systems do not have a proper update process, as in the past it was not needed as much. This is nowadays a problem specially because these systems are designed to last many years and they are exposed to many new and ever-changing threats that need to be addressed.

- **Use of proprietary protocols**: this causes communications to be carried out only between devices from the same manufacturer, and without the option of adding additional security layers to it (unless provided by the manufacturer).

- **SCADA systems' function**: many ICS/SCADA devices are used on remote areas and installations such as oil rigs or power substations. As a result, it is usually hard to access them physically; even more, they can be installed on robots or other devices, which are exposed to extreme environmental challenges and make use of special systems, power controls or interconnections.

In addition, the application of security measures is seen as a potential risk that could adversely affect system stability, efficiency and its operations. This results in patches and updates being rarely applied, keeping systems, devices and controllers in their default state (except if an update is required for compatibility or required functionality reasons).

Regarding incentives, several standards mention different incentive alternatives that could be used to promote the use of security protocols, architectures and assets (amongst others). Nevertheless, there is still a lack of consideration and understanding of the need of adding these security features [45] [46].

- **Security by default**: A common point of view shared by all experts and stakeholders involved in the study is the fact that cybersecurity and confidentiality (privacy) features and needs should be addressed from the design phase onwards to maximize the efficiency and security of the assets developed and minimize the costs required to achieve a certain security level.

- **All agents involved:** All parties involved on the process should be more involved in cybersecurity matters, from Manufacturers and up to the implementers. The need to work together and put in common the needs and measures that can be used is fundamental to achieve a proper implementation, keeping the efficiency at an appropriate level and stopping the costs from skyrocketing. Also, this increased communication will benefit all, as all parties will be aware of the needs and options, and not only forced by procurement or regulation requirements.

6.1.3 Social constraints

Some ICS / SCADA systems fall within the category of industrial environments that are regarded as critical infrastructure, which includes sectors such as energy, oil, gas, water or nuclear, amongst others. These infrastructures are considered critical as they provide vital services to the society, and their failure would have catastrophic effects. Just a mere disruption to one of the services for a few hours can have severe consequences for citizens and the economy.

An attack on the communications of the different assets that are part of these infrastructures and SCADA systems can have the same effect as an attack at the physical assets themselves, compromising the critical infrastructures and affecting the operations.

6.2 Gap analysis

After reviewing all the above factors regarding cybersecurity in ICS/SCADA networks, the next logical step is to detect areas that are weak or have improvement potential (always from the point of view of cybersecurity), taking into consideration the threats they face and the security countermeasures or mitigation features available to prevent or protect the networks against them.

This leads to three main groups: domains that have lesser security improvements, uncovered policy requirements and points raised on the interviews with experts and relevant stakeholders from the sectors in scope.

6.2.1 Domains requiring improvements

There are several domains where the implementation of additional security measures would be greatly beneficial for the general security of ICS/SCADA systems in interconnected environments.

- **Secure communication protocols**: SCADA protocols were not originally designed having security as a point to cover. Therefore, while newer protocols already include many common security features, older ones cannot cover them and still need to be used to interface with older and legacy devices. While in some cases this can be covered by additional security layers or devices, it is not always possible (or efficient), and needs to be taken into account.

- **Interoperable communication protocols:** SCADA devices make use of proprietary protocols from their manufacturers in order to interconnect to other devices; while this is not an issue with devices from the same manufacturer, it becomes a problem when interconnecting devices from different manufacturers. This requires the development and use of compatible protocols that need to be supported by all manufacturers to ensure a good level of interoperability with the least efficiency and security loss.

- **Avoid the use of homebrew protocols:** In line with the previous point, apart from developing compatible protocols, it would also be a good practice to avoid close-source proprietary protocols, as their security cannot be verified, and as it has been seen in many incidents, security through obscurity does not relate directly to proper security coverage.

- **Common frameworks:** On this line, apart from the protocols, the use of common frameworks can also be a factor to help improve the efficiency and security of the devices, especially when interconnecting several ones from different manufacturers.

6.2.2 Policy needs in the SCADA domains

There are also several areas of improvement that have been observed and also been confirmed with the feedback from the interviews and which are related to needs that can be managed via policies in the organization, and can be promoted via regulations and even legislations in several cases.

The most relevant points are:

- **Cybersecurity awareness campaigns for employees and top management:** Many security incidents could be avoided if employees and the top management were aware of the risks they face on a daily basis. Considering not only those that affect SCADA systems but also those that affect IT systems in general, as the last ones can act as an entry points for attacks in SCADA systems, as it has been seen in recent attacks against electric companies [2].

- **Lack of regulatory framework at national or EU level:** Due to the lack of a common European regulation, most European countries are taking their own approach on the matter, establishing their own regulations and compulsory requirements for secure processes on ICS, SCADA and critical infrastructures. This causes that the security status of these systems may vary greatly from one country to another. Some countries are already enforcing minimum security requirements in the sector, developing stricter controls for future iterations of their national regulations.

- **Proper Product Lifecycle Management both for hardware and software:** Because these systems are now interconnected and exposed to the Internet, or large public networks, they are now exposed to many more threats. This leads to the need of a faster update and patching process to protect these interconnected devices. This needs to be worked on as it is not something easily done on critical infrastructures' SCADA assets because it may means stopping the production processes.

- **Involvement of the vendors and manufacturers in the device protection process**: As they are in charge of designing and developing the devices and assets, they are on an ideal position to implement the changes needed. They are able of proficiently and cost-efficiently include new security features or characteristics. This, however, is not only a matter of the manufacturers adding these new features, but also of the organizations accepting the related costs; therefore, a balance between security and cost must be maintained. As the organizations' budgets are limited, the security needs can also be achieved using other means (third-party devices, configurations, isolation, etc.).

6.2.3 Social and staff requirements

Several points were identified in relation to the preparation of the staff and personnel of the organizations, ranging from the technical staff and up to the top management. Furthermore, these points have also been raised by most of the experts interviewed.

- **Awareness**: there is an overall lack of awareness regarding the need of security in ICS/SCADA systems and networks. Even more worrisome is the lack of knowledge regarding the threats they are exposed to due to the high level of interconnectedness, not only on publicly exposed systems, but also on internal private ones. This contrasts with other IT areas, where security has become one of the main concerns due to many cases of incidents and attacks already suffered.

- **Cyber-insurance**: some organizations are contracted with cyber-insurance companies in order to be covered for the most common cybersecurity risks to which they are exposed. As the threats within these environments are quite new (despite being variations of traditional attacks), it is not yet clear to which extent these cybersecurity insurance will be effective, and if compensation will be adequate to the impact of the incidents. Cyber-insurance will undoubtedly become a common factor in these environments, although it is still in its infancy.

- **Training**: it is becoming a common need in order to raise awareness on current threats and risks and to provide knowledge on how to prevent, protect and act in case of a security incident. Most of these processes are managed internally, with each organization having its own training processes. This can, also, be done via informative posters and triptychs that provide good practice recommendations to the employees. The risk needs to be understood with an appreciation for the peculiarities in security practices found in the ICT and ICS realms [47]. As a result, a whole IT/ICS cross-training approach that provides for a better understanding of the risks needs to be made part of the curriculum for the training of both future IT and ICS practitioners.

7. Security good practices

The first point to review are the common security practices for communication networks that are currently available and in use in ICS/SCADA systems in different sectors, including critical infrastructures within the European Member States organizations.

This includes a brief review of applicable standards and more specifically of good practices mentioned in them, regarding the design of systems and critical phases like procurement and testing.

7.1 Standards

There are a lot of standards applicable to different industrial sectors within scope, with part of them already addressing, at least partially, the aspects of cybersecurity that should be covered in ICS/SCADA systems and networks. Furthermore, governments are also starting to implement compulsory legislations to 'force' organizations to reach, at least, a basic level of cybersecurity on their systems, promoting in some cases the use of these standards.

A short list of related standards includes:

- **AGA 12 Part 1** (Cryptographic Protection of SCADA Communications)**:** its main focus revolves around a comprehensive system design proposal to optimize the SCADA systems. This helps to reduce the requirements to carry out maintenance and management processes [48].

- **IEC 61968/61970** (Common Information Model [CIM] – Distribution/Energy management): defines a Common Information Model that can be used for application-to-application interactions between systems on operation centres. It can be applied for transmission, distribution and end-market functions.

- **IEC 62351** (Security in energy management systems)**:** provides security recommendations for many important protocols, most of them used mainly in the energy sector (includes IEC 60870-5, DNP3, IEC 60870-5-101 and IEC 60870-5-104).

- **IEEE P1711** (Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links): defines a cryptographic protocol to provide integrity, and optional confidentiality, for the cyber security of serial links [49].

- **ANSI/ISA 99** (Industrial Automation and Control Systems Security): defines a Security Guideline and User Resource for Industrial Automation and Control System. The development of this standard was stopped when the ISA IEC 62443 was started [5]. The evolution of this standard is the **IEC 62443**, with the intention of completing and expanding its capacity for action [50].

- **NIST SP 800-82** (Guide to Industrial Control Systems)**:** which defines the typical topology of SCADA systems, identifying threats and vulnerabilities and providing recommendations and countermeasures to mitigate these risks.

- **ISO 27000** (Information security management systems): general purpose standard that provides good practices and recommendations for information security management and is normally used for the implementation or management of Information Security Management Systems (ISMS).

7.2 ICS/SCADA systems security

In order to define the appropriate security measures that could be applied to an ICS/SCADA system, it is necessary to properly understand what it is composed of, and the interconnections that have been set within it, not only among components but also with external systems. This makes it possible to fully determine the operations and functionalities covered and the lifecycle of the assets; including updating and patching processes. For this purpose, it becomes necessary to carry out a mapping process that locates and identifies all the assets and connections that comprise the system, and this should contain, at least:

- **Asset inventory**: includes all assets in use, defining their purpose, functionality, hardware and software versions.
- **Connection inventory**: all interconnections between assets, both internal and external ones, and the protocols in use.
- **System diagram**: showing all the intercommunications and the physical/logical location of all the assets of the system.
- **User list**: all the users that need to access the assets, their privileges and their expiration date. It should include also any visiting (guest) users and punctual accesses. It is recommended to make use of a RACI (Responsible, Accountable, Consulted, Informed) matrix in order to map the users to the tasks and/or operations they have to carry out.

In ICS/SCADA systems and networks, there is a set of recommendations and good practices that can be followed in order to protect against some of the new threats faced by these assets. These can greatly increase the protection of the availability, integrity, confidentiality and non-repudiation [51], being the following the most relevant:

- **Network security devices**: these devices (such as firewalls or IDS/IPS) should be used on these networks to detect anomalous or unauthorized traffic.

- **Anomaly detection system**: it can be used to identify any anomalous, unexpected and/or unauthorized behaviour in the ICS/SCADA network and systems, potentially discovering advanced attacks such as APTs or internal employee threats (accidental or intentional).

- **System logging**: the event logging that can be generated by the systems and devices can be an invaluable tool to identify anomalous or malicious behaviours, as well as aid on incident investigations. The time to store these logs before deleting them varies from one recommendation to another, depending on the kind of information managed and the security objectives and risk levels set.

- **Configuration management**: while this is not a security feature per-se, it is fundamental in order to ensure that only authorized actions are carried out by the device, and that any unused function or feature is properly disabled or inaccessible. Many devices also bring default configuration that can be dangerous for the system, such as default access credentials of port configuration parameters. By establishing a configuration management process, multiple devices and systems can be kept properly configured at the same time, ensuring that no misconfigured devices are left operating.

- **Data validation**: a process that checks the validity of the data received in order to ensure that they have not been corrupted, manipulated, or modified by a third party.

- **Source node authentication**: a means for the SCADA devices to validate the authenticity and origin of the connection they have received, allowing the detection of malicious communications sent to them.

- **Trust anchors**: the use of devices that verify the identity of the devices. Its functionality is similar to the certificate trust anchors used to validate the identity of secure web sites or devices.

- **Device communication encryption**: allows the protection of the data transmissions to avoid them from being intercepted and replayed (for malicious purposes). This, however, has to be handled carefully, as many devices have limited capabilities (focused on the efficiency and low resource consumption) and adding encryption in them would cause an overhead or transmission time delays.

- **Internet connection**: Security measures must be in place to ensure that all communications are filtered and checked to avoid unauthorized uses or accesses. Considering a scenario where part of the network is exposed to the Internet, one of the most common recommendation (among many) that should be considered is the use of **DMZ,** a section of the network infrastructure that is used to communicate with the outside and offer services though public networks while ensuring their separation from the internal network and services.

- **MAC Address filtering**: can be used to limit the number of devices connected and detect any unauthorized connections. It can also help to filter unauthorized transmissions and detect unauthorized connection attempts to the network.

- **Network segregation/isolation**: ICS/SCADA systems should make use of their own specific private networks, which should ideally be isolated, although alternatively they should at least be segregated and clearly differentiated from traditional business and internal networks. The use of dual-home devices, while common, is not recommended to segregate networks, as these systems usually lack proper filtering, and could be used by attackers (or malware infections) to jump between zones.

- **Interoperability**: each time a new asset makes use of a new protocol it is highly recommended to verify its compatibility and interoperability with the rest of the system and identify any known or potential vulnerabilities.

- **Role-Based Access Control (RBAC)**: it provides a means of managing the access permissions of the users by establishing a series of roles with predefined privileges. This allows to globally control them, ensuring that, for example, technicians only have the permissions they are meant to have. It also allows to control exceptions from a centralized system, ensuring that assigned privileges are not lost and all are controlled.

- **Threat emulation**: the use of sandboxing environments can be very useful to evaluate and identify malicious software embedded on seemingly harmless files (EXE, PDF, DOC, XLS, etc.).

- **End-user device security**: any end-user computer or device that may interact should be adequately protected, including antivirus, antimalware and other security considerations. Additionally, these systems should be used exclusively to interact with SCADA systems (for operation, monitoring or maintenance) as to avoid unwanted infections to affect these systems (examples of unwanted infections include those that are distributed via malicious e-mail, accesses to malicious internet sites or the download of dangerous files).

7.3 Monitoring, maintenance and mitigation process

The ICS/SCADA systems are now exposed to a large number of threats, which makes necessary the need to not only monitor and control these systems more actively and pre-emptively, but also requires the planning in how to react in case of an incident. Several relevant points to consider are:

- **Planning**: it is necessary to plan in advance the means to counteract an eventual attack, or to recover from its effects. This is something that should be done even for non-critical infrastructures, as they are also exposed and at risk.
- **Interconnection supervision**: all interconnection points between ICS/SCADA networks and other private or public networks must be identified and controlled, as they are going to be attacked in order to gain access to the SCADA systems.
- **Control system and network monitoring**: these must be controlled in order to allow the detection of attacks and incidents in ICS/SCADA systems that are being managed by these control systems.
- **Log management**: the logs generated by the devices are an invaluable information source and for critical systems and infrastructures they should be, at least, processed automatically in order to detect anomalous behaviours, infections or other attack variants.
- **Role/privilege management**: as there will be many technicians, operators and third-party personnel that may require different levels of permissions to access, operate and maintain the systems and devices. Therefore, it is a common recommendation to define and establish different roles with limited privileges to ensure that no user has privileges that he/she should not have.
- **Maintenance management**: establish controlled maintenance processes, including the use of dedicated systems.
- **Reporting**: finally, the incident/attack reports should be as detailed as possible, including not only the events that occurred but also errors and mistakes observed, points of improvement and recommendations to avoid future incidents/attacks of that variant.

All these points should be centralized on a unified control centre to ensure a proper overview of the current status of the ICS/SCADA systems. This also applies to the centralization of security incidents, their details and solutions applied as to be aware also not only of their current state, but also of the overall state.

7.4 Contracting with network operators

There are no specific standards or guidelines defined at EU level to be used by network operators or telecommunication companies regarding cyber security practices in the tender. For example, the IEC 62443 follows a generic approach, not focusing on specific scenarios or sectors. However, the experts mentioned the following points:

- **Service Level Agreements** (SLA): these contracts establish an agreement between the organization and the network operators where the details of the service to be provided by the latter one is defined. This provides a certain level of confidence regarding the quality of the service provided, as these contracts usually detail the availability percentage, minimum bandwidth, support, etc., as well as the fines for the network operator if the objectives set are not met.
- **Network Redundancy/multiple network operators**: in order to ensure that communications are always available with external and remote locations, it is highly recommended to have redundant

communication lines available (ideally, from different providers), as if one of them fails (overload, logical failure, physical damage), the other line will ensure, at least, minimum communications. Even more, ideally these redundant lines should be provided by different network operators as to ensure that an issue in one of them does not compromise all the network connections.

- **Vendor and technology diversity**: another good practice is to use devices from multiple vendors in order to ensure that if one of them is compromised (e.g. using an exploit), the other devices will not be automatically compromised too. Furthermore, it is recommended for the provision of the same service to be in place equipment that makes use of different technologies.

- **Purdue Enterprise Reference Architecture** (PERA): the main concept of this reference model for enterprise architectures revolves around the use of multiple layers in different stages of the architectural lifecycle of a system. This can be applied to ICS/SCADA systems and production environments, as the base concepts can be expanded to cover the specific needs and requirements of these systems.

7.5 Authentication and security mechanism for secure communications

On the industrial sector, the use of common communication protocols has become commonplace. This leads to the availability of already existing security protocols that can be implemented to protect and secure these communications. The interviews with the experts from the different areas have provided further insight into which of the available security protocols (or features) are most commonly used nowadays within the sector.

For this purpose, there are multiple alternatives and solutions available that can be used to secure these communications. Examples include:

- **SSH** (Secure Shell): it establishes a secure remote shell connection to a server, protecting the connection data and avoiding interception of the session.
- **Kerberos**: an authentication protocol that allows two computers to verify their identity against each other on an insecure network, while ensuring the security and validity of the verification process and result [52].
- **TLS** (Transport Layer Security): This protocol provides privacy and integrity between two communication applications that use a standard TCP communication. Alternatively, the SSL (Secure Socket Layer) protocol can be used on legacy systems not supporting TLS, although this protocol (SSL) is now insecure in light of the latest vulnerabilities found regarding its functionality.
- **IPsec** (Internet Protocol security): establishes mutual authentication between agents at the beginning of the session and manages the negotiation of the cryptographic keys to be used during the session.
- **EAP** (Extensible Authentication Protocol): authentication framework frequently used in Wireless networks and point-to-point connections [53].
- **LEAP** (Lightweight Extensible Authentication Protocol): allows for clients to re-authenticate frequently, upon each successful authentication, the clients acquire a new WEP key [54].
- **PEAP** (Protected Extensible Authentication Protocol): it encapsulates the EAP within an encrypted and authenticated TLS tunnel [55].
- **L2TP** (Layer 2 Tunnelling protocol): can be used to support VPNs or as part of the delivery of services by ISPs. This protocol can provide end-to-end encryption and other security features.

7.6 Procurement

The procurement phase is a point of inflexibility that can motivate manufacturers into including more security features by default. As observed from the feedback from the interviews, the security requirements

have become a common request added in SCADA procurement processes. This is something that should be always done in order to ensure that these security processes are properly integrated in the devices and in the device lifecycle. Devices should be configured properly, so that security features are enabled, as default configurations are rarely adequate. This can also help to promote the need to provide periodic patches and updates to ensure that security is kept up to date, as it is a factor that can be added to procurement requests.

Some examples of basic security requirements to request include:

- **Device authentication**: mutual authentication on communications to ensure the validity of the communications. Unknown transmissions should always be dropped and ignored.
- **Device communication encryption**: in cases where sensitive information is sent, transmission encryption is a must to avoid eavesdropping. This also applies to devices performing critical functions, as it stops attackers from gaining insight into the communication patterns and workings.
- **Log traffic details**: source, destination, user/device, timestamp and protocol.
- **Protocol communication validation**: to allow anomaly detection and data manipulation attempts on the communications between the devices.
- **Allowed command identification/validation**: commands must be restricted to ensure that only appropriate commands can be sent remotely and detect any manipulation or attack attempts.
- **Attack payload prevention**: discard any transmission that sends unknown data or payload to prevent attacks such as exploits that are used to gain access or crash the devices.
- **Physical access authentication**: when connecting locally with devices (e.g. for configuration or maintenance purposes), devices should provide an authentication mechanism to avoid unauthorized accesses.
- **Patch and update validation**: a validation process should be implemented to ensure that only authorized updates can be installed to avoid manipulated firmware or patches to be applied.

7.7 Assessing the ICS/SCADA components

Periodically assessing the security status of the ICS/SCADA systems and devices is a must in order to ensure that it complies with the needed security level. This is especially important for Critical Infrastructures, due to their relevance.

Ideally, there are three main functions that should be carried out:

- **Risk Assessment**: evaluate the system to identify the most critical sections, the threats faced and the existing mitigation measures (does not develop new ones). This includes defining the residual risk and the accepted risk to ensure that there are no risks unaccounted for.
- **Vulnerability Management**: ensure that the systems are properly kept up-to-date and all known vulnerabilities are properly patched or mitigated.
- **Penetration Testing**: review the system to ensure that it is properly configured and there are no gaps, systems or services that are vulnerable and could be exploited by attackers.

These should be carried out with a reasonable periodicity (e.g. each year) to ensure that the security is kept on level.

7.8 Forensic analysis on interconnected SCADA systems

Recent security incidents affecting SCADA and Industrial Control Systems emphasise greatly the importance of good governance and control of SCADA infrastructures. In particular, the ability to respond to critical incidents and be able to analyse and learn root causes is crucial. In 2013 ENISA published a relevant study upon forensics in SCADA **"Can we learn from SCADA security incidents?"** [56].

To this point, it is important to consider that investigating incidents involving ICS/SCADA systems is not straightforward and can be much harder than for other IT systems. However forensic considerations must be acknowledged in order to ensure that the control system are not compromised by an unauthorized user or malicious attacker ([57] [58] [59]). Therefore, the main difficulties found when carrying out forensic and incident response follow-up activities on SCADA-based systems are:

- ICS/SCADA systems make use of technologies and protocols very different from those used in traditional IT systems, and as such usual ICT security measures cannot be reused.
- The use of proprietary or specific protocols, processes, data structures and I/O interfaces makes the simulation of attack scenarios very complex, requiring emulation environments that are not always available. There are efforts to design tools to provide these emulation environments in critical infrastructure areas [33].
- Proprietary firmware: similar to the protocols and technologies, the use of proprietary firmware forces the need of specific tool to access it or even analyse its workings to detect anomalies.
- Update processes; these are usually carried out by using standard computers/laptops, or even USB devices, which act as a potential entry point that is sometimes outside of the control of the organization (e.g. third-party maintenance), which complicates the forensic investigation.
- Existing tools for computer forensics cannot be easily applied for SCADA forensics and to industrial environments; specific tools are needed.
- Lack of logging capabilities of many devices, usually for processing/resource reasons, both for legacy and new devices and systems.
- Absence of encryption and authentication/authorization features; apart from the lack of logging capabilities, if a device does not include any security features it is also much more complicated to reconstruct the events that have occurred in a forensic investigation.

ICS/SCADA systems cannot be simply stopped/taken on line for a forensic analysis, as most of the forensic tools work on 'stop-take-a-snapshot' technology.

7.9 Available communication security guidelines

There are multiple good practice guides published and which cover most if not all aspects of ICS/SCADA communications networks, devices and systems, at least on a theoretical level. This section focuses on summarizing those practices that are more relevant for the scope of this study regarding ICS/SCADA systems, architectures and communication networks.

After studying the existing good practices, and sorting them into relevant categories, the next step is to evaluate and organize them, based on their impact. The concepts evaluated are:

- **Complexity**: rate their implementation difficulty based on the requirements related to the domains defined previously: low (feasible), medium or high (not feasible).
- **Cause**: justification of the rating given to the complexity value in relation with the implementation (economical, technical or political).

The following tables displays the good practices listed by the following categories:

- **Security in the SCADA network**
- **Security by Design**
- **Software updates**
- **Defense-in-depth**
- **Secure network communications**
- **Physical Security**
- **Wireless networking**
- **Staff and Top management awareness**
- **Asset Management**
- **Third-parties**
- **Governance and Compliance**
- **Malware protection**

1. Security in the SCADA network

Table 4: Security in the SCADA network guidelines

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
1. External connections: Strict limitations and authentication control are needed for it.	Unauthorized physical access, deliberate damage	MEDIUM	**Technical**: Implement and use only the external network connections needed.
2. Reinforced security system: Hardening of the hosts, networks and DMZ interconnections.	Unauthorized access, malicious code, network outage cascade effect	MEDIUM	**Technical**: Reinforce the security for the internal network by using DMZs (network separation), unidirectional communications.
3. Use of Virtual Private Networks: Enhancing security of remote communications by using VPNs to establish communications.	Eavesdropping, information theft.	MEDIUM	**Technical**: Design and implement security measures for VPN solutions.

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
4. Simplify the internal network: Minimisation of access points to the internal network and improve the monitoring.	Unauthorized access, information theft, malicious code.	MEDIUM	**Technical**: Simplify and monitoring the network.
5. Situational awareness: Regular vulnerability and penetration testing allow the detection of issues and evaluation of the current security level of the system and network.	Attack in Control Centre System, Data Theft, Authentication exploiting.	HIGH	**Economical**: Cost of implementing periodical inspections of the SCADA systems and the related infrastructure.
6. Implement Security Control: Developing control and monitoring methods to cope with any contingencies in the SCADA equipment, such as intrusion detection software, antivirus software and file integrity checking software.	Unauthorized access, information theft, malicious code.	HIGH	**Technical**: Develop and implement control and monitoring methods to cope with any contingencies in the SCADA equipment.
7. Network Segmentation: Using segmentation of security zone within the SCADA network and using distributed firewall within the SCADA environment to protect the end devices.	Unauthorized access, malicious code, cascade effect.	MEDIUM	**Technical**: Design and implement network segregation. Carry out tests in order to verify connections.
8. MTUs and RTUs: These devices should be protected using secure architecture designs and applying features provided by the devices.	Information theft, identity theft, deliberate information manipulation, insider threat.	MEDIUM	**Technical**: Deploy security measures to the MTUs and RTUs.
9. Disconnect unnecessary connection: Disconnect or isolate SCADA network devices and the SCADA network itself from the rest of devices.		MEDIUM	**Technical**: Implement and use only those SCADA network devices needed.
10. SCADA backdoors: Any backdoor access to the SCADA network should be removed unless strictly necessary. If this is not possible, they should be protected with additional security measures.		MEDIUM	**Technical**: Disable unneeded backdoors access to the SCADA networks.

2. Security by Design

Table 5: Security by Design

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
11. Security by Design: Security considerations need to be included in the initial phases of the devices/components design.	All attacks	LOW	**Technical**: Hardware and network security awareness for designers.
12. Security in the lifecycle: Addressing security throughout the lifecycle of the ICS: architecture design, procurement, installation, maintenance.		MEDIUM	**Economical:** Cost of maintenance the security in the whole process.

3. Software updates

Table 6: Software updates

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
13. Software updates: To ensure that all the elements of the network are up-to-date and protected against newly discovered vulnerabilities or bugs.	Attacks related to exploit outdated systems. (Data theft, DDoS).	HIGH	**Technical**: Defining and implementing an update process, can be complex for real-time assets.

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
14. Security patching: Implement processes for deployment of security patches to ICS.		HIGH	**Technical:** Implement process for deployment of security patches to ICS.

4. Defense-in-depth

Table 7: Defence-in-depth

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
15. Develop and implement security: Security policies, procedures, training and educational material that applies specifically to the ICS.	Information theft, identity theft, deliberate information manipulation, insider threat, malware	LOW	**Economical:** Cost of development and implementation of security measures (policies, procedures, etc.).
16. Identify critical systems: Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading effects.		MEDIUM	**Technical:** Designing critical systems to prevent cascade effects.
17. Disable unused ports and services: In ICS devices after testing them, in order to ensure that this measure will not have impact on process operations.		MEDIUM	**Technical:** Use only ports and services needed.
18. Restrict access: Restricting physical and logical access to the ICS network and devices; assigning privileges only to those who require them.		LOW	**Organisational:** Define rules and user privileges to access ICS network and devices.
19. Authentication mechanisms: Using separate authentication mechanisms and credentials for users of ICS network and the corporate network.		MEDIUM	**Technical:** Implement authentication and credential mechanisms for the users.
20. Audit systems: Auditing the systems on critical areas of the ICS.		HIGH	**Economical:** Cost of auditing the systems on critical areas of the ICS.
21. Implementing secure protocols: Implementing and employing reliable and secure network protocols & services where feasible.		MEDIUM	**Technical:** Implement and deploy secure communication protocols.
22. System monitoring: Monitor in real-time ICS process to identify unusual behaviour, which might be the result of an electronic incident.		MEDIUM	**Technical:** Monitor, in real-time, ICS process to identify unusual behaviour.

5. Secure network communications

Table 8: Secure network communications

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
23. Implement secure architecture. Organizations should select and implement technical, procedural and management protection measures to increase the security of process control systems.	Information theft, identity theft, deliberate information manipulation, insider threat.	MEDIUM	**Technical:** Implement procedural and management protection measures to increase the security of process control systems.
24. Secure network proxies: Internal and external network connection should be routed via specific hardened proxies, located in the DMZ.		MEDIUM	**Technical:** Implement and maintain network proxies in the network.
25. Remote Access control points: Control all remote accesses through a limited number of managed access control points.		LOW	**Technical:** Define needed access control points and limit those not required.

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
26. Remote Access inventory: Maintain an inventory of all remote access connections and types. (E.g. VPN or modems).		MEDIUM	**Technical:** Maintain an inventory of all remote access connections and types.
27. Install anti-virus: Protect process control systems with anti-virus software on workstations and servers. If anti-virus software cannot be deployed, other protection measures should be implemented.		LOW	**Economical:** Antivirus and implementation costs.
28. Email and Internet access: Disable all email and internet access from process control systems.		LOW	**Technical:** Disable all email and Internet access from process control systems.
29. System hardening: Undertake hardening of process control systems to prevent network based attacks.		MEDIUM	**Technical** and **organizational:** Implement hardening of process control systems.
30. Resilient infrastructure and facilities: Systems should be installed using appropriate infrastructure such as redundant networks		HIGH	**Technical:** Deploy redundant network using appropriate infrastructure.

6. Physical Security

Table 9: Physical Security

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
31. Physical security measures: Deploy physical security protection measures to protect ICS and associated networking equipment from physical attack and local unauthorized access.	Unauthorized physical access	LOW	**Organizational**: Deploy physical security protection measures to protect ICS from physical attacks and set a regular monitoring process.

7. Wireless networking

Table 10: Wireless networking

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
32. Wireless networks: The following security measures can be used to protect networks in general: - highest encryption possible - Access Control Lists (ACL) - Media Access Control (MAC) address filtering	Information theft, identity theft, session hijacking, information gathering, insider threat.	MEDIUM	**Technical:** Implement security measures to protect wireless communications.

8. Staff and Top management awareness

Table 11: Staff and Top management awareness

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
33. Personnel background checks: Ensure all staff with operational or administration access to ICS are appropriately screened.	Social engineering, insider threat, malware.	LOW	**Economical**: Use of internal/external resources in order to enhance personnel security awareness.

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
34. Password and accounts: Implement and enforce a password policy for all process control systems that covers strengthening of passwords and expiration times. It is recommended that passwords are changed frequently.		LOW	**Technical**: Enforce the correct password policy for all process control systems.
35. Start and finish processes: Implement procedures that ensure new starters receive the appropriate accounts, authorization levels and security training when they join to a process control team.		LOW	**Organizational**: Elaborate and implement the procedures to stablish a correct process control.
36. Device connection: Establish a procedure to verify that devices are free from virus or worm infections before being connected to process control networks.		LOW	**Political:** Elaborate a procedure to verify that devices are free from malware infections.
37. Encryption data: Encryption of emails and blocking of files and directories.	Unauthorized access, information theft, malicious code.	MEDIUM	**Technical**: Implement encryption protocols to protect data.

9. Asset Management

Table 12: Asset management

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
38. Document security framework: A document containing a full inventory of the process control systems and the components, should be created and maintained in order to gain awareness of the whole network, including legacy ones. This inventory should contain the vulnerabilities that impact each one.	Unauthorized access, malicious code, network outage	LOW	**Economical:** Implement the security framework on the organization.

10. Third-parties

Table 13: Third parties

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
39. Communication service providers: It is recommended to use third party telecommunication companies that will be in charge of maintaining and securing the network communications.	DDoS, DNS attacks, unauthorized access.	MEDIUM	**Economical:** Cost of contracting communication services to third party providers.
40. Manage risk in the supply chain: Engage with any organization linked to the process control systems through the supply chain to ensure that their process control security risks are managed.	Social Engineering, information theft.	MEDIUM	**Organizational:** Establish security requirements to suppliers and the external processes contracted.

11. Governance and Compliance

Table 14: Governance and Compliance

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
41. Define roles and responsibilities: Define roles and responsibilities for all elements of process control security and appoint a single point of accountability for process control security risks.	Attack in Control Centre System, Data theft, Authentication exploiting.	LOW	**Organizational:** Define roles and responsibilities for all the elements of the process control security.
42. Develop policy and standards: Define, document, disseminate and manage, under change control, formal policies and standards for process control system security. Ensure that the policy and standards accurately collect the organizational requirements, support business requirements and are agreed by all relevant parties.		LOW	**Political:** National and European regulation will be considered regarding organizational requirements, support business requirements and data protection.
43. Ensure compliance with policy and standards: Implement a security plan to ensure that the process control system policies and the standards are complied.		LOW	**Organizational:** Implement a security plan.
44. Update policy and standards: Establish the mechanisms to ensure that the process control security policy and standards are regularly reviewed and Updated with new threats and legislations, requirements and changes to business and operational models.		LOW	**Political** and **Organizational:** Establish the mechanisms to review national and European regulation in order to ensure that the process control security policy are regularly updated.
45. Incident Response: It is necessary to define the process to manage security incidents. This includes all stages: detection, investigation, analysis, mitigation disaster recovery (DRP), and post evaluation (define measures to prevent future incidents).	All types of attacks (faster detection, mitigation and prevent).	LOW	**Organizational** and **Economical:** Elaborate and implement an incident management and response plan.
46. Relation with third parties: Communication channels between providers and other third parties can be used to receive assistance and share relevant information to prevent incidents or attacks.		MEDIUM	**Organizational:** Collaboration with third parties companies to share relevant information regarding to prevent incidents.

12. Malware protection

Table 15: Malware protection

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
47. Manufacturer code and software validation: Systems should only run the intended functions and applications they were designed to. Manufacturers should provide means to validate the software and firmware installed on the system.	Unauthorized access, information theft, malicious code.	HIGH	**Technical:** Implement code execution validation controls on the embedded systems.
48. Sandboxing: a security mechanism. It is often used to separate running programs without risking harm to the host machine or operating system. Allows the detection of new and cutting-edge threats.		MEDIUM	**Technical:** Implement sandboxing functionality on the protection solution in place to identify unknown threats.

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
49. Least Privilege Access: Ensures that users have access exclusively to those areas and functions that they need in order to carry out their tasks. Additional privileges put the assets at risk, especially by allowing an infection to further spread with higher privileges.		MEDIUM	**Technical:** Define and implement a least privilege access across the devices.

8. High-level recommendations to improve the security and resilience of ICS/SCADA Systems

This chapter includes a list of high-level recommendations for manufacturers, operators and security experts that will help them to improve the security level and resilience of the ICS/SCADA systems and communication network functions.

8.1 List of recommendations

The recommendations proposed are listed in Table 16 and have been further developed in section 8.2:

Table 16: Recommendations

ID	DESCRIPTION
1	Include security as a main consideration during the design phase of ICS SCADA systems.
2	Identify and establish roles of people operating in ICS/SCADA systems.
3	Define network communication technologies and architecture with interoperability in mind.
4	Establish brainstorming and communication channels for the different participants on the lifecycle of the devices to exchange needs and solutions.
5	Include the periodic/SCADA device update process as part of the main operations of the systems.
6	Establish periodic ICS/SCADA security training and awareness campaign within the organization.
7	Promote increased collaboration amongst policy decision makers, manufacturers and operators at EU Level.
8	Define guidelines for the establishment of reliable and appropriate cybersecurity insurance requirements.

8.2 Detailed recommendation

8.2.1 Recommendation 1: Include security as a main consideration during the design phase of ICS/ SCADA systems

Description: traditionally, only safety is included as one of the main considerations during the design of an ICS/SCADA system or infrastructure (alongside efficiency, real-time constraints, etc.). However, the concept of security is not, although it is now one of the main risk sources that should be covered to prevent future attacks and incidents.

Steps: during the design phase, the security of the devices, and the communications between them, has to be one of the main concepts that will impact on the choice of devices, measures to implement, and overall design of the architecture.

- Establish access controls (logical and physical) on all SCADA network communication access points.

- Define security measures to protect and validate communications between SCADA devices.
- Include security-specific devices (e.g. firewalls, IDS/IPS, gateways) on the main system design (instead of being an add-on later on).
- Establish data validation processes among devices, excluding any unknown systems (e.g. source node origin validation, MAC address filtering, etc.).
- Request the implementation of required basic security features to vendors (e.g. authentication or data validation).

Measure of success: the systems' security is increased as many threats have been mitigated. This can be measured via risk assessment, vulnerability assessment or penetration test.

Stakeholders involved: system designers, manufacturers, vendors, top management.

8.2.2 Recommendation 2: Identify and establish roles of people operating in ICS/SCADA systems

Description: The management of privileges of users in an ICS/SCADA system is a critical process. It is necessary to ensure that users only have access to those systems and functions that are required for their daily work assignments. Uncontrolled or unverified access privileges can give place to unauthorized access and increase the risk of insider attacks carried out by disgruntled employees.

Steps: in order to manage the privilege and role assignments to the employees, it is necessary to define the roles of the users and the profiles from the different areas, as well as control means to ensure that they are correctly applied and cannot be manipulated by the employees themselves. Recommendations:

- Limit privileges on a need-to-know basis.
- Any temporary privileges must be revoked as soon as they are no longer necessary.
- External contractors and maintenance personnel must have specific access, which must only be active during their intervention and remain disabled the rest of the time.
- If shared accounts are needed (e.g. limited system capabilities), controls must be put in place to register and control the accesses made to these systems.
- Verification of new employees via background checks during the incorporation process, as well as defining exit interviews when leaving the organisation.

Measure of success: Increased security of the ICS/SCADA systems and avoid unauthorized access.

Stakeholders involved: asset owners, operators, technicians, maintenance personnel.

8.2.3 Recommendation 3: Define network communication technologies and architecture with interoperability in mind

Description: ICS/SCADA systems are becoming more and more interconnected to other systems, not only within the same organizations but also with external ones, both from the same country and from other countries. This can be observed more commonly in some sectors (e.g. energy), but the tendency is to extend to all. This leads to the need to establish compatible means of communication between them that guarantee the veracity and security of the communications, resulting in better operations from both parts (and avoiding issues from miscommunications, which could result even on cascade effects).

Steps: in order to achieve proper intercommunication of the systems from different organizations (within the same country or in different other countries), ensuring efficient, secure and verifiable communications, the following should take place:

- Identify systems, infrastructures and environments that require intercommunication with other systems (internal or external), or that may require this intercommunication within the near future (considering the lifecycle of the devices involved).
- Select protocols that are compatible with the systems identified and the systems from the other organizations or environments. These can be proprietary or open-source protocols, as long as they are compatible with all devices involved; although it is preferred if their internal workings are available as to define security measures and ensure the compatibility.

Measure of success: the systems interconnected or to be interconnected make use of common compatible protocols that are interoperable with other systems. A risk analysis alongside a vulnerability assessment can help to identify which protocols can be used, what risks they involve and how to solve them.

Stakeholders involved: asset owners, operators, technicians.

8.2.4 Recommendation 4: Establish brainstorming and communication channels for the different participants on the lifecycle of the devices to exchange needs and solutions

Description: another point that was often raised in the interviews with key stakeholders and asset owners was the fact that there is a lack of communication between the different participants in the lifecycle of the SCADA assets (manufacturers, vendors, implementers and operators). This leads to the need to establish mechanisms to allow them to better communicate their needs and considerations to increase the commitment of the top management for investment regarding the security of ICS/SCADA systems.

Steps: It requires the implementation of new communication channels:

- Collaborative environments that allow the exchange of information between different parties.
- Identification and exchange in a common platform of the main attack vectors.

Measure of success: increased security communications and working on exchange the vulnerabilities and attacks founded.

Stakeholders involved: asset owners, operators, technicians, maintenance personnel.

8.2.5 Recommendation 5: Include the periodic ICS/SCADA device update process as part of the main operations of the systems

Description: the process of updating the software and firmware of ICS/SCADA devices is a relatively new concept, as it was not needed as much in the past, when there were no network intercommunications between them. Nowadays, these systems tend to be interconnected, depending on their communications to properly carry out their functions. This interconnection is open to a range of threats previously unknown for the sector and which can be mitigated by adding security measures and updating the software/firmware of the devices to fix weaknesses and vulnerabilities. However, the update process is not usually straightforward, and the risk of device corruption or failure acts as a deterrent for operators to apply these

updates, regardless of the low likelihood of this happening. The lack of support from manufacturers in this sense is also another constraint.

Steps: in order to establish this update process for the SCADA devices, the following considerations should be taken into account:

- Identify the different devices that make up the ICS/SCADA network, determining their hardware version and their current software and firmware versions.
- Establish a communication channel with the manufacturers (if possible), to stay up-to-date on any new updates and patches released for the devices owned.
- Define the time periods when the updates are going to be implemented (e.g. periods of lower operations, maintenance times, etc.).
- Make use of redundant systems to maintain operations while main devices are being updated.
- Progressively deploy updates/patches in order to detect any issues early without affecting multiple devices.
- Establish a testing period to verify the correct implementation of the update and ensure that operations continue to run smoothly with the new updates applied.

Measure of success: devices are updated correctly and their implementation has no impact on the operations. Vulnerability audits can be used to verify if the vulnerabilities corrected by the update are no longer present (indicating an adequate update).

Stakeholders involved: asset owners, operators, technicians, top management.

8.2.6 Recommendation 6: Establish periodic ICS/SCADA security training and awareness campaign within the organization

Description: the security of the ICS/SCADA systems and infrastructures has become a must within most sectors, including critical infrastructures. While the concept is security which is already well known in other IT environments, it is not something common in this environment, as there was no need before (due to the lack of interconnections a few years ago). This means that the staff, operators, technicians, etc. are not aware in many cases of this need, the threats they are exposed to and how to prevent them.

Steps: establish training and awareness processes on a periodic basis in order to teach the staff the need for security:

- Awareness campaigns to inform users of the security concepts, both specific for ICS/SCADA systems and traditional IT systems.
- Specific security training to teach how to apply security measures and behaviours on the daily processes with the least impact possible.
- Triptychs that warn about new threats and risks, as well as acting as a reminder of the common security practices and functions (similarly to traditional workplace triptychs).

Measure of success: increased security awareness of the staff and personnel working on premises that interact, directly or indirectly, with the ICS/SCADA systems.

Stakeholders involved: asset owners, operators, technicians, maintenance personnel.

8.2.7 Recommendation 7: Promote increased collaboration amongst policy decision makers, manufacturers and operators at an EU Level

Description: nowadays, critical infrastructures have become linked with the cyberspace, taking advantage of the functionality and benefits it offers. However this brings about the need to make critical systems and infrastructures safer and more reliable, in order to protect them from the new threats that have arisen from this new interconnectivity level. This also needs to be addressed by policy makers, manufacturers and operators in order to ensure that they are aligned with this objective.

Steps: Promote the creation of an industrial control system professional community to help make the needs of operators more visible, serving as an invaluable aid for policy makers in order to ensure that they are aligned with other involved parties and that the measures provided are adequate and increase safety and reliability.

Measure of success: a greater level of collaboration is achieved in these parties, focusing on making critical systems safer and more reliable.

Stakeholders involved: asset owners, operators, technicians, maintenance personnel.

8.2.8 Recommendation 8: Define guidelines for the establishment of reliable and appropriate cybersecurity insurance requirements

Description: the critical infrastructure organizations are now more exposed than ever to threats and attackers worldwide due to the use of networks and even the Internet for SCADA communications. This opens a new scenario where insurance also appears to cover these risks, but it is not clear to what extent this can be helpful and what would be covered.

Steps: this process is similar to the one followed for the definition and establishment of procurement requirements:

- Identify the ICS/SCADA devices, assets, and network systems within the organizations' infrastructure.
- Carry out a risk analysis considering all these systems, devices and assets identified to determine the threats they are exposed to, their likelihood and impact.
- Determine the security measures that are implemented to mitigate these threats (directly or indirectly).
- List the security measures that are to be implemented in the following months/years to improve the security of these devices.
- Obtain the overall risk to these devices considering the initial risk analysis and the mitigation factor of the security measures in place/to be implemented. This provides the residual risk.
- With the direct participation of the top management, determine which risks are acceptable and which need to be covered.
- Those that need to be covered but are not with technical security measures can be requested to be covered with a cyber-insurance. This should stablish the scope, compensations and coverage exceptions.

Measure of success: carry out periodic risk analysis to ensure that the security is within acceptable levels, taking into account not only security measures in place, but also the coverage of the cyber-insurance.

Stakeholders involved: assets owners, operators, top management.

9. Annex - ISA95 levels overview

9.1.1 ISA95 level 1: Production and Control processes

This level (level 1) encompasses all the detection and manipulation physical processes that are in use within the SCADA systems and devices. Most of the hardware elements that can be found in this level are either PLCs or RTUs [60].

The activities within this level do not usually interact directly with the production processes, but can have an indirect effect as any detection and manipulation activity can impact the production processes' status, efficiency and/or configuration. As an example, data from the sensors does not usually feed into the production process, but the values detected can have a direct impact on it. It is important to take into account that this may change in Industry 4.0 environments.

Hardware and Software

There are multiple assets in use within production and control processes; their function is usually to be connected to field control devices which acquire information by them about the physical process' status.

- **Actuators**: interact physically with the assets.
- **IED**: specific smart sensors and devices.
- **Local HMI**: locally control and supervise the processes.
- **PLC**: controls sensors and actuators.
- **RTU**: specific PLC in charge of remote communications.
- **Sensors**: obtain status information from the physical assets.

These control devices take real-world physical input signals from the sensors and instruments, converting the signals into digital data and making decisions based on programmed logic or commands from the system operators to turn other equipment on or off or to change system control parameters.

The software used in this may be off-the-shelf outdated versions or proprietary versions from each manufacturer and their algorithms, internal functions or workings are seldom shared with external sources, except for interoperability purposes. This software is oriented to execute, in real time, all industrial processes, controls and checks needed (e.g. temperature controls). Due to their nature, this software usually makes use of an 'upload and execute' functionality in order to provide further automation of these tasks.

9.1.2 ISA95 level 2: Supervision and monitoring

This level (level 2) covers follow-up activities including monitoring and supervision of the physical control processes. The supervision and monitoring activities carried out at in this level aim to review the interaction that takes place in the control (automated and not automated) and production processes, which can last from a few minutes to as low as a fraction of a second [61]; therefore the devices within this level must be able to cover both extremes.

Hardware and Software

The existing devices in this level use graphic representations of the information gathered during the previous level and provide the distribution of the communication among the different levels. The most relevant hardware devices found in this level include:

- **Centralized HMI**: in charge of controlling the different production systems under supervision.

- **MMI**: similarly to HMI, it is used by operators and technicians to interact with processes.
- **Switches / Gateways**: network devices designed to control and manage the network segments where the supervised processes are located.

The software in this level is usually capable of providing monitoring, supervision and control capabilities, as well as processing the registration and interaction of the data not only with other systems but also with operators through the use of intuitive or easy-to-understand graphic interfaces that provide current status in real time. As it was the case in the previous level, it is common to find these applications running on obsolete OS versions (either old Windows/Linux versions or proprietary ones).

9.1.3 ISA95 level 3: Operation management

The activities needed for the workflow to produce the desired end-products are defined within this level (level 3). The systems covered in this level include those that are tasked with the execution of the manufacture processes (also known as Manufacturing Execution Systems, or MES), and those in charge of the management of the manufacture operations. This stage includes the programming, detailing, production administration and reliability check processes. The workflow optimisation processes should also be included within this level.

Hardware and Software

There are multiple devices and systems that can be used within this level, including several possible communication network varieties as well.

The most relevant systems include:

- **Domain controllers**: managing the assignment of addresses and domains over the SCADA networks.
- **Physical Security appliances**: Firewalls, IDS/IPS, network analysis and sandboxing solutions.
- **SCADA servers**: including data historian and MES.
- **Servers**: containing business functionalities, applications and other functionalities.

The communication networks that can be used include one or several of:

- Internal networks or enterprise LAN.
- Internal operational networks.
- Public networks and the Internet.
- Demilitarized Zones (DMZs) within internal and external networks.

These networks can be used individually for specific uses or a combination of several of them (even all of them in very large scenarios). The use of DMZ is not compulsory but highly recommended in order to safely interconnect internal and external networks when internal services have to be available from external networks. The use of security devices and systems (such as Firewalls or IDS/IPS) is mandatory in any case, regardless of the communication network in use.

The software in use varies from one device to another, especially as they mostly make use of proprietary technology. As in previous levels, it is common to find these applications running on obsolete OS versions (old Windows, Linux or proprietary OS). However, there are two cases whose function are worth describing:

- **Data Historian**: its software is in charge of saving, storing and safeguarding all process data, the status of digital and analogic variables, and any other type of information generated from industrial

processes or their associated infrastructure systems and devices. It is also used as a Batch system in environments based on the management of lots of production across an information system.

- **Manufacturing Execution Systems** (MES): allows the management and optimisation of industrial environments in real-time. It is capable of bi-directionally joining other systems including ERP, CRM, DRP and real-time SCADA devices.

9.1.4 ISA95 level 4: Operation business management

All business-related activities [62] needed to manage a manufacturing organisation are defined in this level (level 4). The ERP systems and other business solutions in relation to planning and the logistics are also usually located within this level. The basic programming of the plant is established here, as well as the use of materials and their distribution in processes that may last days, weeks or even months.

From an industrial cybersecurity perspective, the networks in use within this business environment are considered insecure, as they contain a large number of varied systems and applications, including remote access and external communication solutions. The systems on this network should be separated from operational networks, and if interconnections are needed, they should be tightly controlled, monitored and supervised.

Hardware and Software

The hardware and software devices and systems that are used at this level are not specific ones, but the same as the ones used in other IT areas (computers, tablets, etc.). These systems have been exposed to the Internet and public/private network for a long time, and as such they tend to be more prepared against these threats and have more mitigation measures available.

Some of the most common hardware systems used include:

- **End-user devices**: workstations and corporate laptops.
- **Mobile end-user devices**: smartphones, tablets, PDAs or similar devices.
- **Servers**: containing high-level management applications and operation functions.
- **Wireless networks**: routers, access points, repeaters, etc.

There are many common software applications and solutions that can be used at this level. Among these, there are several solutions that are specific for this area:

- **Enterprise Resource Planning** (ERP): a solution that can integrate one or several business phases (such as planning, manufacturing, sales or finances) [8].
- **Control Room Management** (CRM): used by any controller/operator working in a control room, monitoring and controlling all parts of a pipeline system through a SCADA system [63].
- **Business Intelligence** (BI): is the software designed to analyse business data to better understand an organization's strengths and weaknesses, in addiction it plays a key role in the strategic planning process of the corporation [64].

10. Annex – Known SCADA Exploits

The following table presents a list of some of the exploits known for various different SCADA assets, alongside with references to their technical details:

Table 17: Known SCADA exploits [65]

METASPLOIT	ASSET AFFECTED	REFERENCE
exploit/windows/scada/igss9_igssdataserver_listall.rb exploit/windows/scada/igss9_igssdataserver_rename.rb exploit/windows/scada/igss9_misc.rb auxiliary/admin/scada/igss_exec_17.rb	IGSS	ICS-11-080-03 [66] ICSA-11-132-01A [67]
exploit/windows/scada/daq_factory_bof.rb	DAQ Factory	[68]
exploit/windows/scada/codesys_web_server.rb	CoDeSys	[69]
exploit/windows/fileformat/bacnet_csv.rb	OPC Client	ICSA-10-264-01 [70]
exploit/windows/browser/teechart_pro.rb	Operator Workstation	N/A
auxiliary/dos/scada/beckhoff_twincat.rb	TwinCat	[71]
auxiliary/gather/d20pass.rb	D20 PLC	[72]
unstable-modules/auxiliary/d20tftpbd.rb	DigitalBond S4	[73]
exploit/windows/scada/iconics_genbroker.rb exploit/windows/scada/iconics_webhmi_setactivexguid.rb exploit/windows/scada/iconics_webhmi_setactivexguid.rb	Genesis32	ICS-11-080-02 [74]
exploit/windows/scada/scadapro_cmdexe.rb	ScadaPro	[75]
exploit/windows/scada/moxa_mdmtool.rb	Device Manager	ICSA-10-301-01 [76]
exploit/windows/scada/realwin.rb	RealWIN SCADA	N/A
exploit/windows/scada/realwin_scpc_initialize.rb exploit/windows/scada/realwin_scpc_initialize_rf.rb	RealWIN SCADA	ICS-11-305-01 [77] ICSA-11-313-01 [78]
exploit/windows/scada/realwin_scpc_txtevent.rb	RealWIN SCADA	N/A
exploit/windows/scada/realwin_on_fc_binfile_a.rb exploit/windows/scada/realwin_on_fcs_login.rb	RealWIN SCADA	ICS-11-080-04 [79] ICSA-11-110-01 [80]
exploit/windows/scada/procyon_core_server.rb	Procyon	[81]
exploit/windows/fileformat/scadaphone_zip.rb	ModbusTagServer ScadaPhone	[82]
exploit/windows/scada/citect_scada_odbc.rb	CitectSCADA CitectFacilities	N/A
exploit/windows/scada/winlog_runtime.rb	Winlog	ICSA-11-017-02 [83]
exploit/windows/scada/factorylink_cssservice.rb exploit/windows/scada/factorylink_vrn_09.rb	FactoryLink	ICS-11-080-01 [84] ICSA-11-091-01A [85]
exploit/exploits/windows/browser/teechart_pro.rb	OPC Server	N/A

11. Annex – Known Threats affecting ICS/SCADA systems

THREATS	DESCRIPTION	LIKELIHOOD	IMPORTANCE
Malware (Virus, Trojan, Worms)	Software programs designed to carry out unwanted and unauthorized actions on a system without the consent of the user, resulting in damage, corruption or information theft. Its impact can be severe, and it has been observed that malware can either be common or customised. This type of attacks, especially worms, affect a wide range of assets, from SCADA systems to standard systems.	Very high	High
Exploit Kits and rootkits	An exploit is a specially crafted code designed to take advantage of a vulnerability in order to gain access to a system. It is one of the most important threat to ICS/SCADA networks, as it can be used by low-skilled attackers as well, and they are difficult to be detected.	Medium	High
Advanced Persistent Threats (APTs)	Attacks designed for a specific target that occur over a long period of time, and are usually carried out in multiple stages. The main objective is to remain hidden and obtain as much information, sensitive data or control in order to achieve the goal of the attack. While the likelihood of this attack is low, it is important to take into account the difficulty of detecting them, which usually takes a long time. They are designed for many scenarios, such as stealing sensitive or proprietary information or disrupting operations.	Low	High
Insider Threat (Internal employee incidents)	An employee, contractor or third party that has access to restricted internal systems makes use of this advantage to steal, modify or access without authorization these systems or other that can be accessible through them.	Low	Crucial
Eavesdropping, (MitM, SCADA communication hijacking)	Unauthorized real-time interception of a private communication, such as a phone call, instant messaging session, videoconference or e-mail communications. In this environment, it can also include the interception of SCADA communications, e.g. control commands and even their modification for unauthorized purposes.	Low	High / Crucial
Communication systems (network) outage	An interruption or failure in the network supply, either intentional or accidental. Depending on the network segment affected and the time it requires to recover the communications, the importance of this threat can range from high to critical.	Low	High / Crucial
(Distributed) Denial of Service	This attack consists of multiple systems 'attacking' to a single target in order to saturate it and make it crash. This can be done merely by trying to make too many connections, flooding a communication channel or replaying the same communications over and over. It is of **high** importance if SCADA devices are affected by this attack and may cause a cease of operations.	Low	Medium / High
Data / Sensitive information leakage	Sensitive data is revealed, intentionally or not, to unauthorized parties. The importance of this threat can vary greatly, depending on the kind of data leaked: • **Medium**: standard operational data, internal procedures. • **High**: business data, private user data or industrial property.	Low	Medium / High

12. References / Bibliography

[1] "ISA-95.01 Enterprise-Control Systems Integration," [Online]. Available: www.isa-95.com.

[2] SANS ICS, "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense User Case," E-ISAC, 2016.

[3] NIST, "NIST Special Publication 800-82 Revision 2Guide to Industrial Control Systems," [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[4] "standard ISA 95," [Online]. Available: https://isa-95.com/.

[5] ISA 99 Committee, "ISA 99 Committee Wiki," [Online]. Available: http://isa99.isa.org/ISA99%20Wiki/Home.aspx. [Accessed 19 July 2016].

[6] "standard ISA 99," [Online]. Available: https://isa-99.com/.

[7] D. Clark, *ISA S95: What is it? Why is it Important?,* Invensys Operations Management, 2010.

[8] D. Brandl, *Industrial Best Practices of Manufacturing Information Technologies with ISA-95 Models,* BR&L Consulting, 2008.

[9] K. Stouffer, J. Falco and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," June 2011.

[10] H. Menashri and G. Baram, "Critical Infrastructures and their Interdependence in a Cyber Attack - The Case of the U.S.," March 2015.

[11] P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, "Critical Infrastructure Interdependency Modeling: A survey of U.S. and International Research," 2006.

[12] C. Alcaraz, G. Fernandez and F. Carvajal, "Security Aspects of SCADA and DCS Environments," in *Critical Infrastructure Protection*, Springer Berlin Heidelberg, 2012, pp. 120-149.

[13] Theodora, "Europe Pipelines map," [Online]. Available: http://www.theodora.com/pipelines/europe_oil_gas_and_products_pipelines.html. [Accessed 1 July 2016].

[14] Electricity Information Sharing and Analysis Center, "Analysis of the Cyber Attack on the Ukrainian Power Grid," 2016.

[15] V. Gungor and F. Lambert, A survey on communication networks for eelctry system automation, Computer networks: The International Journal of Computer and Telecommunications Networking, ACM, No7, vol 50, 2006.

[16] IBM Corporation, “ISS,” [Online]. Available: http://www.iss.net/documents/whitepapers/SCADA.pdf. [Accessed 4 July 2016].

[17] M. Smith, Web-based Monitoring & Control for OilGas Industry, SCADA’s Next Step Forward, Pipeline & Gas Journal, 2001.

[18] B. Qiu and B. Gooi, Web-based SCADA display systems (WSDS) for access via Internet, IEEE Transactions on Power Systems, Vol. 5, No. 2, 2000.

[19] WiMAX Forum, “WiMAX Forum website,” [Online]. Available: http://www.wimaxforum.org. [Accessed 7 July 2016].

[20] C. Faulkner, “Techradar - What is NFC? Everything you need to know,” [Online]. Available: http://www.techradar.com/news/phone-and-communications/what-is-nfc-and-why-is-it-in-your-phone-948410. [Accessed 7 July 2016].

[21] MCA Sistemas, “SCADABR Automação Open Source,” 2012. [Online]. Available: http://www.scadabr.com.br/. [Accessed 15 09 2016].

[22] Schneider Electric, “IGSS FREE50,” 2016. [Online]. Available: http://igss.schneider-electric.com/products/igss/download/free-scada.aspx. [Accessed 15 09 2016].

[23] Enscada, “IndigoSCADA Section,” 2016. [Online]. Available: http://www.enscada.com/a7khg9/IndigoSCADA.html. [Accessed 15 09 2016].

[24] SCADA.SL, “SCADA STRANGE LOVE,” [Online]. Available: http://scada.sl/. [Accessed 09 09 2016].

[25] TeslaSCADA, “TeslaMultiSCADA - SCADA for Android to connect Modbus, Ethernet/IP, Siemens,” 2016. [Online]. Available: http://www.teslascada.com/index.php/en/products/teslamultiscada. [Accessed 15 09 2016].

[26] University of Michigan, “Censys,” [Online]. Available: https://www.censys.io/. [Accessed 09 09 2016].

[27] Digitalbond, “Redpoint: Digital Bond's ICS Enumeration Tools,” [Online]. Available: https://github.com/digitalbond/Redpoint. [Accessed 4 10 2016].

[28] scadastrangelove, “SCADAPASS,” [Online]. Available: https://github.com/scadastrangelove/SCADAPASS. [Accessed 09 09 2016].

[29] SCADAhacker, “SCADA Hackers' Toolset,” [Online]. Available: https://scadahacker.com/tools.html. [Accessed 18 07 2016].

[30] Shodan, “SHODAN.IO Search Engine,” [Online]. Available: https://www.shodan.io. [Accessed 22 06 2016].

[31] nmap, “backnet-info,” 2016. [Online]. Available: https://nmap.org/nsedoc/scripts/bacnet-info.html. [Accessed 12 09 2016].

[32] Linux Foundation, “IoTivity,” 2016. [Online]. Available: https://www.iotivity.org/about. [Accessed 22 08 2016].

[33] TACIT Consortium - European Commission, “Threat Assessment framework for Critical Infrastrucutres proTection (TACIT),” [Online]. Available: http://www.tacit-project.eu/.

[34] Linux Foundation, “Civil Infrastructure Platform (CIP),” 2016. [Online]. Available: https://www.cip-project.org/about. [Accessed 22 08 2016].

[35] S. Corporation, “Internet Security Threat Report | Appendices,” VOLUME 21, APRIL 2016.

[36] Kaspersky Lab, “Industrial Control Systems Vulnerabilities Statistics,” 2015.

[37] Patriot-Tech, “Common SCADA System Threats and Vulnerabilities,” 27 10 2015. [Online]. Available: http://patriot-tech.com/common-scada-system-threats-and-vulnerabilities/. [Accessed 14 June 2016].

[38] Thales UK Ltd White paper, “Cyber Security for SCADA Systems,” 2013.

[39] Schneider Electric, “SCADA systems White paper,” 2012.

[40] SANS Institute, “Security for Critical Infrastructure SCADA systems,” 2005.

[41] Homeland Security News Wire, “Cyber mishap causes nuclear power plant shutdown,” 2008. [Online]. Available: http://www.homelandsecuritynewswire.com/cyber-mishap-causes-nuclear-power-plant-shutdown. [Accessed 17 10 2016].

[42] The Decatur Daily, “Cyber threat at Browns Ferry?,” 2007. [Online]. Available: http://legacy.decaturdaily.com/decaturdaily/news/070518/threat.shtml. [Accessed 17 10 2016].

[43] B. Zhu, A. Joseph and S. Sastry, “A Taxonomy of Cyber Attacks on SCADA Systems,” Departmen of Electrical Engineering and Computer Sciences. University of California, Berkley, CA, 2012.

[44] ENISA, “Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors,” 2015.

[45] INCIBE, “Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA),” 2012.

[46] C. Alzaraz, G. Fernández, R. Román, Á. Balastegui and J. López, “Gestión Segura de Redes SCADA,” 2008.

[47] Organization for Security and Co-operation in Europe (OSCE), “Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace,” 2013.

[48] American Gas Association (AGA), Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan, 2006.

[49] WGC6 - Substations Working Group C6, “Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links,” IEEE Project, 2013. [Online]. Available: https://standards.ieee.org/develop/project/1711.html. [Accessed 04 10 2016].

[50] CERTSI, “Cert de Seguridad e Industria,” [Online]. Available: https://www.certsi.es/blog/normativas-seguridad-sistemas-control. [Accessed 19 July 2016].

[51] F. Cleveland, “IEC 62351 security standards for the power system information infrastructure,” *IEC TC57 WG15 Security Standards,* vol. 14, 2012.

[52] Red IRIS., “Kerberos,” [Online]. Available: https://www.rediris.es/cert/doc/unixsec/node27.html. [Accessed 06 09 2016].

[53] M. K. a. R. Bhandhari, “Classification of EAP methods and Some Major Attacks on EAP,” 2016.

[54] CCN-CERT, “LEAP - Lightweight Extensible Authentication Protocol,” [Online]. Available: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=576.html. [Accessed 06 09 2016].

[55] Microsoft, “Protected Extensible Authentication Protocol (PEAP),” [Online]. Available: https://msdn.microsoft.com/es-es/library/ms883449.aspx. [Accessed 06 09 2016].

[56] ENISA, “Can we learn from SCADA security incidents?,” 2013. [Online]. Available: https://www.enisa.europa.eu/publications/can-we-learn-from-scada-security-incidents.

[57] C. W. Johnson, R. Harkness and M. Evangelopoulou, “Forensic Attacks Analysis and the Cyber Security of Safety-Critical Industrial Control Systems,” in *34th International System Safety Conference*, Florida, 2016.

[58] SANS Institute, “Forensic Analysis of Industrial control Systems,” 2015.

[59] M. Abrams and J. Weiss, “Malicious Control System Cyber Security Attack Case Study,” NIST, Australia, 2008.

[60] K. Stouffer, J. Falco and K. Kent, “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security,” September 2006.

[61] R. Mahan, J. Fluckiger, S. Clements, C. Tews, J. Burnette, C. Goranson and H. Kirkham, “Secure Data Transfer Guidance for Industrial Control and SCADA Systems,” September 2011.

[62] D. Brandl and P. Owen, *Manufacturing Operations Management,* University of Cambridge, institute for Manufacturing, 2003.

[63] W. McGaughey, “CRM Control Room Management,” 2009.

[64] J. Theron, “ISA-95: A Foundation Model for Business Intelligence for Manufacturing,” 2008.

[65] SCADA HACKER, “Metasploit Modules for SCADA-related Vulnerabilities,” [Online]. Available: https://scadahacker.com/resources/msf-scada.html. [Accessed 09 09 2016].

[66] ICS-CERT, “ICS-ALERT-11-080-03,” 2014. [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-080-03. [Accessed 12 09 2016].

[67] ICS-CERT, “ICSA-11-132-01A,” 2013. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-11-132-01A. [Accessed 12 09 2016].

[68] “AzeoTech DAQFactory NETB Datagram Parsing Buffer Overflow Vulnerabilities,” 2011. [Online]. Available: https://scadahacker.com/vulndb/2011/ics-vuln-azeotech-11-256-02.html. [Accessed 12 09 2016].

[69] “3S CoDeSys Multiple Vulnerabilities,” 2012. [Online]. Available: https://scadahacker.com/vulndb/2011/ics-vuln-3s-11-336-01.html. [Accessed 12 09 2016].

[70] ICS-CERT, “ICSA-10-264-01,” 2014. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-10-264-01. [Accessed 12 09 2016].

[71] “Beckhoff TwinCAT Network Packet Denial of Service Vulnerability,” 2011. [Online]. Available: https://scadahacker.com/vulndb/2011/ics-vuln-beckhoff-11-256-06.html. [Accessed 12 09 2016].

[72] Rapid7, “Measuresoft ScadaPro Remote Command Execution,” 2011. [Online]. Available: https://www.rapid7.com/db/modules/exploit/windows/scada/scadapro_cmdexe. [Accessed 09 09 2016].

[73] Digital Bond, “Metasploit Modules,” 2016. [Online]. Available: http://www.digitalbond.com/tools/basecamp/metasploit-modules/. [Accessed 12 09 2016].

[74] ICS-CERT, “ICS-ALERT-11-080-02,” 2014. [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-080-02. [Accessed 12 09 2016].

[75] “Measuresoft ScadaPro Multiple Vulnerabilities,” 2011. [Online]. Available: https://scadahacker.com/vulndb/2011/ics-vuln-measuresoft-11-256-04.html. [Accessed 12 09 2016].

[76] ICS-CERT, “ICSA-10-301-01A,” 2015. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-10-301-01A. [Accessed 12 09 2016].

[77] ICS-CERT, “ICS-ALERT-10-305-01,” 2013. [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-10-305-01. [Accessed 12 09 2016].

[78] ICS-CERT, “ICSA-10-313-01,” 2014. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-10-313-01. [Accessed 12 09 2016].

[79] ICS-CERT, “ICS-ALERT-11-080-04,” 2014. [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-080-04. [Accessed 12 09 2016].

[80] ICS-CERT, “ICSA-11-011-01,” 2014. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-11-110-01. [Accessed 12 09 2016].

[81] “Scadatec Procyon Stack Buffer Overflow Vulnerability,” 2011. [Online]. Available: https://scadahacker.com/vulndb/2011/ics-vuln-scadatec-11-216-01.html. [Accessed 12 09 2016].

[82] “ScadaTEC Modbus TagServer and ScadaPhone Remote Buffer Overflow Vulnerability,” 2011. [Online]. Available: http://www.scadahacker.com/vulndb/2011/ics-vuln-scadatec-11-255-01.html. [Accessed 12 09 2016].

[83] ICS-CERT, “ICSA-11-017-02,” 2014. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-11-017-02. [Accessed 12 09 2016].

[84] ICS-CERT, “ICS-ALERT-11-080-01,” 2014. [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-080-01. [Accessed 12 09 2016].

[85] ICS-CERT, “ICSA-11-091-01A,” 2014. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-11-091-01A. [Accessed 12 09 2016].

[86] Centre for the Protection of National Infraestructure CPNI, “Securing the move to IP-Based SCADA/PLC networks,” November 2011.

[87] Homeland Security, “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,” 2009.

[88] National Communications System, “Supervisory Control and Data Acquisition (SCADA) Systems,” 2004.

[89] Project SHINE, “SHodan INtelligence Extraction,” 2014.

[90] G. Tzokatzio, L. A. Maglaras, H. Janicke and Y. He, “Exploting SCADA vulnerabilities using a Human Interface Device,” 2015.

[91] GitHub, Inc, “How people build software - GitHub,” [Online]. Available: https://github.com. [Accessed 21 07 2016].

[92] Y. Sahu, “SCADA system vulnerabilities and threat to critical infrastructure”.

[93] Centre for the Protection of National Infrastructure CPNI, “Good Practice Guide. Process control and SCADA security,” 2008.

[94] AEGIS, “Automatak,” [Online]. Available: https://www.automatak.com/aegis/. [Accessed 09 09 2016].

[95] Digital Bond, “Digital Bond,” [Online]. Available: http://www.digitalbond.com/tools/basecamp/metasploit-modules/. [Accessed 09 09 2016].

[96] Rapid7, “New Metasploit Module to Exploit GE PLC SCADA Devices,” 2012. [Online]. Available: https://www.rapid7.com/docs/pr_2012-Digital-Bond_Rapid7_SCADA.pdf. [Accessed 12 09 2016].

[97] SCADA Security636, “The Metasploit SCADA modules and the modscan tool,” [Online]. Available: https://scadasecurity636.wordpress.com/2014/06/25/the-metasploit-scada-modules-and-the-modscan-tool/. [Accessed 09 09 2016].

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

TP-06-16-344-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-192-2
DOI: 10.2824/397676