

Jami Sivén

Securing Profinet Networks

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

11 May 2015

Author(s) Title	Jami Sivén Securing Profinet Networks
Number of Pages Date	50 pages 11 May 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Antonio Ramirez, Project Engineer – Mission Critical Networks Marko Uusitalo, Senior Lecturer
<p>This Thesis was made to study Profinet networks and means to secure them. The assignment for this Thesis came from Mission Critical Network team of Pöyry Finland Oy.</p> <p>The objective of this thesis was to study Profinet networks; what they are, how they differ from standard office networks and how they are secured.</p> <p>The first part of the thesis covers some basics of Ethernet technology along with the networking reference models OSI and TCP/IP. The second part is about Profinet itself and how Profinet networks are designed. The final part includes common methods for securing Profinet networks and descriptions of three attacks against Profinet.</p> <p>Industrial systems are moving towards Industrial Ethernet which is based on standard Ethernet used everywhere nowadays. It is a totally different world from the traditional serial based field bus systems which were designed to be implanted in totally isolated networks where cyber security was not a concern unlike today when everything is connected via different networks. Today, network engineers designing industrial networks need to know the demands and requirements of automation applications along with the threats of modern networks and how to protect against them.</p> <p>As a conclusion, Profinet seems like a solid concept but the devices it is used in have vulnerabilities. Vendors are working on updates but the updates need to be done and deployed fast. Meanwhile vendors just give advice on how to mitigate problems but this is not acceptable. Problems need to be resolved, not just trust in firewalls to keep the attackers out. For the most part, Profinet networks are secured with the same technologies as other Ethernet based networks. The only exception comes from how security aspects are emphasized. In automation networks the emphasis is more on availability when office environments consider confidentiality to be more important.</p>	
Keywords	Profinet. Industrial Ethernet, Cyber security, automation network, control network

Tekijä(t) Otsikko	Jami Sivén Securing Profinet Networks
Sivumäärä Aika	50 sivua 11.5.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Projekti-insinööri, Mission Critical Networks Antonio Ramirez Lehtori Marko Uusitalo
<p>Tämän työn tarkoituksena oli tutustua Profinet –verkkoihin, niiden tietoturvaan ja ottaa selvää miten Profinet –verkoista tehdään tietoturvallisia. Työ tehtiin Pöyry Finland Oy:n MCN teamin toimeksiannosta.</p> <p>Työssä käydään ensin läpi Ethernet –tekniikkaa sekä teollisuusympäristöihin suunnattua teollisuuden Ethernet –tekniikkaa yleisesti läpi. Tämän jälkeen tutustutaan Profinet –tekniikkaan ja sen vaatimuksiin. Viimeisessä osassa käydään läpi teollisuusverkkojen ja Profinetin tietoturvaa ja esitellään kolme Profinettiin liittyvää hyökkäystä.</p> <p>Teollisuusverkot siirtyvät yhä enenevässä määrin Ethernet –pohjaisiin teknologioihin, joita kutsutaan Teollisuus-Ethernetiksi. Tämä asettaa aivan erilaisia vaatimuksia teollisuusverkkosuunnittelijoille. Vanhat sarjapohjaiset tiedonsiirtoteknologiat on suunniteltu sijaitsemaan täysin omissa suljetuissa verkoissaan, joten tietoturvalle ei ollut tarvetta samalla lailla kuin nykyään, kun kaikki ovat yhteydessä toisiinsa erilaisten verkkojen välityksellä. Tämä kaikki asettaa vaatimuksia tänä päivänä teollisuusverkkoja suunnitteleville tietoverkkosuunnittelijoille; heidän pitää tuntea teollisuusympäristöjen vaatimukset sekä modernien verkkojen uhat ja puolustuskeinot hyökkäyksiä vastaan.</p> <p>Profinet vaikuttaa olevan vankalla pohjalla mutta itse laitteissa, joissa Profinet –protokollaa käytetään, on haavoittuvuuksia. Valmistajat kyllä tekevät korjauksia ohjelmistoihin paikatakseen aukkoja, mutta näissä päivityksissä yleensä kestää ja valmistajat tyytyvät vain antamaan neuvoja miten lieventää haavoittuvuuksien vaikutuksia. Tämä lähestymistapa ei ole oikea tapa hoitaa haavoittuvuuksia. Haavoittuvuudet pitää paikata mahdollisimman nopeasti eikä vain luottaa siihen, että hyökkääjät eivät pääse sisälle verkkoon. Profinet-verkot suojataan pitkälti samalla lailla kuin mikä tahansa muu Ethernet –pohjainen verkko. Eroja tulee siinä miten tietoturvanäkökulmia painotetaan. Teollisuusverkoissa painotetaan verkkojen käytettävyyttä ja saatavuutta, kun taas toimistoverkoissa voidaan kärsiä hieman verkkokatkoksista kunhan data pysyy tallessa.</p>	
Avainsanat	Profinet, Teollisuus-Ethernet, tietoturva, automaatioverkot, hallintaverkot

Contents

List of Abbreviations

1	Introduction	1
2	Networking Reference Models	2
2.1	OSI Model	2
2.2	TCP/IP Model	4
3	Ethernet	5
3.1	Variants of Ethernet	5
3.1.1	Twisted Pair	5
3.1.2	Fiber Optics	6
3.2	Comparison	9
4	Industrial Ethernet	9
4.1	Same Technology, Different Approach	9
4.2	IT Meets Automation	12
4.3	Special Requirements	12
5	Profinet	13
5.1	Profinet Versions	15
5.1.1	Profinet CBA	16
5.1.2	Profinet IO	17
5.2	Application Profiles	20
5.2.1	PROFIsafe	20
5.2.2	PROFIenergy	20
5.2.3	PROFIdrive	21
5.3	Network Topology	21
5.3.1	Star Topology	21
5.3.2	Tree Topology	22
5.3.3	Line Topology	23

5.4	ProfiCloud	23
5.5	Transmission	25
5.6	Integration with Overall Network	26
6	Security of Profinet Networks	26
6.1	Hacks and Vulnerabilities	28
6.1.1	Siemens Simatic S7 PLC Exploit	28
6.1.2	Emulation of Profinet IO-Devices	30
6.1.3	ProFuzz	32
6.2	Connecting Automation and Office Networks	33
6.2.1	Physical and Logical Separation	34
6.2.2	Logical Integration through Firewall	35
6.2.3	Common Physical Topology with Logical Separation	36
6.3	Network Security Measures	37
6.3.1	Firewall	37
6.3.2	IPS/IDS	39
6.3.3	Physical Protection	40
6.3.4	Redundancy	41
6.3.5	Remote Access	43
7	Discussion and Conclusions	46
	References	48

List of Abbreviations

MCN	<i>Mission Critical Networks.</i>
PI	<i>Profibus and Profinet International.</i> Automation community responsible for Profibus and Profinet
OSI	<i>Open System Interconnection model</i>
TCP/IP	<i>Transport Control Protocol/Internet Protocol.</i> 1. A layered model for computer communications. 2. Layer 4 and 3 protocols in the OSI model respectively.
HTTP	<i>Hypertext Transfer Protocol</i>
LAN	<i>Local Area Network</i>
TLS	<i>Transport Layer Security</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
SMF	<i>Single Mode Fiber</i>
MMF	<i>Multimode Fiber</i>
LED	<i>Light Emitting Diode</i>
VCSEL	<i>Vertical Cavity Surface Emitting Laser</i>
SNMP	<i>Simple Network Management Protocol</i>
LLDP	<i>Link Layer Discovery Protocol</i>
VPN	<i>Virtual Private Network</i>
DHCP	<i>Dynamic Host Control Protocol</i>

ICS	<i>Industrial Control System</i>
PAC	<i>Programmable Automation Controller</i>
DMZ	<i>Demilitarized Zone</i>
RSTP	<i>Rapid Spanning Tree Protocol</i>
HMI	<i>Human Machine Interface</i>
PLC	<i>Programmable Logic Controller</i>
IPS	<i>Intrusion Prevention System</i>
IDS	<i>Intrusion Detection System</i>
ARP	<i>Address Resolution Protocol</i>
VLAN	<i>Virtual Local Area Network</i>

1 Introduction

The automation field is at one of the greatest turning points in its history. Field communication systems are moving towards more flexible Ethernet-based communication standards from the old serial communication standards. These new Ethernet-based technologies demand a new way of thinking from both network and automation engineers.

One of the fastest growing Industrial Ethernet standards is Profinet which is the successor to the widely used field communication standard Profibus. As the demand for Profinet continues to rise so does the demand for network engineers who are familiar with industrial environments and their special requirements for networks.

The purpose of this thesis is to get familiar with Profinet, get to know how to secure Profinet networks and to produce general guidelines to the MCN team for designing secure Profinet networks. The idea for this thesis came from Mission Critical Networks (MCN) team of Pöyry Finland Oy which designs networks and provides consulting services for mainly industry clients.

The thesis starts with a brief look at the OSI and TCP/IP models and Ethernet. The second part of the thesis covers Industrial Ethernet and Profinet itself. The final part is about securing Profinet networks and common methods for securing industrial networks. The final part also includes the description of three attacks against Profinet networks.

2 Networking Reference Models

Networking reference models are an integral part of modern networks. They set a basis for data communications between different systems by defining a common architecture. The two models used are called the OSI model and the TCP/IP model. OSI model is the older from the two and uses seven layers to define the data communication of systems compared to the five layers of the TCP/IP model.

2.1 OSI Model

The Open Systems Interconnection (OSI) model is commonly used to describe the layers by which data is processed in modern communication systems. The OSI model is produced by the International Organization for Standardization (ISO) in the late 1970s which makes it one of the oldest standards in use in telecommunications. [1]

Although OSI model is almost 40 years old, it still succeeds in describing modern communication systems. Figure 1 illustrates the structure of the OSI model and how it does the partitioning of the different functions into seven abstraction layers. By doing this the upper layers do not have to take part in the tasks of the lower layers and vice versa. For example a browser in the application layer does not have to take care of bit encapsulation in the physical layer.

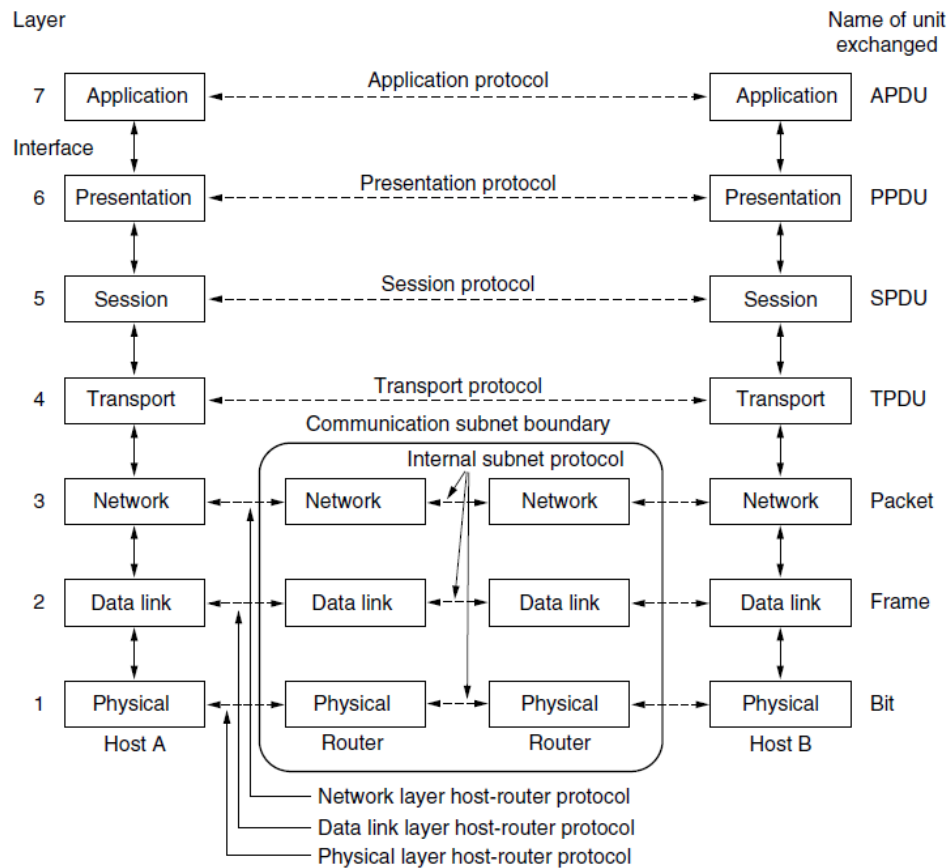


Figure 1. OSI model [2].

Each of the seven layers serves a layer above them and is served by a layer below through services. [2: 40]

An interface acts as a tunnel between layers enabling them to communicate with a layer above and below it. Communication begins in the topmost layer, goes down through all the other layers to the lowest layer where the data is sent to the receiving device. For example when a user wants to look at a web page the browser sends a request for the web page using HTTP. This request goes all the way through to the physical layer where it is encapsulated and sent to the server hosting the web page. The server then replies and sends the requested web page to the browser for the user to look at. Because interfaces are precisely defined and the standards used are common the communication between devices from different vendors is possible.

2.2 TCP/IP Model

The TCP/IP model is a computer networking model which defines a set of protocols and rules for communication across interconnected networks such as the Internet. The TCP/IP model is named after the two best known and most used protocols which are Transmission Control Protocol (TCP) and Internet Protocol (IP). The TCP/IP model is a result of research funded by the Advanced Research Projects Agency (ARPA) [4: 2]. The TCP/IP model specifies common applications such as electronic mail, terminal emulation, HTTP and file transfer in addition to the lower-layer protocols (such as TCP and IP).

As Figure 2 illustrates the TCP/IP model is also a layered model but it has only four layers compared to the OSI model's seven, though the functions of the layers are equivalent. The network access layer is identical to the OSI model layers 1 and 2. The Internet Protocol layer is equivalent to layer 3 in OSI model. The Host-to-Host Transport layer (TCP and UDP protocols) is comparable to layer 4 in OSI and lastly the application layer is comparable to the OSI layers 5, 6 and 7 combined.

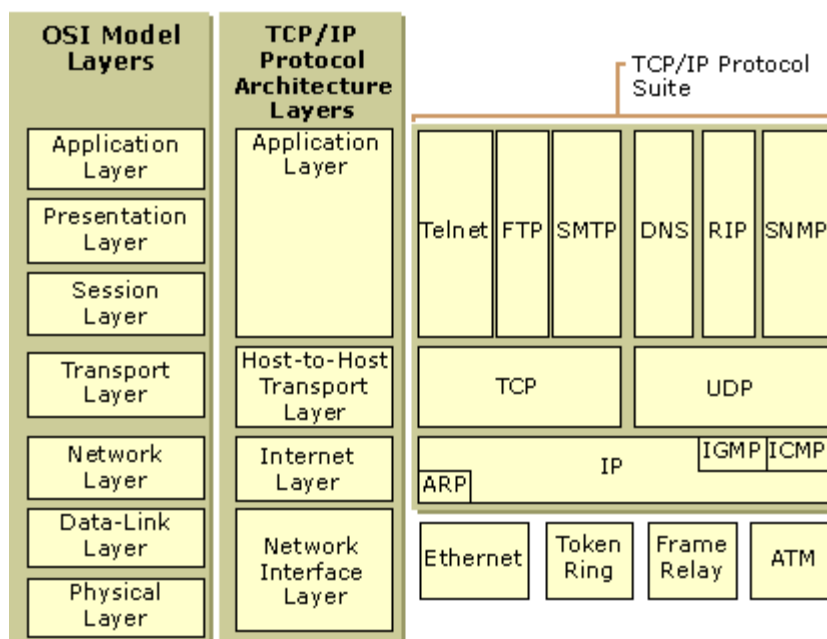


Figure 2. OSI vs. TCP/IP model (Microsoft, 2015)

Although the architecture the OSI model is more widely used than that of the TCP/IP some of the protocols of OSI model are not valid anymore. Only a handful of the protocols of the OSI model are still used, for example ISO-TSAP in industrial networks. The

protocols of the TCP/IP model are considered to be better suited for modern networks but the model itself is not used so much. [2: 45].

3 Ethernet

Ethernet was invented at the Xerox Palo Alto Research Center (PARC) by Metcalfe and Boggs [5: 15]. Over the course of 30 years the Ethernet standard has existed it has become the most popular and widely used network standard. Ethernet has grown from just connecting devices inside Local Area Networks (LAN) to being a universal connectivity standard. [6] Ethernet has even been adapted to industrial environments (e.g. Industrial Ethernet) where it is starting to replace old serial based transmission technologies.

3.1 Variants of Ethernet

Several versions of Ethernet have been developed throughout its history. Originally Ethernet devices were connected through linear coaxial cables. This was in the 1980s when the data rate of the technology was 10 Mbps. Modern Ethernet supports six different data rates through twisted pair and fiber optic cables. [7] Coaxial cables are sometimes used but since twisted pair and fiber optics are more common today, only they are included at the following sections.

3.1.1 Twisted Pair

Twisted pair cable consists of strands twisted together in pairs, as shown in Figure 3, to prevent electromagnetic interference (EMI). Twisted pair cables can reach up to speeds of 100 Gbps. The two most common twisted pair based technologies today are Fast Ethernet which refers to Ethernet standards with data rate of 100 Mbps and Gigabit Ethernet with data rate of 1000 Mbps. These standards use Category 5 (Cat5) and Category 6 (Cat6) twisted pair cables. [8]

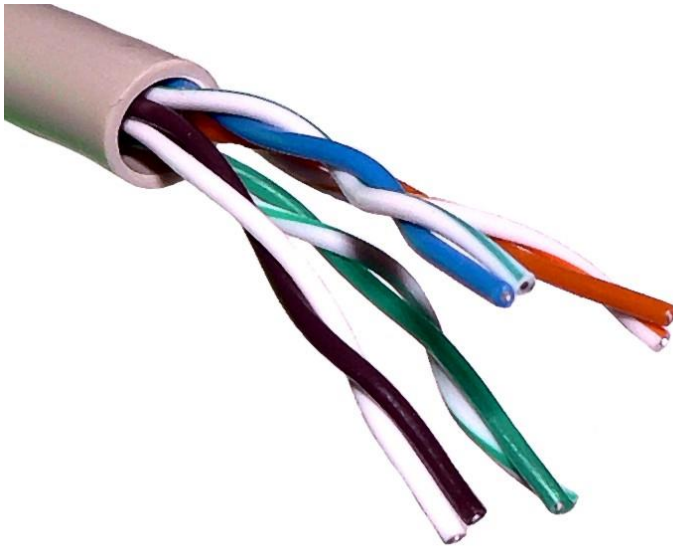


Figure 3. Unshielded twisted pair (UTP) cable with different twist rates (Wikipedia, 2015)

It is possible to reach 40 Gbps or even 100 Gbps with twisted pair cable according to IEEE in the Ethernet standard but this higher bandwidth requires the use of newer Category 7 and 8 cables. [7]

3.1.2 Fiber Optics

Optical fibers are usually thin strands of glass but cheaper plastic variants also exist. Because of the flexibility of optical fibers they can be bundled together as fiber optic cables. As can be seen in Figure 4, inside a fiber optic cable there are bundles of optical fibers. These bundles are placed around a central member which strengthens the cable. Around all of this is different jackets and coatings depending on the application the cable is intended to be applied to. Fiber optics also offer a much more secure and resilient transmission medium compared to traditional copper alternatives. This is due to electromagnetic interference (EMI) which is not an issue with fiber optic cabling since the data is transferred through pulses of light. This also prevents eavesdropping of the transferred data almost completely and gives a tremendous advantage for using in difficult industrial environments.

While traditional copper based cables are used at the edge of networks in the access layer to connect end users and devices to the network, fiber optic cables are used in the backbones of networks. This is due to the installation costs of fiber optics compared to copper based solutions. There are two types of fiber optics available today, multi-

mode fiber (MMF) and single mode fiber (SMF). [9] Figure 4 illustrates an optical fiber cable.

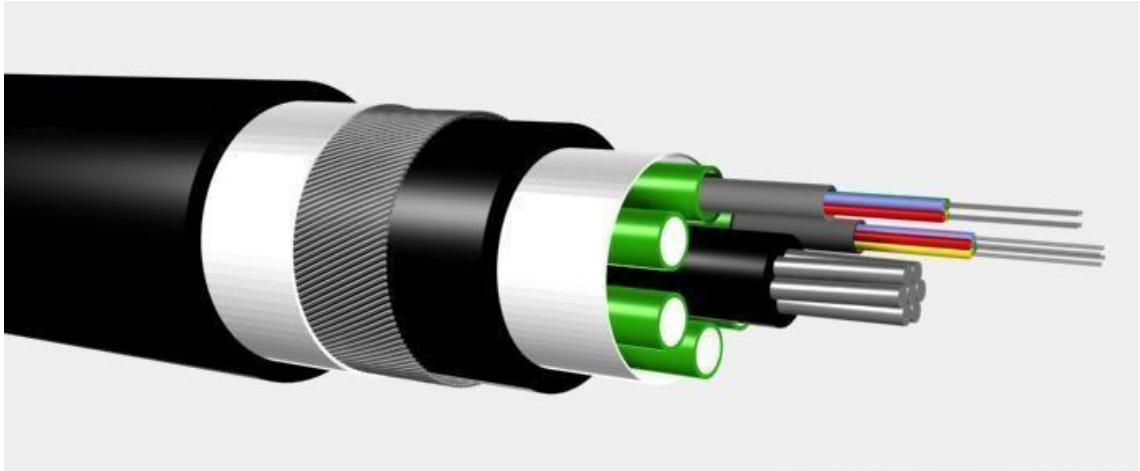


Figure 4. Optical fiber cable (Wikipedia, 2009)

Multimode Fiber

Multimode fiber was the first optical fiber type to be manufactured and used commercially. The multimode fiber gets its name from the fact that it carries multiple light rays, or modes, within the fiber core. Due to multimode fiber's ability to carry multiple signals the fiber's core is much larger than the ones found in single mode fibers. Multimode fiber's core diameter is most commonly 50 or 62,5 μm . [10] The wavelengths used in multimode fibers are 850 and 1300 nm. The ISO 11801 standard determines three different multimode fiber classes.

1. OM1 62,5/125 μm
2. OM2 50/125 μm
3. OM3 50/125 μm

The first two classes, OM1 and OM2, are considered as legacy multimode fibers. If multimode fiber is installed today, it is the Laser Optimized 50/125 μm multimode fiber (OM3). It has a core diameter of 50 μm and a cladding of 125 μm . OM1 and OM2 multimode fibers support speeds up to 1 Gbps using Light Emitting Diode (LED) transmitters. OM3 on the other hand is powered with Vertical Cavity Surface Emitting Laser

(VCSEL) which makes it possible to reach even 100 Gbps speeds but still retains the support for slower speeds. This makes it ideal for new installments. [11]

Single Mode Fiber

Single mode fibers are usually used in backbone networks and in communications between buildings. Because the cost of single mode fibers and the optics used with them has been steadily decreasing to the same level with multimode fibers so the use of single mode fibers in LANs has become a valid option.

Single mode fibers have a core diameter of $9\ \mu\text{m}$ and $125\ \mu\text{m}$ cladding most commonly. Single mode fibers use wavelengths of $1310\ \text{nm}$ $1550\ \text{nm}$ for carrying the signal. As you can see from the figure 5 single mode fiber carries only one light pulse whereas multimode fiber carries multiple light pulses which bounce between the core walls. By only carrying one light pulse single mode fiber avoids dispersion caused by multiple pulses travelling in the core. Single mode fiber also has lower fiber attenuation than multimode fiber which enables single mode fibers to transmit more information in the same amount of time compared to multimode fiber. These traits enable single mode fiber to carry information much longer distances than multimode fiber. [9] Figure 5 illustrates light propagation in fiber.

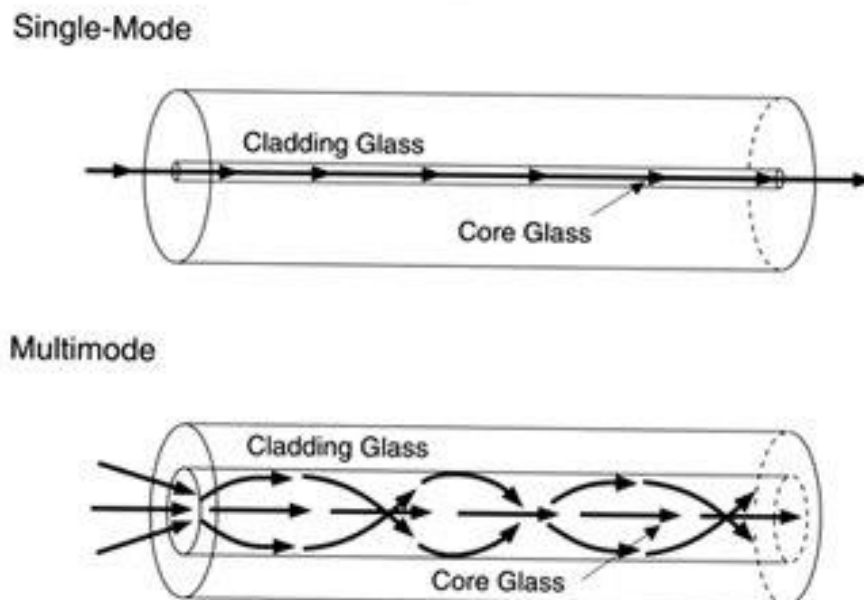


Figure 5. Light propagation in fiber (Lascomm, 2005)

3.2 Comparison

Due to the fact that data communication over fiber optic cables is not affected by EMI it is very well suited for difficult and often harsh industrial environments. Fiber optic cables are also a good choice for communications over long distances since twisted pair cables can only be 100 meters long. Downside is that fiber optics costs more than traditional twisted pair cable solutions. This is not because fiber cable materials cost more but the installation is more demanding due to the need to splice optical fibers and fiber splicing requires specialized and expensive equipment along with expertise.

4 Industrial Ethernet

As Ethernet has established itself as the leading networking solution with its flexibility, performance and cost-effectiveness, many industry organizations have turned their attention towards it. Industry organizations have started integrating existing fieldbus architectures to industry environments by leveraging Ethernet technology and are calling this Ethernet designed specifically for industry needs the Industrial Ethernet

4.1 Same Technology, Different Approach

. Demand for real-time and deterministic communications are perhaps the biggest differences when comparing traditional “office Ethernet” to Industrial Ethernet [12]. As Figure 6 illustrates the further away we move from an office environment and traditional IT services towards plant floor automation the faster respond times are correspondingly needed.

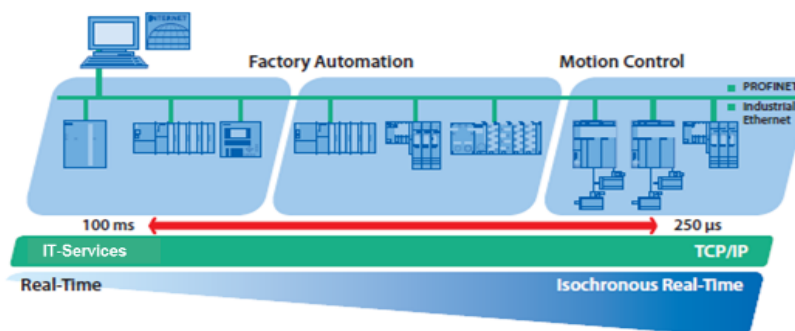


Figure 6. Demands for response times (PI North America, 2015)

In addition to custom protocol stacks and services Industrial Ethernet also refers to physical network components such as cables, connectors and network active devices. These components are often more rugged than their standard counterparts so that they can stand the harsh environments of most industrial premises.

Industrial Ethernet takes the existing Ethernet standards and implements them to different industrial environments such as manufacturing control networks.

For example in Figure 7 we see that Profinet implements its own real-time channel and QoS parameters at OSI layers 2, 3 and 4 which makes it possible to run time-dependent and deterministic applications on top of normal Ethernet stack. [13]

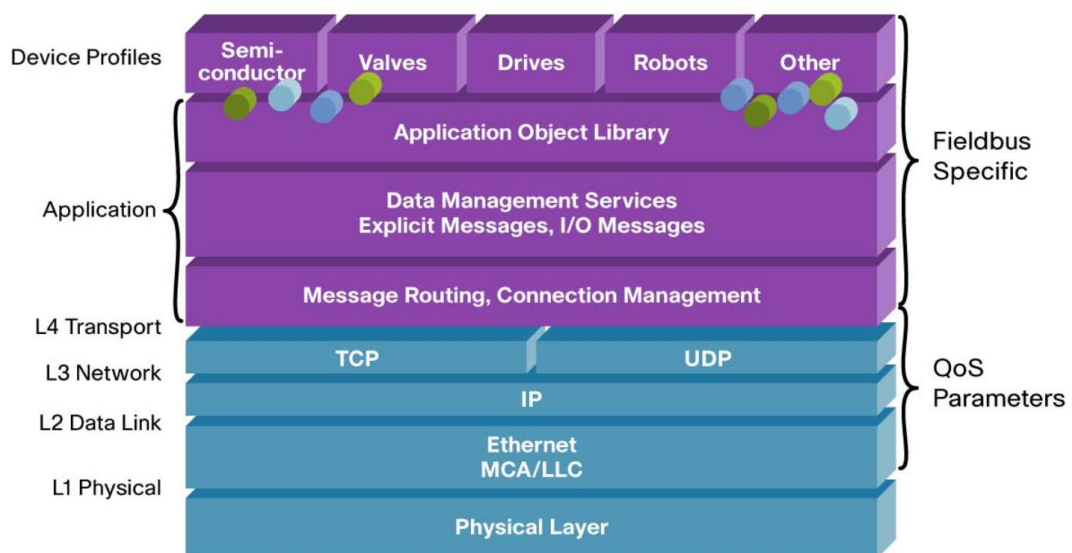


Figure 7. Using intelligent Ethernet for automation control [12].

Industrial Ethernets approach implementing standard Ethernet in industrial environments in three different ways depending on the real-time and cost requirements of applications. These three approaches are illustrated in Figure 8.

1. The first approach, also known as Class A, uses standard Ethernet as defined in the IEEE standard 802.3, standard TCP/IP stacks and standard hardware. This approach is also considered to be the “best effort” approach since the real-time performance is somewhat limited due to unpredictability in network active devices, for example switches.

2. The second approach, also known as Class B, takes into account the demands of real-time applications. It still uses standard networking hardware and standard Ethernet but adds prioritization to the table. This is done by bypassing the standard TCP/IP stack with custom process data protocol on OSI layers 3 and 4. This protocol resides in the Ethernet frame where it is tagged to give it priority. This does not mean that TCP/IP protocols are abandoned, they still exist but their access to lower layers are limited by a custom layer that can be considered to act like a timing layer.

3. The third approach, also known as Class C, highlights performance even further compared to the second approach. In addition to using the same prioritization techniques and custom protocols also dedicated hardware is implemented to increase performance. For example Profinet uses switches called the Special Real-time Ethernet Controllers. This approach is adapted if maximum real-time performance and determinism are required from the application, for example motion control. This approach also covers other communication types via various channels parallel to the real-time channel. TCP/IP channel also exists although it is bypassed by the real-time channels. Determinism is achieved through a technique called scheduling that enables the use of fixed transmission cycles and cyclic synchronization of network nodes.

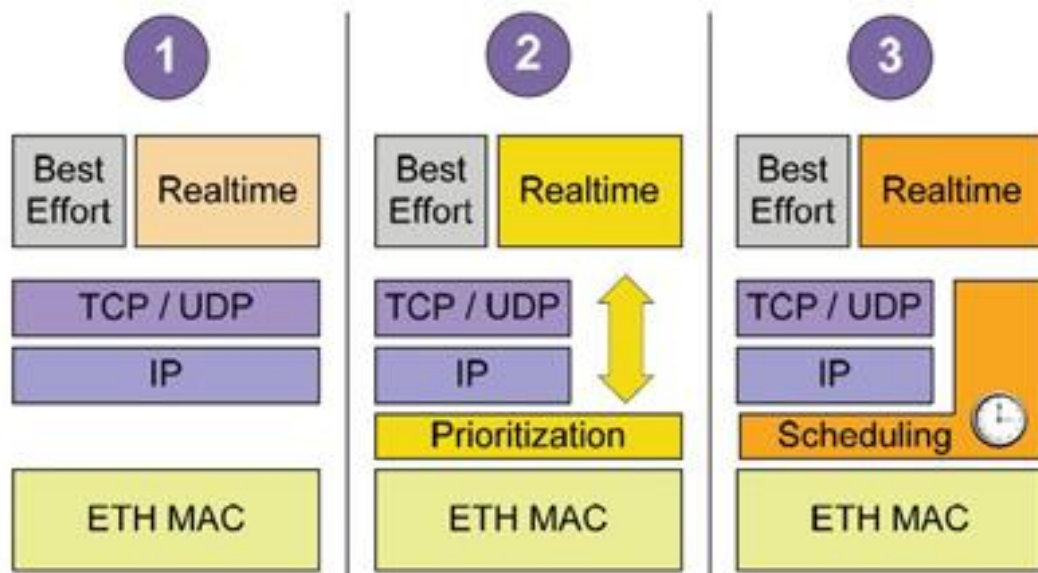


Figure 8. Different approaches for achieving real-time communications (Industrial Ethernet Book, 2012)

From the three approaches shown in Figure 8, Profinet adapts approaches two and three. By doing that Profinet covers many varying scenarios in the world of automation while still being able to provide real-time performance and determinism when needed. [14]

4.2 IT Meets Automation

Automation and corporate networks are traditionally separated from each other but as the automation field is moving towards Industrial Ethernet the separation of office and automation networks is not so absolute anymore. This brings many challenges for both automation and IT departments.

Networking world with its myriad of protocols is familiar to IT departments, they know how networks work and are familiar with different protocols that run on networks. Automation department can leverage this knowledge of networks and protocols to make it easier to manage Ethernet based industrial networks. For example simple network management protocol (SNMP) provides diagnostic data such as retry counts and bandwidth among others which can be very useful and valuable to industrial system management. Another useful protocol is link layer discovery protocol (LLDP) which allows the discovery of the logical topology of the network among other things. [17]

When integrating plant floor automation and other industrial systems to same networks IT department needs to recognize the unique requirements industrial environments and systems put on networks on both application and physical levels. This means that although the corporate and industrial networks are physically connected, logically they are separated with for example firewalls. [17]

4.3 Special Requirements

Industrial Ethernet has some special requirements when compared to traditional office Ethernet. As mentioned before, industrial environments are often much harsher than traditional corporate office, this is maybe the most obvious difference. Plant floors can be full of oily vapors, the atmosphere is very hot and humid and EMI can be a real issue. These environmental conditions are addressed by using, for example, M12 con-

nectors for terminating data cables, devices with high Ingress Protection rating, e.g. IP6x, and EMI protection.

Response times must be much faster than in the office world where for example email can take several seconds to reach its destination. This is not the case in industrial networks where control messages have to arrive in milliseconds with a jitter of microseconds, especially when motion control applications are concerned. [15: 35]

In addition to speed, determinism is also an important aspect. Arrival of the packets must be predictable.

Ensuring uptime is crucial in industrial systems since even a little outage in production of for example a paper mill can cause a massive loss of income for the company. Uptime is often ensured with redundancy on both logical and physical levels, for example redundant uplinks and redundancy protocols such as RSTP (Rapid Spanning Tree) and MRP (Media Redundancy Protocol).

5 Profinet

Profinet is an open Industrial Ethernet standard developed by the world association of Profibus and Profinet manufacturers and users, the Profibus International (PI). Profinet is standardized in IEC 61158 and IEC 61784. Profinet encompasses applications with a wide range of real-time requirements.

Profinet is a successor for the world's most used field communication standard, Profibus. Profibus is a serial based industrial communications standard which is over 25 years old. Two variations of Profibus exist today; the more common of the two is Profibus DP (Decentralized Peripherals) which is simple, low cost and high speed field-level communications technology, and the other common variation is the Profibus PA (Process Automation) which is a more application specific technology. Profibus DP is generally designed for internal uses, like cabinet mounting, when Profibus PA is meant more for field implementations. Profibus DP devices use RS485 shielded twisted pair cabling in addition to fiber optic cables and Profibus PA runs on Manchester Bus Powered (MBP) cable. Profibus utilizes master-slave communication technology with token

passing between masters. [16] Figure 6 illustrates the integration of Profinet to different system levels.

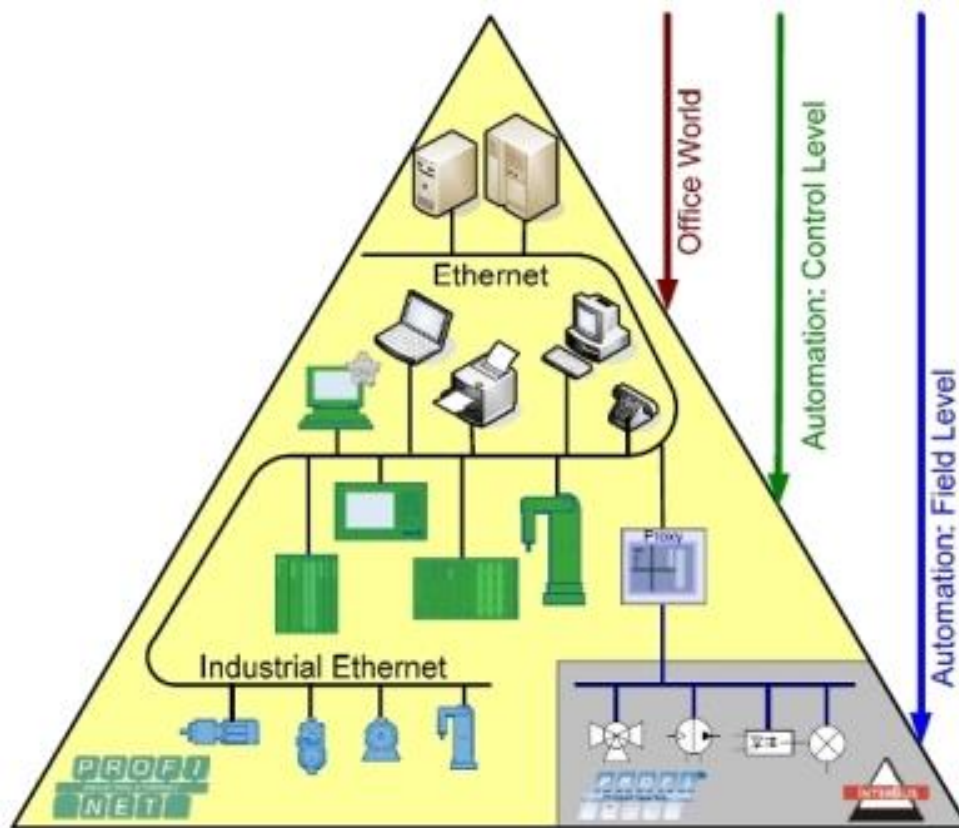


Figure 9. Integration of Profinet to different system levels [17]

The use of Profinet is very cost-effective due to its ability to integrate very well to existing networks without the need to modify the superordinate network. It can also be used to connect existing fieldbus systems to Ethernet-based networks through proxies as the figure 9 illustrates.

All Profinet devices, both active and passive, are designed to function in the harsh industrial environments. Profinet can also be run on standard network devices if real-time requirements are met. [17]

The development of Profinet started in 2000 and the first specification released was the Profinet CBA (component-based automation). Profinet CBA was designed for component-based machine-to-machine communication via TCP/IP and object-oriented programming. Profinet CBA is fully compatible with standard networking hardware. Another version of Profinet is the Profinet IO which includes both Profinet RT and Profinet

IRT. Since Profinet is modular in nature the user can select the functions required by utilizing Profinet IO or CBA or both.

5.1 Profinet Versions

Profinet follows the three approaches of Industrial Ethernet with Profinet IO and Profinet CBA. From these two versions the former is meant for communication between controllers and IO devices with RT and IRT requirements and the latter for communication among controllers via TCP/IP with some RT requirements. Figure 10 shows the real-time requirements of Profinet versions.

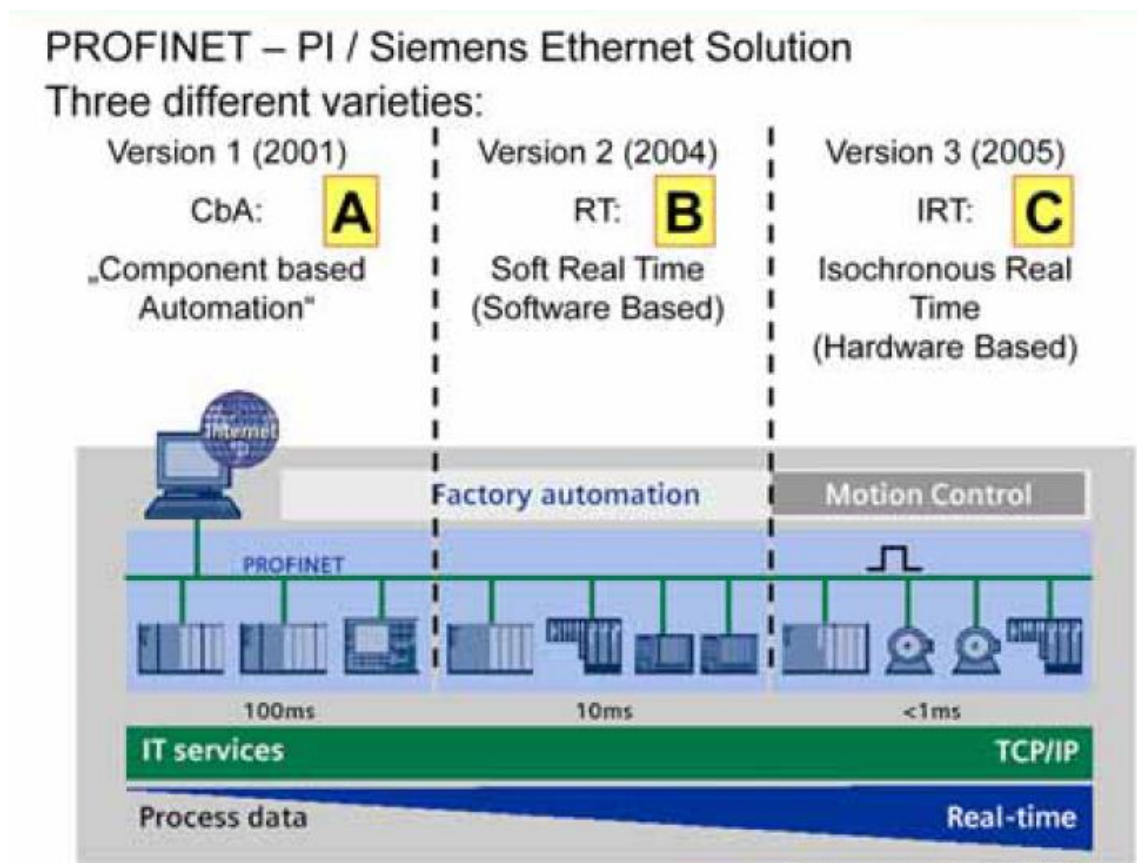


Figure 10. Real-time requirements of Profinet versions (Profibus International, 2014)

In Figure 10 we see that Profinet CBA is mainly for non-real-time while Profinet RT handles factory and process automation and Profinet IRT is for the most demanding motion control applications such as robots on assembly lines.

5.1.1 Profinet CBA

Profinet CBA, also known as Profinet Class A, is designed for machine-to-machine communication over TCP/IP and object-oriented programming. The idea behind Profinet CBA is that the system can be implemented by deploying different intelligent and autonomous subsystems which communicate with each other through controllers, i.e. controller/controller communication.

Profinet CBA is a class 1 approach which supports the trend of shared automation systems where automation functions are divided between intelligent subsystems, this is illustrated in Figure 11.

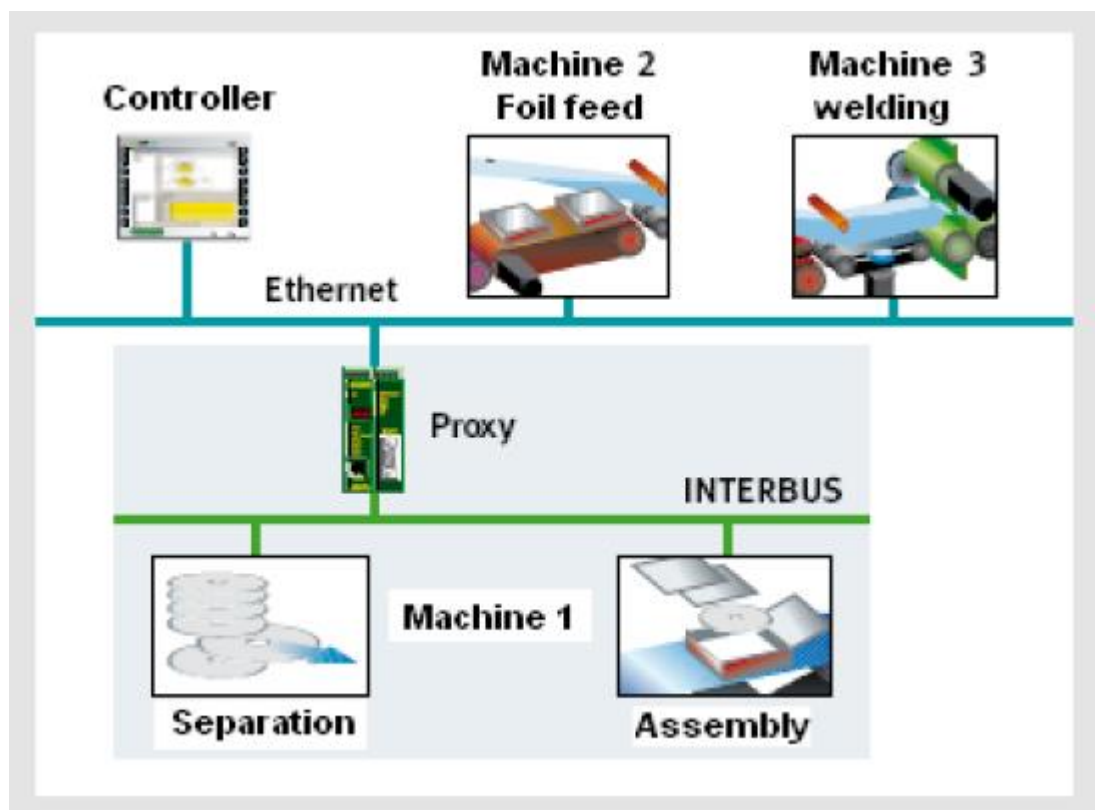


Figure 11. Profinet CBA supports modular and intelligent distributed systems (Phoenix Contact, 2010)

Profinet CBA is an automation concept which uses both cyclic and acyclic communication with even 10 ms response times. This is well suited for communication between controllers. When used solely TCP/IP communication, Profinet CBA supports systems with response time requirements of 100 ms and above. [18]

5.1.2 Profinet IO

The system which Profinet uses to connect distributed I/O-devices directly to Ethernet is called Profinet IO. Profinet follows the provider/consumer model where provider sends the data to be handled to the consumers. Figure 12 illustrates the three device classes distinguishes by Profinet.

IO-controller is typically the device where the automation program runs, i.e. programmable logic controller (PLC). The output data for IO devices is administered by IO controllers.

IO-device operates as a distributed I/O field device that is connected to one or more IO-controllers via Profinet IO.

IO-supervisor acts as an engineering tool for diagnostics and parameterization. The IO-supervisor can be a personal computer (PC), human machine interface (HMI) for commissioning and diagnostic purposes. [18] Figure 12 shows the device classes and communication paths for Profinet IO.

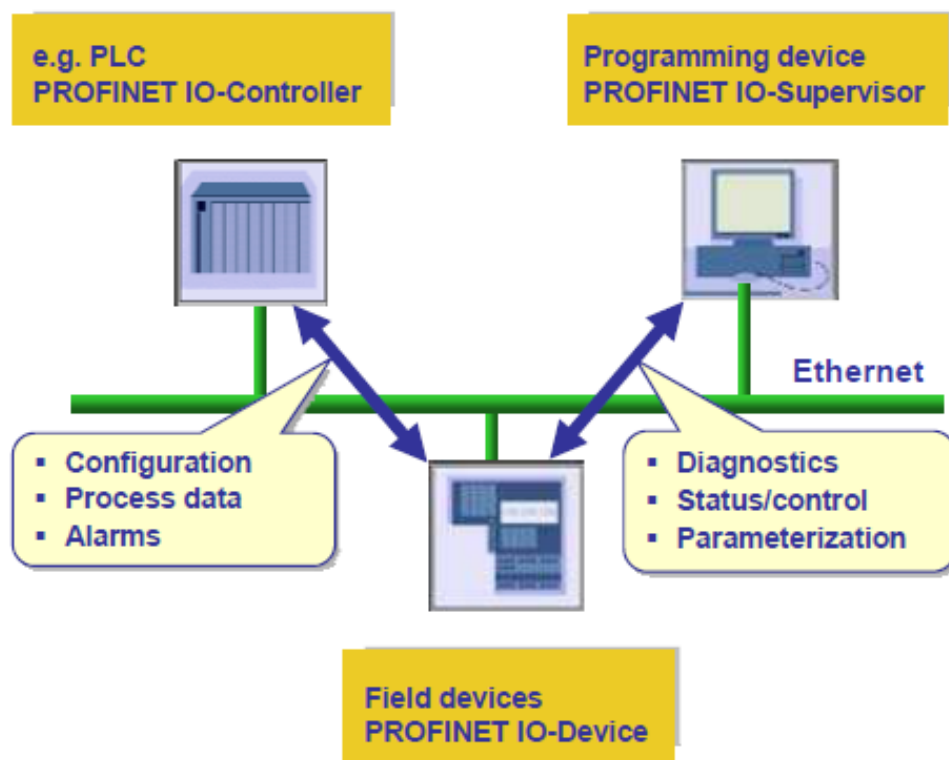


Figure 12. Device classes and communication paths for Profinet IO (PI, 2011)

Communication happens mostly via unmodified Ethernet and TCP/IP packets and network devices in Profinet environments. This enables integration into office network quite painlessly.

In Profinet RT, also known as Profinet Class B, the process data communication occurs via optimized protocol stack on OSI Layers 3 and 4 in parallel with TCP/IP. Every device gets an IP-address through the TCP/IP which also allows communication via other protocols such as HTTP. In addition to optimized protocol, prioritization is also used. Figure 13 illustrates how the Ethernet frame looks like in Profinet RT communications.

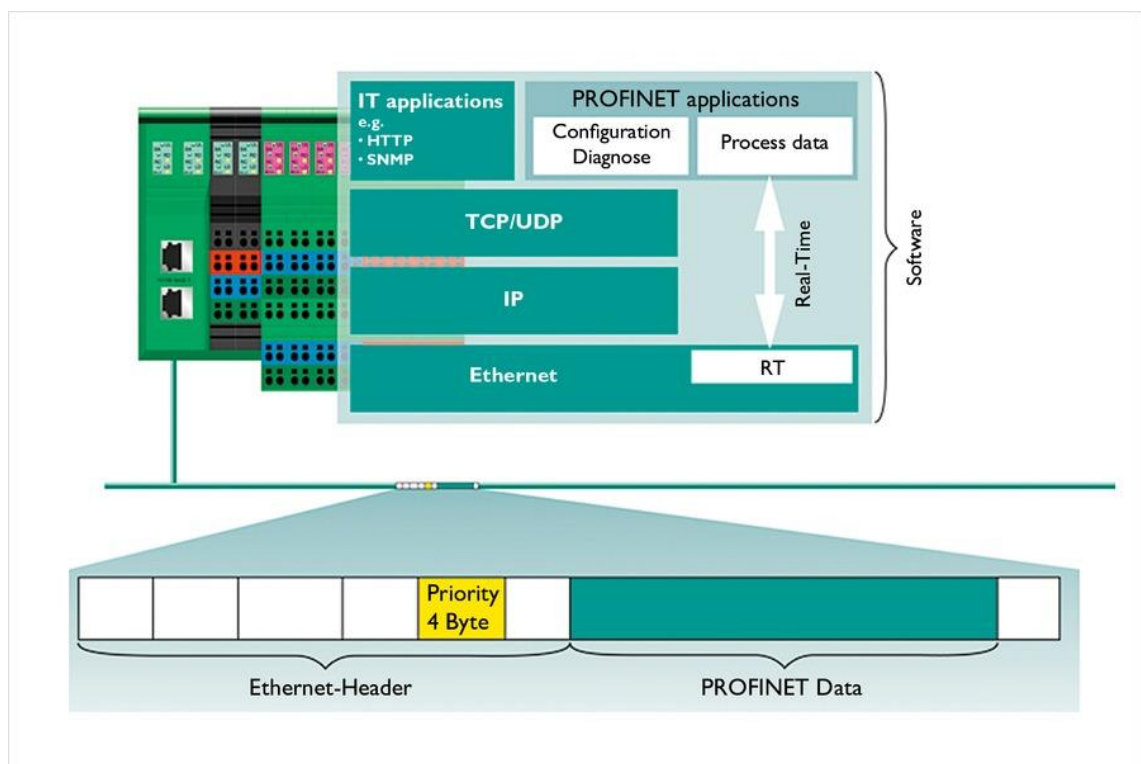


Figure 13. Data transmission of Profinet RT in the Ethernet frame [18].

In Figure 13 we see an Ethernet frame and the protocol stack. This Ethernet frame is comprised of a header and a Profinet data partitions. The possible prioritization tag of Profinet real-time messages is located in the Ethernet header. [17]

Prioritization is implemented by assigning VLAN ID 0 with priority 6 in accordance with the IEEE 802.1Q standard. For this to work, though, messages with Ethernet type

0x8892, which tells that the packet contains Profinet data, must be accepted and forwarded in the used switches.

preamble (8 byte)	dest. address (6 byte)	source address (6 byte)	priority tag	Eth type 0x8892	automation data (+ Pad)	checksum (4 byte)
----------------------	---------------------------	----------------------------	-----------------	--------------------	----------------------------	----------------------

Figure 14. Ethernet frame with Profinet RT protocol data and priority tag [17].

Figure 14 shows how priority tag and an Ethernet type 0x8892 is used in the Ethernet frame to tell that Profinet communication is taking place in Profinet RT and IRT.

Profinet IRT, also known as Class C, is used when maximum real-time is needed, for example motion control applications. The feature set of Profinet IRT is equivalent to Profinet RT but real-time performance is increased with special hardware. Profinet IRT is based on an extension of the Ethernet stack as shown in Figure 15.

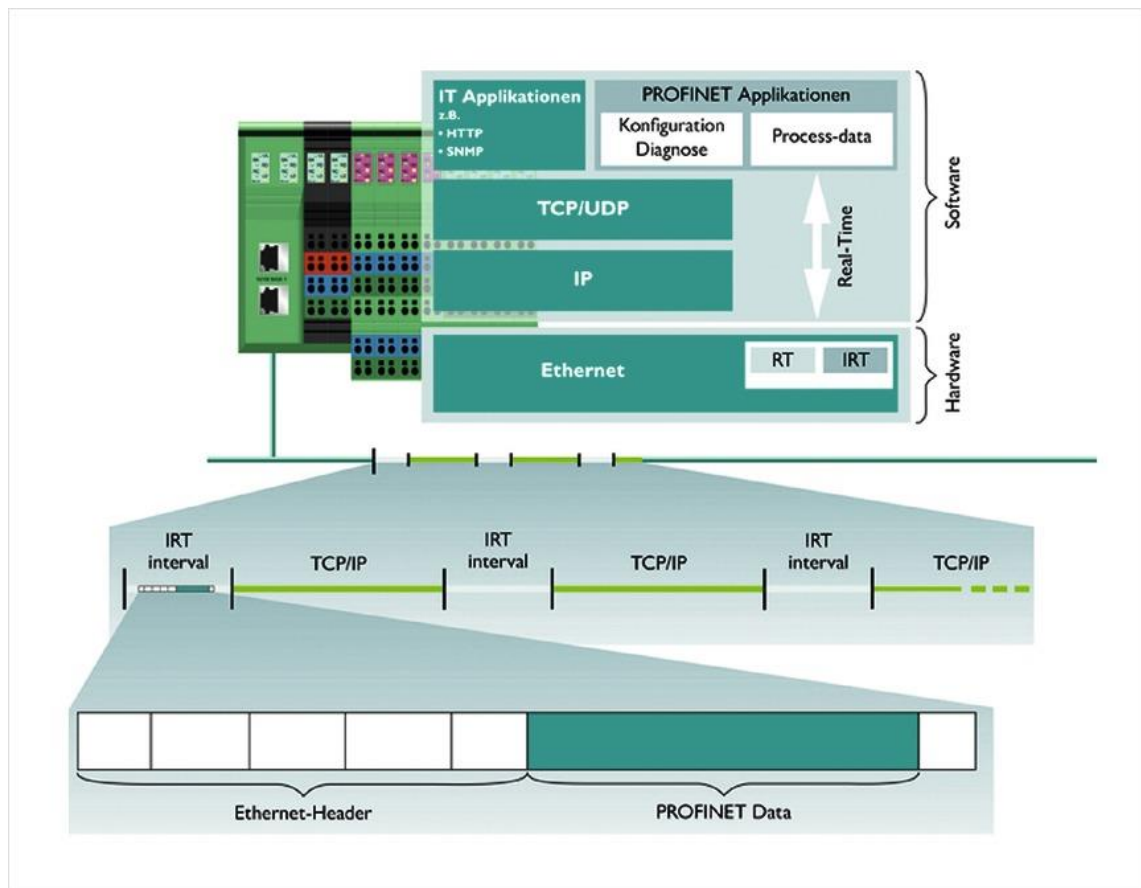


Figure 15. Data transmission of Isochronous Real-time [18].

Profinet IRT allows devices on the Profinet network to synchronize their communication with the use of scheduling, i.e. time-slot technology. Scheduling means that in every communication cycle a slot is specified for IRT data and clock signal.

Profinet RT and IRT communications use optimized protocol stack on OSI Layer 3 and 4 for the real-time channel. This means that Profinet RT and IRT communication bypasses the whole TCP/IP portion of the protocol stack and does not get an IP address. In other words RT and IRT communications are restricted to one logical subnet [17]. This does not mean that packets cannot be routed from one subnet to another. Profinet CBA can be used to pass packets via TCP/IP although this introduces minor delay compared to plain real-time communication. [17]

5.2 Application Profiles

Profinet application profiles are used to specify different features and functions, such as particular properties, performance characteristics, of Profinet for use in specific devices or applications. Roughly two groups of applications are distinguished; general application profiles that can be applied to different applications in general, for example PROFIsafe and PROFIenergy, and specific application profiles that are developed for specific use cases such as PROFIdrive for drive technology. [19]

5.2.1 PROFIsafe

PROFIsafe is a standard for functional safety (fail-safe) in accordance with the safety standard IEC 61508. PROFIsafe eliminates the need for additional wiring by enabling the fail-safe messages to be transmitted directly to the process controller. PROFIsafe is compatible with both Profinet and Profibus alike. PROFIsafe can handle different fault situations like address errors, significant delays and data loss with for example time monitoring and authenticity monitoring. [19]

5.2.2 PROFIenergy

High cost of energy and legal obligations forces industry to come up with greener and more efficient energy technologies. PROFIenergy is Profinet's answer to this.

PROFenergy is an effective, active energy management technology which saves energy and reduces energy costs by purposefully switching off unneeded devices. [19]

5.2.3 PROFdrive

PROFdrive is an application-oriented profile for Profibus and Profinet which contains syntax and semantics for drives and automation systems to communicate with each other. It is standardized in IEC 61800-7. PROFdrive's goal is to offer vendor neutrality, interoperability and investment protection. [19]

5.3 Network Topology

Since Profinet is Ethernet based technology it supports very flexible networks with an almost unlimited number of options for topology. PI organization introduces three basic topologies for Profinet; star, tree and line.

5.3.1 Star Topology

In a star topology all devices are connected to one central switch with its own cable as shown in the figure 16. This central switch, or node, acts as a repeater for data flow. The main advantage with star topology is that if one node fails, the others are not affected by it. The main disadvantage is that if the central node fails, all the other nodes lose connectivity. The star topology is particularly useful if devices are physically located near each other, e.g. in a cabinet. [20] Star topology is illustrated in Figure 16 below.

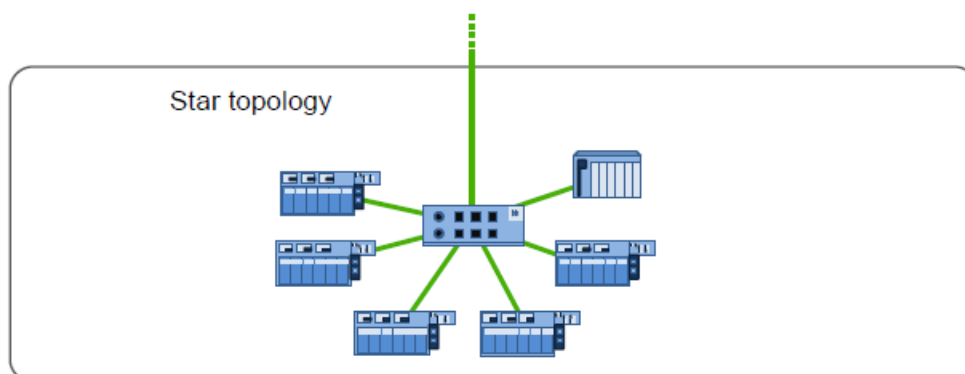


Figure 16. Star topology [20].

5.3.2 Tree Topology

A tree topology is basically a combination of star topologies. For example in an industrial plant different parts of the plant can be designed with star topology and then connected to each other via neighboring switches as seen in figure 17. The main advantage is that a large network can be “divided” into smaller more easily manageable parts. The main disadvantage of the tree topology is the same as in the star topology. If the central node fails, all the other nodes lose connectivity. [20] Tree topology is illustrated in Figure 17 below.

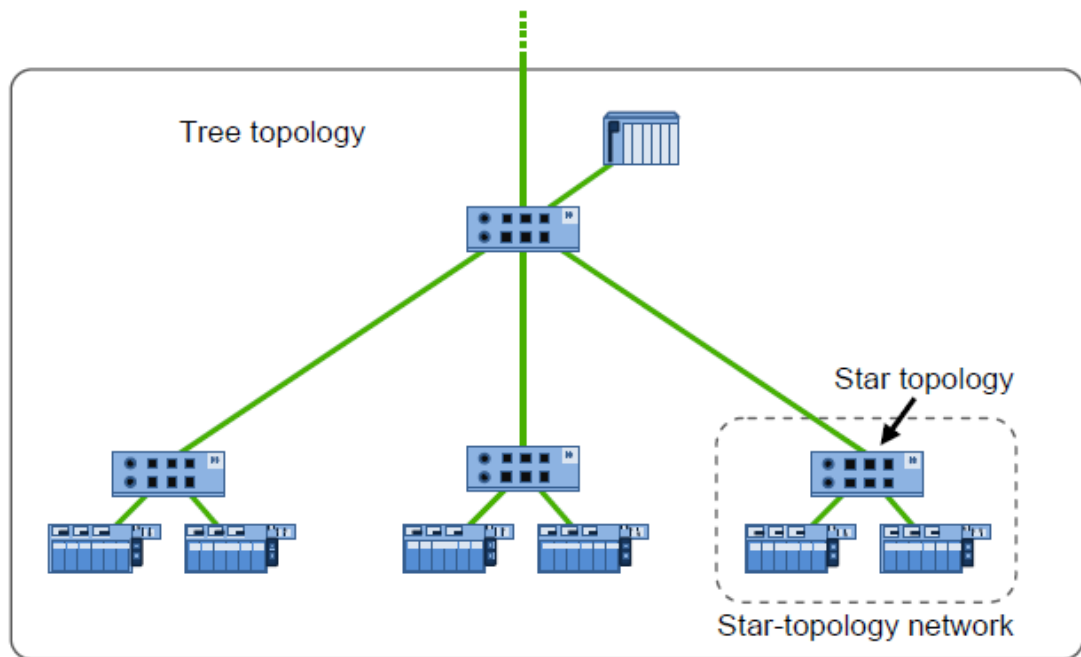


Figure 17. Tree topology [20].

5.3.3 Line Topology

In automation the line topology is a well-known concept where devices, or nodes, are linked to each other in series as illustrated in figure 18. Profinet environments all Profinet devices equipped with integrated switching capability can form a line topology thus eliminating the need for discrete switches. The main advantage of line topology is its easy installation and the simplicity of design. The main disadvantage is that if one device in the line fails the others lose connectivity unless the line is extended to a ring topology which increases the system's redundancy. Ring topology is essentially a line topology where both ends of the line is connected to a central switch. [20] Line topology is illustrated in Figure 16 below.

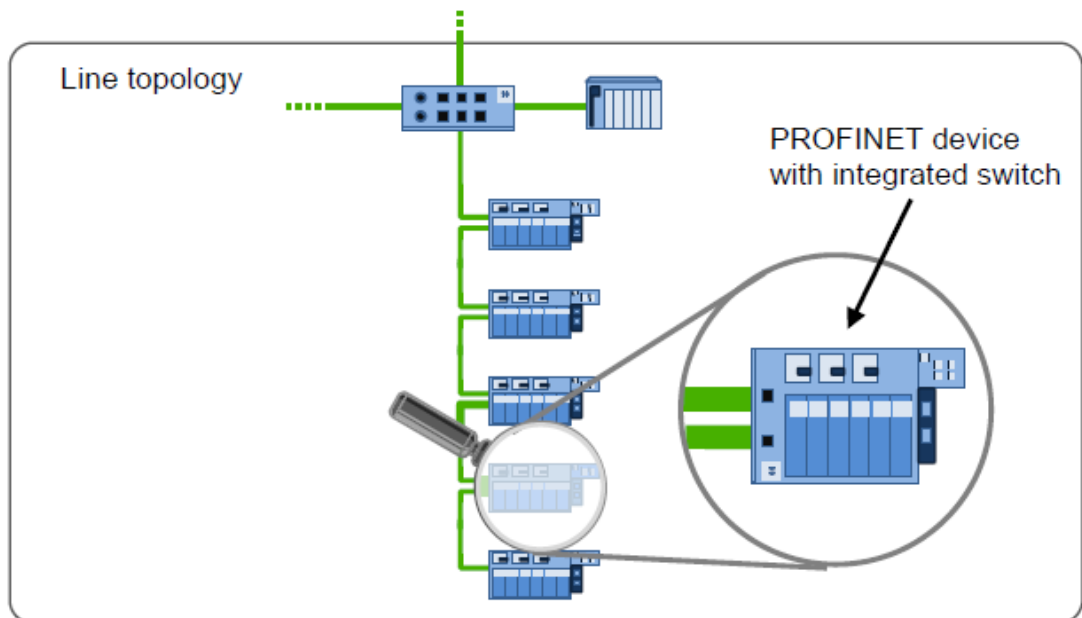


Figure 18. Line topology with integrated switching capabilities in Profinet devices [20].

5.4 ProfiCloud

Profinet also supports cloud functions via a technology called Proficloud. The cloud functions can also be added to existing installations. Proficloud, as illustrated in figure 19, allows Profinet users to utilize modern cloud services and telecontrol applications with ease to control remote locations centrally. With Proficloud users can import valuable data from Profinet systems to cloud servers such as usage and network statistics.

Proficloud implementation has always at least one cloud coupler and one cloud device. In Figure 19 we see how Profinet devices are connected to Proficloud. The cloud coupler has two Ethernet ports, one for the local network connection and one for connecting to the Internet. The coupler automatically sets up a connection to the Proficloud so that it is operational after a short period of time. This is accomplished by preconfiguring the cloud devices before setting them up at the preferred location. With preconfigured devices Proficloud tries to reduce complexity of setting up a VPN connection. Network data is obtained via DHCP. [21]

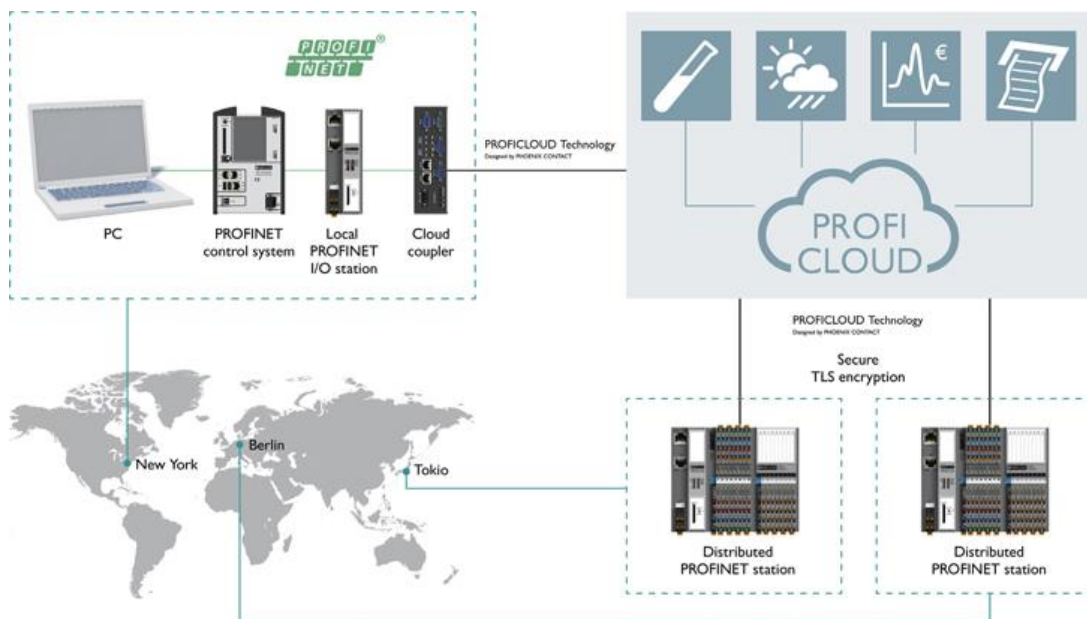


Figure 19. Overview of the Proficloud concept [21].

Data transmission is encrypted with TLS encryption which is also used, for example, in banking solutions. With the use of WebSockets as data transfer points, Proficloud aims to be firewall friendly. This is because WebSocket is a standardized web mechanism which uses ports 80 and 443. [21]

Connecting devices to the Internet presents a risk for unauthorized access. Proficloud takes this into account by only allowing outbound traffic. Connections from the Internet are denied. In addition Proficloud devices do not have any open ports.

Connecting production networks straight to the Internet is not considered to be a good method. The cloud coupler contains two separate network cards for local network and the Internet, these network cards are not linked via TCP/IP. The communication be-

tween the network cards is handled solely on the application layer and is limited to Profinet-relevant data. [21]

5.5 Transmission

Profinet supports full-duplex Ethernet network where it offers two options for transmission media in RT and IRT applications; fiber optic and copper cables. Profinet allows communication also via wireless media, such as WLAN and Bluetooth, when Profinet CBA is used. These cables can be terminated with different connectors depending on installation location needs. Profinet uses 2-pair cable for 100 Mbps and 4-pair cable for Gigabit cabling systems. Figure 20 illustrates the different industrial plugs used in Profinet installations.







	Copper		Fiber Optic	
IP 20 Inside	RJ 45 		SC-RJ 	
IP 65/67 Outside	RJ 45 	M12 	SC-RJ 	M12 

Figure 20. Industrial plug connectors for Profinet [19].

In Figure 20 we see different industrial plug connectors for Profinet cabling. Profinet can use standard connectors when installing devices in non-industrial environments where rugged connectors are not needed. SC-RJ connector is a small-form-factor fiber optic connector designed for industrial use. It is small enough to fit in the same space as an RJ45 connector but is based on an SC connector. M12 connector is a connector designed

for industrial use. It uses a locking system to ensure connectivity harsh industrial environments. [23] M12 features Ingress Protection up to IP68 (dust tight and protection against long periods of immersion under pressure) [24].

5.6 Integration with Overall Network

Integration of automation areas with real-time communication into overall network is generally a problem-free procedure. However, a fact that Profinet RT and IRT communication can only happen at layer 2 domain must be taken into consideration. Profinet RT and IRT communication can be routed via TCP/IP by using Profinet CBA but this method introduces a moderate decrease in the real-time performance. [22]

Even the use of prioritization does not limit integration of Profinet to the overall network since Profinet and other Industrial Ethernet solutions use the same ordinary QoS (Quality of Service) mechanism, such as the priority byte in the Ethernet packet as described in the standard 802.3Q, as in the office world. [17]

Since Ethernet based communication systems are increasingly responsible for communications in industrial environments in the form of Industrial Ethernet, the need for security is also on the rise. This does not mean that security has not been a concern before but the nature of security has changed towards modern technologies and techniques such as firewalls and IPS/IDS systems.

6 Security of Profinet Networks

Ethernet based Profinet and Industrial Ethernet offers excellent performance, scalability, flexibility and integration for industrial applications. In addition to enabling the use of open and standardized IT technologies, such as WLANs and web applications, they offer a wide range of network security measures for protecting manufacturing devices and other automation components. [26]

Availability, integrity and confidentiality are often considered as the three most important points of network security in automation networks. From these three availability is often considered to be the most important from the manufacturing angle. This means that automation and control systems must be operational at all times, no downtime is

allowed. Integrity means that systems and data must be kept intact and protected from intentional or accidental modification. Confidentiality ensures that unauthorized users cannot access data. [26]

Security cannot be pinned down to just one place. Everything and everyone is part of the system security. This includes both IT and automation departments, management, site/company security and guards as well as automation component manufacturers. Company policy plays also a big role in security. Company policy defines to a large extent the security measures and approaches which will be implemented. [26]

Profibus International offers following guidelines for a good security architecture.

- Strong enough to protect systems but at the same time simple enough to be manageable with tolerable effort and understood by everyone involved, whether it is the installer or security expert.
- Universal so that it can be applied to similar cases. Myriad of exceptions makes the system unmanageable and difficult to detect violations and deficiencies.
- Supported by all parties. If everyone supports the cause and knows why security architecture is relevant, they will probably work more effectively.
- Called into question by everyone. When a weak point, deficiency, a bug or other anomaly in the network is discovered, it should be reported and fixed as soon as possible.
- Made into a daily activity. It should not left as it were on the installation day. [25]

All of the above aspects make up a unified security design, i.e. security architecture, which addresses potential risks and requirements for the network in different scenarios and environments.

6.1 Hacks and Vulnerabilities

When the protocols used in industrial systems, such as ISO-TSAP (International Standards Organization Transport Access Point), were designed the security concepts of that day were considered. It meant that the protocols had no security since the control systems were designed to be deployed in completely isolated networks. Same goes for the PLCs, they were designed and built without security since they were deployed in isolated networks. [28]

The situation today is that the security concepts used have not caught up with the profound change we have seen in cyber security in recent years. Even isolated or separated networks aren't safe, this was demonstrated by a computer worm Stuxnet which spread via an infected USB flash drive and attacked industrial PLCs in Iran in 2010. [28]

The following sections introduce three different exploits or hacks. What all these methods have in common is that they are conducted from within the automation network and they are aimed at devices capable of running Profinet and other industrial protocols. These hacks and vulnerabilities expose the devices for reconnaissance and exploitation which allows the attacker to collect valuable information or even physically brake crucial process components, for example Stuxnet caused the fast-spinning centrifuges to tear themselves apart in the Iranian nuclear plant.

6.1.1 Siemens Simatic S7 PLC Exploit

PLCs are devices responsible for controlling critical processes in the field. PLCs can be found in myriad of places, such as energy plants, gas and oil refineries railways and pipelines. PLCs are relied to control and automate processes that require ladder logic and different input and output layouts. [28]

Considering that PLCs are responsible for ensuring critical automation tasks, for example the flow of electricity to homes, businesses and factories, it is odd that the security was almost completely ignored when the PLCs were designed and built. [28]

PLCs have been evolving to take advantage of common networking standards like IEEE 802.3 Ethernet and IEEE 802.11 WiFi. The newer devices also support more

complex logics through increased storage space and processing power and capabilities.

The Simatic S7 exploit is not directly against Profinet itself but Profinet is used to connect to the network. The attack itself takes advantage of ISO-TSAP which is used by Siemens engineering software to communicate and program all S7 PLCs made by Siemens. Other vendors also use ISO-TSAP but this section concerns only Simatic products. [28]

From attackers point of view the fact that Simatic S7 PLCs communicate with ISO-TSAP on TCP port 102 is interesting since packets transmitted over ISO-TSAP communication are in plain text with no encryption, thus making it possible to launch man-in-the-middle and replay attacks. It also allows easy capturing of packets travelling between engineering workstation and the PLC, thus enabling the attacker to reverse the protocol and generate their own packets for malicious purposes. Everything required to do this is baked in the Step 7 engineering software application. [28]

In addition to using ISO-TSAP, the S7 PLCs has one other big weakness; the authentication is flawed. An attacker with captured packets containing the authenticated server session can just re-authenticate using the same packet. This can be very dangerous because of the way how the S7 PLCs handle the authentication process. [28]

When the user sends an authentication packet to the PLC the password or hash in the packet is compared to the one configured in the device, if the comparison returns a value that is true, the device then grants access and allows read/write/execute permissions to the PLC's memory. This means that the attacker can configure the PLC any way he/she wants. [28]

The Attack Vector

1. Capture the traffic between the engineering workstation and the PLC.
2. Extract and analyze the client portion of the packet.
3. Build your own packet based on the extracted client portion.

4. Replay the crafted packets to the PLC.

This type of exploit is easily avoidable by not letting people with malicious intents into the network but nowadays when everything is connected it is highly possible that someone will hack his way into the network eventually. In the situation of breached network, the use of common security measures, such as secure transmission channels, encrypted messages and the use of IPS/IPS, can prevent leaking of confidential data or at least greatly hinder the attacker so that the damage caused by the breach can be mitigated as much as possible.

6.1.2 Emulation of Profinet IO-Devices

Since Profinet IO uses standard Ethernet network components, it means that Profinet systems are also generally susceptible to same threats that are present in standard Ethernet networks, such as a man-in-the-middle (MITM) attack as seen in Figure 21, even ARP attacks like ARP poisoning can be conducted. In MITM attack a device, often a regular PC, poses as a valid communication partner for two devices by pretending to be something it is not, for example an IO device for an IO controller and vice versa. This allows the attacker to capture the communication between the two, send it to some unknown remote server or even inject modified configurations for the devices. These types of attacks are unknown for traditional fieldbuses. [29]

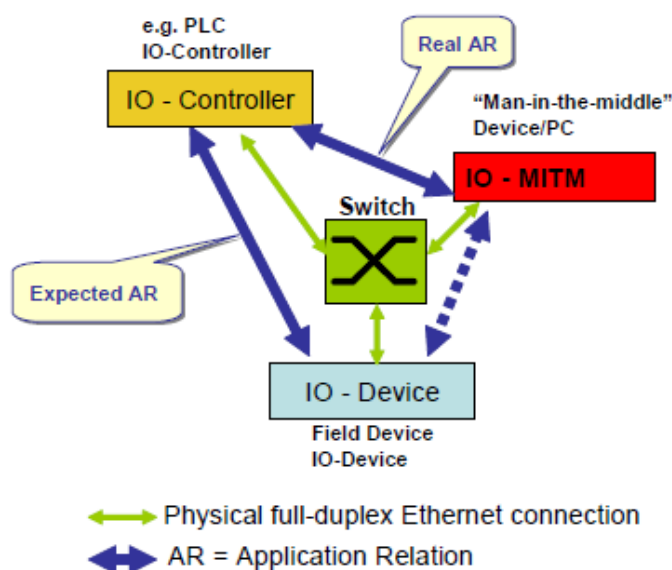


Figure 21. Man-in-the-middle attack in Profinet system [29].

The Profinet system in its basic form includes an IO controller and one or more IO devices. These two components make up a connection called Application Relation (AR) between them. This is done by the IO controller via UDP/IP with Distributed Computing Environment/Remote Procedure Calls (DCE RPC), which is a framework for client/server applications. Profinet IO controller is responsible of assigning an IP address for IO devices. [29]

Profinet IO devices are not only identified with IP addresses but Profinet names are also used, in fact Profinet devices are identified based on Profinet names rather than IP addresses. The Profinet names are assigned during the engineering phase and then saved in the IO device's non-volatile memory. These names are then configured to the IO controller responsible of them along with the desired IP addresses. When the IO controller starts it first sends DCP-identify message to verify that the IO devices are reachable and have valid names. After querying of the names and before assigning the IP addresses, the IO controller checks with ARP requests whether any IO device has been configured with duplicate IP addresses. If duplicate IP addresses are not present, the IO controller assigns an IP address, establishes an AR and sends configurations via TCP/IP to the IO device. After sending configurations cyclic data transmission takes place and IP addresses are not used anymore until configurations are needed to change again. [29]

This kind of setup is prone to errors if configuration is done carelessly. Two most critical and possible errors are duplicate IP addresses and Profinet names. These errors can be leveraged to launch MITM and ARP attacks in Profinet network, but few conditions must be met; the attacking machine must be able to meet the same timing requirements as the Profinet devices, for example if frames are sent in 1 ms cycles, the MITM machine must forward its own frames within the 1 ms cycle. If the MITM machine fails to do this, the whole attack fails for the reason that the switch updates its MAC table every time it receives a frame from the IO device. [29]

Michael Baud and Max Felser from the Berne University of Applied Sciences experimented on emulating a Profinet IO device in the Profinet system with an open-source MITM attack tool called Ettercap. They did not have any success in performing a MITM attack with Ettercap. The main reason for this was that the cyclic nature of data transmission was too much for the software which supports cycle times of 1 second and above while Profinet can use 1 ms cycle times. In other words every time they started

an ARP poisoning attack by sending ARP frames with the intention to overwrite the ARP table of the target device, the valid IO data of the actual IO device resets the ARP table because the cyclic time is so much smaller than what Ettercap is capable of. [29] Figure 22 illustrates how the MITM attack is performed in the “bridged” mode.

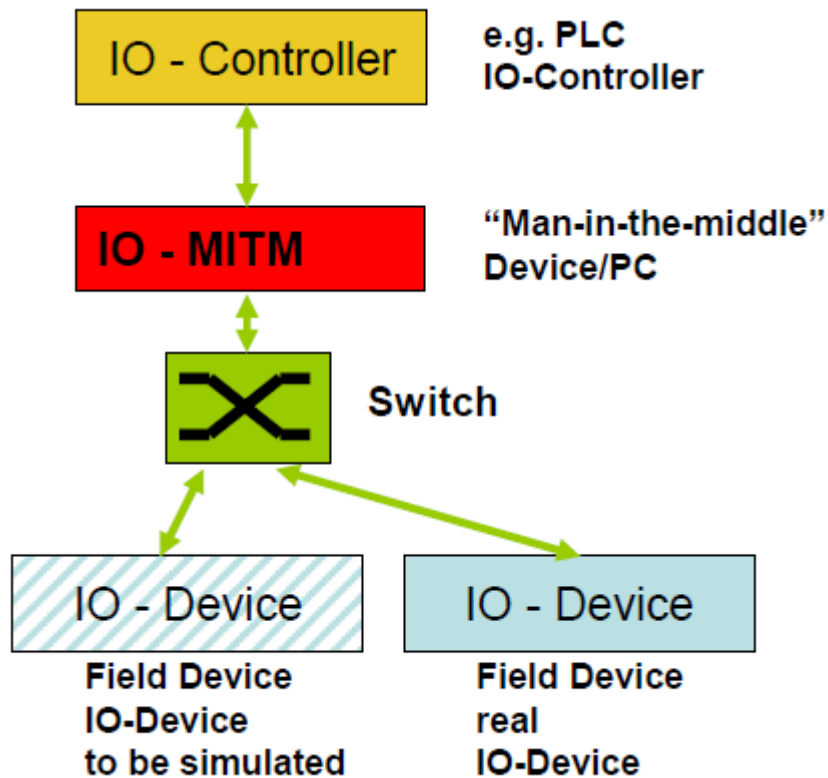


Figure 22. Performing the MITM attack in “bridged” mode [29]

However, Baud and Felser were successful on their attempt with ARP poisoning when they modified their attack to be in “bridged” mode, this means that the MITM machine is between the IO controller and the actual IO device as illustrated in Figure 22. In this “bridged” mode the attacker physically connects himself inside the Ethernet connection he is interested in sniffing with two Ethernet ports. [29]

6.1.3 ProFuzz

Fuzzing, or fuzz testing, is a Black Box technique for testing software which is conducted by injecting random, invalid or unexpected data to the inputs of a computer program. It can be semi-automated or even fully automated process. The basic idea be-

hind fuzzing is that every program has bugs which are waiting to be discovered and a systematical approach will reveal them sooner or later. [30]

ProFuzz is a Profinet fuzzer developed and released by Roland Koch and students at the University of Applied Sciences in Augsburg. ProFuzz uses the fuzzing framework of powerful packet manipulation program Scapy. ProFuzz supports fuzzing the following Profinet frame types. [31]

- afr (Alarm Frame Random)
- afo (Alarm Frames Ordered)
- pnio (Cyclic RealTime)
- dcp (DCP Identity Request)
- ptcp (Precision Transparent Clock Protocol)

ProFuzz fuzzer can be especially useful for vendors who develop their own Profinet stacks. [31]

6.2 Connecting Automation and Office Networks

Traditionally automation systems were built as stand-alone systems. These systems had little in the way of security but the Internet and Ethernet with their ubiquitous protocols and networks changed everything. Today ICSs (Industrial Control System) are often connected one way or another to the corporate network, thus being potentially reachable from outside networks such as the Internet by a malicious party.

Security goes both ways; while automation network must be protected from threats of the superordinate network and Internet, the overall network must also be protected from the threats of automation network. For example devices of external vendors which connect to the automation network are normally not subject to the security specifications, thus being potential middlemen in forwarding malicious software, e.g. Trojans, worms, malware. [17]

Profibus International introduces three common schemes for connecting automation and office networks; both physically and logically separated networks, logical integration into the overall network through firewall and logically separate networks with common physical topology. [17]

6.2.1 Physical and Logical Separation

Figure 23 illustrates the design of physical and logical separation of office and automation networks with the use of firewalls as logical transition points. This design gives the automation and office network their own physical and logical networks in parallel to each other.

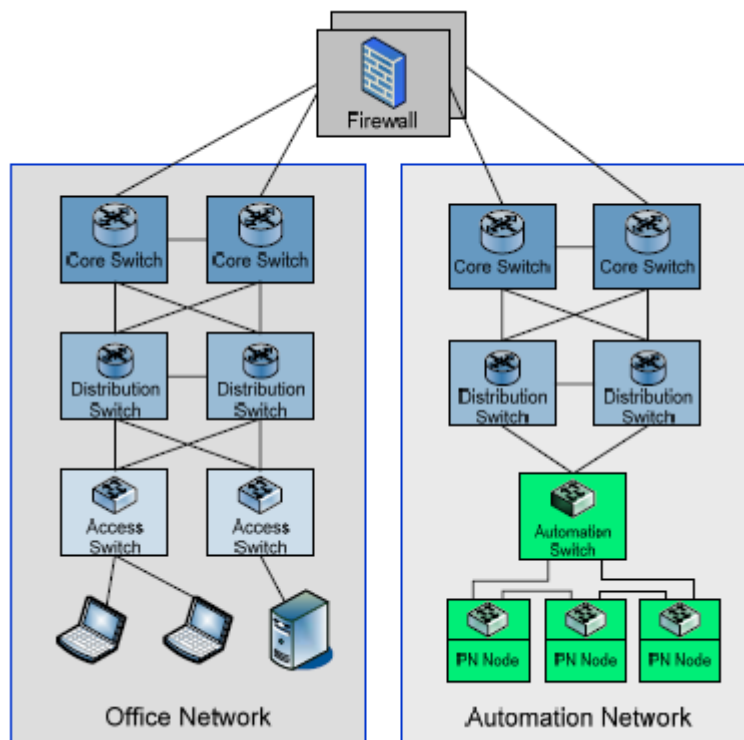


Figure 23. Logical and physical separation of office and automation networks [17].

A complete physical and logical separation design offers a clear separation between the office and automation networks which makes protecting and administering of the network less complicated. On the other hand investment and operating costs are higher due to the number of active and passive equipment needed to build two separate networks.

6.2.2 Logical Integration through Firewall

Figure 24 illustrates how logical integration of automation cells can be done basically the same way as adding access switch to the distribution switch. In other words like connecting layer 2 switch to layer 3 switch. Profibus International recommends placing firewalls between layer 3 switches and automation networks in this design. Multiple automation areas can be protected with same firewalls. [17]

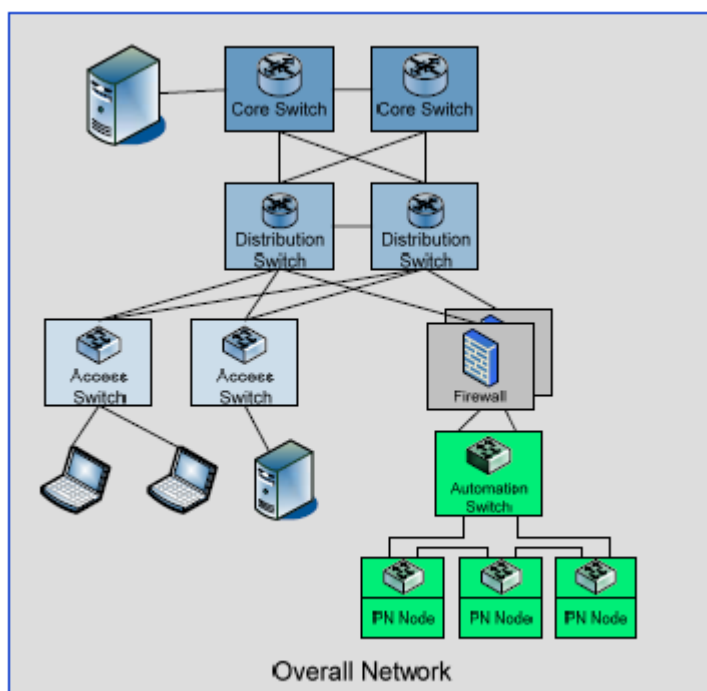


Figure 24. Logically integrating automation network to the overall network through firewall [17].

This design offers a simple and easy way to integrate automation cells to existing networks. In addition it is highly expandable with new automation cells. The number of devices needed is greatly decreased as a result of sharing core and distribution layers. Therefore, investment costs with this design are much smaller compared to a design with full physical separation. [17]

With this solution automation operators are more dependent on the superordinate IT network than in the previous solution which means that some sort of regulations may be in order, for example service level agreements. [17]

6.2.3 Common Physical Topology with Logical Separation

The final design solution presented by Profibus International is a complete logical separation. This design approach, as illustrated in Figure 25, differs from the previous design in that both the office and automation networks have common physical topology and use the same transition point, most commonly a firewall, for communication [17].

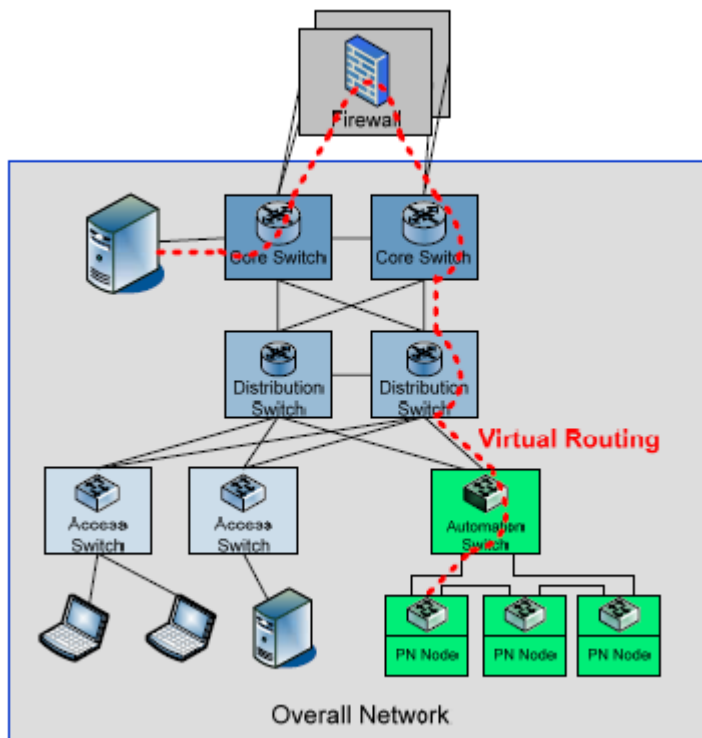


Figure 25. Logical separation via a firewall with common physical topology [17].

This approach gives complete and clear logical separation, thus granting protection from unauthorized access, virus and other malicious behavior. On the other hand the complexity of system architecture quickly rises when adding network components and software based connections which leads to high maintenance and operation costs. Especially troubleshooting becomes more difficult when network errors occur. This solution also makes automation operators dependent on the superordinate IT network. [17]

6.3 Network Security Measures

This chapter introduces some common security measures used in Industrial Ethernet networks. Since Industrial Ethernet is based on standard Ethernet, the same methods used to secure Ethernet networks also apply to Industrial Ethernet.

6.3.1 Firewall

Firewall is a network security system that acts as a barrier between networks. The traffic through a firewall is controlled with a set of rules applied to outgoing and incoming traffic. Firewall can be software based running on for example a server, or hardware based as a discrete device. Software based firewalls can be found everywhere, for example the most used operating system Windows has a built-in software firewall. Hardware based firewalls are very versatile nowadays, they can be used, for example, for routing purposes or as a DHCP server in addition to protecting the network.

Modern firewalls can inspect all the traffic going through them, even the contents of the packets with a process called deep packet inspection, and blocks the packets that does not meet the security criteria. Firewalls can also maintain the stateful information of the network, i.e. keeps track of the states of the connections in the network. Firewalls are used at connection points of networks, for example Internet and local network. [26] Figure 26 illustrates a layered industry network with separated production and corporate networks.

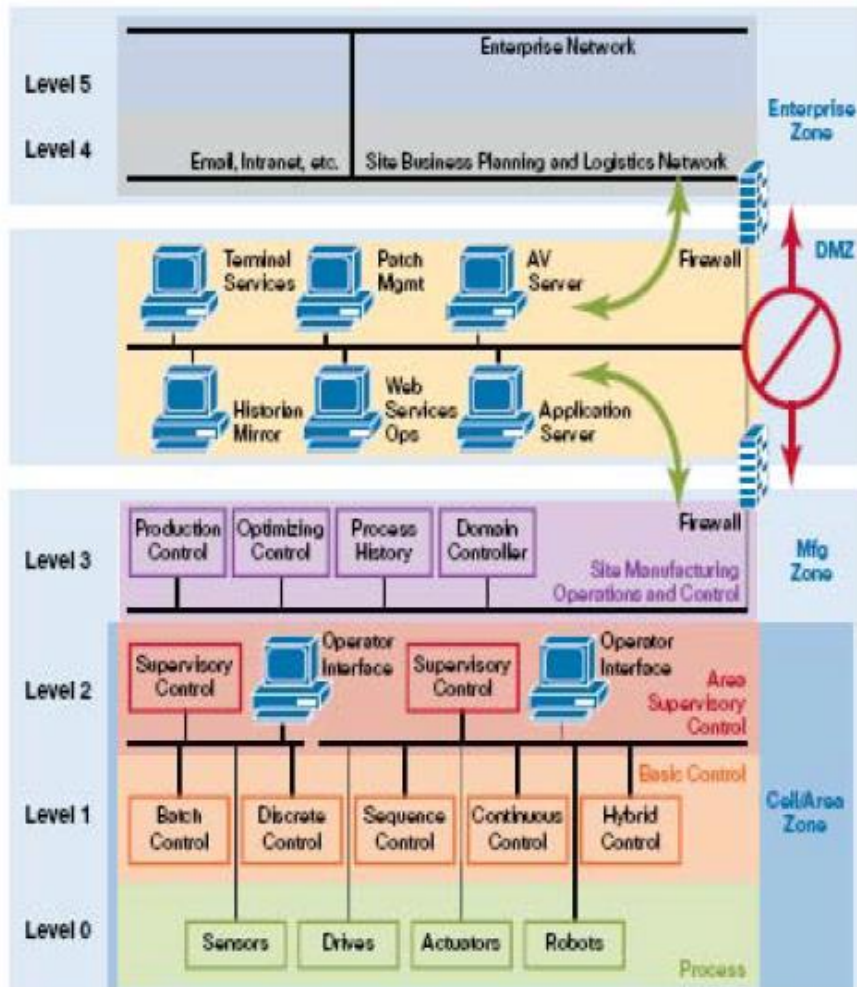


Figure 26. A layered industry network with separated production and office networks [26].

In industrial networks firewalls are used to separate production and office networks from each other, often by demarcating a DMZ between them as illustrated in Figure 26.

A buffer zone between networks is called a DMZ (demilitarized zone). DMZ is used as a security measure for it allows the control of how data and services are shared between different zones, for example various servers can be located in a DMZ. [26]

Firewalls can be divided in several types based on their functionality, though modern firewall and security systems have all these functions more or less integrated to them as well as some anti-virus functionality. These types of “hybrid” firewalls are generally referred to as Unified Threat Management (UTM) systems.

So called first generation firewalls were based on packet filtering. This means that packets are inspected and compared to the filtering rules set in the firewall configura-

tion. If a corresponding rule is found, the packet is either passed through or dropped depending on the rule set. Firewalls with only packet filtering do not care if packet is part of an existing stream, they just filter the packets based on the information inside the packet itself, for example source and destination address, protocol and port. Packet filtering firewalls work generally on first four layers of OSI model. [33]

Second generation firewalls, or stateful firewalls, have the same functionality as packet filtering firewalls but they can operate up to the layer 4 of the OSI model and add the state of the connection to list of criteria used by the ruleset. Stateful firewalls can record all connections passing through and detect whether or not the packet is a part of an existing connection or start of a new connection. This is done through a technique called stateful packet inspection. [33]

Third generation firewalls, also known as the next-generation firewalls or application layer firewalls, can detect anomalies within the applications and control input, output or access to and from applications. This is done by a technique called deep packet inspection where the firewall inspects the packets for unwanted connections. The firewall can block connections in otherwise allowed ports if an unwanted protocol wants to use it or detect and block protocols that are exploited. In other words next-generation firewalls are able to “understand” some protocols, such as File Transfer Protocol (FTP), Domain Name System (DNS) and HTTP. [33]

6.3.2 IPS/IDS

Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) are usually deployed inside networks where they monitor network traffic for anomalies, such as malicious code and unusual behavior that could give away hackers, and then log and even block connections if anything comes up. [27]

IPS and IDS systems synergize well with firewalls. Functionalities of firewalls are based on rules that tell whether to block or not the packet whereas IPS and IDS analyze the packets more thoroughly and can decide whether the traffic is legit. [27]

IPS and IDS are usually used against, policy violations, exploits, reconnaissance and DOS/DDOS attacks.

- Policy violations include infringed rules, protocols, packet designs etc. such as an IP packet with incorrect length.
- Exploits are attempts to abuse or manipulate systems or programs through vulnerabilities. Buffer overflow attack is a good example of an exploit of a hole in programs code.
- Reconnaissance attacks are a common way for attackers to obtain information from systems through, for example, port scans to determine open ports.
- (Distributed) Denial of Service attack (DoS/DDoS) is an attack that attempts to overthrow a system by flooding it with external requests. [27]

IPS and IDS function almost identically, the only difference comes from IPS's ability to block or quarantine connections and IP addresses. Both systems look for suspicious traffic by inspecting the header and data portions of packets. It then compares the results to a signature database compiled from past and potential attacks, some vendors even support integration with antivirus software, and then decides what to do based on rules defined by policies. IPS and IDS solutions are able to learn to differentiate normal network traffic from abnormal network traffic, this is called anomaly based detection. Rule based systems are also supported. In rule based IPS and IDS systems a knowledge base of programmed rules is used alongside an inference engine. The beauty of the inference engine and knowledge base lies in the way how the IPS and IDS systems can mimic the way human mind deduces, thus making assumptions of the network traffic and then decide the appropriate action to be taken. IPS and IDS can be powerful devices when used correctly since they can produce intolerable amounts of false positives if configured vaguely or with insufficient knowledge of the normal data traffic of the network. [27]

6.3.3 Physical Protection

Physical protection is a security aspect many fail to grasp with the importance it should be. Every device from cross connection to servers should be placed installed and placed appropriately, usually in network cabinets, in a way that prevents unauthorized access to input interfaces, such as USB and Ethernet ports, and protects the devices from tampering. Environmental conditions have to be considered if the network devices

are installed outdoors. Good example of failed physical security is Stuxnet which spread through an infected USB flash drive that someone plugged into an unattended computer.

6.3.4 Redundancy

Automation applications must be available at all times with zero tolerance for downtime due to the real-time nature of the applications. Continuous uptime can be ensured with redundancy measures in both data link and physical layers of OSI model. [26]

Common ways to achieve high uptimes and availability at the physical layer are the use of devices with resilient features, for example multiple power supplies. Some devices even support inline upgrade of components which means that they can be repaired without disrupting the services they are responsible for, this is a great way to improve MTTR (mean time to repair). The use of multiple redundant devices also improves availability and resiliency of the network through technologies such as Cisco's Virtual Switching System (VSS) and HP's Intelligent Resilient Framework (IRF) that allows switches to be clustered in a manner that in the case of one switch malfunctioning the other switch in the cluster takes over. [26] Figure 27 illustrates a star topology with redundant links to layer 3 switches.

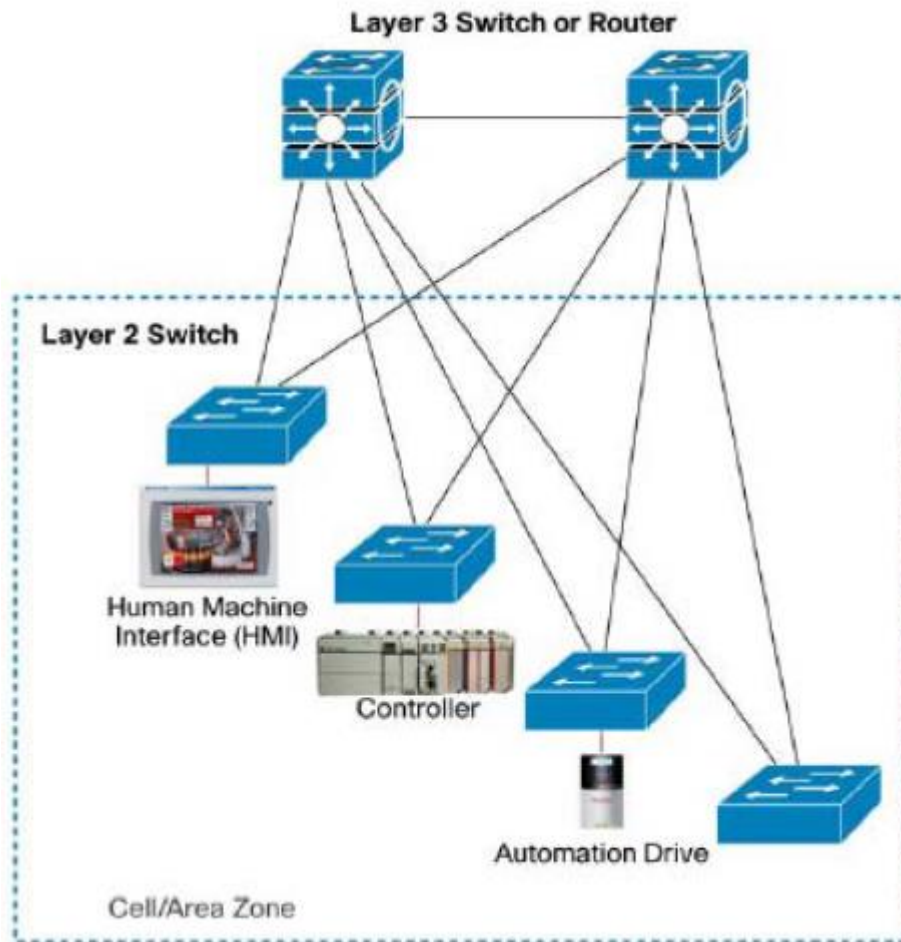


Figure 27. Star topology with redundant links [26].

Redundancy can be also achieved through implementations in the data link layer with redundant links and redundant paths for data transmission. This is done by using redundant network topologies such as redundant star topology or redundant ring topologies. In a redundant star topology, as shown in figure 26, access layer switches are connected to every distribution layer switch, thus creating multiple redundant paths for data transmission. [26]

A ring topology is formed when each device is connected to its neighbor, in other words ring topology is a line topology which is connected at both ends. Access switches form the actual ring which is then connected to the distribution switches. This allows the data to flow uninterrupted when any one of the devices in the ring malfunctions. Figure 28 illustrates a ring topology with redundant links to layer 3 switches.

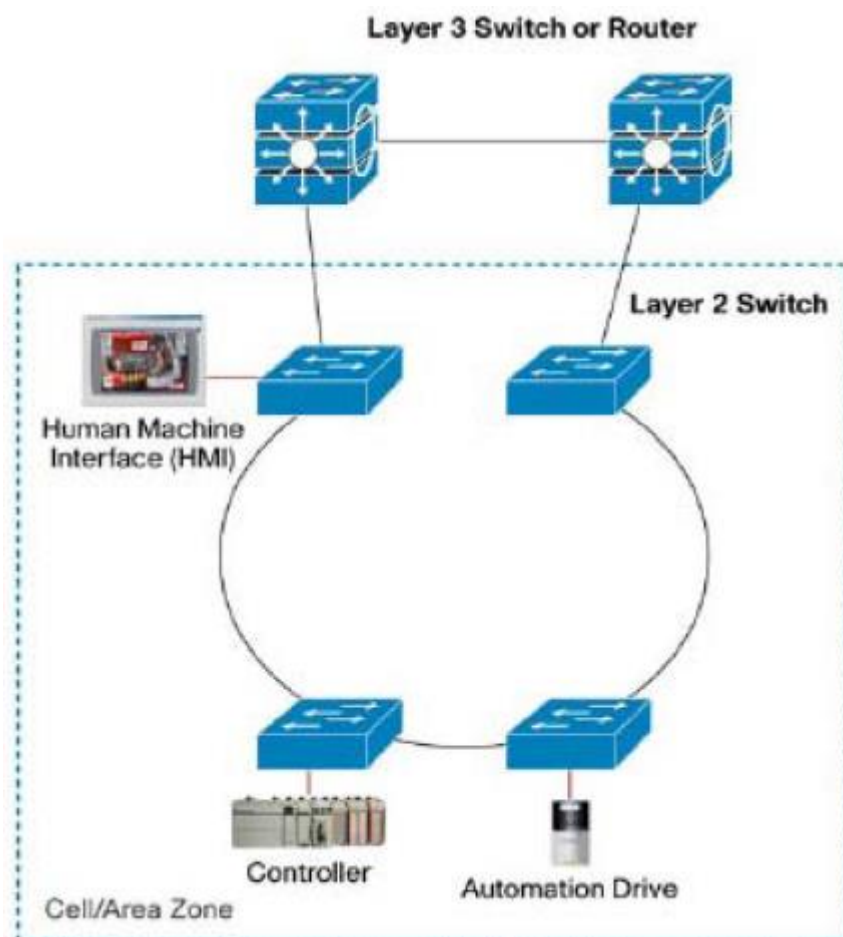


Figure 28. A ring topology [26].

Profinet uses two mechanisms for recovering from failure of any one device in the ring; Media Redundancy Protocol (MRP) and Media Redundancy for Planned Duplication (MRPD). MRP is used in rings where TCP/IP and Profinet RT frames and has recovery times under 200 ms. MRPD is used with Profinet IRT communications due to its ability to offer smooth and seamless switchover of communication paths in the event of failure of any one device. This is done by preloading the communication path data to the devices at the system startup. [19]

6.3.5 Remote Access

Allowing remote access to the network always poses a risk for the whole network. Therefore sufficient security measures must be taken. Profinet uses Virtual Private Network (VPN) technologies to establish a secure connection between two networks or to enable a remote connection from a workstation to the control network. Two ma-

chines, often firewalls, form a secured VPN tunnel which basically acts like an extension of the private network. [17] Figure 29 shows a simple remote access concept.

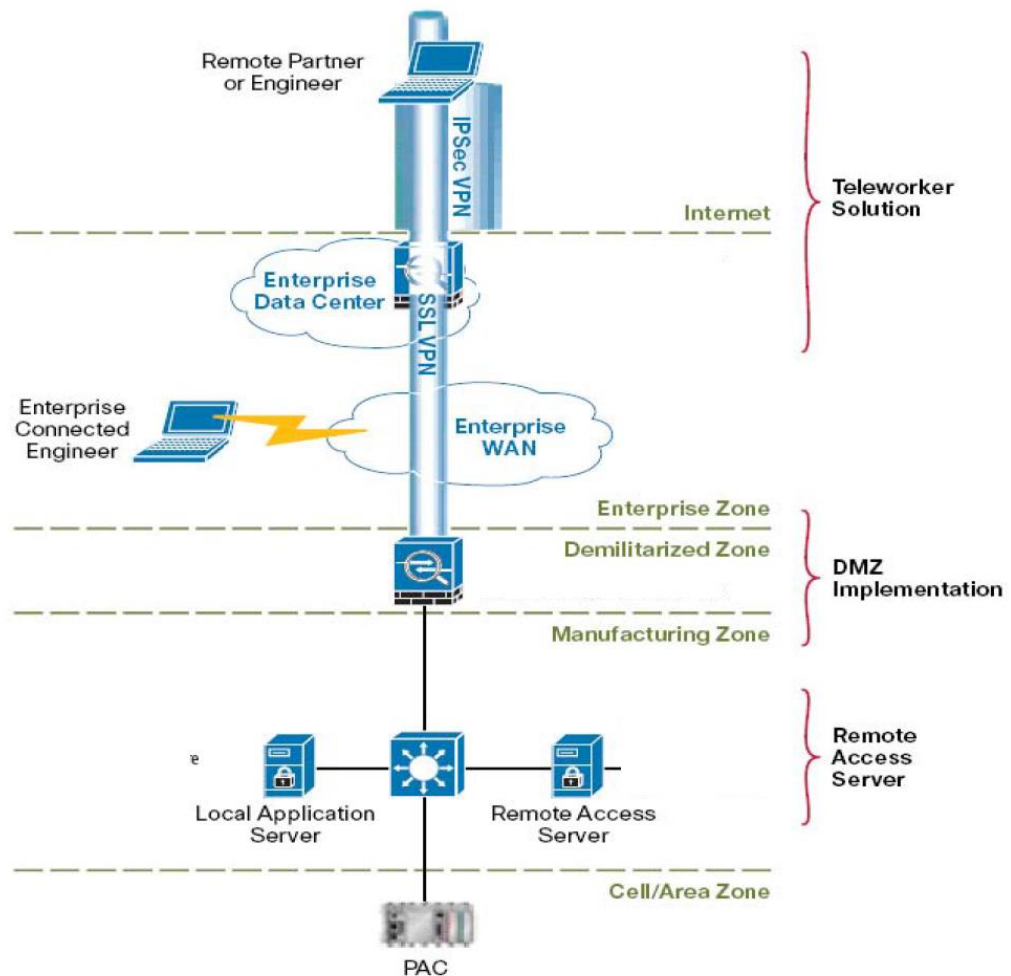


Figure 29. Simple remote access concept [26].

VPNs encrypt the messages travelling through the tunnel created between the end-points. This encryption is done by utilizing security protocols such as IP Security Architecture (IPsec), Secure Socket Layer (SSL) and Transport Layer Security (TLS). Two main types of VPNs exist based on how they are used. These are a site-to-site VPN for connecting multiple remote locations into a single network and a remote access VPN for connecting individual users to the private network. [32]

The site-to-site VPN is established between two devices located at both sites, usually a router or a firewall. This allows the two sites to act as a single network although they are physically in different locations. Encryption and decryption can be software or hardware based. Site-to-site links can be implemented with, for example, IPsec or

MPLS VPN. MPLS VPN is very flexible and scalable option for site-to-site connection but it is not as easy to set up as other option available. [32]

Remote access VPNs are used mainly for allowing individual users to connect to private networks over public networks such as the Internet. One of the most commonly used remote access VPN protocol is the SSL protocol which creates a secure connection for Internet applications, for example a connection from a PC browser to application server can be encrypted by using SSL. One major advantage of SSL is that it can be used without any dedicated software since it uses the browser as the client application. [32]

The use of VPNs alone does not offer a full protection for remote access connections. What if an unauthorized person gets his hands on your computer? If that computer happens to have access data saved the unauthorized person can connect to the private network and do something harmful. This can be prevented with the use of different authentication methods. In addition to configuring a VPN connection, a passwords can be used. Passwords can be fixed or generated every time with a dedicated password generator. Passwords can also be used together with some other verification method such as verification code sent via SMS message. This is called a two factor authentication (2FA). Certificates are also a common method to verify connections as is the case with SSL.

7 Discussion and Conclusions

Ethernet is steadily establishing itself as the bedrock for almost all communication. This is possible due to Ethernet's flexibility, universality and very cost-effective pricing. Even the industry has started the migration to Industrial Ethernet. The world's most used field bus technology, Profibus, has a successor, Profinet, which uses Ethernet based communications. This means that network engineers need to educate themselves with basic knowledge of automation systems, or at least get familiar with them, and automation engineers need to know the basics concerning Industrial Ethernet applications and protocols such as Profinet.

The main problem with traditional Profinet and other industrial protocols is that they use very old and obsolete devices and technologies. A good example is the ISO-TSAP protocol which is used between Profinet IO controller communications, such as Siemens Simatic S7 controllers. It is over 20 years old and uses no encryption at all but is still included and used in new industrial devices because that is the way things have been always done. The use of ISO-TSAP is most likely just the tip of the iceberg. If something as old as ISO-TSAP is used then probably something else that leaves the devices vulnerable is also used. Problematic is also the thought that networks are safe as long as they are physically and logically separated from the corporate network with DMZ and firewall solutions. This is not enough as the three attacks introduced Chapter 6.3 demonstrate. Security is also needed inside the networks and this can be done with, for example, IPS/IDS solutions which actively monitor the network.

The majority of vulnerabilities come across in the present study were not directly targeted to Profinet itself but against the devices Profinet is used in and the attackers must first try to get in to the network. Profinet itself seems like a very solid concept overall but the devices that use it have some critical vulnerabilities. This is very concerning since the devices responsible for providing electricity to our homes or keeping nuclear plants from blowing up are the ones using Profinet devices with these vulnerabilities. Fortunately vendors are working on software updates and patches, even though the speed with which they are done is not very high, meanwhile they just advise the users of the products not to let bad people into the networks.

In other words Profinet networks are secured, for the most part, in the same manner as every other Ethernet based network. The only difference comes from the security as-

pects emphasized. The top priority is generally given to availability so that Profinet and other automation systems are available at all times whereas in office networks the confidentiality has the top priority so that data loss is prevented. Of course both aspects are important in both networks, but still one is emphasized slightly more than the other depending on the case.

It seems that the future of industrial networks is in Ethernet based technologies such as Profinet due to Ethernet's versatility and performance. It is also interesting to see how Industrial Ethernet will adapt to cloud computing and software defined intelligent networks that seem to be the trend in networking. The first steps in cloud technologies have been taken by Profinet with Proficloud.

Further development of this subject could include designing and building a small Profinet test system with at least one IO controller and one or more IO devices and then reflect the design and security aspects introduced in this thesis to the process. In addition, the three attacks could be also tested in a controlled environment.

References

- 1 Wikipedia. OSI Model [WWW document] http://en.wikipedia.org/wiki/OSI_model. (Accessed March 17, 2015)
- 2 Tanenbaum, A.S., Wetherall, D.J. (2011). *Computer Networks*. Prentice Hall. 5th edition.
- 3 Cisco. TCP/IP Overview [WWW document] <http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html#tcpiptech>. (Accessed March 20, 2015)
- 4 Comer, D.E. (2000). *Internetworking with TCP/IP Vol I: Principles, Protocols, and Architecture*. 4th edition.
- 5 Robertazzi, T. (2013). *Basics of Computer Networking*. Springer Science+Business Media.
- 6 IEEE (2013) IEEE 802.3 'Standard for Ethernet' Marks 30 Years of Innovation and Global Market Growth [WWW document] http://standards.ieee.org/news/2013/802.3_30anniv.html. (Accessed March 31, 2015)
- 7 IEEE (2012) IEEE Standard for Ethernet. [WWW document] <http://standards.ieee.org/findstds/standard/802.3-2012.html>. (Accessed April 1, 2015)
- 8 Wikipedia. Twisted pair [WWW document] http://en.wikipedia.org/wiki/Twisted_pair. (Accessed April 3, 2015)
- 9 Fiber-Optics.Info. Types of Optical Fiber [WWW document] http://www.fiber-optics.info/articles/types_of_optical_fiber. (Accessed April 4, 2015)
- 10 ARC Electronics. The Basics of Fiber Optic Cable [WWW document] <http://www.arcelect.com/fibercable.htm>. (Accessed April 5, 2015)
- 11 Fiber Optics Tech Consortium. About Fiber [WWW document] <http://www.fols.org/technology/>. (Accessed April 6, 2015)
- 12 Cisco (2010) Industrial Ethernet: A Control Engineer's Guide [PDF document] http://www.cisco.com/web/strategy/docs/manufacturing/industrial_ethernet.pdf. (Accessed April 8, 2015)
- 13 Wilamowski, B. (2011). *Industrial Communication Systems*. CRC Press. 2nd edition.

- 14 Rostan, M. (2014) Industrial Ethernet Technologies [PDF document] http://www.ethercat.org/download/documents/Industrial_Ethernet_Technologies.pdf (Accessed April 16, 2015)
- 15 Feld, J. (2004). Profinet – Scalable Factory Communication for all Applications. *2004 IEEE International Workshop on Factory Communication Systems*. 33-38. IEEE
- 16 Thomas, P. (2014) PROFINET - Applying the Ethernet Standard to Industrial Automation [WWW document] <http://www.slideshare.net/ProfibusUK/profinet-applying-the-ethernet-standard-to-industrial-automation-peter-thomas>. (Accessed 25 April 2015)
- 17 PI International (2008) PROFINET AND IT [WWW document] <http://us.profinet.com/white-paper/profinet-and-it/>. (Accessed April 26, 2015)
- 18 Phoenix Contact (2010) Profinet Basics. [WWW document] http://www.switchingonthefuture.be/downloads/manualsfabrikanten/PHOENIX%20CONTACT/Profinet%20Basics/PN_Basics.pdf. (Accessed April 29, 2015)
- 19 Profibus International (2014) Profinet System Description – Applications and Technology. [PDF document] <http://www.profibus.com/nc/download/technical-descriptions-books/downloads/profinet-technology-and-application-system-description/download/18676/>. (Accessed April 29, 2015)
- 20 Profibus International (2010) Profinet Design Guideline. [PDF document] <http://www.profibus.com/nc/pi-organization/regional-pi-associations/belgium/downloads/downloads/guidelines-1/download/10707/>. (Accessed May 1, 2015)
- 21 Industrial Ethernet Book (2015) Taking Profinet Networks into the Cloud. [WWW document] <http://www.iebmedia.com/index.php?id=10745&parentid=74&themeid=255&hpid=2&showdetail=true&bb=1&appsw=1>. (Accessed May 2, 2015)
- 22 Henning, C. (2009) Is Profinet Routable? [WWW document] <http://us.profinet.com/is-profinet-routable-report-from-vancouver/>. (Accessed May 2, 2015)
- 23 Industrial Ethernet Book (2008). Tough choice: M12 vs RJ45 Ethernet connection systems [WWW document] <http://www.iebmedia.com/index.php?id=5873&parentid=63&themeid=255&showdetail=true>. (Accessed May 2, 2015)
- 24 Thompson, T. (2011). What is IP rating, and why is it important? [WWW document] http://www.2mcctv.com/blog/2011_10_11-ip-rating-chart/. (Accessed May 2, 2015)

- 25 Profibus International (2013). Profinet Security Guideline. [PDF document] <http://www.profibus.com/download/specifications-standards/>. (Accessed May 4, 2015)
- 26 Rojas, C. Morell, P. (2010). Guidelines for Industrial Ethernet infrastructure implementation: A control engineer's guide. [PDF document] http://web-post.www.plantservices.com/assets/Media/1102/WP_Ethernet.pdf. (Accessed May 4, 2015)
- 27 Internet-Computer-Security.com. IPS (Intrusion Prevention System) and IDS (Intrusion Detection Systems). [WWW document] <http://www.internet-computer-security.com/Firewall/IPS.html>. (Accessed May 7, 2015)
- 28 Beresford, D. Exploiting Siemens Simatic S7 PLCs [PDF document] <http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/beresford.pdf>. (Accessed March 5, 2015)
- 29 Baud, M. Felser, M. Profinet IO-Device Emulator based on the Man-in-the-middle Attack [PDF document] <http://felser.ch/download/FE-TR-0604.pdf>. (Accessed March 6, 2015)
- 30 OWASP. (2013) Fuzzing [PDF document] <https://www.owasp.org/index.php/Fuzzing>. (Accessed March 6, 2015)
- 31 Peterson, D. (2012) PROFINET Fuzzer Released [WWW document] <http://www.digitalbond.com/blog/2012/12/17/profinet-fuzzer-released/>. (Accessed March 6, 2015)
- 32 Raju, P.P. Different Types of VPN Protocols [WWW document] <http://techpp.com/2010/07/16/different-types-of-vpn-protocols/>. (Accessed March 11, 2015)
- 33 Wikipedia. Firewall (computing) [WWW document] [http://en.wikipedia.org/wiki/Firewall_\(computing\)](http://en.wikipedia.org/wiki/Firewall_(computing)). (Accessed May 11, 2015)