Protocols and network security in ICS infrastructures

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

SPANISH NATIONAL CYBERSECURITY INSTITUTE

Authors

Miguel Herrero Collantes

Antonio López Padilla

First published in May 2015

Updated by CERTSI in February 2017

CERTSI_GUIA_SCI_001_ProtocolosRed_2017_v2

CONTENTS

1 INTRODUCTION

The growth of the Internet and the huge increase in devices with connectivity and processing capacities have brought new security challenges that also affect critical infrastructures. Such infrastructures, normally run by specific industrial control systems for monitoring and managing the processes typical of the industry concerned, are more and more exposed to interaction with other systems in the Internet environment. The trends in threat detection that have been observed lately have made it clear that industrial infrastructures have become a major target for attacks involving participants connected with terrorism, governments, industrial espionage and the like. One proof of this is the increasing appearance of incidents and events related to this kind of infrastructure, as may be seen from the following time line:

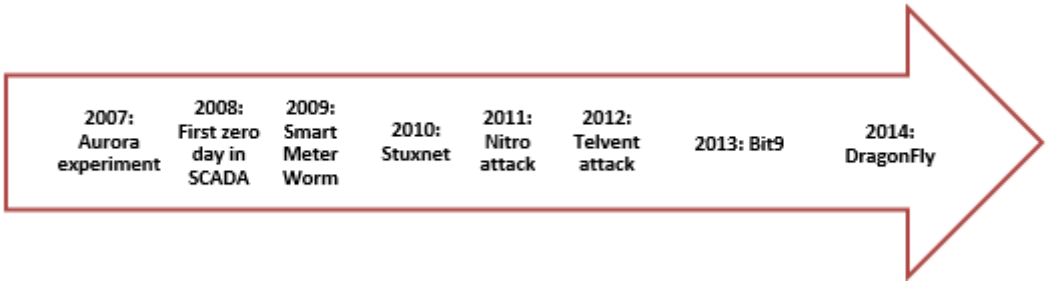

Illustration 1. ICS threats timeline

As stated by the expert Marina Krotofil[1], among the security community dealing with critical infrastructures it is clear that it is not enough just to put in place ordinary information technology (IT) security measures, such as perimeter protections and safe segmentation of networks. Similarly, unlike what happens with standard IT systems, in industrial systems it is dangerous to transfer a solution directly from one system to another, as the characteristics of the second may include factors that make such a direct integration vulnerable.

All this means that a detailed awareness of the protocols involved in industrial processes is crucial in understanding which weak points, attack vectors and possible defensive measures should be taken into account when implementing or enhancing an industrial control system.

1.1. ORGANIZATION OF THIS DOCUMENT

This document is made up of two chapters. In the first, on ICS Network architecture the intension is to provide readers with certain basic facts about how development of an industrial control system should be undertaken to ensure the greatest possible security.

[1] http://www.marinakrotofil.com/p/home.html

The second chapter, on communication Protocols in ICS, attempts to give a high-level overview of the design, operation and security characteristics of these various protocols. The study concentrates on the protocols most widely used in ICSs in Europe and above all in Spain, without distinctions between the various sectors of industry in which they are used. The aim is to give readers the knowledge they need to understand the properties, functionalities, strengths and weaknesses in their implementation and system monitoring. A set of specific security recommendations for each individual protocol are also outlined, although such security measures should be looked at carefully before being put into operation, so as not to affect operations.

2 ICS NETWORK ARCHITECTURE

From the point of view of security, when a network architecture is being designed it is always advisable to set up a model with differentiation of network segments. Separation of networks into sections with differing functions and purposes makes it possible to apply greater granularity in security measures and to avoid unnecessary flows of information.

Along the lines of such recommendations the network segment for industrial control systems (ICS) should be kept separate from the corporate network segment, as the nature of the traffic in these is obviously different. In the corporate network area there is a need for services, including access to the Internet, e-mail, file transfer protocols (FTP) and others, such that they would involve risks for the ICS network area.

Hence, an appropriate design with differentiated zones and mechanisms for controlling traffic between the various segments should always be the first step towards safe implementation of a network architecture.

Thus, it is advisable to establish different levels in the network architecture as an initial move in planning an ICS infrastructure. Each segment should be identified in accordance with its mission in the platform.

The ICS architecture that is put forward as a norm by the *International Society of Automation* (ISA) [1] in its ISA-95 standard on the integration of business and control systems is an example of this kind of separation by levels. This standard proposes a model called the Purdue Enterprise Reference Architecture, which establishes five logical levels on which elements of the architecture with different functions are to be grouped, as may be seen in Illustration 2. This proposal for segmentation simplifies the designing of security strategies that adopt specific measures on each of the levels and establish safe mechanisms for information flows among them.

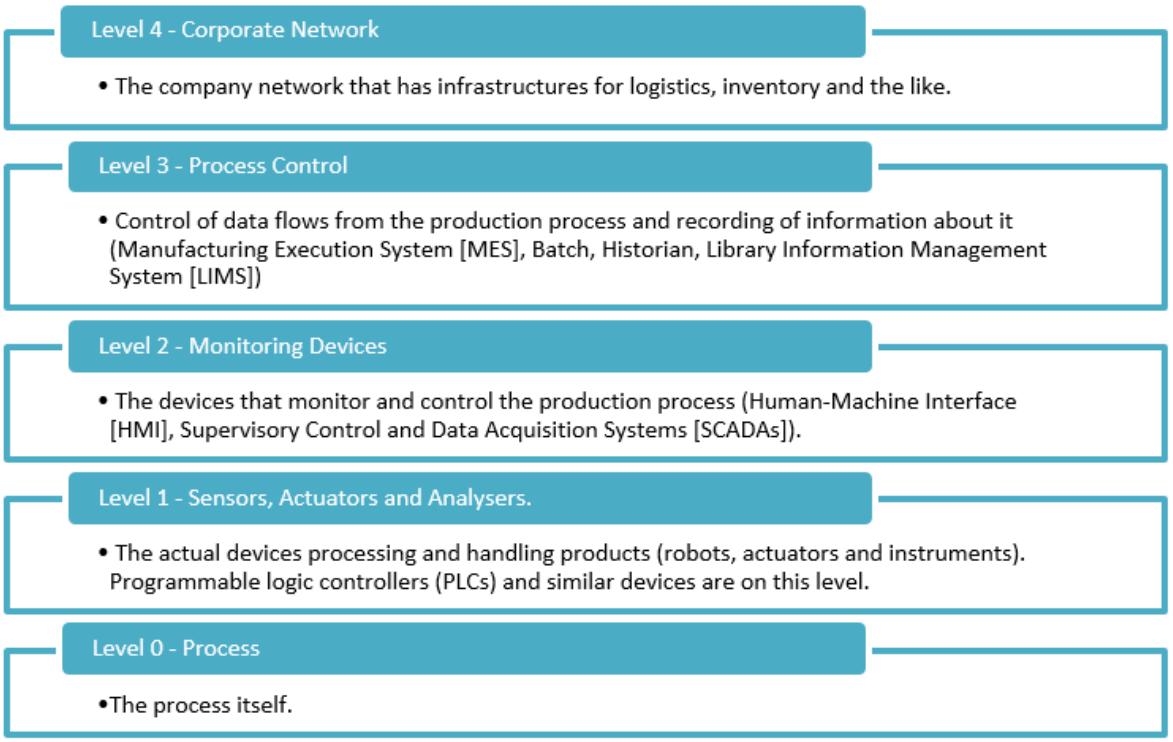

Illustration 2. ICS Reference Architecture

2.1. BASIC SECURITY IN DESIGNING AN ICS NETWORK

Based on a network architecture separated by zones, network should be divided into the number of segments needed in order to ensure they are differentiated and provided with appropriate security and traffic control arrangements. This separation is a concept that is both effective and essential when planning any network architecture and is equally applicable to industrial control systems. This sort of design, combined with suitable controls over data flows between the domains defined, will minimize the damage caused by any possible compromising of a device in a given domain.

2.2. NETWORK SECURITY

This objective may be achieved by incorporating the usual design solutions for separating and protecting network segments. This will take the following into account:

- **Segmentation into zones**, which means dividing the network architecture into zones differentiated by function so as to match as closely as possible the standards proposed in ISA-95. As may be seen from illustrati, there should be at the very least **three areas**, with separation of Network Control, the “demilitarized zone” (DMZ) and the corporate local area network (LAN). This measure allows an infection to be contained within a single zone, making it difficult for it to jump to other zones.
-

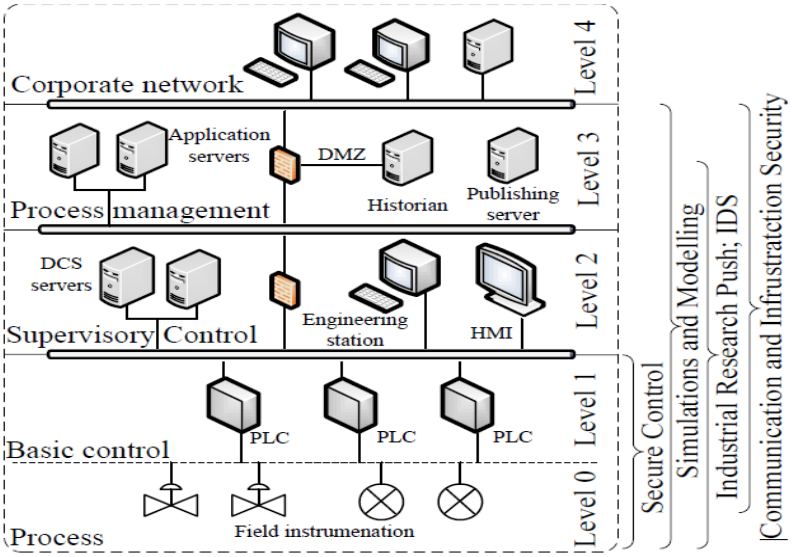

Illustration 3. A Reference Architecture for ICS [2] Matching the ISA-95 Model.

- **Encryption of communications and logical isolation** between network segments using virtual local area network (VLAN) and virtual private network (VPN) technologies. This measure also serves to avoid an infection jumping from one layer to another.
- **Control and filtering of traffic** by means of firewalls[2], proxies, and elements intended to identify and separate traffic and communications at the level both of the network (IP, routing) and of the port, protocol and applications layer. This measure will aid in detecting an infection when it attempts to change zone. If in addition the network has elements such as an intruder detection system (IDS) or security information and event management (SIEM) for controlling events, intruder alerts, and logs, its configuration will be on the lines shown in Illustration 4.

[2] General recommendations for rules for firewalls and other services may be found in Appendix I

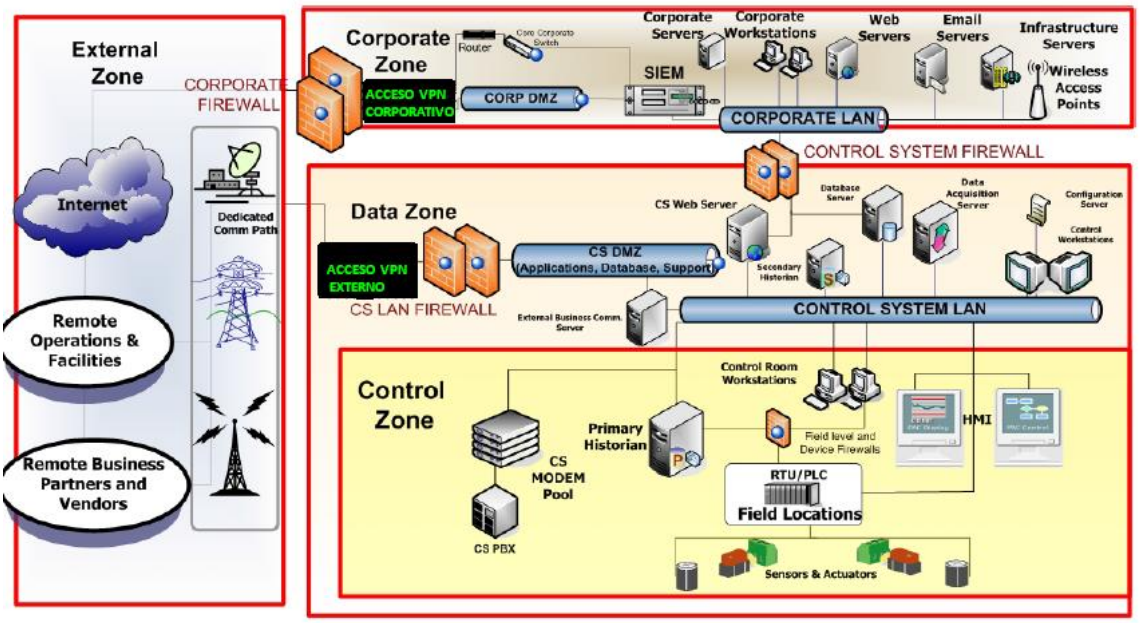

Illustration 4. Network Segmentation and Communications Controls [3]

- **Extending security to the data-link and application layers** brings in security measures for the data-link layer, such as access controls in accordance with 802.1x and filtering by media access control (MAC) address, and for the applications level through the use of a web application firewall (WAF).
- **Access control** based on whitelisting, implementing rules for access based on recognized elements and denying access to all others.
- **Wireless networks** involve an additional risk. Hence, they should be implemented only when absolutely necessary or because of a specific decision by the organization and always with clear justification. In their case, IEEE 802.1x mechanisms will be used for authentication, involving extensible authentication protocol transport layer security (EAP-TLS) that authenticates clients with certificates, or a RADIUS server may be used. Access points will be situated on networks that are isolated or have the minimum possible interconnections with the ICS control network (none at all if this can be achieved). A robust protocol for wireless communications, such as WPA2, will be in place and additionally a characteristic and unique service set identifier (SSID) will be used, with broadcast deactivated, but with filtering by MAC address in operation.

2.3. ENCRYPTION OF COMMUNICATIONS

Most industrial control protocols do not incorporate encryption in their implementation. Thus, any successful unauthorized access to the network would allow an attacker to inspect and manipulate traffic. For this reason, the use of hypertext transfer protocol secure (HTTPS), secure shell (SSH), and simple network management protocol (SNMP) Version 3 as far as this is possible is highly advisable for authentication and access to services on the network or to the devices composing it.

2.4. AUTHENTICATION AND ACCESS CONTROL

Appropriate management of privileges through role-based access control (RBAC)[3] is a measure that brings more security through restrictions set for each profile. Hence, the creation of various differentiated user profiles and the assignment of an operational role to each, depending on its functions, would be a worthwhile complement. Adding further measures, such as warning messages, helps to identify the service being accessed as a guard against possible unintentional errors.

2.5. REMOTE ACCESS

If access from infrastructures external to the control network is necessary, the use of VPN solutions would bring the encryption and authentication necessary to protect the connection. Specialized software, hardware, or both, should be used for remote access, together with suitable security policies in relation to updates, and to managing access and users.

2.6. AVAILABILITY

In a system controlling processes, latency and the speed of transmission of messages are critical. Hence, they are a factor that determines whether the design of the control network is able to face up to potential problems of congestion or loss of connectivity. Recommendations for enhancing the resilience of a network to these problems would be:

- Using switches that at network functionalities to segment a VLAN and prioritize certain types of traffic of the basis of quality of service criteria[4].
- Using redundant topologies to bolster availability, as also implementing the Spanning Tree Protocol (STP) to keep control of the formation of network loops.
- Using the internet group management protocol (IGMP)[5] together with a VLAN to provide better performance and restrict multicast messages in accordance with the type of traffic and the devices concerned

2.7. SECURITY MANAGEMENT POLICY

All the components contributing to the security of the infrastructure must get periodical monitoring and follow-up to determine whether there is a need for patches or updates, or there are other problems arising from the emergence of vulnerabilities or defects that may be detected in periods of functioning.

2.8. PHYSICAL SECURITY OF END-USER DEVICES

Restricting physical access to process control devices and to elements of the network is a necessary complement to restrictions on remote access and to authentication. Similarly,

[3] http://en.wikipedia.org/wiki/Role-based_access_control#RBAC_and_employees.27_responsibilities_alignment
[4] http://en.wikipedia.org/wiki/Quality_of_service
[5] http://es.wikipedia.org/wiki/Internet_Group_Management_Protocol

connection panels, cabling, power supplies, and similar items must be suitably protected against unauthorized access.

3 COMMUNICATION PROTOCOLS IN ICS

3.1. PROTOCOLS TO BE CONSIDERED

In this chapter the safety of communication protocols in the industrial control systems in widest use in Europe and more specifically in Spain will be considered, with no distinctions being made between the sectors in which individual protocols are most predominant. The protocols to be analyzed are the following:

- Common Industrial Protocol (CIP).
- MODBUS
- DNP3
- Profibus
- Profinet
- PowerLink Ethernet
- OPC
- EtherCAT

3.2. LAYERS OF OPERATION OF PROTOCOLS

Although the seven-layer OSI model of the International Standards Organization is very popular, this document will use the TCP/IP model of just four layers will be used so as to simplify analysis and comparison.

The four layers are:

- The application layer: comparable to Layers 5, 6 and 7 of the OSI model.
- The transport layer: similar to Layer 4 of the OSI model.
- The internet layer: equivalent to Layer 3 of the OSI model.
- The network access layer: comparable to Layers 1 and 2 of the OSI model.

A comparison between the OSI and TCP/IP models may be seen in Illustration 5.

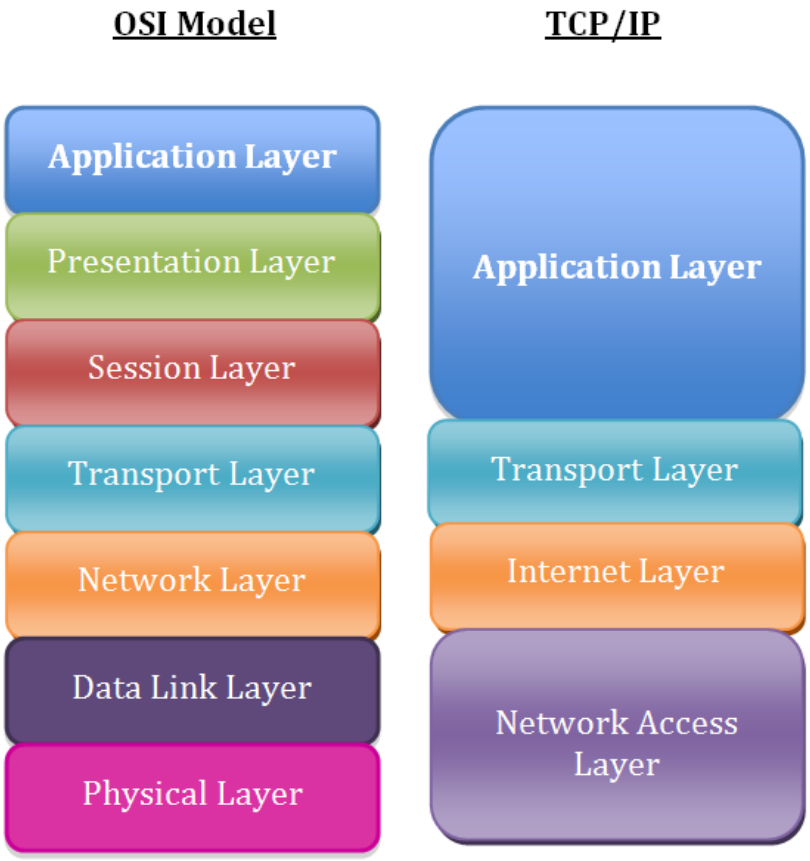

Illustration 5: Relationship between the OSI and TCP/IP Models

Layer 1 in this model, the network access layer, is responsible for the transmission of individual bits between stations and so includes measures to check that bits have been correctly transmitted. However, it contains no security measures properly so called at this point. It does also have security mechanisms, such as 802.1x, to check that access to the network is gained only by authenticated devices.

As each of the protocols is considered individually, an analysis will be given of the specific security measures of the higher layers, complementary to the generic measures of the network access layer.

3.3. COMMON INDUSTRIAL PROTOCOL (CIP)

3.3.1. Description

The Common Industrial Protocol (CIP) is a protocol created by the ODVA company[6] for automating industrial processes. CIP comprises a set of services and messages for control, security, synchronization, configuration, information, and so forth which can be integrated into Ethernet networks and into the Internet. CIP has a number of adaptations, providing intercommunication and integration for different types of networks. These are:

- **Ethernet/IP**: an adaptation of CIP to TCP/IP.
- **ControlNet**: an integration of CIP with concurrent time domain, multiple access (CTDMA) technologies.
- **DeviceNet**: an adaptation of CIP with controller area network (CAN).
- **CompoNet:** a version adapted to time division multiple access (TDMA) technologies.

An indication of how the various different families of this protocol fit the OSI model, with their levels of equivalence, may be seen in Illustration 6.

[6]https://www.odva.org/

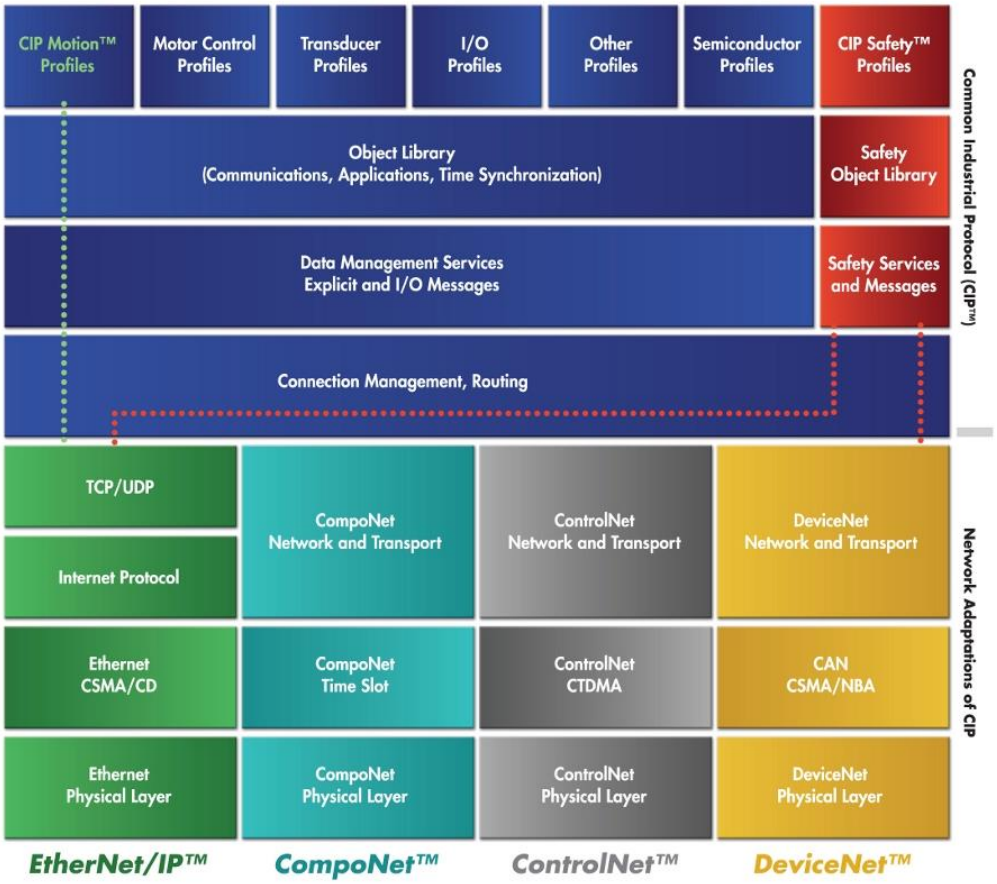

Illustration 6. How the CIP Architecture Fits the OSI Model for Networks. Source: odva.org

3.3.1.1. The CIP Model for Objects

CIP is a protocol that follows a *model for objects*. Each object is made up of attributes (data), services (commands), connections and behavior (the relationships between data and services). CIP has an extensive range of objects to cover typical communications and functions with common elements in automation processes, such as analog and digital input or output devices, HMI, movement controls and so forth. To ensure intercommunication, any given CIP object implemented on different devices must behave identically on all, which constitutes what is termed a “device profile”. Hence, any device that takes on a profile will respond in the same way to any given command and have the same network behavior as any other device with the same profile.

3.3.1.2. CIP Messages

CIP follows a *producer-consumer* pattern. This type of architecture, unlike the older origin-destination format, is of a *multicast type*. This means that messages are put into circulation by a producer and it is the various consumer nodes in the network that decide whether a given message is for them or not, on the basis of an identifier field that accompanies messages.

Thus, two types of message can be distinguished, more or less identified with one of the two architectures:

- Implicit messages (Illustration 7), which have only an identifier rather than origin and destination addresses, so that it is the consumer nodes that known whether the message concerns them and what action to take if so, on the basis of this identifier.

- Explicit messages (Illsutration 8), which contain information about the origin and destination addresses for devices and information about a specific action as in an IP model.

Some implementations of CIP, such as Ethernet/IP or ControlNet do also make some use of explicit messages.

Illustration 7. The producer-consumer model of message (multicast)

Illustration 8.The Origin-Destination Model of Message.

3.3.2. Implementations of CIP: DeviceNET, ControlNET and CompoNET

3.3.2.1. Description

These families of CIP technologies use different media for transmissions. Respectively, they use a CAN bus[7], coaxial RG-6[8] and round cables (replacing flat cables[9]).

[7]http://en.wikipedia.org/wiki/CAN_bus
[8]http://en.wikipedia.org/wiki/RG-6
[9]http://en.wikipedia.org/wiki/Ribbon_cable

3.3.2.2. Security

The difference between the three implementations lies in the physical mechanism for transmitting information, which has no particular capacity to provide any security measure.

3.3.2.3. Security Recommendations

The best security measure to protect these implementations of CIP lies in a logical separation from the rest of the network, which means they must be deployed in such a way that they are isolated from any external connection. In addition, systems for inspecting traffic, detecting intruders, or both (intrusion detection system [IDS] or intrusion prevention system [IPS])[10] are advisable.

3.3.3. CIP Implementation: Ethernet/IP

3.3.3.1. Description

Ethernet/IP was introduced in 2001 and is one of the protocols implementing CIP that is most widespread, tested and complete in respect of the automation of manufacturing industry. Thus, Ethernet/IP is the adaptation of CIP to the Ethernet network model which is inherently linked to TCP/IP. Consequently, Ethernet/IP uses the TCP/IP stack for all transport and network tasks, adapting CIP for the application layer, as may be seen in Illustration 9.

[10] http://en.wikipedia.org/wiki/Intrusion_detection_system

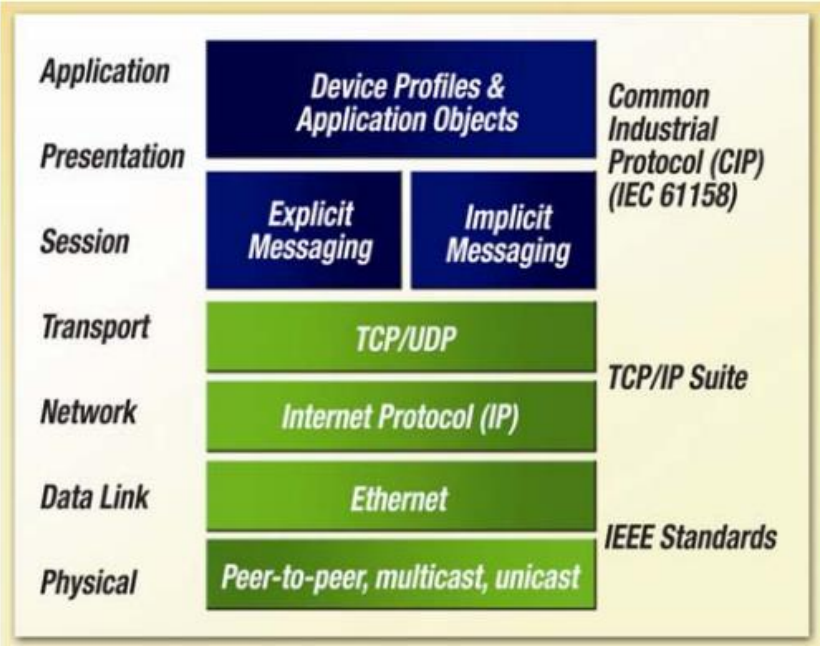

Illustration 9. The Ethernet/IP Implementation in the OSI Model. Encapsulation in the TCP/UDP Framework

As a CIP protocol, Ethernet/IP defines two connection methods for its TCP/IP communications. These are explicit messages, using transmission control protocol (TCP), and implicit (input or output) messages using user datagram protocol (UDP). Explicit messages follow the client-server or request-response pattern of connection. Among them there are messages between programmable logic controllers (PLCs) and human-machine interfaces (HMIs), diagnostic messages, and file transfers. The port used is TCP 44818.

Implicit messages are those which are critical and are employed for real-time communications, such as the transmission of data, and they generally operate with *multicast* addresses for efficiency. Thus, a message destined for a number of different devices need only be sent once. They are transmitted using port UDP 2222. Illustration 10 shows this type of communication.

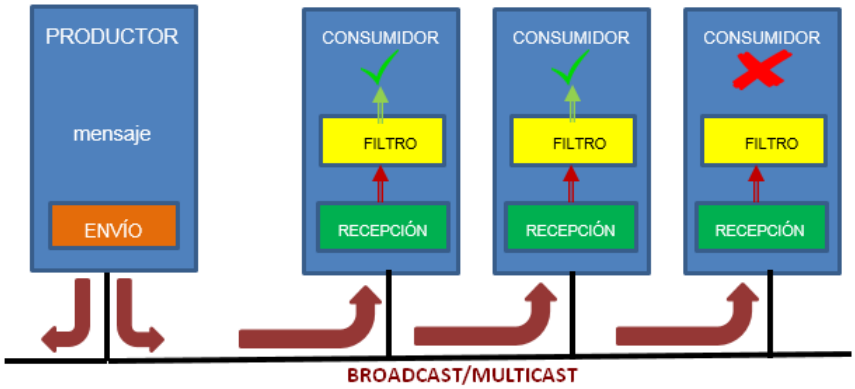

Illustration 10. CIP Producer-Consumer Model of Messaging in Implicit Multicast Communication

3.3.3.2. Security

Ethernet/IP is susceptible to being affected by all the vulnerabilities of Ethernet, such as identity theft or traffic capture. Moreover, since it uses UDP for its implicit messages, and this lacks transmission controls, it is possible to injection malicious traffic and to manipulate the transmission route by using IGMP.

3.3.3.3. Security Recommendations

As Ethernet/IP is a protocol based on Ethernet that uses UDP and IGMP, it is necessary to provide the perimeter of the Ethernet/IP network with all the safety mechanisms that are based on Ethernet and IP. It is also advisable to undertake passive monitoring of the network so as to ensure that Ethernet/IP traffic is associated solely with explicitly identified pieces of equipment and does not come from outside the network.

3.3.4. CIP Security

Although CIP uses a well-defined model for objects, it does not define any mechanism, whether implicit or explicit, for security. Furthermore, it has obligatory objects for identifying devices, which might make it easier to find out about equipment in the network, providing targets to attackers. As it also has common application objects for exchanging information between devices, an intruder is able to manipulate a large range of industrial devices by adjusting and sending this type of object. Moreover, the characteristics of some messages in CIP (real-time, multicast) are incompatible with the encryption of communications, so that CIP has no provision for mechanisms permitting it.

3.4. MODBUS

3.4.1. Description

Modbus is one of the oldest industrial control protocols. It was introduced in 1979 using serial communications to interact with PLCs. In the 1990s it saw a considerable spurt of growth and with the aim of achieving greater integration with modern systems a version for TCP/IP networks, Modbus/TCP, appeared in 1999. This step consolidated Modbus as one of the most widely used protocols in industrial control. At the present day it is extensively used in a broad range of industries, including critical infrastructures. Modbus is a protocol for industrial communications that is sited in the application layer, which thus permits different physical means to be used for transport. It provides communication in client-server mode among differing sorts of equipment connected through different technologies on lower layers, which include but are not limited to, the TCP/IP protocol layer.

It can thus be said that there are two kinds of implementation of Modbus:

- Serial Modbus: The transmission technology used is the high-level data link control (HDLC) standard[11], if Modbus proper is being implemented, and RS232 or RS485 if it is being implemented in a master-slave mode.
- Modbus-TCP: This uses the TCP/IP protocol stack to transmit information.

Since the Modbus protocol is common to all implementations, security measures implemented on Layer 7 will be independent of those set on lower layers.

3.4.2. Security

Implementations of serial Modbus use both RS232 and RS485, which are physical layer communication protocols. These protocols, by definition, are responsible for transmitting bits from one station to another and define the conditions under which a bit is understood as a bit. It makes no sense to speak of security on this layer, as these are functionalities that are developed on higher layers. Above physical access to media there are data link level protocols, HDLC and Ethernet according to the implementation (serial or TCP, respectively). Modbus does not implement any security characteristics at this level.

In respect of the security offed by the application layer, Modbus was designed to be used in highly controlled environments and it does not include any security mechanism on this layer. Hence, it lacks authentication, so that all that is necessary for the Modbus session is an address and function code that are valid. This is information that can easily be obtained over the Internet using a network sniffer. Likewise, it does not allow for encryption of information. These functionalities were not added when the possibility arose of using TCP/IP stack for protocols for lower layers. It is possible to apply generic measures for the TCP/IP stack (IDS

[11] http://en.wikipedia.org/wiki/High-Level_Data_Link_Control

or a firewall, say), but only for implementations based on Ethernet and never those based on the serial bus.

Moreover, in serial implementations commands are issued broadcast, which means that all connected elements might be affected by one single denial of service attack.

All of these deficiencies are magnified by the fact that Modbus is a protocol designed for programming control elements like remote terminal units (RTUs) or PLCs, so that the injection of malicious code into these elements becomes possible.

3.4.3. Security Recommendations

Owing to the security problems mentioned above, communication between devices using Modbus should be controlled. Hence, deployment of a traffic analyzer to check that Modbus traffic is allowed only from specific devices and only with permitted functions might help palliate communications problems when using this protocol.

Furthermore, checks should be made of those Modbus TCP packets with erroneous data about their size and of traffic through port TCP 502 will incorrectly formed packets. As an additional measure, those functions that force slaves to go into listen-only mode, functions forcing re-initiation of communications, those erasing or resetting diagnostic information such as that from counters or traffic from one server to multiple slaves should also be actively monitored to make the network more secure.

There are generic IDS solutions, like Snort, and others specially adapted for Modbus, like the IPS Tofino TCP Enforcer LSM, which are highly advisable for enhancing security in this protocol.

3.5. DNP3

3.5.1. Description

DNP3 is a communications protocol developed in 1993 which is widely implemented in the electricity sector, principally in the U.S.A. and Canada. It is only sparsely used in Europe, because there are alternatives such as IEC-60870-5-101 or IEC-60870-5-104. It is a three-layer protocol operating at the data link, application and transport layer levels[12].

3.5.2. Security

DNP3 is a protocol designed to maximize system availability, and puts less care into factors of confidentiality and data integrity.

[12] This might be better termed pseudo-transport, as it does not correspond precisely to the transport layer of OSI.

At the data link level the functions typical of this are included, such as the detection of transmission errors by means of cyclical redundancy check (CRC) calculation. This latter is not a security measure, since anybody wanting to modify frameworks should be capable of changing the CRC. Furthermore, it includes no additional security measure that is not already offered by the Ethernet protocol.

At the application level some efforts have been being made to provide a safe authentication standard in DNP3 [4], promoted by the DNP3 Users' Association. This authentication is carried out at application level so as to guarantee communications from start to finish, since DNP3 is a protocol that can be used on different technologies for Layers 1 and 2.

This standard for safe authentication resolves several problems:

- Identity theft, generally for malicious use.
- Modification of messages in such a way that the functioning of the system may be altered.
- Attacks involving re-injection of traffic, consisting of the malicious or fraudulent transmission of valid data.
- Eavesdropping, in other words fraudulently tapping into information circulating over the network, although usually only exchanges of cryptographic keys and not the rest of the data moving over the network.

The standard has an operations model based on challenge and response, so that when a request is made for a function that requires authentication, the request is not processed unless an authentication challenge is resolved. This form of communication is shown in Illustration 11.

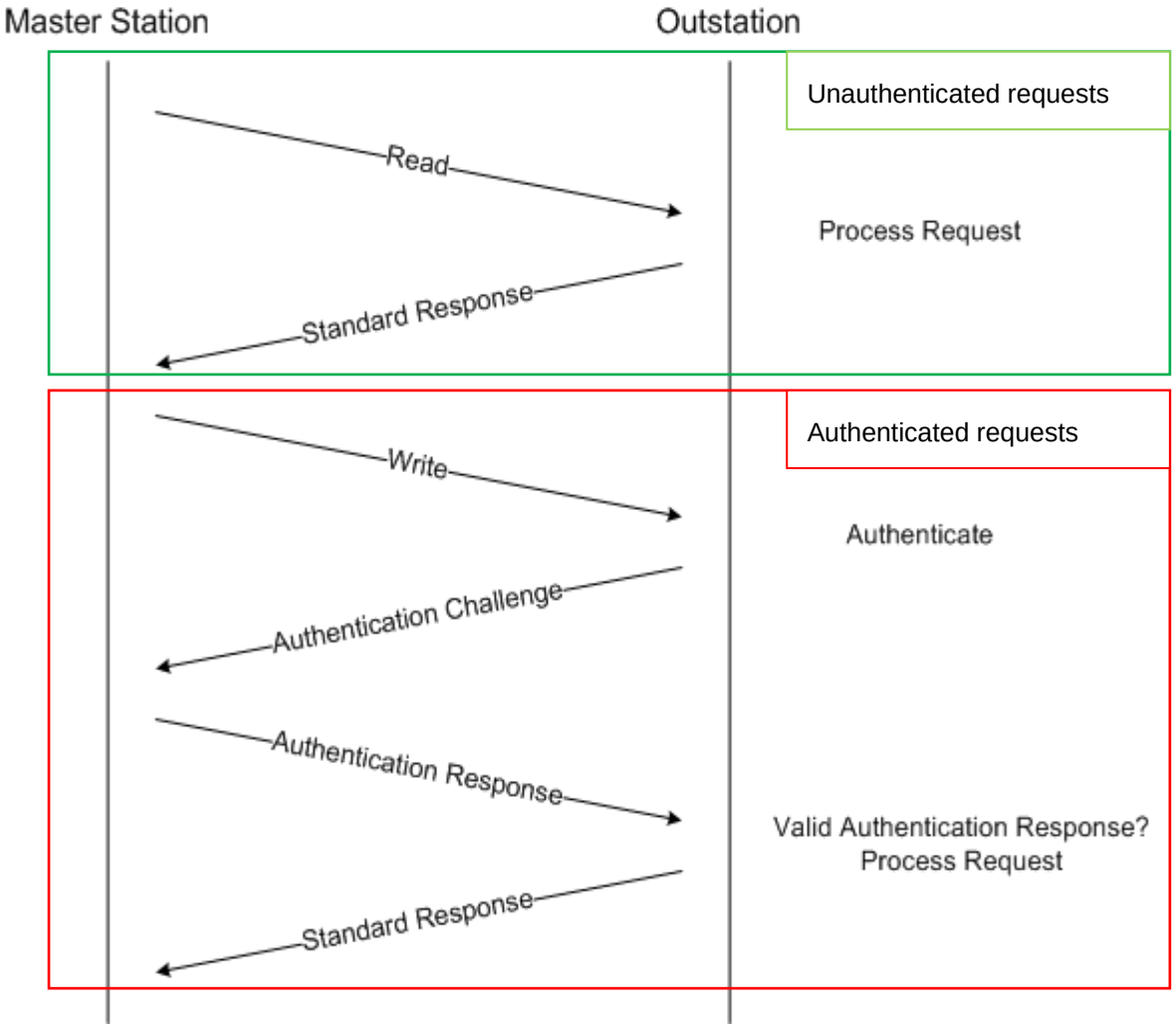

Illustration 11: Different Types of DNP3 Request.

This mode of operation may involve delays and network overload, so it may be configured in an “aggressive” mode, with the request and the response to the challenge being sent together.

3.5.3. Security Recommendations

Since DNP3 has a safe implementation, the main recommendation would be to deploy only secure DNP3. This deployment may not be possible because of a number of different factors, such as the manufacturer’s media. In such cases it is advisable to use DNP3 encapsulated

within a secure transport protocol like TLS. There are currently several manufacturers, like PJM[13], that offer this type of deployment [5], as may be seen from Illustration 12.

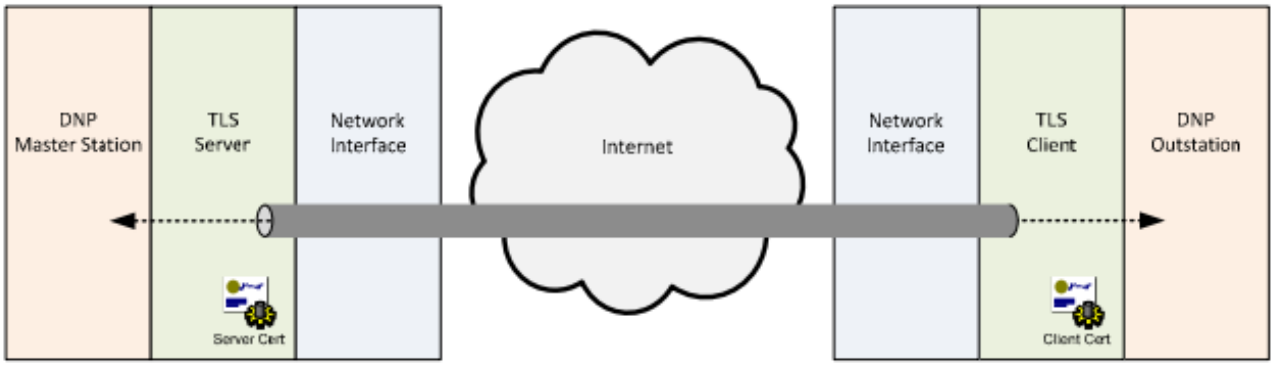

Illustration 12: DNP3 Encapsulated within TLS.

In addition, it is advisable to monitor any non-DNP3 communication through ports normally used by DNP3 (TCP/UDP 20000), as well as paying special attention to function codes 4, 5 and 6 (*Operate, DirectOperate* and *DirectOperate no ACK*), 18 (*Stop Application*), and 21 (*DisableUnsolicitedMessages*)[14].

3.6. PROFIBUS

3.6.1. Description

Profibus (an acronym from PROcess Field BUS) is a standard for communication through Fieldbus promoted in 1989 by the German Department of Education and Research and used by Siemens. It is based on serial communications by cable (RS-485, MBP) or optical fiber cable.

It currently has two variants, as may be seen in Illustration 13: **Profibus DP** (for decentralized peripherals) used to operate sensors and actuators through as central controller and **Profibus PA** (for process automation) used to monitor measuring equipment through a process control system.

[13] http://www.pjm.com/
[14] A full list of the applications functions of DNP3 may be consulted on [7]. It should be noted that in this list the notation is hexadecimal, whilst in the text decimal notation is used.

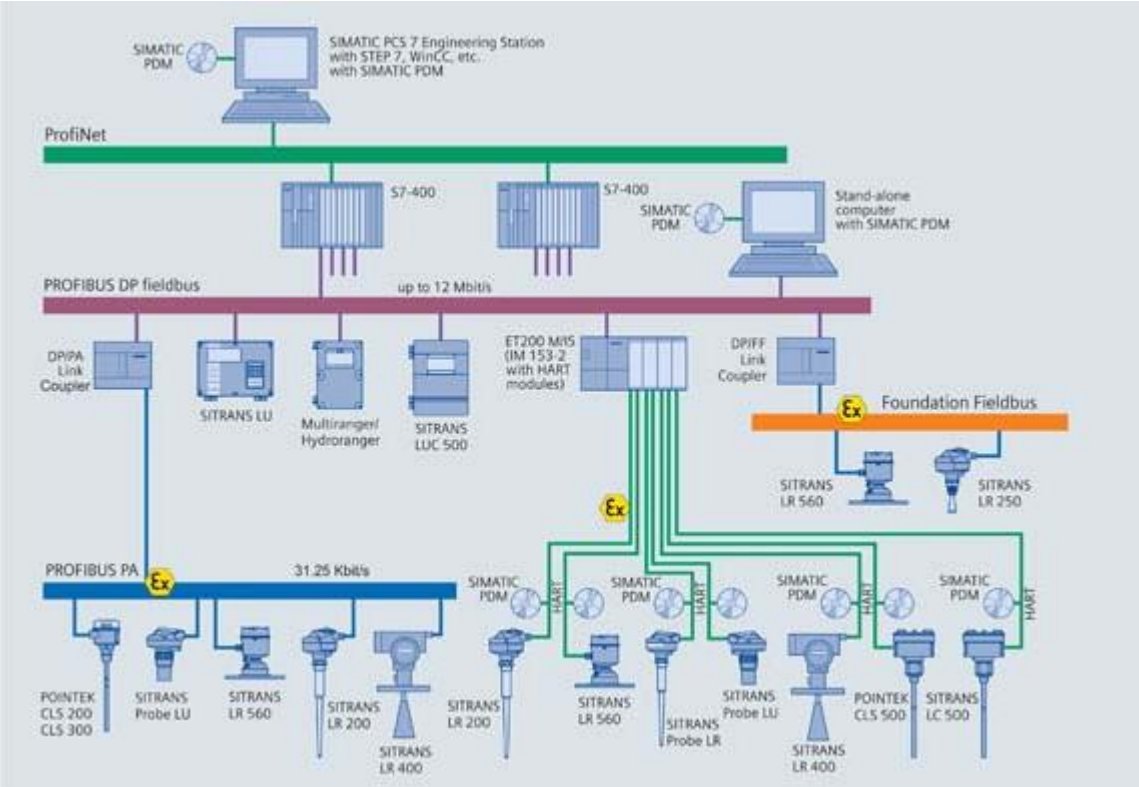

Illustration 13: The Architecture of Profibus

3.6.2. Security

Profibus is a protocol operating in the application, link and physical layers. The link layer in this protocol uses FDL (Fieldbus Data Link) as a mechanism for managing access to the medium. It functions with a hybrid access method that combines master-slave technology with the passing on of a token which indicates who can initiate communication and occupy the bus. These measures ensure that devices do not communicate simultaneously, but they do not constitute any sort of safety mechanism and may be susceptible to attacks involving traffic injection or denial of service.

On the application layer, there are three levels of use: DP-V0 for exchanging periodical data, DP-V1 for communications that have no fixed periodicity and DP-V2 for asynchronous communications through broadcast messages. The documentation available does not allow any inference to be drawn that Profibus adds any layer of security to communications on this level.

There are some services offered by Profibus than can use TCP/IP as a transport protocol, but only during an initial phase for device assignment. In these services it is possible to add IT security elements, as long as they do not prejudice the operations of the system.

3.6.3. Security Recommendations

As with other protocols in the Fieldbus family, the absence of any authentication and the lack of security in the protocol require the bus to be isolated from the remaining components in the network. Perimeter security should be very strict to avoid any unauthorized or suspicious traffic.

3.7. PROFINET

3.7.1. Description

Profinet is a standard based on Profibus that adopts Ethernet as its physical interface for connections rather than RS485, and has a repetition system based on passing on tokens. It offers the complete TCP/IP functionality for data transmission, which allows for wireless applications and high-speed transfers. Equipment using Profinet is oriented toward reliability and real-time communications, together with usability. Illustration 14 shows the architecture of Profinet.

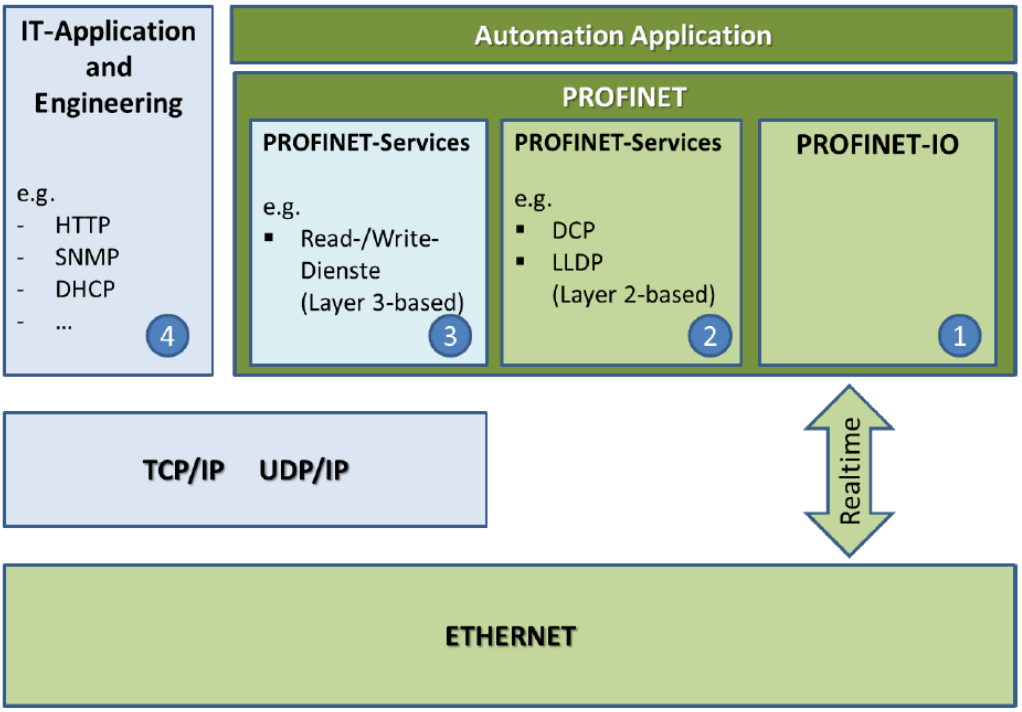

Illustration 14: The Architecture of Profinet

3.7.2. Security

Profinet equipment lacks any native security functions, in the sense of end-point security. Hence, preventing attacks on Profinet equipment is crucial. The measures incorporated into the protocol concentrate on improving system availability and operational reliability, together with robustness of equipment when faced with high volumes of traffic at certain points. The

PROFINET Security Guideline [6] document provides recommendations on preventing potential attacks on such systems, including long-standing IT practices such as segmentation of networks with VLANs or the setting up of DMZs, as can be seen in Illustration 15.

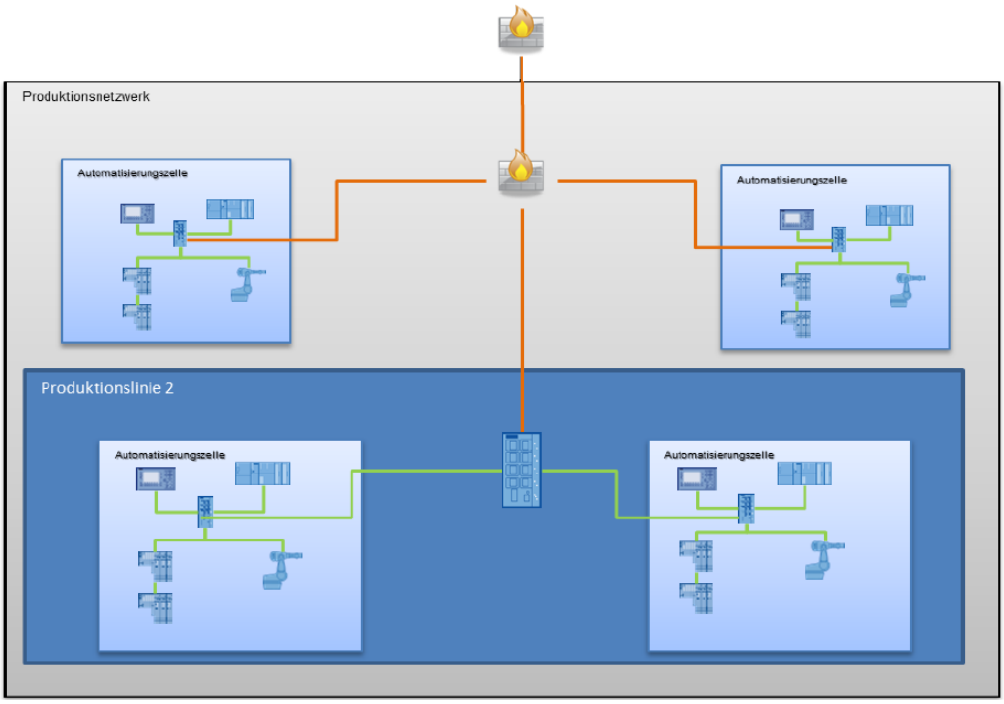

Illustration 15: One of the Architectures Proposed for ProfiNet.

3.7.3. Security Recommendations

As with other protocols originally created for communication through Fieldbus[15], the absence of authentication and lack of security in the protocol require isolation from the rest of the network. In addition, the use of IT methods to authenticate components in the network, together with encryption of communications within it is good practice. Finally, perimeter security should be very stringent so as to avoid any unauthorized or suspicious traffic.

3.8. POWERLINK ETHERNET

3.8.1. Description

PowerLink over Ethernet [7] is a communication profile for Ethernet in real time. It extends Ethernet in accordance with the IEEE 802.3 standard, with mechanisms for transmitting information with precise synchronization and predictable intervals, with an architecture that

[15] It should be remembered that Profinet is an adaptation of Profibus for the Ethernet protocol, so that the application layer was originally designed for Fieldbus.

can be seen in Illustration 16. The specification for the protocol [8] can be downloaded from the website of the Standardization Group for Ethernet PowerLink [16].

PowerLink provides mechanisms to ensure:

1. Transmission of information for which time is critical in asynchronous cycles. The exchange of information is based on a publication and subscription method.
2. Synchronization of nodes in a network with great precision.
3. Transmission of information for which time is not so crucial upon demand. Asynchronous communication may use protocols from the TCP/IP stack or from higher layers such as HTTP, FTP and others.

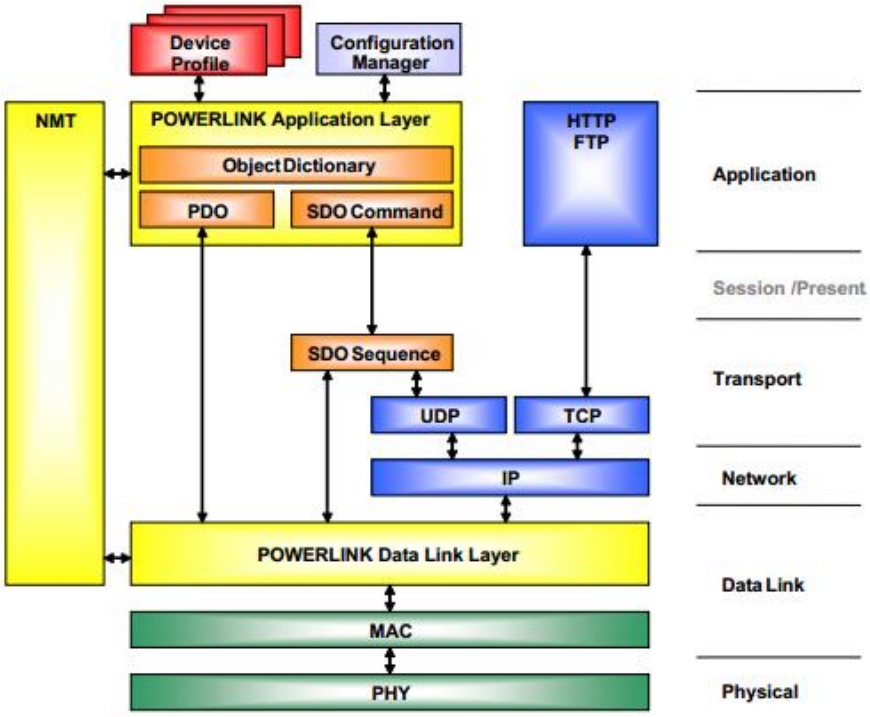

Illustration 16: Reference Model for Ethernet PowerLink.

Traffic over the network is managed in such a way that intervals of time are set aside for synchronous and asynchronous transmissions, while it is ensured that only equipment in the network can access the transmission medium. This makes sure that information transmitted asynchronously does not interfere with synchronous transmissions and that communication intervals maintain. This mechanism, known as *Slot Communication Network Management (SCNM)* is controlled by a piece of equipment in the network, the Management Node (MN).

[16] http://www.ethernet-PowerLink.org/

The rest of the nodes are called Controlled Nodes (CN). CN can use only those transmission intervals assigned by the MN. All the nodes in the network have to be configured in the MN and just one MN is permitted in any given network. Moreover, only the MN may send messages independently, whilst CN send messages only when the MN requests them to do so. CNs send the information requested by the MN in broadcast form, so that it can be received all over the network. Illustration 18 displays this process.

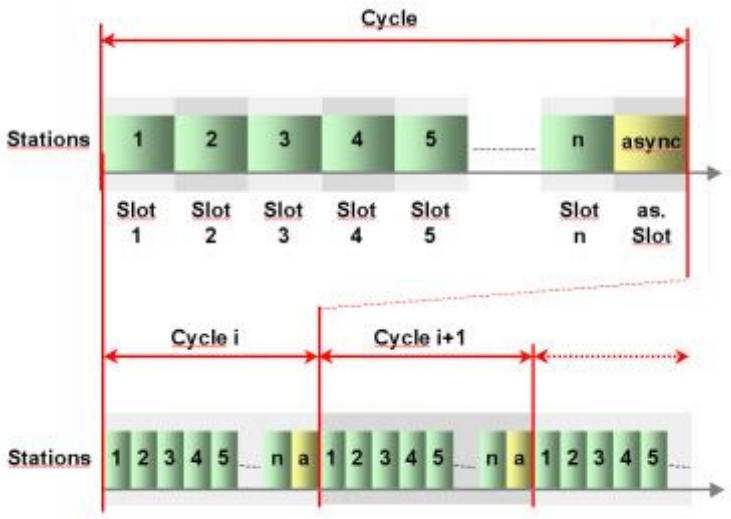

Illustration17: Slot Communication Network Management in Ethernet PowerLink

3.8.2. Security

As in other industrial protocols, mechanisms for checking the authenticity of nodes and messages are missing from this protocol. Whilst it is true that a node can transmit only when the MN requests it and assigns it a time period, there is no mechanism for checking that the information received does come from the node. Thus, it is reasonably simple to alter traffic in the network by faking legitimate nodes or trigger a denial of service (DoS) merely by flooding the network with messages.

The use of broadcasting for transmissions also allows an intruder to get hold of all the information sent by CNs. There is no sort of encryption intended to avoid this.

3.8.3. Security Recommendations

The sensitivity of SCNM to delays requires Ethernet PowerLink to be deployed isolated from any other network based on Ethernet. Perimeter security should thus be very strict so as to keep the protocol isolated from the rest of the network and prevent malicious traffic.

3.9. OPC

3.9.1. Description

OPC (OLE for process control) is not an industrial communications protocol, but rather an operational framework for communications in process control systems based on Windows that use object linking and embedding (OLE), which in turn use communication protocols like RPC. Hence, OPC is a set of protocols that jointly allow process control systems to communicate using come of the capacities for communication in Windows.

OPC connects Windows systems, normally through TCP/IP. OPC was originally based on DCOM and many OPC systems still use this, even though there is an updated version called OPC Unified Architecture (OPC-UA) that allows the use of SOAP over HTTPS, which is much more secure.

3.9.2. Security

The use of DCOM and RCP makes OPC very susceptible to attacks, apart from which it can be affected by all the vulnerabilities occurring in OLE. Moreover, OPC is executed only on Windows systems, so that it can also be hit by all the weaknesses from which this operating system suffers.

As it is inherently difficult to apply patches to industrial control systems, many vulnerabilities that have already been discovered for which there are patches available continue to be exploitable industrial control networks. OPC-UA does, however, possess a model for security which can be found in a white paper [9], bringing greater security to the architecture, so that it is advisable to deploy OPC-UA rather than the classic version of OPC.

3.9.3. Security Recommendations

As far as possible, it is OPC-UA that should be deployed. Apart from this recommendation, OPC servers should be suitably hardened, shutting off all the ports and services that are not necessary.

In addition, all those non-OPC ports and services initiated by the OPC server should be carefully monitored, as should the appearance of vulnerabilities affecting Windows, OPC, OLE RPC or DCOM. OPC services initiated from unknown OPC servers and authentication failures on OPC servers should also be actively monitored so as to improve security of deployments of OPC.

3.10. ETHERCAT

3.10.1. Description

EtherCAT (Ethernet for Control Automation Technology) is an open-code communications protocol used to incorporate Ethernet into industrial environments. This protocol gelled as a standard in IEC 61158[17], within the standardization of Fieldbus. EtherCAT is used in automation applications with short updating cycles (≤ 100µs) and with a jitter[18] ≤ 1µs. It is thus the fastest system currently available.

In this system the Ethernet packet is not received, interpreted and sent (as in the long-standing store and resend approach), but rather is processed on the fly in every slave node (with updating of the relevant information) as it is sent on to the next device. Delays are thus reduced to a mere few nanoseconds. The fabric of EtherCAT is shown in Illustration 18.

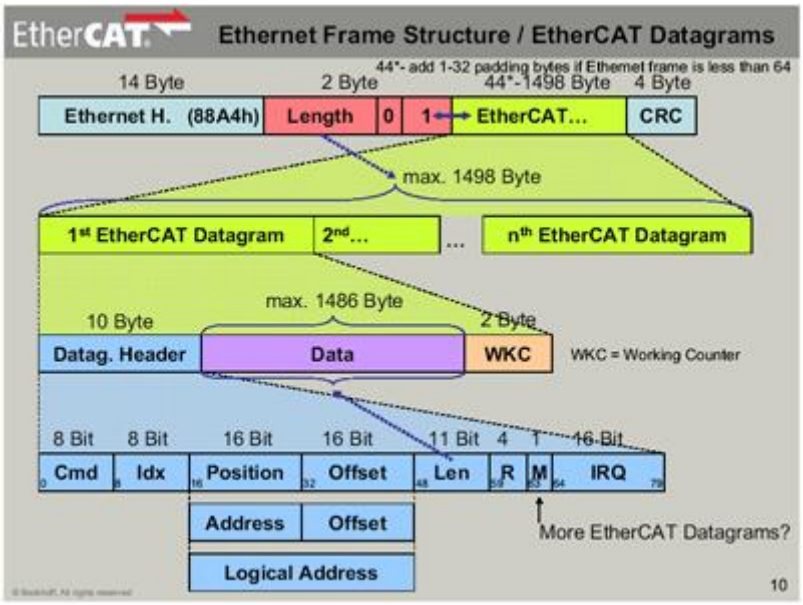

Illustration 18: The EtherCAT Framework Structure.

3.10.2. Security

As EtherCAT is a protocol derived from Ethernet, it is susceptible to all of the vulnerabilities in Ethernet, and thus at risk to a large range of denial of service attack. EtherCAT services can easily be modified through the insertion of Ethernet packets into the network in such a way that they interfere with synchronization and they are vulnerable to forgery and MITM as a

[17]http://en.wikipedia.org/wiki/Fieldbus
[18]http://en.wikipedia.org/wiki/Jitter

consequence of the lack of authentication, so that it is advisable to separate the EtherCAT network from any other Ethernet systems.

3.10.3. Security Recommendations

As has already been mentioned, EtherCAT must be deployed in isolation from any other Ethernet networks. It is also advisable to carry out passive monitoring of the network in order to ensure its integrity, checking that EtherCAT traffic originates exclusively from those devices that are explicitly authorized for it.

APPENDIX I: COMPARATIVE TABLE OF ICS PROTOCOLS

Protocol		Characteristics	Security		Protocol layers implemented				Security measures
	Variant		Cipher	Authentication	Media Access	IP	Transport	Application	
Common Industrial Protocol (CIP)	DeviceNET	Adaptation for CAN	No	No	X	X	X	X	CIP have CIP SafetyTM technology at application level Complement with well-known measures about control network segmentation and isolation
	ControlNET	Adaptation for CTDMA	No	No	X	X	X	X	
	CompoNET	Adaptation for TDMA	No	No	X	X	X	X	
	Ethernet/IP	Adaptation for TCP/IP	No	No				X	
Modbus	Serial	Open standard Widely used in Industry	No	No	X			X	Adopt, if it's possible, cypher (SSL, VPN) or traffic inspection measures such as IDS (Snort), IPS (Tofino), etc.
	TCP		No	No				X	
DNP3		Electric Sector Low presence in Europe	No	Yes (DNP3 secure)		X	X	X	Implement DNP3 Secure
ProfiBus		Open Standard Profibus DP & PA variants	No	No	X	X		X	Network segmentation, data cipher and traffic inspection
ProfiNET		Profibus evolution for Ethernet	No	No				X	Follow "Profinet Security Guide"
Powerlink Ethernet		Open standard	No	No				X	Network segmentation and apply normal Ethernet security measures
OPC		Communications operation framework Originally Windows-based	No	Yes (OPC UA)				X	Implement OPC UA
EtherCAT		Open standard For very low update cycles	No	No				X	Network segmentation and apply perimeter security

APPENDIX II: GENERAL SECURITY RECOMMENDATIONS

I. GENERAL RECOMMENDATIONS FOR FIREWALLS.

As a complement to the recommendations put forward for network architectures that are described in Section 2.2, the following rules of a general nature may also be applied:

- The basic rule set should be a blanket refusal, followed by allowing communications or services in response to definite needs (with whitelists).
- Ports and services between the control network environment and the corporate network should be enabled and specifically permitted on a case by case basis only when there is a clear need for them. There should be documented justification with a risk analysis and an individual should be responsible for every inward or outward flow of data that is allowed.
- All rules allowing access should be set with an IP address and a specific TCP/UDP port with checks on its state.
- All rules should be defined in such a way as to restrict traffic to one single IP address or a clearly specified range of addresses.
- Direct traffic from the control network to the corporate network should be barred. All control traffic should end in the DMZ.
- Every protocol permitted between the control network and the DMZ should **not** be explicitly allowed between the DMZ and corporate networks (and vice versa).
- Any outward traffic from the control network to the corporate network should be strictly limited by source and destination, and also by service and port.
- Packets going outwards from the control network or the DMZ should **only** be authorized if they have a correct IP address as origin that is assigned to the control network or devices in the DMZ network.
- No access should be permitted to Internet devices in the control network.
- Control networks should **not** be connected directly to the Internet, even if they are protected by a firewall.
- Any firewall administration traffic should take place through one of the following: a separate network, secure management (for example, outside normal bandwidth), or an encrypted network with authentication of multiple factors. Traffic should also be restricted by IP address to specific management stations.
- All firewall policies should be periodically checked.
- All firewalls should be backed up immediately before start-up.

II. GENERAL RECOMMENDATIONS FOR SERVICES

As an add-on to the general rules described in the previous section, the following general firewall rules are proposed in accordance with the service or protocol in question:

SERVICE	RECOMMENDATION
DNS	Use should be made of a local internal DNS server restricted to the control network. In cases where there are few elements, local host files may be employed.
HTTP	The protocol used to access the web with browsers is very useful and convenient. Nonetheless, if the version in use is not HTTPS, which has encrypted transmissions, it should be barred between the corporate or public network and the control network. In addition: ▪ Whitelists should be used to filter IP addresses for web access by services in the control or physical network. ▪ There should be access control both for origins and for destinations. ▪ Authorization at application level should be implemented. ▪ The number of technologies supported should be restricted so as to decrease the range of vulnerabilities. ▪ Both actual use and attempts at use of access to services should be recorded and monitored.
FTP and TFTP	These two file transmission protocols are widely used in ICSs. However, the absence of any encryption renders them vulnerable to the theft of credentials and information. They should be avoided as far as possible and replaced with encrypted versions like SCP or SFTP. In cases where it is strictly necessary to use them, they should be limited to transmissions that are not critical or employed with tunnel encryption.
TELNET	This access and communication protocol has no encryption, which makes its use inadvisable. In case of need a private network or virtual private network (VPN) should be used to protect transmissions.
DHCP	This protocol was designed for automatic configuration of networks of devices and is very useful, but brings with it security risks, as it can be used for MITM attacks and for intercepting traffic. As far as possible its use should be avoided, but if it is necessary traffic inspection rules should be implemented, so as to defend against rogue DHCP servers, along with measures against the spoofing of ARPs and IPs.
SSH	A proper use of SSH should be seen as an effective measure for establishing secure communications between segments or elements of

	networks that have sensitive traffic. It should be permitted and can replace FTP, TELNET, RCP and other unsafe protocols.
SOAP	The simple object access protocol (SOAP) uses XML syntax to exchange messages. It is a mechanism without any control over states and thus is rather vulnerable to falsification and interception. Hence, traffic inspection rules at application level are advisable to check the content of messages.
SMTP	This protocol, which is used for e-mails, should be barred in the control network. SMTP traffic outward from the control network to the corporate network may be permitted to allow the sending of alerts as e-mails.
SNMP	SNMP is the protocol used for control and monitoring of network elements and is very useful. However, in Versions 1 and 2 it uses non-encrypted communications and generic passwords. SNMP Version 3 solves these problems, but is not always compatible with all devices. If versions before V3 have to be used, it is advisable to separate SNMP traffic off into a management network.
DCOM	The distributed component object model (DCOM) is the protocol on which OPC (OLE for Process Control) is based. It uses a remote procedure call (RPC) service, which should be appropriately patched, as it otherwise has multiple vulnerabilities. Moreover, OPC through DCOM makes use of dynamic ports (running from 1024 to 65535), which increases the difficulty of establishing solid rules for firewalls. Traffic under this protocol should be permitted only between control networks and the DMZ. In addition, it is advisable to apply DCOM configurations for devices that reduce the range of dynamic ports available.

REFERENCES

[1] ISA-95. [on line]. Available from: https://www.isa.org/standards-and-publication.

[2] D. G. Maryna Krotofil, *Industrial Control Systems Security: What is happening?*.

[3] Homeland Security U.S., *Improving Industrial Control with Defense in Depth Strategies*, 2009.

[4] IEEE, *IEEE Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3)*, 2010.

[5] PJM, *Jetstream Guide DNP SCADA over Internet with TLS Security*, 2013.

[6] P. -. Profinet, *Profinet Security Guidelines. Guidelines for PROFINET*, 2013.

[7] *DNP3 Quick Reference Guide*, 2002.

[8] E. P. S. Group, *Ethernet POWERLINK Communication Profile Specification*, 2008.

[9] P. H. Randy Amstrong, T*he OPC UA Security Model for Administrators*, 2010.

[10] Rockwell Automation, *Reference Architectures for Manufacturing*, 2011.

[11] E. D. Knapp, *Industrial Network Security*, 2011.

[12] L. A. a. C. M. P. Hollman, *Compromising Industrial Facilities from 40 Miles Away*, 2013.

[13] University of Leon, Department of Computer Engineering and Computer Science, *Security Considerations in SCADA Communication Protocols*, 2004.

[14] S. C. C. Agency, *Guide to Increased Security in Industrial Control Systems*, 2010.

[15] ISA, *ISA-99 Industrial Automation and Control Systems Security*.