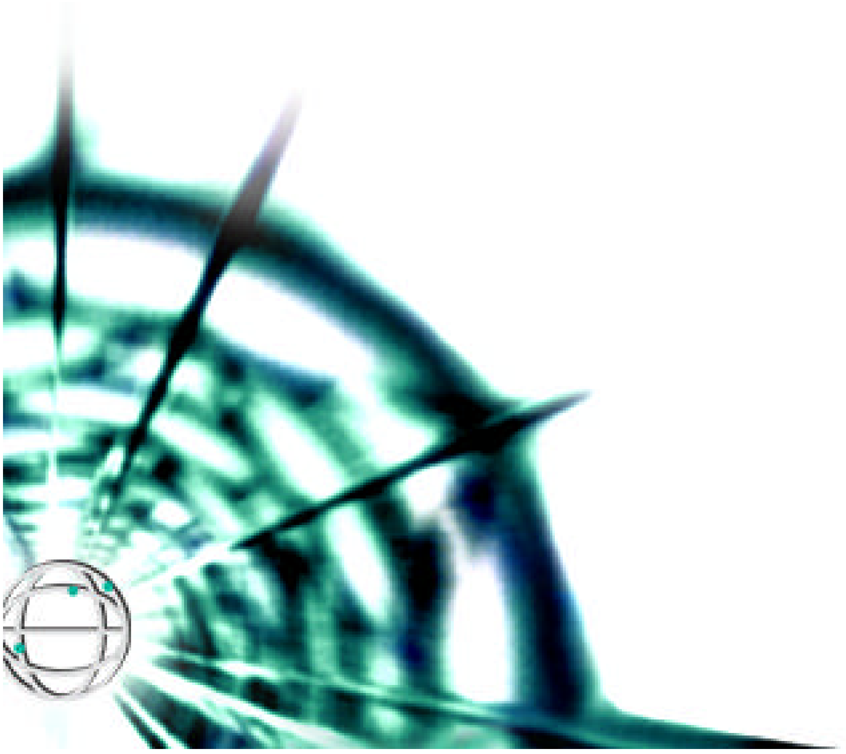
IAONA Handbook

Network Security

Version 1.5



The IAONA Handbook for Network Security

Version 1.5 - Magdeburg, June 6th 2006

Publisher:

Industrial Automation Open Networking Alliance e.V.
Universitätsplatz 2
39106 Magdeburg
Germany
info@iaona.org
www.iaona.org

Editors:
Dipl. Ing. Matthias Dehof
Marcus Tangermann
Dr.-Ing. Arndt Lüder
Otto-von-Guericke Universität Magdeburg
Center Verteilte Systeme
Universitätsplatz 2
39106 Magdeburg
Germany
www.uni-magdeburg.de/iaf/cvs

Based on the work of IAONAs Joint Technical Working Group (JTWG) Network Security.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

The following parties have contributed to this document:

DEHOF Computertechnik	Matthias Dehof (Chairman JTWG Network Security)
ABB	Martin Naedele, Dacfey Dzung
Data Systems	Detlef Kilian
Innominate AG	Steffen Bruß, Frank Merkel
iniNet GmbH / VPI	Peter Brügger
Hirschmann AC GmbH	Klaus Reister, Ralf Kaptur
TRUMPF Laser GmbH + Co. KG	Rainer Thieringer
Heyfra	Marcus Tangermann
WAGO Kontakttechnik	Christoph Möller

All illustrations, charts and layout examples shown in this document are intended solely for purposes of example. IAONA assumes no responsibility or liability (including intellectual property liability) for actual use based upon examples given in this publication.

Contents

1 Introduction

Ethernet based communication systems have entered the factory floor. During the last 5 years different fields of application using different Ethernet based communication protocols and technologies have been established ranging from web based management of devices to motion control applications.

This increasing use of Ethernet based services and devices came for many companies through the backdoor: first a simple FTP session for firmware uploads and a telnet session for changing settings, then a web server for advanced and comfortable configuration and diagnostics, and finally the use of real-time Ethernet communication protocols for device communication within control applications. It was a small step from using these devices point-to-point connected to a serviceman's laptop to connecting the devices to a company network. With the broad use of PC based devices, it was possible to connect anything and for quite a time, finally, the network was just what is was made for.

But with the increasing use of Ethernet based communication technologies also the problems of this technology have entered the factory network. The possible data exchange using eMails or direct device access will enable an undue influence on the devices by hackers, with-collar criminals, or even unilluminated employees.

When more people were accessing the network - and an increasing number of non-technicians and non-employees were among them - the network was opened to the Internet and was used for web-access and eMail services. Thereby, viruses and worms coming with laptops and eMails, some of them do no harm but others may cause the loss of a complete production line. Even when these viruses have no direct effect on devices, overloaded network traffic is even worse than a single deleted hard disk.

The direct access to control devices using HTTP or SNMP based device management systems will, in principle, enable unauthorized people to acquire control system and production system sensitive data and to change sensitive system settings causing economic disadvantages.

As a matter of fact, the IT departments are confronted with a complete new line of problems. Any intrusion, by accident or intention has a bigger effect than in the office world.

An automation network needs to be fail-safe. Data within an automation system need to be protected from unauthorized access. The unauthorized change of control relevant data or even the circumvention of a data exchange may result in a production system break down. A down time of a production line of a few minutes can cost some thousands of Euros because it may take some hours to restart the complete line. In contrast to this a short breakdown in the office environment is equally disturbing, but the consequences are different.

To cope with the mentioned problems and to ensure the security of industrial communication systems special technologies and strategies have been developed or even from the office world adapted to the factory floor. One important role within this process has been played by the IAONA Joint Technical Working Group (JTWG) “Network Security”. Within this JTWG the state of the art of network security technologies for industrial application have been collected and aggregated to an advice for best practice.

Based on the results of the IAONA JTWG “Network Security” the Handbook - Network Security has been created. It will be maintained by the members of the JTWG and reflects the current status of technology. The Handbook is not a static book, but subject to change to keep up with threats and developments.

The Handbook was designed to

- establish "know-how" for network security in industrial applications and make this accessible for to users
- give recommendations on how to plan secure networks
- provide tools for network analysis and escalation schemes
- create guideline for network security to be provided to IT and factory floor personnel
- give input to normative committees, such as IEC

The user's benefits are

- support for security risk analysis,
- support in the selection of appropriate security measures and
- most important - the avoidance of production down time caused by security leaks.

All-in-all, the IAONA Handbook - Network Security will provide interested people with the necessary knowledge about existing security problems, useable security architectures, and all necessary activities to establish these architectures.

To follow this aims the handbook is organized as follows.

Within the following (the second) chapter necessary basics about network security will be described. This includes a definition of the term “Security”, the term of IAONA Security Classes, the description of basic protocols, structures, and architectures and its security problems, defense strategies, and security components with its security relevant behavior.

The third chapter will describe in detail the security methodology developed by IAONA JTWG “Network Security” with strategies, structures, devices, protocols, and defense measures.

Chapter four can be seen as a cookbook for network security providing best practice scenarios for special application cases.

Chapter five introduces the IAONA Security Data Sheet, a mean for collection and distribution of security relevant information of devices, systems, and networks based on the IAONA Security Methodology. Within this chapter the IAONA Security Data Sheet will be described in detail and its application and benefits in practice will be considered.

The handbook will conclude with three annexes. The first annex will provide a template of the IAONA Security Data Sheet and the second one will give the XML schema used for the computer based processing of the IAONA Security Data Sheet. The third annex will provide a detailed listing and description of 28 Ethernet based communication protocols used within factory communication systems including a security relevant survey of each protocol.

2 Basics for Industrial Ethernet Security

The aim of the following section is the provision of basic information about network security problems and its avoidance or protection. Therefore, some basics for Industrial Ethernet Security will be given.

First of all, the term “Security” is defined and different security objectives are introduced. Based on this definition a classification of security levels is introduced.

To ensure the understandability of the majority of security relevant problems within this chapter three main communication system relevant topics will be picked up. At first the IP protocol and its application and security relevant problems within Ethernet based communication systems will be considered, at second different communication scenarios used in practice will be observed in a generic way, and at third usually used network structures will be sketched.

Based on this set of prerequisites existing network security approaches and devices usable within them will be analyzed. The main interest here is placed on the hard-perimeter approach and the defense-in-depth approach as the two important security architectures and on the mainly used security architecture components Packet Filter, Application Gateway, and Demilitarized Zone.

2.1 What is Security?

A very important issue for further discussions is a clear definition of what "Security" means.

In contrast to "Safety" which concerns operators, users and the general public, "Security" addresses the prevention of illegal access - in the widest sense - to the automation system. Security thus has implications for safety as well.

In this handbook, Security is used in the sense of "IT Security" and is concerned mainly with securing hosts and devices, the overall network and the automation system of a production system with respect to a proper system behavior. Note however, that IT security is not purely a technical issue - the foundation for a successful technological solution is an appropriate security policy.

In detail, we define security in terms of the following security objectives [Bis03, Schn03]:

- Availability
- Third-party protection
- Integrity
- Auditability
- Authorization (access control)
- Authentication
- Non-reputability
- Confidentiality

The following table [MaNa04] gives a detailed description of these items.

Security objective	Description	Benefits
Availability	Availability refers to ensuring that unauthorized persons or systems cannot deny access/use to authorized users. For automation systems this refers to all the IT elements of the plant, like control	The network and connected sys-tems shall be able to

	systems, safety systems, operator workstations, engineering workstations, manufacturing execution systems, as well as the communications systems between these elements and to the outside world. Violation of availability may cause safety issues, as operators may lose the ability to monitor and control the process. This may also lead to severe loss of production.	transport data and respond to any requests wit-hin an expected time.
Third party protection	The third party protection objective refers to the prevention of damages effectuated to third party systems caused by an unexpected and mainly unintended behavior of the own IT system. This type of security objective will not refer to damages of the own system or safety hazards of the controlled plant. A successfully attacked and subverted automation system could be used for various attacks on the IT systems or data or users of external third parties, e.g. via distributed-denial-of-service (DDOS) or worm attacks. Consequences could reach from a damaged reputation of the automation system owner up to legal liability for the damages of the third party. There is also a certain probability that the attacked third party may retaliate against the subverted automation system causing access control and availability issues. This type of counter attack may even be legal in certain jurisdictions.	A failure of a single device or service shall cause no harm to others.
Integrity	The integrity objective refers to preventing modification of information by unauthorized persons or systems. For automation systems this applies to information coming from and going to the plant, such as product recipes, sensor values, or control commands, and information exchanged inside the plant control network. This objective includes defense against information modification via message injection, message replay, and message delay on the network. Violation of integrity may cause security as well as safety issues, whereby, equipment or people may be harmed.	A user can be sure that his data was not modified, is complete and with respect to the sender correct.
Auditability	Auditability is concerned with being able to reconstruct the complete behavioral history of the system from historical records of all (relevant) actions executed on it. While in this case it might very well be of interest to record also who initiated an action, the difference between the auditability security objective and non-repudiability is the ability of proving the actor identity to a third party, even if the actor concerned is not cooperating. This security objective is mostly relevant to discover and find reasons for malfunctions in the system after its occurrence, and to establish the scope of the malfunction or the consequences of a security incident. In the context of automation systems this is most important in the context of regulatory requirements, e.g. FDA approval. Note that auditability without authentication may serve diagnostic purposes but does not provide accountability.	This covers that e.g. information from log files is complete and can be tracked.
Authorization	The authorization objective, also known as access control, is concerned with preventing access to or use of the system or parts by persons or systems without permission to do so. In the wider sense authorization refers to the mechanism that distinguishes between legitimate and illegitimate users for all other security objectives, e.g. confidentiality, integrity, etc. In the narrower sense of access control it refers to restricting the ability to issue commands to the plant control system. Violation of authorization may cause safety issues.	Only authorized communication partners can access the device. Beside malicious attacks this measure can protect against problems caused by accidental access.
Authentication	Authentication is concerned with determination of the true identity of a system user (e.g. by means of user-supplied credentials such as username/password combination) and mapping of this identity to a system-internal principal (e.g. valid user account) under which this user is known to the system. Authentication is the process of determining who the person is that tries to interact with the system, and whether he really is who he claims to be. Most other security objectives, most notably authorization, distinguish between authorized and unauthorized users. The base for making this distinction is to associate the interacting user by means of authentication with an internal representation of his permissions	This covers the determination of the identity of a communication partner, which is necessary for authorization.

	used for access control	
Non-reputability	The non-reputability objective refers to being able to provide irrefutable proof to a third party of who initiated a certain action in the system. This security objective is mostly relevant to establish accountability and liability with respect to fulfillment of contractual obligations or compensation for damages caused. In the context of automation systems this is most important with regard to regulatory requirements, e.g. FDA approval. Violation of this security objective has typically legal/commercial consequences, but no safety implications.	This covers that e.g. information from log files is true and cannot be denied.
Confidentiality	The confidentiality objective refers to preventing disclosure of information to unauthorized persons or systems. For automation systems this is relevant both with respect to domain specific information, such as product recipes or plant performance and planning data, and to the secrets specific to the security mechanisms themselves, such as passwords and encryption keys.	Data is encrypted with an appropriate algorithm and a user can be sure that no third-party has accessed this data.

2.2 Security Classification

Almost everybody in industry knows the IP - Industrial Protection classes, describing the robustness of device against dust and water.

An approach of a similar, easy to understand classification for security needs and features called IAONA Security Classes has been proposed by the IAONA JTWG “Network Security” and is shown in the figure below.

	Classification			
	none	low-medium	high	very high
Integrity	log data failure events	repeat data, use checksum	rare failure acceptable, production loss	no failure acceptable, severe production loss
Non-repudation	no measures	store access information to log files	use authorization and backtrace	use of certificates and secure servers
Confidentiality	data are public available, not protected	use basic mechanisms, single failure may occur	secure data chanels, active protection	encrypted data, failures are not acceptable
Availability	no measures, downtime: some hours	using backup, downtime: <1h	quick replacement, downtime: <5min	redundant system, no downtime
Authentication	without any access control	using passwords	using server based user authentication	use of certificates, smart-cards, etc.

Figure 1: Security Classification

The IAONA Security Classes map the five security criteria Integrity, Non-repudiation, Confidentiality, Availability and Authentication described within the previous subchapter to four classes of importance (security levels) ranging from none over low-medium to high and very high.

Each class describes several measures that have to be taken to fulfill the security requirements of the class.

Based on the IAONA Security Classes a mapping of security requirements of a system to security measures of the used security architecture and available security functionalities and mechanisms of devices and communication protocols is possible.

The following examples explain the application of these classes to more real-world examples.

2.2.1 Security Classification Example - *Light Bulb Factory*

Within the following example the Classified security level "none" will be considered.

Let's assume a production of few different types of light bulbs. The factory manufactures a few thousands of a kind to fill their stock and needs then some time to switch production to another type.

The factory communication system is an completely Ethernet TCP/IP based communication system and its is not connected to any other Ethernet based system.

Data integrity is no problem within the example factory, because every device is using TCP/IP communication, making sure that data is delivered and in the right order.

Non-repudiation is no problem within the example factory, because the production network is an isolated network, without any connection to Office IT or the Internet.

Confidentiality is no problem within the example factory, because data consists only of process data images, unauthorized people have no access to the network and there is no need to protect this data.

Availability is no problem within the example factory, because we have floor personnel available to solve every problem within one hour and since production is buffered by the company's stock, some downtimes are acceptable.

Authentication is no problem within the example factory, because access to the shop floor is controlled and without a PLC programming device, someone cannot manipulate anything.

Conclusion: This is a cheap production line, using Industrial Ethernet just to save money and without any need of sophisticated security mechanisms.

2.2.2 Security Classification Example - *Automotive parts*

Within the following example the Classified security level "medium" will be considered.

Let's assume now a plant for just-in-time manufacturing of automotive parts using an Ethernet TCP/IP based communication system. The system is protected by a firewall-gateway and an access control mechanism.

Data integrity is ok within the example factory, because every device is using TCP/IP, making sure that data is delivered and in the right order - or UDP/IP for some configuration services.

Non-repudiation is ok within the example factory, because the production network is using a firewall-gateway to the office network, allowing only HTTP. Access to devices is controlled by login (user/password) and this information is locally stored. A dedicated modem allows remote service without bridging into the office network.

Confidentiality is no problem within the example factory, because unauthorized people have no access to the network and the data is not important enough to spend much money on encryption.

Availability is no problem within the example factory, because the firewall protects the network from unwanted traffic and overload. Physical access to the production network is only allowed to registered service people. In case of failure, replacement devices are available, backups are frequently made on a server and the personal is well-trained.

Authentication is ok within the example factory, because access to devices requires the user to login with username and password, this information is not public available, every with granted access has signed a letter of confidence.

Conclusion: This company is running production 24/7 - any downtime problem can be fixed within one hour, with remote service, an expert hotline can access some machines and assist. The risk of security leaks is quite low, the company has an internal handbook for security events.

2.2.3 Security Classification Example – *Pharmaceutical process*

Within the following example the Classified security level "high" will be considered.

This example addresses a company manufacturing medical or pharmaceutical products. Failures are not acceptable at all, many procedures are required by law. The communication system is based on an Ethernet TCP/IP network. The network is protected by special devices, special topologies, special access control mechanisms, data encryption, and special internally used protocols.

Data integrity is guaranteed by using IP-based protocols. In addition, the network data flow is monitored to detect anomalies, packet-smoothers avoid overflow and bandwidth problems. Rules were set to describe the “normal” behavior of the network and in case of anomalies, there is an instant notification.

Non-repudiation: is required by law to track any intervention. Any personnel has security clearance and access (physical as well as virtual) is controlled by smart-cards, login information is stored on redundant servers, using RADIUS.

Confidentiality: Production data needs to be encrypted, because this know-how is vital to the company. Any network data outside machines is using data encryption, at least IPSEC. People with access to the machines have security clearance and are frequently trained. Any failure might cause espionage and result in severe financial loss.

Availability is highly needed because production downtimes of single machines affect the whole production process. Redundant PLCs are used as well as redundant network topologies.

Authentication is important, any unauthorized access has to be prevented. Identification of floor personnel is controlled by security staff and using state-of-the-art access technology.

Conclusion: Proper network operation is highly important to this company. They need to be able to track anything any failures is not acceptable.

2.3 The IP protocol family

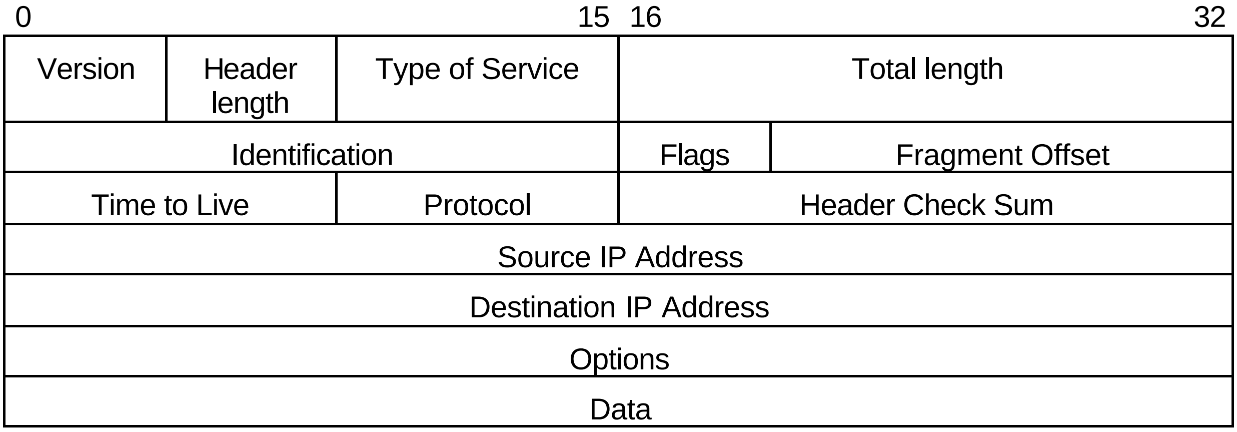
After defining the term “Security” by describing the objectives intended by security activities, mechanisms, and architectures and given examples on the classification of Security measures within the following chapter basic information about the most used Ethernet based protocol family, the IP protocol family; will be provided.

Today, large communication between networks is driven by the Internet Protocol (IP) family. Whether an eMail is sent or a web site is visited, the data flow is controlled by IP. Even the largest network of the world, the Internet, uses these protocols and shows obviously, that IP has proven its capabilities for exchanging high volumes of traffic dependably. Also, in automation networks, IP is widely used for high traffic communication between different automation cells, MES and the office world. However, there are known problems caused by design flaws in the IP family which can cause security problems.

Thus, this chapter will give a short introduction into the design of the IP family and describes some resulting security flaws. For more information on the IP family please also refer to the IAONA Handbook Industrial Ethernet [IndI06].

2.3.1 Design of the IP family

To understand security related problems of IP, a basic knowledge of the IP design is necessary. The figure below shows the structure of an IP packet (also called datagram). Since this section provides only a basic introduction to the topic, only the most important fields for understanding the functionality are described. For a detailed description of IP, please refer to [Stev94].



<table>
<tr><td>0</td><td></td><td>15</td><td>16</td><td>32</td></tr>
<tr><td>Version</td><td>Header length</td><td>Type of Service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Check Sum</td></tr>
<tr><td colspan="5">Source IP Address</td></tr>
<tr><td colspan="5">Destination IP Address</td></tr>
<tr><td colspan="5">Options</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Figure 2: IP Header

Each datagram consists of the fields shown in the figure above.

- **Version:** The version of the IP protocol. Currently, version 4 is mostly used.
- **Type of Service (TOS):** The TOS field describes requirements for the transport of data. This can be minimized delay, maximized throughput, maximized reliability and minimized monetary cost. It is route dependent whether this field is interpreted or not.
- **Identification:** The identification field identifies each datagram sent by a host. In fact the physical layer (in our case the Ethernet) is not able to transmit a datagram at once, it is fragmented (split into several IP datagrams) at a router and reassembled at the target. Fragments of a datagram contain all the same identification number.
- **Flags:** The Flags field describes whether a datagram may be fragmented or whether it is a fragment of another datagram.
- **Fragment offset:** The fragment offset determines, where the data of a datagram which is a fragment is located in the original datagram. This information is necessary to reassemble fragmented packets.
- **Protocol:** This field describes the protocol of the contained data such as the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP).
- **Header Check sum:** The Check sum field contains the calculated check sum of the datagram header used to identify transmission failures.
- **Source IP address:** This field contains the IP address of the sender.
- **Destination IP address:** This field contains the IP address of the target.
- **Options:** This field of variable length can contain several information. Among others, this can be
    - the route this packet has taken (stamp of each router the datagram has passed)
    - the route this datagram has to pass to the destination (known as source routing).
- **Data:** The Data field is a field of variable length containing the user data of the datagram.

Within an IP network the datagram structure is used to route the datagram in the right way from the source to the destination.

To work correctly, IP relies upon the Internet Control Message Protocol (ICMP). This protocol is responsible for communicating error messages and other conditions that require attention. Among others, this includes information about unreachable destinations, traffic rates that the target cannot cope with (called a source quench), or bad headers in IP datagrams.

One well-known application of the ICMP is the ping command which is used to determine whether a host is reachable via the network. Therefore, ping issues a special ICMP packet (called “echo request”). If the host receives such packets, it replies with an “echo reply” showing that it is able to communicate over the network.

2.3.2 Security Problems of IP

There are a couple of problems resulting from the way, the IP protocol family works. In this section, two exemplary problems, acting as references for the majority of problems, will be described.

The first considered problem of the design of IP is the non-reliability of the authenticity of a source address. This non-reliability results from the specification of the IP protocol family.

A very popular approach to attack networks based on the non-reliability of the authenticity of a source address is to fake the source address of an IP packet (IP Spoofing) as illustrated in the figure below.

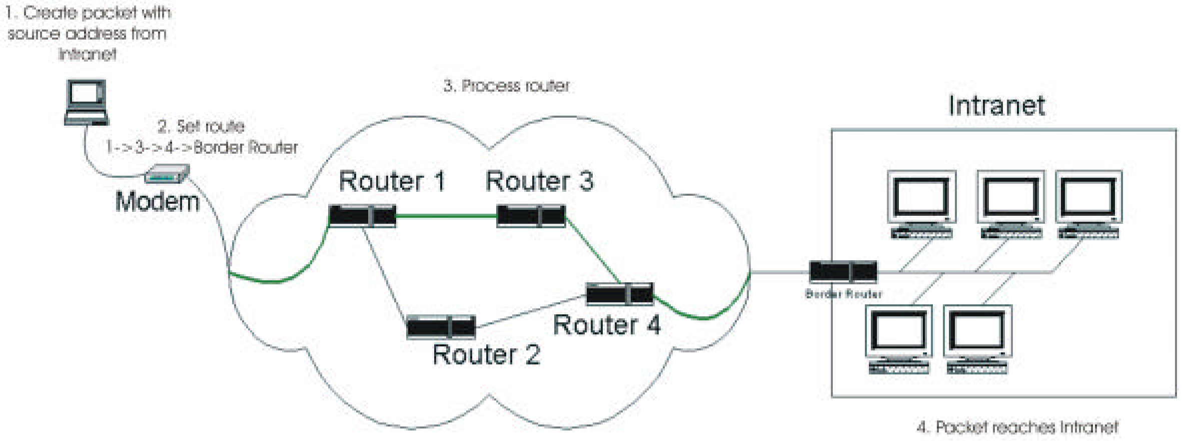

1. Create packet with source address from Intranet
3. Process router
Intranet
2. Set route 1->3->4->Border Router
Modem
Router 1
Router 3
Router 4
Router 2
Border Router
4. Packet reaches Intranet

Figure 3: Source Routing

An external device will create a packet with an source address used within the Intranet. Using the possibility of the definition of the router path the packet has to follow to its destination by a special option in the option field of the packet (the so called Source Routing of the IP protocol) the packet will be routed to the borders of the Intranet. The packet with the bogus address then appears at the router network card connected to the Internet and the routing forwards this packet to the internal network card. The target system will finally receive the packet as a packet from one partner within the Intranet. Using this method a system outside the Intranet can pretend to be a system within the Intranet without recognition by the Intranet members.

In this way one can create network traffic within the Intranet, the causer seems to origin from the local network. A corrupt router implementation may forward the normally not routable packet to the target without checking the impossible source address. It has to be mentioned that some large Internet provider still allow IP spoofing so this is an up-to-date problem. Recognizing faked packets from the Intranet is much more difficult since the alleged originator may be the real originator.

Another problem are amplifier networks depicted in the figure below.

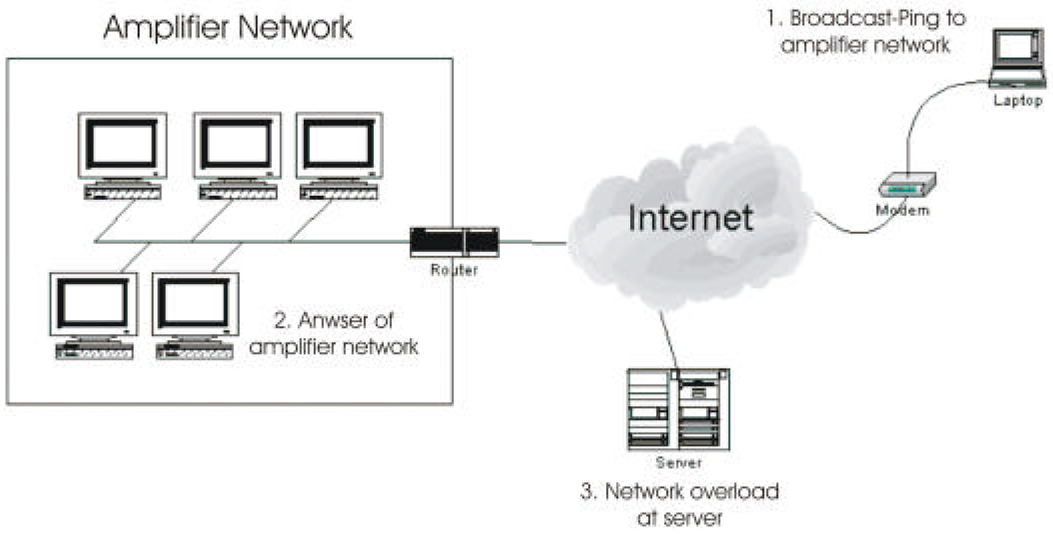

Amplifier Network
1. Broadcast-Ping to amplifier network
Laptop
Modem
Internet
Router
2. Anwser of amplifier network
Server
3. Network overload at server

Figure 4: Amplifier Network

An ICMP packet with a faked source address will be forwarded to a broadcast address of a network. Bad configured router allow the forwarding of the packet, the consequence is the answer of all active hosts within the local network to the faked source address. The target host will be flooded with packets and can not answer to normal traffic (Denial of Service, DOS). With a large amplifier network you can interfere a T1 connection (1.544 mbps) with just 14.400baud modem. In this context its interesting that bad configured network components can cause this problem by just a type.

2.4 Communication relations in an enterprise network

When setting up the protection of a network, it is important to realize what communication relations exist in a company, between company sites and to the outside world and which of these relations have to be protected. Therefore this section analyses a generic company network and explains the communication within.

The next figure shows two company sites (Intranet Company A & B) and several remote access points to these company sites. The communication between the companies and to the remote access points takes place via the Internet.

The common architecture of larger company networks consists of different Intranets that communicate over the Internet. The term Intranet describes in this context a local area network (LAN) that offers the most common services that are known from the Internet like Domain Name Service (DNS), E-Mail (SMTP, IMAP, POP3) or web servers (HTTP, HTTPS) based on the IP protocol suite. Within the Intranet two logical subnetworks exist: Office and Factory. Every Intranet represents a branch of the company.

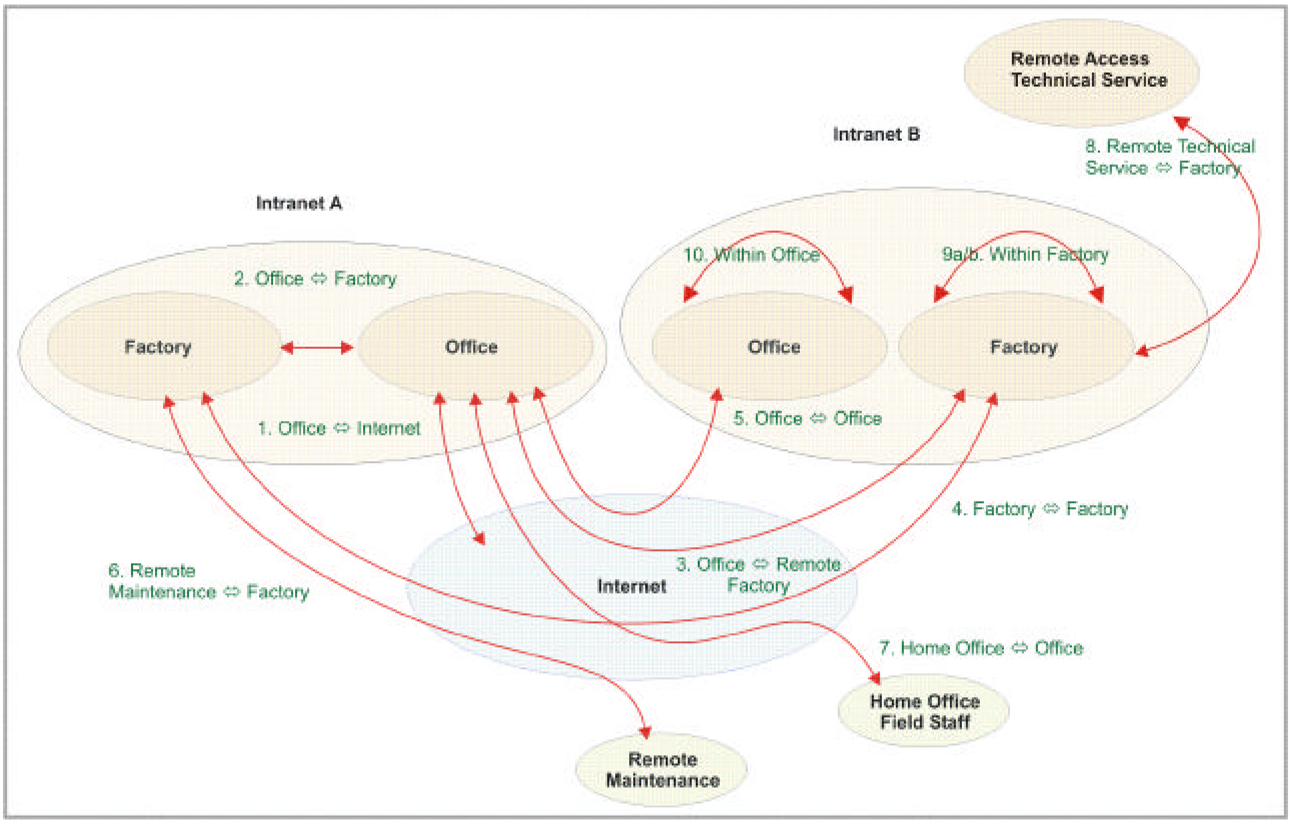


Figure 5: Communication relations of a company network

The office network consists mostly of common PC technology equipped with Ethernet network interfaces used to fulfill common management tasks. The most common factory relevant applications within this area are office applications of the ERP level. The mostly used Ethernet based protocols are the usually known Internet protocols like ordinary Ethernet TCP/IP, HTTP, FTP, and others.

The factory network represents the different production facilities within a branch and connects the different production units with its devices to a proper behaving production control system. The data transmitted within the factory network are produced by different levels of control applications ranging from typical the Manufacturing Execution System (MES) applications like order management or tool management over quality assurance applications down to real-time control applications within a special manufacturing cell. Also used applications within the factory network are maintenance and service applications. The protocols used within the factory network are the same as in the office network but extended by special industrial Ethernet protocols like EtherNet/IP, Modbus/TCP, Ethernet Powerlink, EtherCat, and Sercos III, reflecting the different real-time requirements of industrial control systems.

In this context the Internet is treated as a large network of interconnected networks defined by the Internet Engineering Task Force (IETF) in the Request for Comment (RFC) 2026 as a loosely-organized international collaboration of autonomous, interconnected networks, which supports host-to-host communication through voluntary adherence to open protocols and procedures defined by Internet standards.

According to the figure above showing a distributed network of a company the different communication relations will be described.

Communication relation	**Content**	**Time constraints**
1: Office ⇔ Internet	The office PCs communicate with the Internet to access information resources that are located in this network e.g.	Non time critical

	accessing web servers (HTTP) or download files (FTP).	high volume
2: Office ⇔ Factory	ERP (Office) and MES (Factory) communicate with each other for coordinating manufacturing processes.	Slightly time critical medium volume
3: Office ⇔ Remote Factory	ERP (Office) and MES (Remote Factory) communicate with each other for coordinating manufacturing processes.	Slightly time critical medium volume
4: Factory ⇔ Factory	To coordinate production processes between different production facilities, the MES of the facilities must communicate with each other.	slightly time critical medium volume
5: Office ⇔ Office	Office application must share data between the branches for example sharing documents, coordinating management processes, or exchange data between ERP application parts	non time critical high volume
6: Remote Maintenance Factory	For remote maintenance manufacturers must access devices within the factory network. This could be done via Internet, Intranet or right away in the factory	non time critical medium volume
7: Home Office/Field Staff ⇔ Office	Home Office workers and field staff members must access and share their data within the office network.	non time critical high volume
8: Remote access of technical service ⇔ Factory	A technical service provider may access the factory bringing with him a PC, a device or only a storage unit	non time critical medium volume
9a: Within factory	To coordinate the manufacturing process the MES system has to exchange data with the field control devices within the factory floor control system	slightly time critical medium volume
9b: Within factory	To control the manufacturing process different control system devices will exchange data.	high time critical low volume
10: Within office	Office applications must share data within the office network for example sharing documents, coordinating management processes, or exchange data between ERP application parts	non time critical high volume

2.5 Network architecture for Industrial Ethernet

Though a standard for wiring office networks is well established, currently there exists no adopted standard for Ethernet networks in the factory environment. To overcome this problem the Joint Technical Working Group (JTWG) “Wiring Infrastructure” of IAONA modified the standard for structured IT cabling according to EN 50173 and ISO/IEC 118101 to fit the special purposes of factory networks.

The work has resulted in the “IAONA Industrial Ethernet Planning and Installation Guide” [IAONA03] which describes the architecture needed for the special requirements of a factory level network. Based on this guide IAONA has initiated the standardization of wiring industrial networks within IEC were first draft standards will be available.

The following figure has been taken from the “IAONA Industrial Ethernet Planning and Installation Guide”. It describes the architecture of such a network and especially introduces the Machine Distributor (MD):

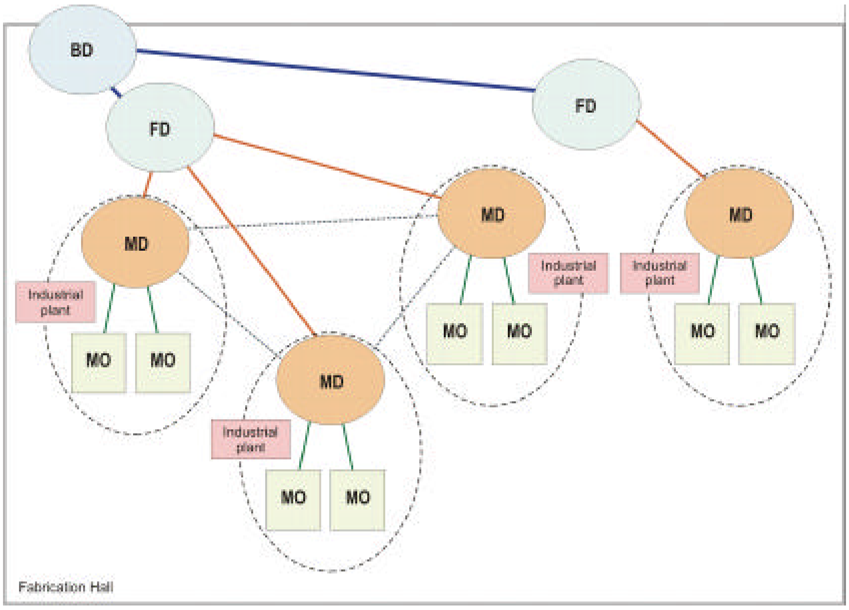


Figure 6: Fabrication hall with ring topology

Not shown in the figure above, the basic element of a production plant is the campus distributor (CD) which consists of level-3-switches, an alternative to the common backbone technology that eliminates the router bottleneck of conventional network architectures by integrating routing functionality in the switch.

The figure above shows the three layered architecture of fabrication hall as specified in the “IAONA Industrial Ethernet Planning and Installation Guide”. A factory hall is connected to the campus distributor via the building distributor (BD) which provides access to the floor distributors (FD). The machine units themselves are connected via the machine outlets (MO) to the machine distributors (MD) which in turn are connected to the floor distributors (FD). To provide fail save connectivity a hierarchically interlinked ring topology can be established which can bypass single failures of network connections.

Every distributor can be considered as an own sub-network to reduce network traffic between the different network segments that even occur with the application of switches especially in the case of broadcast messages.

Since traffic within the MD sub-network is used for control purposes of the machine units (communication scenario 9b of subchapter 2.4) hard real-time requirements must be met to guarantee secure operations. On the other hand it may be necessary to transmit data between different MD sub-networks e.g. in the case of work piece handover.

The figure below shows an example of the structure described above.

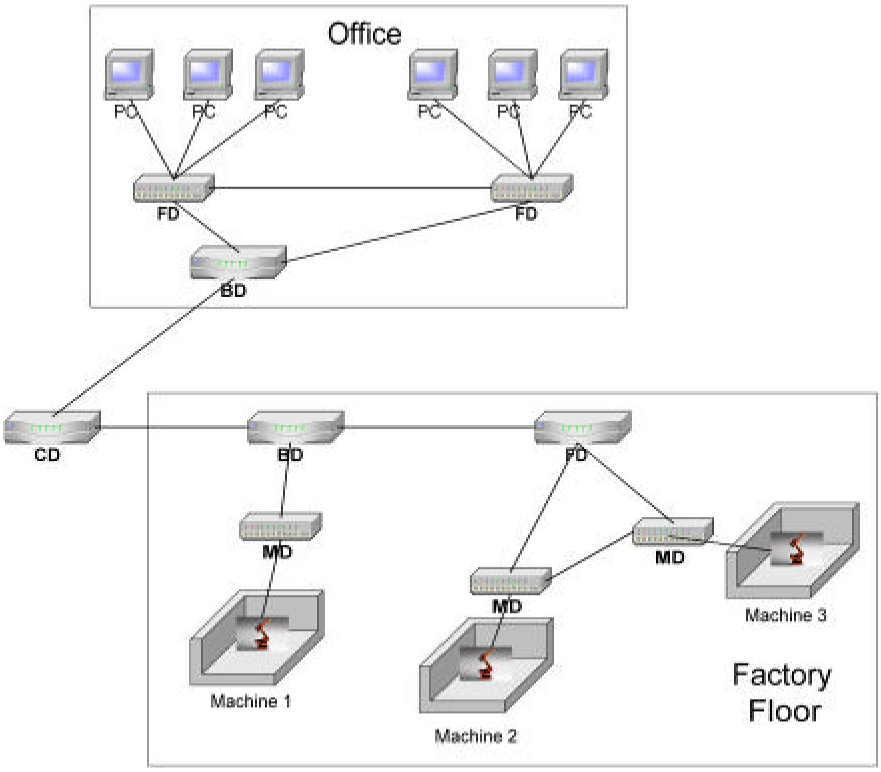


Figure 7: Example of a network topology according IAONA

The figure above shows the case of integration of a new production system based on 3 machines containing distributed intelligence, i.e. intelligent sensors and actuators with Ethernet enabled Onboard-PLCs.

The different buildings (office, floor) are connected to the backbone via Building Distributors (BD). Within a factory building, the different elements such as the are connected to the network via Floor Distributors (FD) and Machine Distributors (MD).

Within the office building additional Floor Distributors (FD) are installed to connect the floors of the building with the local backbone.

The local backbone is connected to the overall backbone of the company or the Internet via a Campus Distributor (CD).

2.6 Defense strategy

When dealing with network security, an important issue forms the strategy of defending a network against outside attackers. Nowadays, two concurrent approaches are used in the IT world [MaNa03b]:

- Hard-perimeter
- Defense-in-depth

Within the following sub-chapter both approaches will be described in detail to provide a basement for further understanding of the IAONA network security approach.

2.6.1 Hard-perimeter

The Hard-perimeter approach focuses on a impenetrable wall around the system. The complete internal network system will be connected with the Internet via a single security device or a single security device set (depending on the implementation). Any communication between Intranet and Internet has to pass this single connection point and will be observed with respect to the implemented security objectives.

Despite its simplicity this approach faces some serious problems. Among others these are [8]:

- Monocultures: This approach is based on one single methodology for securing a system. If the methodology fails, then the whole approach fails.
- Communication ports: The systems must have communication ports for communication with other systems. These entries are potential security threads.

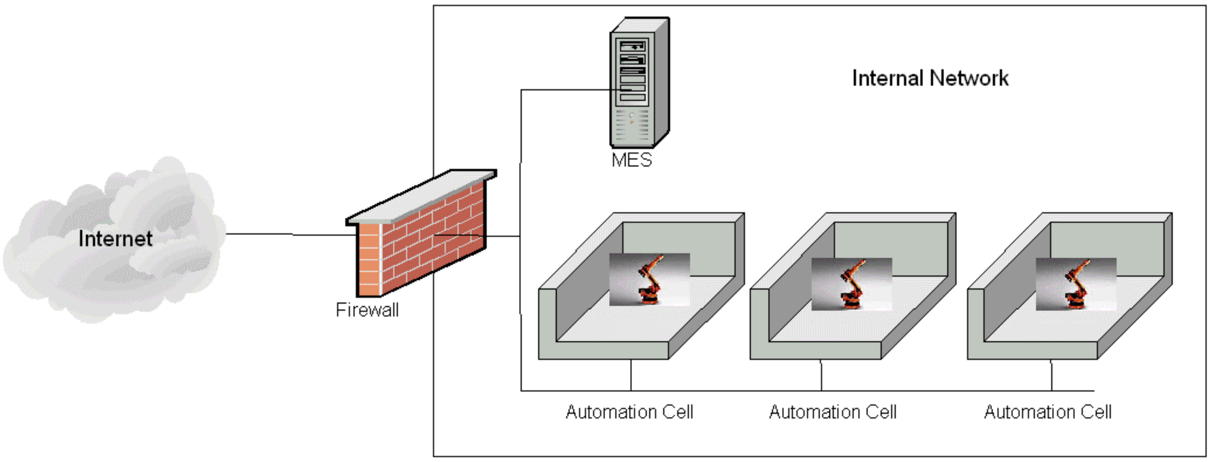


Figure 8: Hard perimeter

A simple example of a hard perimeter can be seen in the picture above. An internal network consisting of several automation cells and a MES application represents a local production facility. To coordinate production between different production facilities and to provide remote maintenance capabilities, the system is connected to the Internet via a firewall. This firewall represents the hard perimeter: If an attacker is able to circumvent the firewall, the network is completely open for attacks.

2.6.2 Defense-in-depth

An alternative approach to the hard-perimeter, named defense-in-depth, replaces the single system security philosophy by a multi-level security system. It builds several zones for network security, each one equipped with a different security methodology and different security relevant devices (maybe provided by different device vendors). The shell system resulting from this approach shows a higher complexity but provides several advantages:

- Different security technologies raise the time necessary for intrusion
- The different stages allow different mechanisms for security defense e.g. for intrusion detection
- The raised intrusion time allows a better recognition of intrusion

The picture below shows the production facility from the example above with a more complex security system using the defense-in-depth approach.

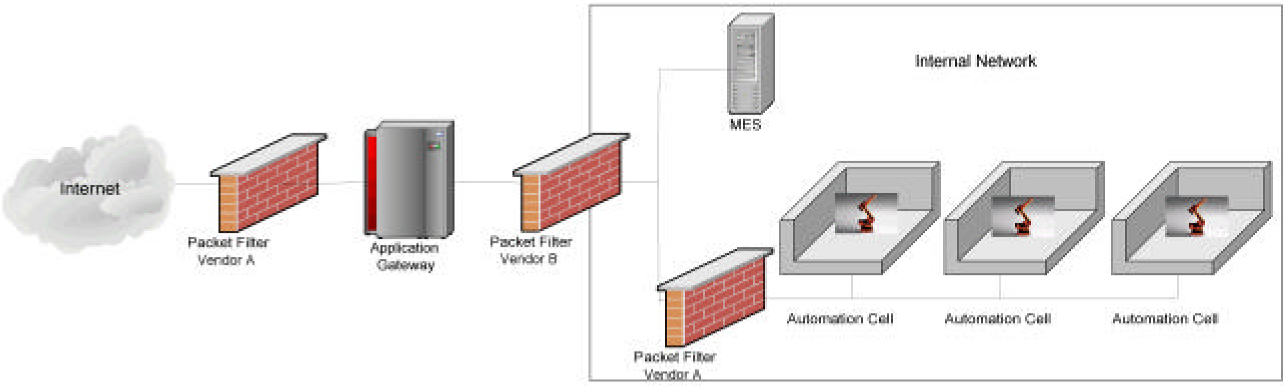


Figure 9: Defense in depth

To infiltrate the network, now the attacker has to bypass several security measures. First, he has to circumvent the first packet filter which has been implemented by a vendor A. Then, he has to take over the Application Gateway. An application gateway is used to decouple networks logically and physically. To communicate with a communication partner outside the internal network, any component from the internal network connects to the Application Gateway. The Application Gateway analyses the traffic, checks for any suspicious or forbidden action (e.g. accessing illegal content on a web server) and forwards the data to the destination. In the direction of the internal network, the Application Gateway is protected by a packet filter from vendor B. Finally, the Automation Cells are additionally protected by a packet filter.

Using different products in a defense-in-depth system can raise the security: If a security flaw is found for the packet filter of vendor A, the packet filter of vendor B is still secure.

2.7 Security Components

To implement a security system within the network additional devices implementing special mechanisms have to be integrated. Therefore, several components and concepts exists, that can help to secure an Industrial Ethernet network. The following sub-chapter will give a brief introduction to the most important concepts of a Packet Filter, an Application Gateway and a Demilitarized Zone (DMZ).

2.7.1 Packet Filter

A packet filter analyses and controls each individual incoming or outgoing packet passing a network border system and decides, using a rules table, whether a packet is valid and has to be forwarded or it should be dropped [Le03].

The packet filter can be integrated either within a sub-net bordering system representing an entry point to the sub-network or within the entrance system (network card) of an individual device. In both cases the entrance is protected by observing the packet flow through the system border.

The packet filter itself is integrated within the Ethernet TCP/IP protocol stack of the network cards used. The scheme of the integration of a packet filter is shown in Figure 10.

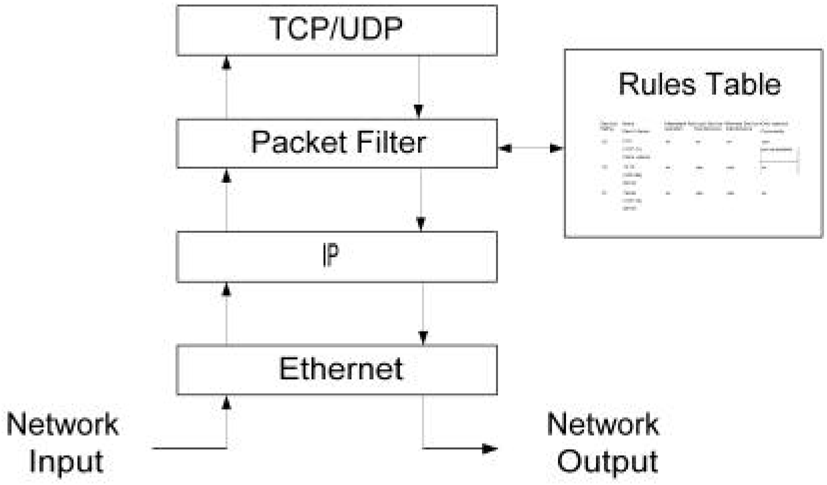


Figure 10: Concept of a Packet Filter

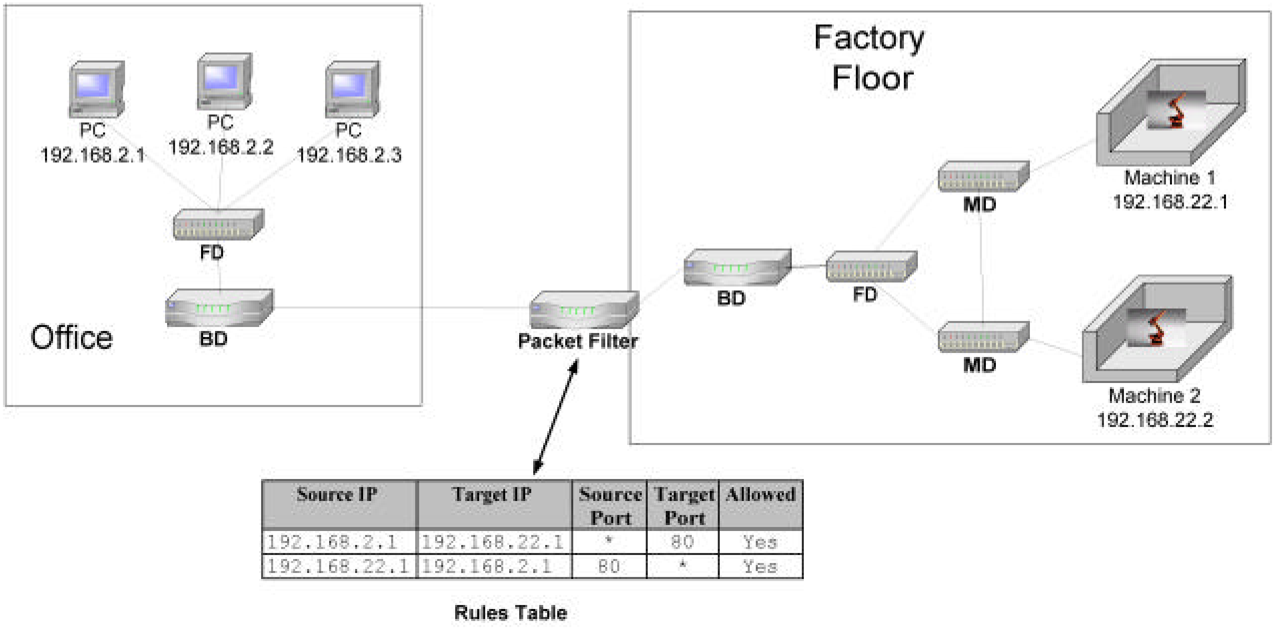
It can be seen, the a packet filter is located between the basic IP functionality and the TCP/UDP part of the IP stack. If an IP packet is received by a packet filter device, the packet has to pass a basic sanity check by the basic Ethernet and IP functionality (calculating checksum, comparing size of the header etc.). As a next step, the packet is forwarded to the packet filter code. The filter now decides based on a set of rules whether to allow the the packet to proceed or to drop. If the packet is allowed to proceed, it is forwarded to the TCP/UDP part of the IP stack.

The set of rules can be composed of several options, among others these are:

- IP Source address
- Source port
- IP Target address
- Target port
- TCP packet type (Synchronize, Acknowledge etc.)

In general, packet filters follow two different approaches when dealing with its rules. The first one, called “Deny”, drops all packets that are not explicitly allowed by a rule in the rules table. The source of the address will be informed using the ICMP protocol. The second one, called “Drop”, simply discards all packets that are not allowed by the rules without notifiy the packet source.

The following example shows a simple application of this concept.



Source IP	Target IP	Source Port	Target Port	Allowed
192.168.2.1	192.168.22.1	*	80	Yes
192.168.22.1	192.168.2.1	80	*	Yes

Rules Table

Figure 11: Packet Filter Example

Figure 11 shows a network split into two parts: an office network containing several workstations and a factory floor containing two machines. For the office network, it shall only be allowed for the PC with the address 192.168.2.1 to access the web server of Machine 1 with the address 192.168.22.1. Thus, the rules table of the packet filter contains two rules:

First, allow packets from 192.168.2.1 with any source port to 192.168.22.1 with target port 80, which is the standard port for HTTP (see annex 0). HTTP is based on TCP which result in a bi-directional communication. Thus, it is necessary to allow the way back or the PC will never receive the requested web page. This is done using the second rule: Allow packets from 192.168.22.1 with source port 80 to 192.168.2.1 with any target port.

Any other packet that tries to pass the packet filter will be discarded.

A more sophisticated king of packet filter are the dynamic packet filter, also called state full inspection. The example above has one main disadvantage. Any packet from Machine 1 is allowed to pass to the PC as long as the source port is set to 80. Dynamic packet filter provide a way to filter packets depending on connections. For the example above, a dynamic packet filter would only allow packets from the machine to the PC that belong to a connection which was established by the PC. In this way, only data that belongs to the requested web page is delivered. Any other packets are discarded by the packet filter.

2.7.2 Application Gateway

An Application Gateway is able to inspect protocols on the fly and can decide, based on a ruleset, which commands in a protocol are allowed and which ones have to be denied [Bre01]. Figure 12 shows the schematic structure of an Application Gateway.

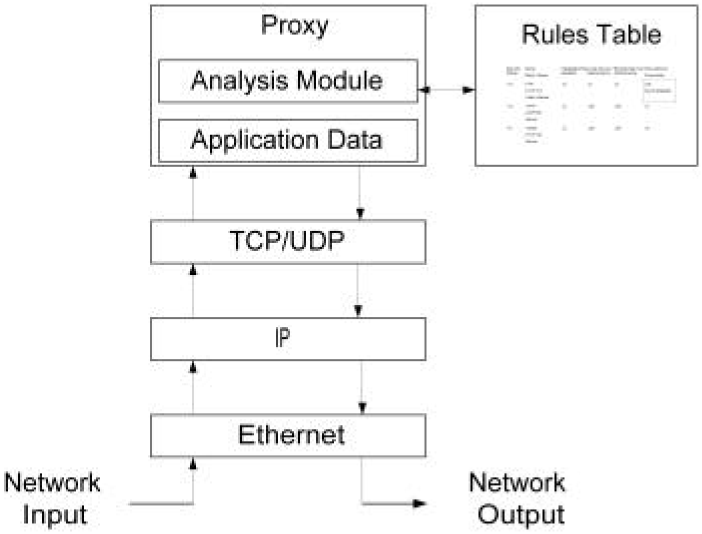


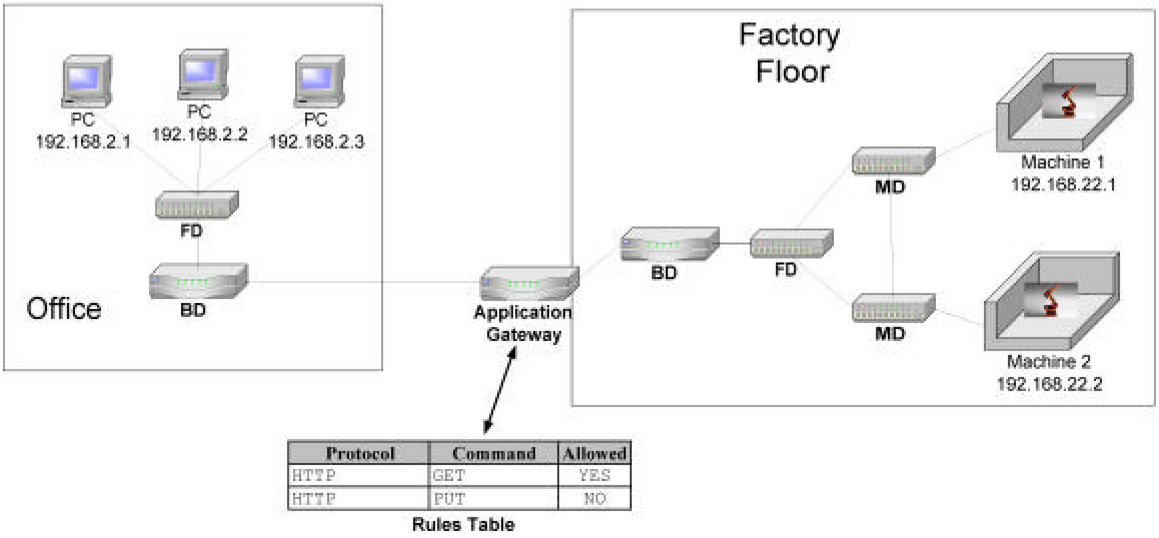
Figure 12: Application Gateway

As can be seen, an Application Gateway works on top of the IP stack. For each protocol, a so called proxy containing an analysis module has to be installed, that is able to analyse the protocol. A proxy reads data from the network, reassembles the whole command and analyses it. If the command is allowed to proceed according the the rules table of the proxy, the data is then sent to the target. Further on, it is possbile to filter out given content type such as, in case of web sites, Java Script or Java Apllets. This procedure allows a logical and physical decoupling of connections between source and target.

One disadvantage of this security component is the fact, that only standard protocols such as HTTP or SMTP can be secured since only proxies for those protocols exist. Other protocols cannot pass the Application Gateway. At the moment, there are no known proxies for Industrial Ethernet protocols such as EtherNet/IP or Modbus/TCP.

Optionally, an Application Gateway can be extended with further components such as Logging facilities or User authentication.

The following figure shows an example of the usage of an Application Gateway.



Protocol	Command	Allowed
HTTP	GET	YES
HTTP	PUT	NO

Figure 13: Usage of an Application Gateway

The example above reuses the network example from section 2.7.1. This time, the networks are not decoupled by an Packet Filter but by an Application Gateway. If the user of the PC with the address 192.168.2.1 tries to acces the web page on the Machine 1, the request has to pass the Application Gateway. The Application Gateway analyses the incoming command and checks against its rules table, whether the command is allowed. A simple retrieval of a web page is normaly done using the GET command of the HTTP protocol. According to its rules table, this command is allowed. Thus, the request will be forwarded to the Machine 1 and also the reply will be allowed. Additionally, an Application Gateway is able to inspect the contents of web page. In case the web page contains a Java applet for configuring parameters of Machine 1 which should only be accessible from within the Factory Network, the Application Gateway can filter out such contents, so this applet is not accessible from the office network.

In case, the user of PC of the office network tries to store a web page on the Machine 1 using the PUT command, this will be denied by the application gateway.

2.7.3 Demilitarized Zone (DMZ)

A Demilitarized Zone (DMZ, also called Screened Subnet), is a decoupled, isloated network that is integrated between two networks to decouple an unsecure network from a secure network [Mai03].

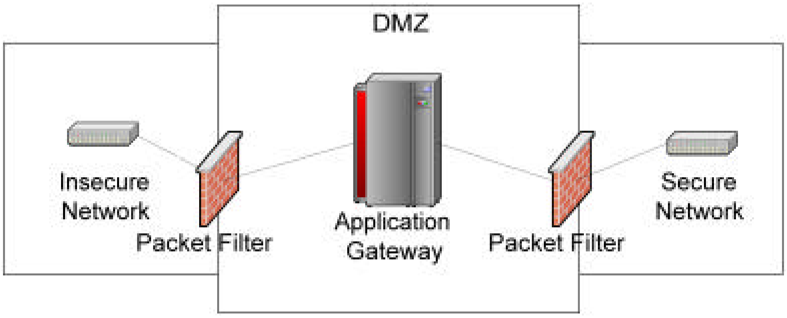


Figure 14: Demilitarized Zone (DMZ)

The DMZ is protected by two packet filters. The outer packet filter (the one directed to the insecure network) protects the DMZ against attacks from the insecure networks and also protects components located within a DMZ.

The inner packet filter protects the DMZ against attacks from the secure network, which can happen e.g. in case of virus spreads in devices of the secure network. Additionally, the packet filter provides another barrier for attackers that try to access the secure network in case that the protection of the outer packet filter fails.

Optionally, within a DMZ an Application Gateway can be integrated. The location within a DMZ offers additional protection for an Application Gateway.

A more complex application scenario for a DMZ is discussed in section 3.4.

2.7.4 Switches

A well-known problem of Ethernet networks are broadcast which can cause a high amount of traffic and may influence the performance and functionality of the system. Thus, it is necessary to restrict broadcast load on the system. Most modern switches provide functionality to influence the maximum broadcast load on the systems, thus the definition of network load limits or early warning systems for increasing network load can be done via the infrastructure components (e.g. MD, BD, see section 2.5) and need no additional security components.

2.7.5 Router

Router as fundamental infrastructure components of IP based networks have also possibilities to support the security of the communication.

In section 2.3.2, we have described special attacks that are based on flaws in the IP protocol, especially issues with faked addresses and source routing. Routers can be configured to only route packets with valid addresses and thus help to reduce such attacks.

The figure below shows, how a router can account for network security. It depicts a router that is connected to two networks:

- Network A with a network address of 192.168.22.0 and
- Network B with a network address of 192.168.2.0

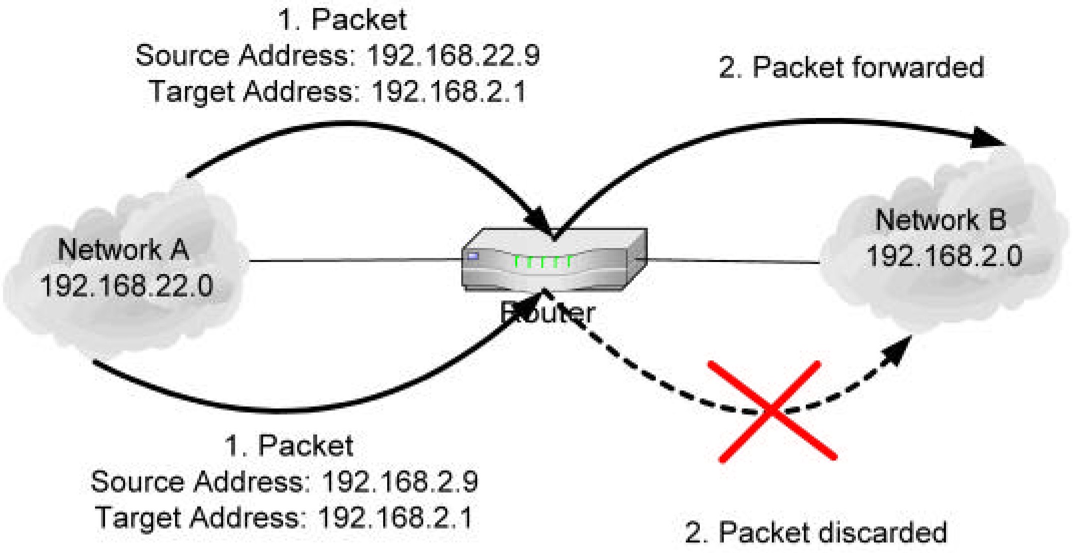

1. Packet
Source Address: 192.168.22.9
Target Address: 192.168.2.1
2. Packet forwarded
Network A
192.168.22.0
Router
Network B
192.168.2.0
1. Packet
Source Address: 192.168.2.9
Target Address: 192.168.2.1
2. Packet discarded

Figure 15: Filtering packets with invalid addresses

As can be seen in the figure above, first a packet with a source address of 192.168.22.9 and a target address of 192.168.2.1 shall be routed. Since there is no evidence that the address is incorrect (the source address belongs to the connected network), the packet gets routed.

In the second case, a packet with a source address of 192.168.2.9 shall be routed to the destination 192.168.2.1. The router now recognizes that the source address does belong to the target network (network B). It is impossible that this packet comes from network A. Thus, the routing algorithm decides to discard the packet. In this way, a router can help to reduce problems resulting from address spoofing.

2.8 Differences between Office and Automation Networks

The following table illustrates differences between typical office and automation networks and devices.

The table addresses mainly client- or end-devices in the office or automation environment, such as users workstations or field devices. Highly concentrated server areas in the office IT can be compared to line controlling PLCs and may need a different point of view.

	Office-IT	**Automation-Network**
Network-Structures	typical: redundant tree structures, reconfiguration (if automated) / recovery within 1 minute	need recovery after physical network failures within 1 sec
Behavior on high network loads	best effort	needs to limit network load (traffic shaping, network balancer) to guarantee operation of devices

Real-time communication	defined by user's expectations, reaction time up to 1 minute may be acceptable	"real-time" conditions within automation networks can be < 1 ms (depending on devices and services)
Life Cycles	Devices and Software may have life cycles of typ. 3-5 years	devices and software have support and life cycles of typically > 10 years
Virus Scanning	Performance drop is acceptable Using updates and patches every few days or weeks are acceptable	is in most cases unacceptable inside automation networks and devices due to the fact, that side-effects and performance issues are unknown Support during life cycle is usually not possible
Device Performance	outdated devices are easily replaced	regarding life-cycles, performance of devices may be statically limited
Power Consumption	System design keeps care of modern CPU's with high power dissipation.	System design may restrict device performance. Redundant power supplies, fan less devices are required.
Patch Management	Patch Management has higher priority than device operation. Automated Update services are available. Booting devices (and downtimes) is acceptable	Patch must not influence the device operation, must be tested prior to use. Booting of devices must be avoided.
Availability / Downtime	Failure of single or few devices may be acceptable and does not cause any general downtimes. Downtimes of a few minutes up to hours may be acceptable.	Failure of a single device may cause complete failure of production lines. Downtimes are usually acceptable of up to 5 minutes.
Device replacement	Replacement by software re-installation, hardware replacement may take days. Loss of user data may be acceptable. Replacement by maintenance personnel	Device and software replacement is needed within few minutes, No loss of user data and configuration. No trained personnel available
Applications	heterogeneous environment, type and number of applications is determined by user's needs. Harder to use certificates	well-defined and limited environment, use only applications needed for the device's operation. possibility to "stamp" applications
Network protocols	Need to use high number of protocols, message formats and broadcast messages.	The number of automation protocols is restricted, thus, the network traffic can be restricted to use only defined TCP/IP and UDP/IP connections.
Hardware Platforms	Mainly PC architectures using Windows operating system	many hardware platforms and legacy systems, using a high number of different OS's, versions and network stacks

Communication relations	highly dynamic client server and peer-to-peer communications	restricted number of communication relations.
	high number of used protocols and ports	possibility to control protocols and ports

The table above can help people to better understand the needs and requirements for Industrial Ethernet applications. Many products and solutions are based on developments made for and within Office IT - this discussion shall help to close the gap between these worlds.

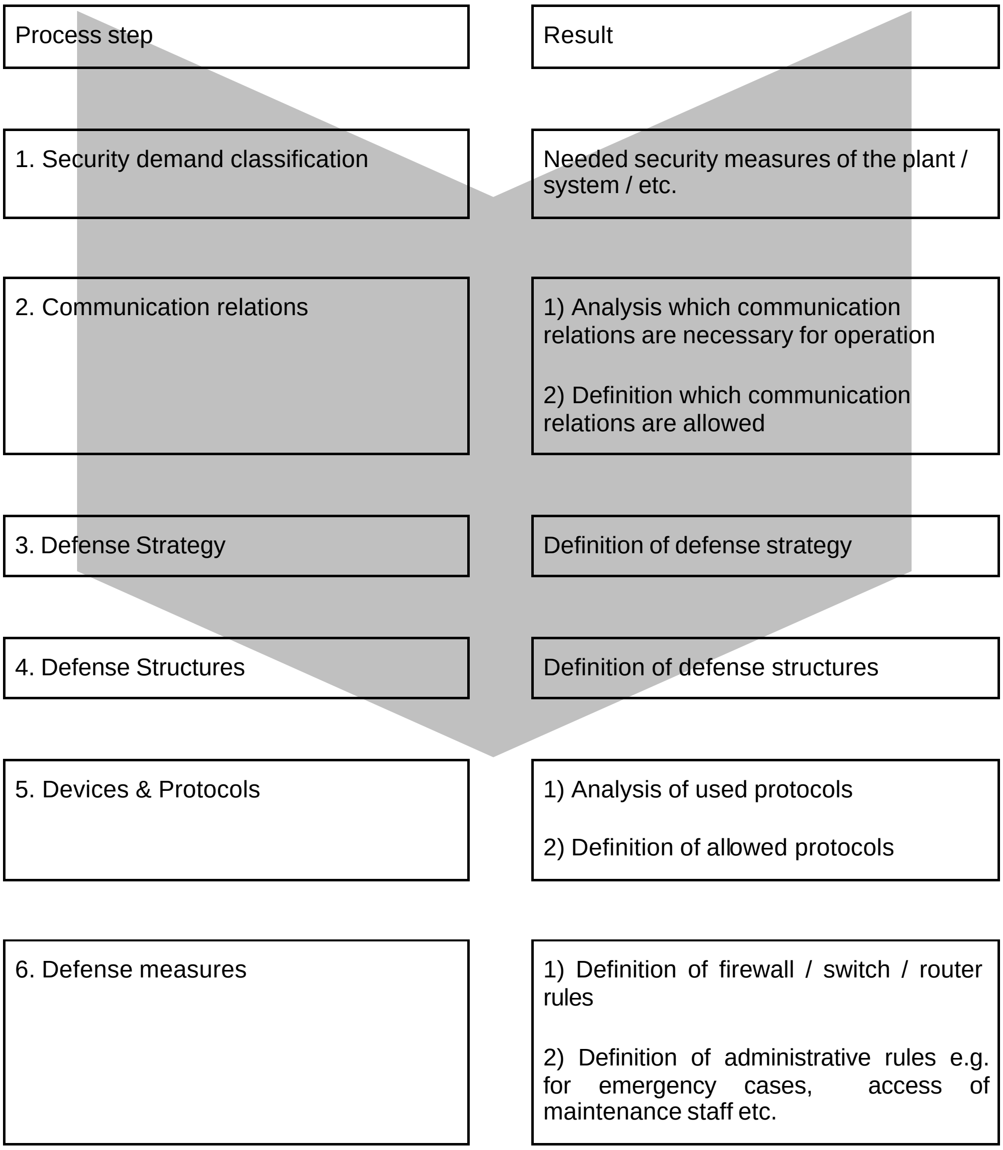
It is important to understand, that industrial Ethernet is not as heterogeneous as Office IT is - and this makes some things easier - like identification and controlling of network traffic. On the other hand, some requirements of industrial Ethernet are hard to cope with when using Office IT equipment: usually the boot time of a device, which is typically some 10-20 seconds, is not even mentioned - but using such a device on a robots tool-changer, the machine has to wait 10-20 seconds before continuing its work, and this is a killing factor to use such devices.

3 IAONA Security Methodology

When setting up network security for Industrial Ethernet networks, the following methodology should be pursued by system integrators or network administrators.

This methodology follows a step by step process in which each step generates results which have to be used in the following step.

The following figure shows the overall process:



Process step	Result
1. Security demand classification	Needed security measures of the plant / system / etc.
2. Communication relations	1) Analysis which communication relations are necessary for operation 2) Definition which communication relations are allowed
3. Defense Strategy	Definition of defense strategy
4. Defense Structures	Definition of defense structures
5. Devices & Protocols	1) Analysis of used protocols 2) Definition of allowed protocols
6. Defense measures	1) Definition of firewall / switch / router rules 2) Definition of administrative rules e.g. for emergency cases, access of maintenance staff etc.

This methodology will now be explained in more detail in the following chapters.

Note: It is important to understand that this methodology does not have to be sequential. Each step may have influence on other steps. For example, it may be possible that some communication relations cannot be secured in the required way, thus, a new structure for the network has to be found.

3.1 Security demand classification

In order to define, what security demand a single system has, first it is necessary to define a set of categories on which a malfunction of a device can have effects on:

- **affects production**
  describes the effects of a failure of a service or device on the production environment
- **user safety** (health and life)
  describes how a failure may effect the safety of a user
- **affects privacy** (access to person-related data)
  describes how a failure may lead to a violation of person-related information
- **affects company image**, publicity
  describes how a failure may cause damage to the company image
- **financial loss**
  describes how severe the financial loss due to a failure may be
- **violation of contracts/laws**
  describes how a failure may lead to a violation of patent rights or confidential data

The following table is showing what behavior may be acceptable for a certain category, depending on the security level (non, low-medium, high and very-high). The details in these sections, especially downtimes, are only suggestions and may be discussed individually.

	Security Level			
	None	**low-medium**	**high**	**very-high**
affects production	any effect on production / breakdown is possible stop and restart time doesn't matter	local, partial breakdowns are acceptable downtime does not exceed 6 hours loss may be compensated thru manual workers, buffering products, repeating of transmission etc.	local, partial breakdowns are acceptable downtime does not exceed 6 hours loss may be compensated thru manual workers, buffering products, repeating of transmission etc.	no breakdowns are acceptable downtimes are not acceptable loss cannot be compensated
user safety	no effects	any effect is not likely	any effect is not likely	failures are likely to affect safety systems
affects privacy	no personal data present, all data is public	personal data is present, access through other persons is possible and may be accepted, no loss of social state	personal data is present, access through other persons is possible and may be accepted, no loss of social state	personal data gets lost, tracking not possible loss of social state
affects company	neutral	only internal	only internal	information about the failure is public
financial loss	not relevant	within budget / calculation	within budget / calculation	severe financial damages threatens the company
violation of	not applicable	violation causes very	violation causes very	severe violations, may

contracts/ laws		limited damages	limited damages	cause legal suits

Based on the table above the user can define his necessary Security Level. This is done by checking for each item which of the four possible effects is true. The required overall Security Level is the highest marked security level of any category.

This example shows how the definition of security terms may be used on an IO-device.

Classification	
affects production	**low-medium** failure can easily be detected replacement with spare parts in short time
user safety	**none** this device does not interfere the overall safety circuits
affects privacy	**none** does not collect any personal data
affects company	**low-medium** unlikely to have any external effect
financial loss	**low-medium / high** cost for spare part and replacement diagnostic and restart may be cost intense
violation of contracts/laws	**low-medium** contracted availability may be affected

In this example, the necessary Security Level for the system would be low-medium / high due to the possible effects regarding financial losses.

3.2 Communication relations

As a second step, the different communication relations which are needed for the operation of the production system need to be analyzed. This analysis can be done using the proposed generic communication relations given in chapter 2.2 of this handbook (please refer to the template in chapter 6).

For the analysis of the communication relations the template can be gone through and all irrelevant data can be removed. The following table is an example of a filled out communications relations table:

Communication Relations Table		
Project: ***Example***	Date:	
Communication relation type (According to IAONA Handbook Network Security - Chapter 2.4)	Comment	Classification
1: Office ⇔ Internet	*There is no need to access the internet, however it can be allowed (as usual)*	Optional
2: Office ⇔ Factory	*Communication SAP to MES*	Necessary
3: Office ⇔ Remote Factory	*Only one factory*	Not applicable
4: Factory ⇔ Factory	*Only one factory*	Not applicable/
5: Office ⇔ Office	*Only one factory*	Not applicable
6: Remote Maintenance ⇔ Factory	*Not planned yet*	Optional
7: Home Office/Field Staff ⇔ Office	*No need for that*	Not applicable
8: Remote access of technical service ⇔ Factory	*Due to security considerations*	Forbidden
9a: Within factory	*Ethernet is used as communication bus*	Necessary
9b: Within factory	*Ethernet is used as communication bus*	Necessary
10: Within office	*Ethernet is used in the office*	Necessary
Communications Relations Table complies with the IAONA Handbook Network Security (Version 1.3)		

Necessary: A communication relation is necessary for operation and has to be established. If this communication relation is not established, the system might not work.

Optional: A communication relation is not necessary for operation. If this communication relation is not established, the system will still work.

Forbidden: A communication relation is not allowed. If this communication relation is established, the system might not be protected against attacks from this communication relation.

Note: This step is strongly depending on the starting point of planning the network security activities. If an already established network shall be secured based on this methodology, the table described above acts as the documentation of the structure of the network and the resulting communication paths for the communication relations. This documentation provides a basis for planning defense structures (c.f. section 3.4) and defense measures (c.f. section 3.6).

In case, a new network shall be secured it is strongly recommend to plan the network in strong collaboration with the planning of the defense structures c.f. section 3.4) and measures (c.f. section 3.6).

3.3 Defense Strategy

Based on the results of chapter 3.2 now the defense strategy has to be defined. Thus, the question, whether a defense-in-depth approach (cf. section 2.6.2) or a hard perimeter (cf. section 2.6.1) approach has to be answered.

The choice of the defense strategy of course is subject to the user's individual security tolerance, a general guideline can hardly be given. The next table tries to summarize the important points which should be considered when choosing a strategy.

Aspect	Hard-perimeter	Defense-in-depth
Security Demand	Minor threat Minor possibilities for damage	Serious threat Possibilities for damage
Communication relations	Only few communication relations to the outside	Multiple communication relations to the outside
Communication structure	Only few (one) access point to the network	Multiple access points to the network (internet, wireless, sneaker net, etc.)

3.4 Defense Structures

Based on the Defense Strategy, now the Defense Structures need to be specified. This means, how the defense will take place, e.g. by means of firewall, routers or switches and where are they positioned in the communication architecture. The requirements for the defense structures of a system result from its structure and its communication relations with its individual performance requirements (Real-Time, throughput etc). For planned networks, it is strongly recommended, to plan defense structure together with the whole network design.

For applying defense structures, the different elements described in section 2.7

- Packet Filter,
- Application Gateway,
- DMZ,
- Switches and
- Router

can be used. Based on the wiring example in Figure 7, some communication requirements and resulting security measures will be explained. The result is depicted in Figure 16.

The data within a MD subnetwork must be prioritized against network traffic from outer networks (e.g. traffic for web-based management) to guarantee soft real-time. This must be secured in both the case of malfunction and malicious actions. Therefore, a packet filter will be applied at the MD, that restricts the amount of incoming traffic from the building distributor.

The MD subnetworks must not influence each other. A mechanism is needed to guarantee a defined maximum delay between different subnetworks without influencing the behavior of the target network (throughput, delay, jitter). This must be secured in both the case of malfunction and malicious actions. Thus we configure the different switches in the network to reduce broadcast load. This functionality is additionally supported by the packet filter at the MDs. They are able to restrict the maximum amount of traffic between networks to a given value.

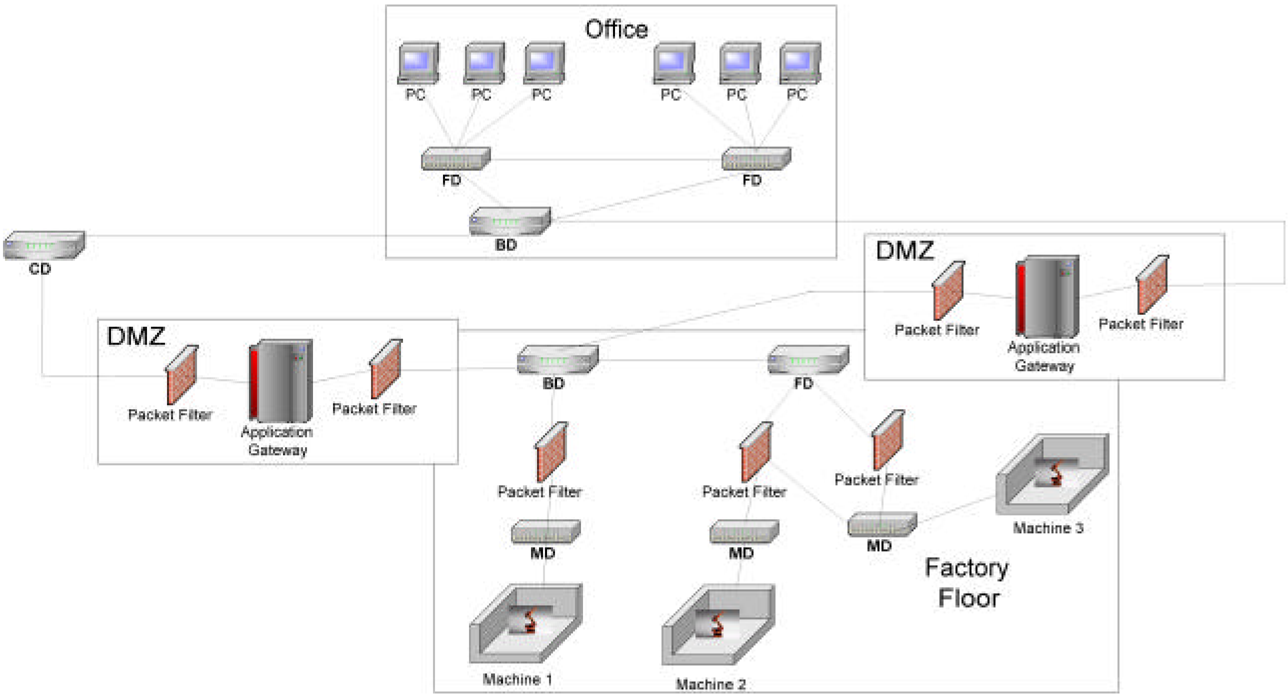


Figure 16: Defense Structures

Note: In the figure above, the term "Machine" refers to a set of different devices ranging from sensors to actuators. These devices are grouped together to a machine in a so called automation cell. The communication within a cell is normally realized in real-time. Grouping of devices to cells can also be considered as a defense structure. For cells, the border component that connects the cell with the network plays an essential role regarding the security of the cell.

The network traffic from outside the factory floor network must be restricted to

- Traffic that is not malicious and
- Allowed personnel.

The solution to this problem is provided by DMZ (c.f.2.7.3) that protect the BD of the factory floor network against traffic from the office network. In this example, two DMZ were added to the system to provide redundant access to the factory network which provides an additional protection against Denial of Service attacks.

The application gateways decouple the factory floor network physically from the campus backbone and are able to filter out malicious code from protocols. For example, only GET and POST commands are allowed for the HTTP protocols. PUT requests are filtered out and logged. Additionally, the Application Gateways are equipped with an Authentication Proxy which allow distinguished services for authenticated personnel only.

Each application gateway is protected by one Packet Filter to the outer network and one Packet Filter to the inner network. The packet filter for the inner network protects the Application Gateway against attacks from the Factory Floor networks e.g. by Trojan Horses or Viruses that have infiltrated the network e.g. caused by external maintenance staff. This structure helps to stern the spread of malicious software. The Packet Filter to the outer network protects the Application Gateway against attacks from the campus network, especially against Denial-of-Service attacks that can render the Application Gateway useless by generating high traffic and system load.

3.5 Devices / Protocols

As a next step, the single devices have to be looked at regarding their communication relations and the protocols which are used in these communication relations. This especially refers to the used automation protocols such as Modbus/TCP, EtherNet/IP, Ethernet Powerlink or EtherCAT and their used ports. The documentation of this data is a required for defining the defense measures by means of defining firewall rules.

In doing this, the IAONA Security Data Sheet (SDS) can be of great help. If a manufacturer of a device, cell or network provides a SDS, the user practically has all relevant information he needs.

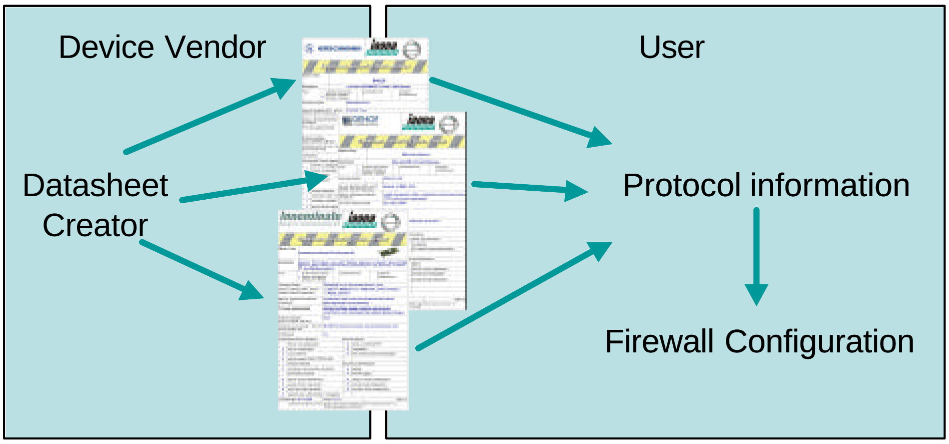


Figure 17: SDS workflow

As shown in the figure above, the user or a system integrator collects the different SDS of the devices in his automation system and derives from these SDS the information about the different protocols he needs in order to administer his firewall. The SDS is also available in an XML format (c.f. Annex 8), thus tools that can read and process a SDS can automate the process of configuration of firewalls and other security components. In this way, the complexity of applying security to an Industrial Ethernet network is reduced significantly.

The following table sums up the information the user can get from the SDS:

	Firewall Configuration	Router Configuration	Switch Configuration	Other
Page 1:				
Type: Device / production cell / network				
Operating System	(X)	(X)	(X)	Patch management
Network Interfaces			X	
Backup-Restore				Set up of recovery policies
Firmware update				Set up of additional protection against manipulation of firmware
External Interfaces				Set up of security policies
Behavior on power loss				Set up of recovery policies
Certification				

Page 2:				
Security Rating	X	X	X	
Name + Client/Server	X	X	X	
Needed for operation	(X)	(X)	X	
Local service + maintenance	(X)	(X)	X	
Remote service + maintenance	X	X	X	
Optional / comments				Additional information e.g. about ports of custom software installations

In Annex 9, a wide list of common protocols applied in the Industrial Ethernet environment ranging from the common automation protocols to supporting protocols such as HTTP for exchanging web information or SMTP for sending e-mails is given. Each protocol is characterized by:

- A short description,
- The used UDP/TCP ports,
- Security Rating and Classification,
- Information about usage and functionality of the protocol and
- Security related application recommendations.

The Security Rating describes the security of a protocol design ranging from 1 (insecure) to 5 (secure). The Classification for a protocol gives a recommendation whether a protocol should be used ranging from 1 (not recommended) to 5 (highly recommended). This split-up of the evaluation of a protocol comes from the fact, that in some cases an insecure protocol is necessary to run a network. An example for this case is the ICMP protocol (for a more detailed description see section 2.3.1 and annex 9.1). Since ICMP has no security feature that protects it against being used for attacks, it has a security rating of 1 (insecure). Unfortunately, it is often problematic to run large IP networks correctly without ICMP, so the Security Classification is rated with 3 (tradeoff between security and functionality). Additional information is given in the “Measures for security” section to reduce the risk resulting from ICMP.

3.6 Defense measures

Based on the analysis of communication relations, defense structures and the applied protocols and devices, the rules for the different application components can be developed. All rules have to be documented at length.

For an example of the application of defense measure, again, the example from chapter 3.4 will be used.

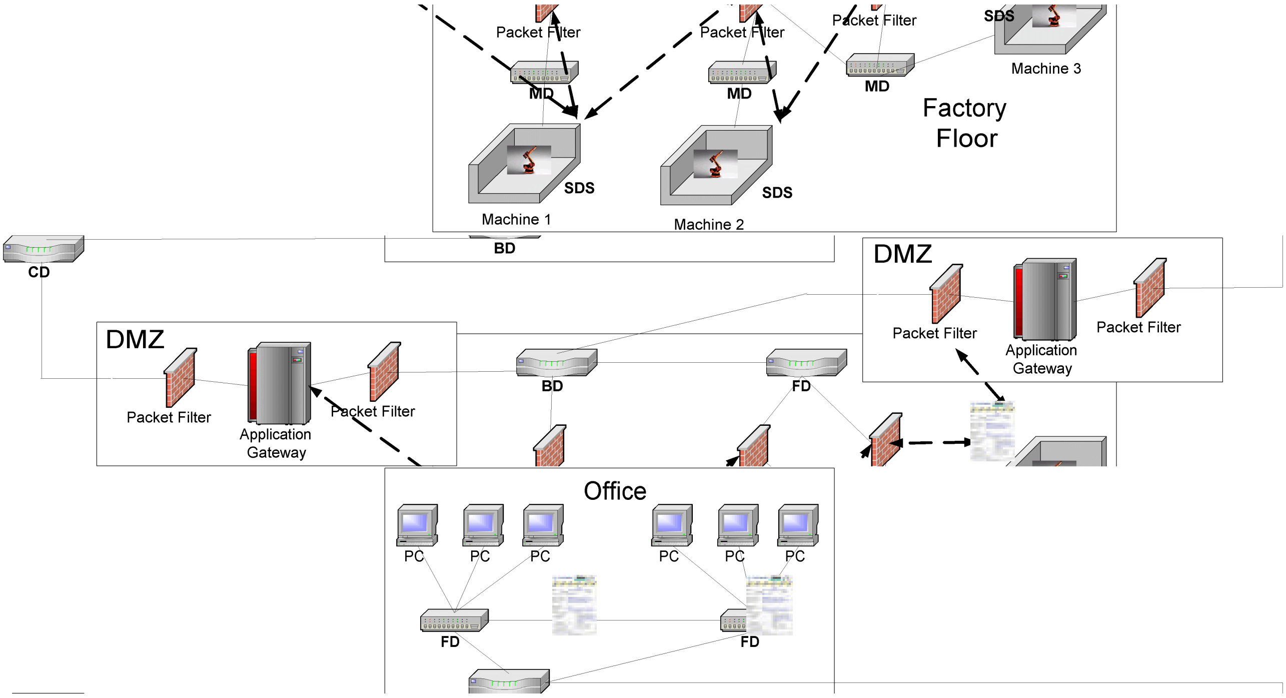


Figure 18: Application of defense measures

It is assum ed that for each machine, an IAONA Security Datasheet (SDS) is available (in the figure above this is depicted by the small SDS). Within step 2 (Communication relations, see chapter 3.2) it is known that Machine 1 and Machine 2 communicate with each other as well as Machine 2 and Machine 3. Additionally, the status of Machine 1 and Machine 3 shall be accessible via a web browser by PCs of the office network. From the SDS of the machines we can get the information that Machine 1 and Machine 2 can communicate over Modbus/TCP and Machine 2 and Machine 3 communicate over EtherNet/IP. Additionally, the status of Machine 1 and Machine 3 can be accessed over HTTP using port 80.

Based on this information, we can configure the defense structure that was defined in step 4 (Defense structures, see chapter 3.4). The use of the SDS in packet filters and application gateways is shown in the figure above by arrows. The packet filter that connects Machine 1 to the BD has to allow communication between Machine 1 and Machine 2 over Modbus/TCP. Hence it has to allow packets over TCP with destination address of Machine 1 and destination port 502 as well as packets over TCP with destination address of Machine 2 and destination port 502. Again, this information can be derived from the service description of the IAONA Security Datasheet of Machine 1 and Machine 2. The same rules apply for the packet filter that connects Machine 2 to the BD.

Additionally, since EtherNet/IP communication is necessary between Machine 2 and Machine 3, the appropriate packets must be allowed within the packet filter of Machine 2. The SDS describes, that port 44818 over TCP and 2222 over UDP must be allowed. Thus, the packet filter has to allow packets over TCP with destination address of Machine 3 and destination port 44818 and vice versa. Additionally, UDP packets from Machine 3 with destination port 2222 have to be allowed as well as vice versa. The same rules apply for the packet filter of Machine 3.

Finally, the application gateways that connect the factory floor with the campus network have to be configured. As stated above, the status of Machine 1 and Machine 4 shall be accessible by given office PCs. Thus, the Application Gateway will be equipped with an HTTP proxy (for a description of the Proxy concept see chapter 2.7.2). Additionally, the packet filter of the DMZs are configured to only allow packets from authorized office PCs to proceed to the application gateways. According to the SDS of Machine 1 and Machine 3 the communication over HTTP has to be realized over port 80. Thus, the packet filters have to be configured to allow the communication.

Organizational rules

But planning of defense measures does not end with the security component configuration. Further on, it is of high importance to define rules for handling security in the daily work. In general, this includes procedures for

- checking equipment of external staff that want to connect to the network
- guidelines for emergency cases such as a recognized attack attempt, stolen equipment etc.
- procedures for allowing remote maintenance etc.

In the following, some recommendations regarding service and maintenance procedures as well as general administrative rules are given as a hint for defining defense measure procedures.

Rules for service and maintenance

- Describe who is allowed to access which devices.
- Define access levels (installation, configuration, see VDI/VDE guideline 2187).
- Document the direction of allowed data flow (upload, download) for the maintenance case.
- Describe, what needs to be done if a device is replaced (check policies, security-keys etc)
- Describe, what requirements devices of external maintenance staff e.g. laptops have to fulfill to be allowed within the internal network. For example, this describes the required virus protection policies.

Administrative rules

- Explain how virus protection and detection works for your party.
- Describe the procedure for security related incidents, e.g. a Virus occurs or an attack attempt was detected. This includes the description of responsibilities.
- Describe, what needs to be done, when an employee is laid off.
- Describe, what needs to be done, when a hardware e.g. a laptop gets lost.

4 The Security Cookbook

This chapter describes sample solutions for common security related problems.

4.1 Remote Access

A very common demand for any machine or line builder and his customers is how a remote service scenario can be set up.

The following two paragraphs are showing how an approach to this demand can look like. The first suggestion uses one central instance to control remote traffic – which we call a terminal server – the second uses a "network manager" to control traffic between a service provider and the end devices.

4.1.1 Terminal Server

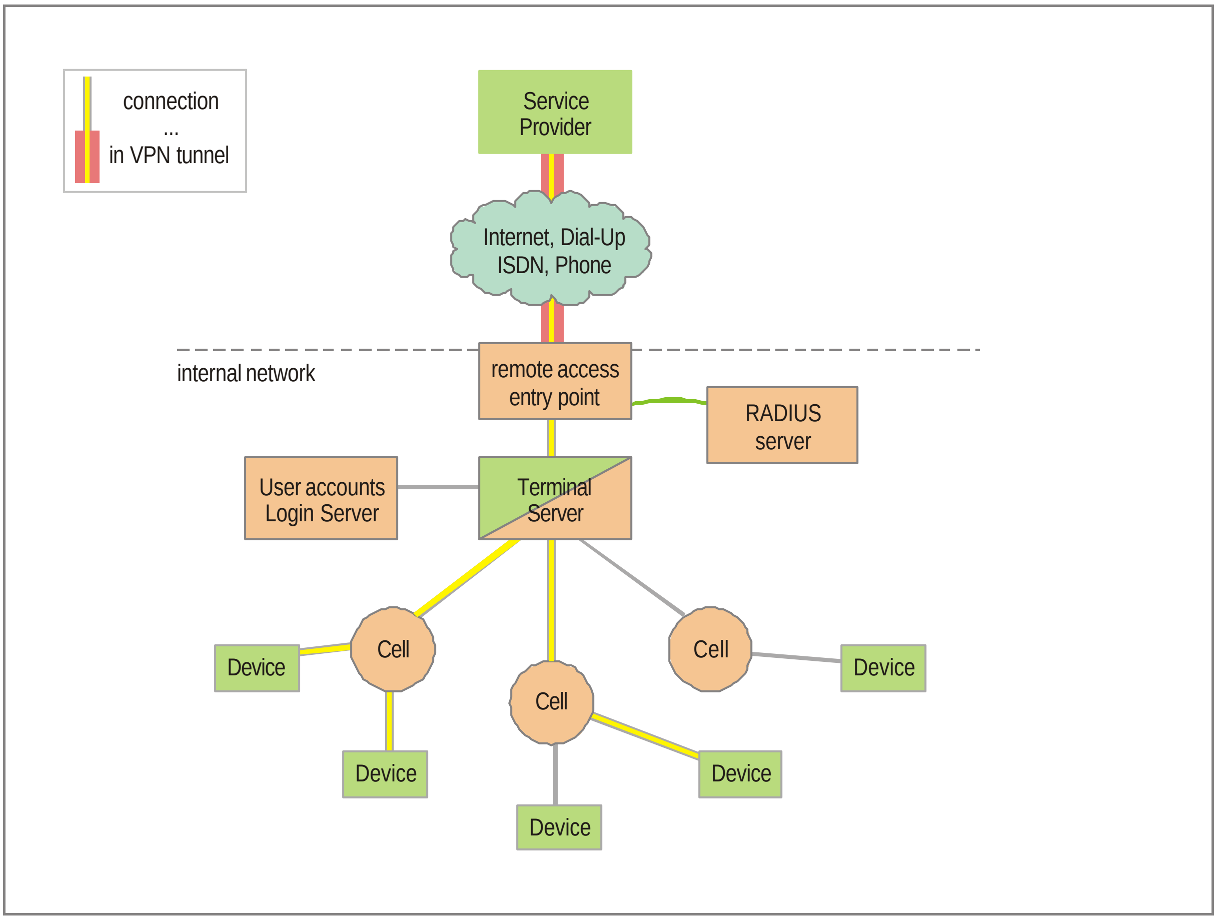


Figure 19: Security Gate as Terminal Server

The Security Gate acts as a Terminal Server - not a terminal server as we know from old Unix days - a terminal session server, where a remote worker uses a remote user interface. Any software like VNC could be used for this purpose.

This is a highly secure machine with up-to-date virus pattern and firewall rules. Any service user dialing into the RAS point comes first to the security gate and uses then a second, cascaded communication link to the end device.

File access and data transfer to the terminal server could also rely on unsecure protocols (such as FTP) when a secure connection (e.g. using VPN) is used.

There is no direct access to end devices from outside, any access requires custom software installed on the Security Gate. Also HTTP Web Access should not be allowed directly to device level, but some kind of centralized access control mechanism could be used to ease administration (such as e.g. IBMs Tivoli)

+ highly secure solution

-/+ an increased demand for administration, to control network connections

+ single point for administration

- needs to provide every software which is necessary for remote workers

- requires system performance

- each customer/application may require a single server

+ easier to provide virus protection

+ protocol and logfiles can be collected on the server. Automatic access is possible

4.1.2 Network Manager

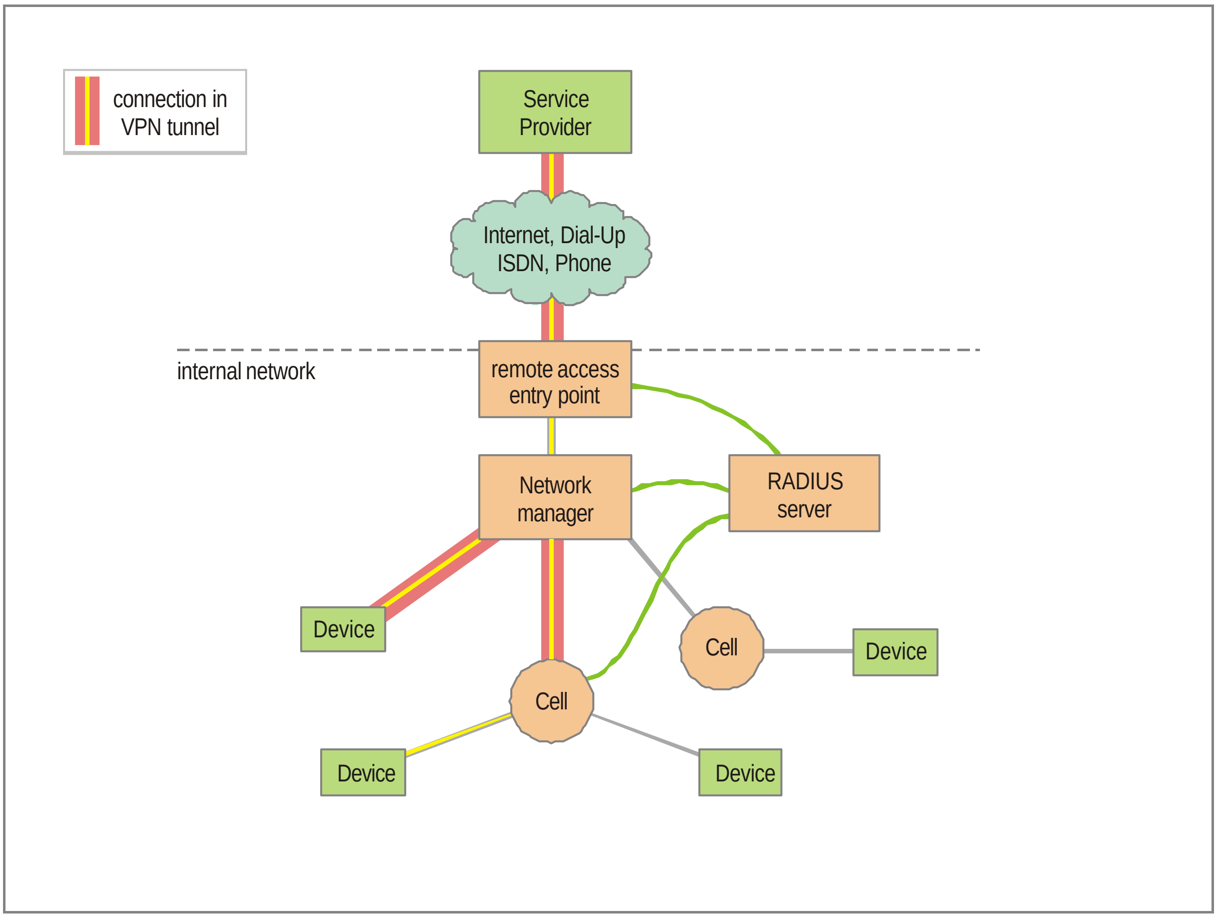


Figure 20: Security Gate as Network Manager

The Security Gate controls the network traffic and communication links, based on lists and rules for communication links (IP addresses) and associated network ports. In detail, this allows to administrate access control mechanisms.

As a result, this solution suggests distributed security, where multiple components cooperate to reach the desired level of security. The network manager can allow or deny connections to end devices or cells, based on user authentication.

+ medium/highly secure solution

- requires knowledge about communication links

+ single point for administration

+ no need to install specific software

- virus-scanning is hard to accomplish, some devices may not be able to run
anti-virus software (requires store-and-forward)

Since this solution creates high demands for the network manager, any secure connection should terminate at the end device level or at least at cell level.

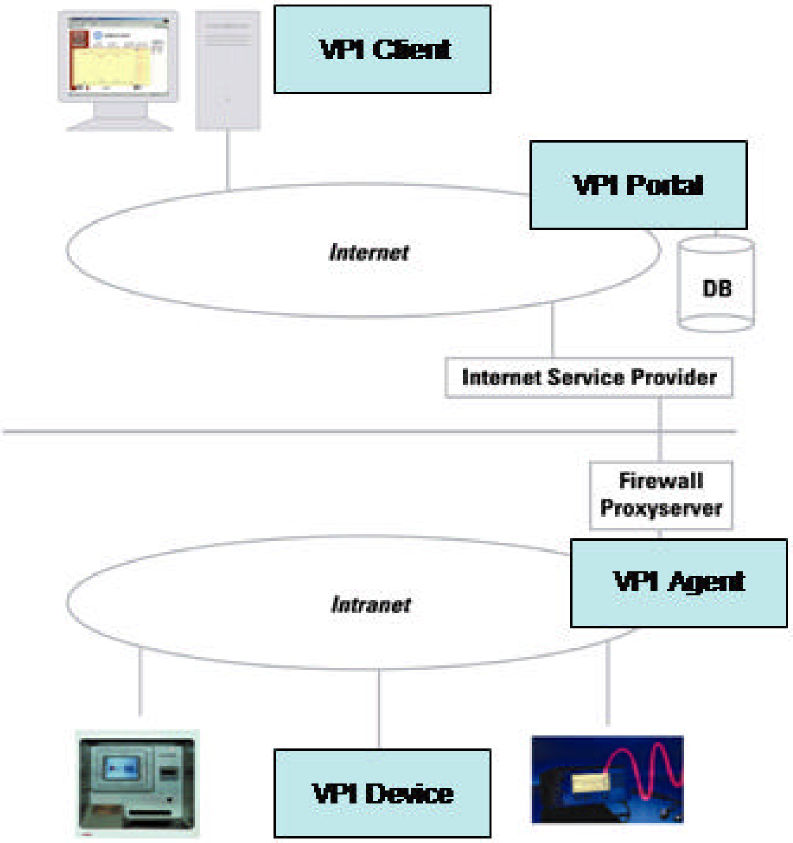
Recommendations for Network Access on the plant

- use VPN software on service laptops to connect to the plant network – all traffic is routed through the Security Gate and then access to the end devices is possible. Important: use virus scanning on all external interfaces
- any physical access to the switch and its ports is not possible, a dedicated service network port is somewhere in each production cell - or even better - use secure gates in the plant network to define communication from/to the devices. Example: a service port with pre-defined rules.

the network administrator may decide whether he uses the switch' port security feature to monitor events only, or restrict access to certain devices etc.

4.2 Distributed Web-Server Access (VPI)

This chapter introduces a HTTP-based concept for user interface and management: the Virtual Private Infrastructure VPI.



The previously mentioned examples are suitable to realize a remote access on existing (also legacy) applications, using a variety of protocols. More and more devices and applications offer a pure HTTP-based interface for both user interaction (MMI's) and remote procedure calls (e.g. SOAP). As HTTP provides its own naming scheme using URL's, distributed HTTP servers can be organized through proxy- and relay-servers, which can more easily hide the underlying IP-adress scheme. The management of such a concept can therefore be easier and less demanding. Such an approach was proposed by an industry initiative called 'Virtual Private Infrastructure' (VPI).

Virtual Private Infrastructure (VPI) systems connect remote devices to the Internet via a VPI Portal. VPI uses HTTP from the VPI Portal to the VPI Agent to communicate with the remote device. The VPI Portal forwards the HTTP requests to the VPI Agent, which acts as relay station and forwards it to the VPI Device itself.

A VPI Portal is a communication platform that has to be transparent on HTTP-level. It receives requests from VPI Clients via TCP port 80 and relays them to VPI Agents. This also includes the transparent relay of remote procedure calls (RPC). In the same way, it relays the responses of VPI Agents to VPI Clients. VPI Agents may be reached via public internet facilities, but also via private dial-up or leased wired or wireless lines.

Thus, a VPI Portal is more than just a HTTP Proxy. It is the central administration platform for all target devices in the system. It runs a list with the links of all target systems to which he has right of access. When a target is selected, a transparent HTTP connection is established to the VPI agent.

VPI Portals are mandatory in VPI Architecture: No VPI client is allowed to communicate directly with VPI Devices. Thus, availability, flexibility and security are enhanced. The VPI Agent is used to make devices within an intranet accessible from the VPI Portal. The operator of the intranet has control over the VPI Agent and can define at any time which target systems should be visible on the Internet. Additionally, the available procedures, variables and devices are provided as process points.

In most cases the VPI Agent is a software module which can be deployed on any system within the intranet, e.g. a PC, a server or a suitable embedded device. For operability behind firewalls, it is required, that the VPI Agent's HTTP server works via TCP Port 80.

4.3 VPN based approach and Security Portals

Many discussions about network security are answered with VPN technology in these days. Using VPNs is not an easy task, an broad variety of protocols and mechanisms for authentication, encryption and authorization are incompatible regarding the fact, that only well-trained users are able to initiate such systems.

5 IAONA Security Data Sheet

The IAONA Security Data Sheet (SDS) is a single device's type plate for network security. It gives a short and comprehensive overview for network security administration. It is meant to help operators or system integrators when protecting their systems against malicious attackers. This usually means the administration of firewalls. Here rules for access to devices behind the firewall have to be defined and exactly this is eased by the SDS.

The IAONA SDS can be applied to any kind of product in the domain of industrial Ethernet which has an IP-Address, it is not limited to a special type of protocol.

The IAONA SDS shall be filled out and provided together with the product by the supplier of

- a device
- a productions cell or
- a network infrastructure component.

The idea of the SDS is to provide information (ports used and protocols supported) about a device or a product and enable your customers to work securely with your product. The list of used ports / protocols will enable the user to decide how to configure firewalls / routers / switches.

The data sheets targets several issues:

- describe your product
- enable your customer to see what's inside your product
- describe the network behavior
- describe the network ports and services

The SDS is either provided as a paper version or as an XML-File. A template for the paper version and the XML-Schema for the XML-File can be found in the Annex.

For the SDS there is no certification process. IAONA follows a self certification procedure: Each manufacturer can simply fill out the SDS and then use the logo to show that there is a SDS available.

IAONA is supplying a tool for its members to help filling out the SDS, the SDS Creator (SDS-C). This tool automatically generates XML-Files and PDFs for print out. Single SDS can be saved, changed, copied etc.

5.1 How to fill out the SDS

The following section give a brief introduction how to fill out the IAONA Security Datasheet.

5.1.1 General

If your are not using the SDSC, please follow the following guidelines:

- please use "Arial 10pt (bold)" as font for the data sheet
- the data sheet shall describe your device or product to your customers - keep in mind that their technical skills might be different from yours
- if you feel that our data sheet is missing details, please add some comments

5.1.2 Page 1 - General

Page one contains general information about the product.

Name of item: Give a name of your device, something like: "Eagle-X1" or "PC/4711"

Description: Give a short description of your device e.g. "Router" or "IO-Interface"

Type

Device: Select this, if your device is any passive or active network device (end-point devices as well as infrastructure devices)

A production cell: Select this, if you want to describe a production cell or a complex machine with an internal network.

A network: Select this, if you want to describe a complete network, service or infrastructure

Operating System: Describe the operating system and its version e.g. “Linux 2.4.12”

Network Interfaces: Describe the physical network interface and connector type like "10/100 MBit", "RJ45-VarioSub", "MTRJ" etc.

Backup-Restore: Describe how backups and restore are supported by your device e.g. "Floppy Disks", "manually by user", "FTP over network" etc.

Firmware update: Describe whether and how it is possible to upgrade firmware.

External Interfaces: Describe any external interface, like floppy disk drives, USB etc so the user can decide how to use and protect those.

Behavior on power loss: Describe what happens in case of power failure. How much time needs the device to restart (boot)? Is it necessary to restore any configuration data ?

Certification: Describe any certificates for your product (something like CC=common criteria, ISA99 etc) .

Date: Please use an easy to understand date coding, like "23. Dec 2004"

Version: The Version of the datasheet shall go like "v01.00"

Implemented Security features: Please select the features your device/cell/network supports.

Network features: Please select the features your device/cell/network supports.

Service and Maintenance: Please select the features your device/cell/network supports.

5.1.3 Page 2 - Network Ports and Services

The information provided in this list shall enable the user to decide whether to use a service or not - the information about TCP und UDP ports will help to administrate firewalls, switches and routers to control network traffic.

Service: The name of the service to describe e.g. DHCP or FTP

Ports*:* Specify which ports are necessary to operate the service e.g. for FTP port 21.

TCP: Select this if the service is running over TCP.

UDP: Select this if the service is running over UDP.

Other: Select this if the service is running over other packet types e.g. plain IP in case of ICMP.

Client: Select this if the client part of the protocol is implemented.

Server: Select this if the server part of the protocol is implemented.

Protected: Select yes if the service has an additional protection e.g. user/password protection for FTP.

Can be disable: Select this if the service can be disabled.

Needed for operation: Select yes if it is not possible to disable the service without influencing the proper work of the device.

Local Service/Maintenance: Select yes if this service is necessary to perform local service/maintenance.

Remote Service/Maintenance: Select yes if this service is necessary to perform remote service/maintenance.

Description: Here, describe the service further and give additional comments..

Security Rating: Select the appropriate security rating for the service. A detailed description of the security rating can be found in section 3.5 and annex 9. For common services in Industrial Ethernet environments, security ratings are already defined by the IAONA JTWG Security. These ratings can be found in annex 9.

Security Classification: Select the appropriate security classification for the service. A detailed description of the security classification can be found in section 3.5 and annex 9. For common services in Industrial Ethernet environments e.g. Modbus-TCP or EtherNet/IP, security classifications are already defined by the IAONA JTWG Security. These ratings can be found in annex 9.

5.1.4 Naming Conventions

The document name of the data sheet shall be like this

```
SDS_<Company>_<Device Name>_<Draft/Version>.<doc/pdf>
```

See these examples

```
SDS_ACME_0815-4711_Draft.doc
SDS_MyCompany_NetDevice-22_v01.pdf
```

5.2 Security Data Sheet Creator (SDS-C)

Currently IAONA iprovides a tool for its members to help filling out the SDS. This tool automatically generates XML-Files and PDFs for print out. Single SDS can be saved, changed, copied etc. The tool is available for Linux and Windows.

For a description of this tool, please refer to its handbook.

6 Annex: Communication Relations Table Template

Communication Relations Table		
Project:	Date:	
Communication relation type (According to IAONA Handbook Network Security - Chapter 2.4)	Comment	Classification
1: Office ⇔ Internet		Not applicable/ Necessary/ Optional/ Forbidden
2: Office ⇔ Factory		Not applicable/ Necessary/ Optional/ Forbidden
3: Office ⇔ Remote Factory		Not applicable/ Necessary/ Optional/ Forbidden
4: Factory ⇔ Factory		Not applicable/ Necessary/ Optional/ Forbidden
5: Office ⇔ Office		Not applicable/ Necessary/ Optional/ Forbidden
6: Remote Maintenance Factory		Not applicable/ Necessary/ Optional/ Forbidden
7: Home Office/Field Staff ⇔ Office		Not applicable/ Necessary/ Optional/ Forbidden
8: Remote access of technical service ⇔ Factory		Not applicable/ Necessary/ Optional/ Forbidden
9a: Within factory		Not applicable/ Necessary/ Optional/ Forbidden
9b: Within factory		Not applicable/ Necessary/ Optional/ Forbidden
10: Within office		Not applicable/ Necessary/ Optional/ Forbidden
Communications Relations Table complies with the IAONA Handbook Network Security (Version 1.3)		

7 Annex: Security Data Sheet Template

(Company Logo)	iaona ethernet security data sheet
Name of item	**(Device Name)**
Description	**(Device Description)**

Type	X	a device (any device, active and passive devices, switches)	X	a production cell	X	a network (infrastructure)

Operating System	**(Operating System, Version)**
network interfaces (RAS, built-in Modem, Network Gateways)	**(Network-Interfaces)**
Backup, replacement features / procedures	**(Backup-Restore)**
Firmware update Applications	**(Description)**
External interfaces (FDD, CD-ROM, USB etc)	**(Interfaces)**
behavior on power loss / network communication loss	**(Description)**
Security Certifications	**(Certificates)**

Implemented Security features		Network features	
x	firewall, not configurable	**x**	needs / provides DHCP
x	firewall, configurable	**x**	manageable
x	virus protection	**x**	MAC-address based authentication
x	data encryption	**x**	IP-address based authentication
x	intrusion detection	Service and Maintenance	
x	robustness, stack overflow protection	**x**	logging
x	redundancy possible	**x**	ready for remote maintenance
x	secure remote maintenance	**x**	provides local configuration
x	access control, user levels	**x**	provides remote configuration
x	local user access possible		
x	supports user authentication, manageable		

for more informations : http://www.acme.com/catalog/dev0815.htm		
Release date: **(Date)**	Version: **(x)**	Page 1/2
Data sheet complies with the rules set in the IAONA Handbook for Network Security (Version 1.3)		

(Company Logo)	**(Device Name)**	iaona ethernet security data sheet

Used Network ports and services

Service	Port(s)	TCP	UDP	Other	Client	Server	protected	can be disabled	Needed for operation	Local Service / Maintenance	Remote Service / Maintenance	Description	Security Rating	Security Classification
FTP	**21**	**x**			**x**		**yes**	**x**	**no**	**no**	**no**		1	3

Legend	Security Rating: 1- unsecure mechanisms, unprotected; 2- minimum security; 3- common security features, basic protection; 4- most security features available; 5- fully protected, state-of-the-art security	
	Security Classification: 1- not recommended to use; 2- may be used with caution; 3- usually advisable; 4- low risk, advisable to use; 5- highly recommended	
Release date: **(Date)**	Version: **(x)**	Page 2/2
Data sheet complies with the rules set in the IAONA Handbook for Network Security (Version 1.3)		

8 Annex: Security Data Sheet XML Schema

```
<?xml version="1.0" encoding="iso-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" attributeFormDefault="unqualified">
   <xs:element name="DataSheet">
      <xs:complexType>
         <xs:sequence>
            <xs:element name="GeneralInformation">
               <xs:complexType>
                  <xs:sequence>
                     <xs:element name="CompanyLogo" type="xs:string"/>
                     <xs:element name="DeviceName" type="xs:string"/>
                     <xs:element name="Description" type="xs:string"/>
                     <xs:element name="Contact" type="xs:string"/>
                     <xs:element name="Date" type="xs:string"/>
                     <xs:element name="Version" type="xs:string"/>
                     <xs:element name="Type">
                        <xs:complexType>
                           <xs:sequence>
                              <xs:element name="isDevice" type="xs:boolean"/>
                              <xs:element name="isProductionCell" type="xs:boolean"/>
                              <xs:element name="isNetwork" type="xs:boolean"/>
                           </xs:sequence>
                        </xs:complexType>
                     </xs:element>
                  </xs:sequence>
               </xs:complexType>
            </xs:element>
            <xs:element name="DeviceInformation">
               <xs:complexType>
                  <xs:sequence>
                     <xs:element name="OperatingSystem" type="xs:string"/>
                     <xs:element name="NetworkInterfaces" type="xs:string"/>
                     <xs:element name="Backup-Restore" type="xs:string"/>
                     <xs:element name="Firmware" type="xs:string"/>
                     <xs:element name="ExternalInterfaces" type="xs:string"/>
                     <xs:element name="PowerLoss" type="xs:string"/>
                     <xs:element name="Certifications" type="xs:string"/>
                  </xs:sequence>
               </xs:complexType>
            </xs:element>
            <xs:element name="SecurityFeatures">
               <xs:complexType>
                  <xs:sequence>
                     <xs:element name="Firewall-wo-Config" type="xs:boolean"/>
                     <xs:element name="Firewall-w-Config" type="xs:boolean"/>
                     <xs:element name="VirusProtection" type="xs:boolean"/>
                     <xs:element name="DataEncryption" type="xs:boolean"/>
                     <xs:element name="IntrusionDetection" type="xs:boolean"/>
                     <xs:element name="Robustness" type="xs:boolean"/>
                     <xs:element name="Redundancy" type="xs:boolean"/>
                     <xs:element name="SecureRemoteMaint" type="xs:boolean"/>
                     <xs:element name="AccessControl" type="xs:boolean"/>
                     <xs:element name="LocalUser" type="xs:boolean"/>
                     <xs:element name="UserAuth" type="xs:boolean"/>
                  </xs:sequence>
               </xs:complexType>
            </xs:element>
            <xs:element name="NetworkFeatures">
               <xs:complexType>
                  <xs:sequence>
                     <xs:element name="DHCP" type="xs:boolean"/>
                     <xs:element name="Manageable" type="xs:boolean"/>
                     <xs:element name="MACAuth" type="xs:boolean"/>
                     <xs:element name="IPauth" type="xs:boolean"/>
                  </xs:sequence>
               </xs:complexType>
            </xs:element>
            <xs:element name="Maintenance">
               <xs:complexType>
                  <xs:sequence>
                     <xs:element name="Logging" type="xs:boolean"/>
                     <xs:element name="RemoteMaint" type="xs:boolean"/>
                     <xs:element name="LocalConfig" type="xs:boolean"/>
                     <xs:element name="RemoteConfig" type="xs:boolean"/>
                  </xs:sequence>
               </xs:complexType>
            </xs:element>
            <xs:element name="NetworkServices">
               <xs:complexType>
                  <xs:sequence>
                     <xs:element name="Service" maxOccurs="unbounded">
                        <xs:complexType>
                           <xs:sequence>
                              <xs:element name="ServiceName" type="xs:string"/>
                              <xs:element name="Port" type="xs:string"/>
                              <xs:element name="TCP" type="xs:boolean"/>
                              <xs:element name="UDP" type="xs:boolean"/>
                              <xs:element name="Other" type="xs:boolean"/>
                              <xs:element name="disabled" type="xs:boolean"/>
                              <xs:element name="Server" type="xs:boolean"/>
                              <xs:element name="Client" type="xs:boolean"/>
                              <xs:element name="protected" type="yesno"/>
                              <xs:element name="isNeeded" type="yesno"/>
                              <xs:element name="LocalMaintenance" type="yesno"/>
                              <xs:element name="RemoteMaintenance" type="yesno"/>
                              <xs:element name="optComment" type="xs:string"/>
                              <xs:element name="Rating" type="einsfuenf"/>
                              <xs:element name="Class" type="einsfuenf"/>
                           </xs:sequence>
                        </xs:complexType>
                     </xs:element>
                  </xs:sequence>
               </xs:complexType>
            </xs:element>
         </xs:sequence>
      </xs:complexType>
   </xs:element>
   <xs:simpleType name="yesno">
      <xs:restriction base="xs:string">
         <xs:enumeration value="yes"/>
         <xs:enumeration value="no"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="einsfuenf">
      <xs:restriction base="xs:string">
         <xs:enumeration value="/"/>
         <xs:enumeration value="1"/>
         <xs:enumeration value="2"/>
         <xs:enumeration value="3"/>
         <xs:enumeration value="4"/>
         <xs:enumeration value="5"/>
      </xs:restriction>
   </xs:simpleType>
</xs:schema>
```

9 Annex: Network Services

The following section - which does not claim to be complete - is a summary of network services of which we think are relevant for industrial automation networks and should be a help for anyone trying to understand firewalls and routers or switches and who is perhaps trying to set up some rules and policies to make his network more safe.

Since we are in the special environment of an automation network, we set up some restrictions that may not survive in the 'office world'

- all traffic over cells is routable IP protocol, either TCP/IP or UDP/IP
- any non-IP protocol will be blocked by the switches and does not leave a cell
- real-time protocols exist only within real-time domains, even when some cells are one real-time domain, the rules above apply then to this real-time domain.

Security

To make reading easier, the following quick rating scheme is used through the datasheets

1 insecure mechanisms, no protection at all, information can be read with packet-analyzers

2 a minimum of security is provided, e.g. by using proprietary mechanisms ("security by obscurity". Once someone has worked out the weakness and posted it, it degrades to -1-)

3 common security features are present, basic protection

4 most security measures are applied, e.g. encryption etc.

5 secure services with state-of-the-art protection against manipulation

Classification

The following rating is for the recommendation of services

1 is not recommended to use, as this service is insecure

2 may be used temporarily, shall be monitored

3 tradeoff between security risks and functionality

4 low security risks, usually secure to use

5 highly recommended to use

Quick Overview - Security Relevant Network Services

Synonym Name	Ports	Description	Chapter
FTP FTPS	(20) 21	File Transfer Protocol do. secure	0
HTTP HTTPS	80 443	Hypertext Transfer Protocol do. secure	0
SNMP	161, 162	Simple Network Management Protocol	0
DNS	53	Domain Name Service	9.4
DHCP	67, 68	Dynamic Host Configuration Protocol	9.3
SSH	22	Secure Shell	9.9
iPSEC	500	IP Security Protocol	9.21
SMTP	25	Simple Mail Transfer Protocol	9.8
TELNET	23	Terminal Emulation	9.7
TFTP	69	Trivial File Transfer Protocol	9.6
SOAP	80, 443, 25	Simple Object Access Protocol	9.24
RPC	135 + more	Remote Procedure Call	9.18
DCOM	135 + more	Distributed Component Object Model	9.18
DynDNS	110	use POP3 for dynamic DNS	0
SNTP		Simple Network Time Protocol	
NTP	123 UDP	Network Time Protocol	
RFC1588		Network Time synchronization	
ICMP (Ping)	*(no port)*	Internet Control Message Protocol	
ARP	*(no port)*	Address Resolution Protocol	
LDAP	389, 636	Lightweight Directory Access Protocol	0
RADIUS	1812, 1813	Remote Authentication Dial-In User Service	0
PPTP	1723	Tunneling Protocols	9.22
L2TP	1701	Layer 2 Tunneling Protocol	9.23

Kerberos	88, 4444, 749, 464	network authentication	9.20
MODBUS-TCP	502	Modbus over TCP	9.14
EtherNet/IP	44818, 2222	Rockwell's Procotols	9.15
NDDS	7400	Real-Time middleware	0
PROFINet	135 + more	Siemens' Ethernet Procotol	
MAP/MMS	*No information available*	Manufacturing Automation Protocols	9.27
Powerlink	*none*	EPSG Ethernet Protocol	9.17
EtherCAT	*(no ports)*	Beckhoff Ethernet Protocol	0
Safe Ethernet	*No information available*	HIMA Safety Ethernet Protocol	
Sercos III	*Information not yet available*		
Custom -Ports	*(individually)*	*must be individually rated*	
SQL-Server	*(individually)*	*(---)*	
"SAP"-Services	*No information available*	*not sufficient data available*	
Remote Access Services	*(individually)*	VNC, pcAnywhere, PC-Duo	
File "Browser"	137-139, 445	NetBios over TCP	

9.1 ICMP

Basis protocol for IP networks - the PING tool is based on it.

Name	ICMP
Description	Internet Control Message Protocol
Port number	ICMP is on IP layer - no port
Security Rating	1 (1=insecure ... 5=secure)
Classification	3 (1=do not use ... 5=advisable)
Recommendation	only use for non-critical applications
Function	exchange IP related control messages or diagnostic information
Usage	ICMP echo (with the "ping" tool), control messages like host unreachable, network unreachable, source quench and any others

Security	not designed with security in mind, not encrypted
Worst-Case	denial-of-service attacks can be used to overload (lower layers of) devices traffic is sniffed by a man in the middle, can be used to get information about target network topology
Measures for security	Although the ICMP services are not very secure, blocking ICMP traffic is an issue to be discussed. Within the 16 ICMP services most of them are for information about routers, but also PING and BOOTP needs ICMP. It may be a suggestion to allow ICMP internal and to the outside of a network, but block incoming traffic. Keep in mind that some IP-stacks can be overflowed with large PING packets.

9.2 ARP

Protocol to assign layer 3 (IP) addresses to layer 2 (physical MAC) addresses, widely used, not secure.

Name	**ARP**
Description	Address Resolution Protocol
Port-Nr	-
Security Rating	1 (1=insecure ... 5=secure)
Classification	not possible, as any IP communication won't work without ARP
Recommendation	-
Function	handles assignment of layer 3 (IP-)addresses to layer 2 (physical) addresses in local networks
Usage	Internal used in all Ethernet devices. An ARP Request (broadcast) is sent to all devices in a local network to get information about the Ethernet address of a device.

Security	not designed with security in mind. ARP spoofing is widespread.
Worst-Case	Simulation of wrong IP address is used to attack integrity of documents and also with the goal of hurting the privacy
Measures for security	Tools are available to watch changes of assignment Ethernet address – IP address Example: arpwatch (Linux)

9.3 DHCP

Dynamic Host Configuration Protocol - mainly used to obtain IP addresses and network configuration parameters (like gateways, server addresses etc.) on startup

Name	DHCP
Description	Dynamic Host Configuration Protocol
Port number	67, 68
Security Rating	2 (1=insecure ... 5=secure)
Classification	2 (1=do not use ... 5=advisable)
Recommendation	use for closed networks or non-critical applications
Function	provide automatic configuration of hosts using TCP/IP, supplies IP configuration, addresses of name servers, routers, print servers, boot images for diskless clients and many more
Usage	mainly used to provide configuration parameters to Internet hosts. Client machines are provided with their IP addresses as well as other host configuration parameters through this mechanism.

Security	data transfer is unencrypted
Worst-Case	all hosts using DHCP can not use any networking functionality if the DHCP server is broken
Measures for security	use static configuration instead of DHCP

9.4 DNS

Domain Name Service, used to resolve IP addresses from readable names.

Name	**DNS**
Description	Domain Name Service
Port number	53
Security Rating	2 (1=insecure ... 5=secure)
Classification	4 (1=do not use ... 5=advisable)
Recommendation	use for non-critical applications
Function	DNS is used mostly to translate between domain names and IP addresses and to control Internet email delivery. Most Internet services rely on DNS to work, and if DNS fails web sites cannot be located and email delivery stalls.
Usage	hierarchical structure of DNS servers to resolve host names in the internet, provide name resolution in local networks, not for confidential information

Security	not designed with security in mind, not encrypted except for data exchange between name servers (if supported)
Worst-Case	providing wrong data, leading to unwanted access to the wrong host, breaking other important services like email
Measures for security	only use trusted DNS servers

9.5 FTP

Protocol for file transfer, widely used, not secure. Use only with caution.

Name	**FTP**
Description	File Transfer Protocol
Port-Nr	(20) 21
Security Rating	1 (1=insecure ... 5=secure)
Classification	3 (1=do not use ... 5=advisable)
Recommendation	use only for accessing single devices on closed networks
Function	used for transferring files, implemented on almost every platform, well-known protocol, uses minimum processing power
Usage	Up/Download of firmware, access logfiles

Security	login with username and password, not encrypted ! can be read with sniffer, data is not encrypted
Worst-Case	theft of username and password, listen in to data, may result in unwanted access from intruders
Measures for security	use FTP/S or additional authentication with HTTP or scp (ssh2) use additional encryption

9.6 TFTP

Protocol for file transfer, widely used, not secure. Use only with caution.

Name	TFTP
Description	Trivial File Transfer Protocol
Port-Nr	69
Security Rating	1 (1=insecure ... 5=secure)
Classification	3 (1=do not use ... 5=advisable)
Recommendation	use only for accessing single devices on closed networks
Function	used for transferring files, implemented on almost every platform, well-known protocol, uses minimum processing power
Usage	Up/Download of firmware, configurationfiles or any other files

Security	not designed with security in mind, no authorization is required! Can be read with sniffer, data is not encrypted.
Worst-Case	theft of password files, trust relation files may result in unwanted access from intruders
Measures for security	use strict restriction of tftp-server access.

9.7 Telnet

Probably the most known service for interactive sessions.

Name	TELNET
Description	remote login protocol
Port number	23
Security Rating	1 (1=insecure ... 5=secure)
Classification	1 (1=do not use ... 5=advisable)
Recommendation	use only in closed networks and with non-critical data
Function	TELNET is a third-level protocol. The Telnet protocol defines an interactive, text based communications session between a client and a host. Is mainly used for remote login and simple control services
Usage	login to systems with very small resources or to systems without any needs for security

Security	login with username/password, not encrypted
Worst-Case	theft of transferred data, theft of login information to gain illegal access using telnet or other services
Measures for security	use SSH2 instead of telnet

9.8 SMTP

The most used mail transfer protocol.

Name	SMTP
Description	Simple Mail Transfer Protocol
Port number	25
Security Rating	1 (1=insecure ... 5=secure)
Classification	4 (1=do not use ... 5=advisable)
Recommendation	use only within closed networks and with non-critical data
Function	connect to a SMTP server and transmit eMails. Login information is eMail address only - can easily be read - and the server is often not able to verify this authentication.
Usage	The most established service for sending eMails worldwide.

Security	login with username/password, not encrypted all data can be easily sniffed and examined
Worst-Case	theft of user identification to gain access to mail system, read data and use account to fake identity, eMail contents can be accessed by third party. Misuse of SMTP (=eMail) servers for relaying and SPAM. May cause severe load problems to mail servers and infrastructure.
Measures for security	use a SSL connection, use secure authentication, use data encryption mechanisms. PGP (Pretty Good Privacy) can help to identify originator and contents. use POP-before-SMTP as additional authentication

9.9

9.10 SSH

Secure Shell - better alternative to Telnet sessions.

Name	SSH
Description	Secure Shell – SSH2
Port number	22
Security Rating	4 (1=insecure ... 5=secure)
Classification	5 (1=do not use ... 5=advisable)
Recommendation	use for access to single hosts over entrusted networks (SSH1 is not anymore recommended)
Function	SSH (Secure Shell) is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is intended as a replacement for rlogin, rsh, and rcp.
Usage	This protocol accomplishes the same as telnet does. But the complete transmission is encrypted. Used for remote login services, copying files or secure tunnels for TCP protocols that don't provide security measures
Security	user/password authentication, public key authentication for server and client side SSH protects against: • IP spoofing, where a remote host sends out packets which pretend to come from another, trusted host. Ssh even protects against a spoofer on the local network, who can pretend he is your router to the outside. • IP source routing, where a host can pretend that an IP packet comes from another, trusted host. • DNS spoofing, where an attacker forges name server records • Interception of clear text passwords and other data by intermediate hosts. • Manipulation of data by people in control of intermediate hosts • Attacks based on listening to X authentication data and spoofed connection to the X.11 server.
Worst-Case	insecure exchange of public keys may lead to man in the middle attacks, theft of private keys or login information may lead to illegal access
Measures for security	exchange of public keys over trusted channels, careful use of login information and private keys

9.11 SNMP

Protocol for Network Management functions - Used to query information from remote hosts and to send commands: to change the configuration of remote machines, implemented on most TCP/IP capable operating systems.

Name	SNMP
Description	Simple Network Management Protocol
Port-Nr	161 for SNMP Request 162 for SNMP Trap
Security Rating	SNMP v1: 2 (1=insecure ... 5=secure) SNMP v3: 5
Classification	SNMP v1: 3 (1=do not use ... 5=advisable) SNMP v3: 5
Recommendation	SNMPv1: use vendor specific security features if available, if not available: use only for accessing devices on closed networks, SNMPv3: All security levels available
Function	Configuration and Monitoring of Ethernet devices. Used to manage large networks SNMPv1: implemented in many hubs, switches, routers. Supported from almost all network management applications. SNMPv3: not often implemented in network management applications.
Usage	Get an Set variables of devices for configuration and monitoring. Get device-specific Events (Traps)
Security	SNMPv1: login with password (community), not encrypted ! Can be read with sniffer, data is not encrypted. SNMPv3: encryption and authentication available. Definition of user-dependant security levels
Worst Case	SNMPv1: theft of community password, listen in to data, may result in unwanted access from intruders
Measures for security	SNMPv1: use in closed areas, all network management systems support it, apply read-only settings to devices SNMPv3: use in open areas, note: configuration is costly

9.12 HTTP

Hypertext Transfer Protocol for web based services, very common - security depends on implementation and environment.

Name	HTTP / HTTPS
Description	Hypertext Transfer Protocol over TLS/SSL
Port number	80 (HTTP) 443 (HTTPS)
Security Rating	HTTP 2 (1=insecure ... 5=secure) HTTPS 5
Classification	HTTP 3 (1=do not use ... 5=advisable) HTTPS 5
Recommendation	Useful for large local networks or internet services
Function	Mainly used for websites, also for file transfers and other services embedded into the HTTP protocol. Servers and clients are implemented on most TCP/IP capable operating systems.
Usage	Provide access to websites, file download and transfer method for text based services.

Security	HTTP is not encrypted, HTTPS provides SSL encryption and x.509 certificates
Worst-Case	HTTP transfers can be sniffed, faked authenticity of a HTTPS server due to entrusted distribution of x.509 certificates.
Measures for security	Simple: do not publish any critical information use HTTPS for confidential data or to ensure the servers authenticity, secure exchange of x.509 certificates Recommend basic authentication only over SSL/HTTPS, for HTTP use only digest authentication to prevent clear text password transmission (see [THMC03])

9.13 DynDNS

DynDNS is used to have an Internet DNS address while the IP address may change (typical for DSL connections) – is implementation specific.

Name	DynDNS
Description	Dynamic DNS (see RFC 2136)
Port number	110
Security Rating	3 (1=insecure ... 5=secure)
Classification	3 (1=do not use ... 5=advisable)
Recommendation	use DynDNS to make your devices public available with an URL while IP addresses are changing on PPPoE connections.
Function	the client device (usually a router or similar device) connects to a DynDNS server frequently and transmits its own IP address and connection parameters.
Usage	the device "acme" is registered at "dyn.example.com" and can then be accessed with the URL "acme.dyn.example.com"

Security	DynDNS Server needs user login (account)
Worst-Case	someone may steal the login information (not encrypted) and use this to register a false IP address to reroute traffic to another IP address.
Measures for security	Other protocols for login can used.

9.14 Modbus-TCP

Modbus-TCP is the TCP/IP based implementation of the Modbus Fieldbus Protocol.

Name	**Modbus**
Description	Modbus Protocol
Port number	502
Security Rating	1 (1=insecure ... 5=secure)
Classification	3 (1=do not use ... 5=advisable)
Recommendation	restrict access to ports on border of production cells
Function	Automation protocol with lots of subfunctions. Especially read/write of variables, Up/Download of applications Well-known, easy to implement, request/response protocol - using a minimum of resources
Usage	Up/Download of applications to PLCs, monitoring reading and writing variables (sensors/actors), controlling

Security	no authorization, no confidentiality, no integrity
Worst-Case	depends on used devices
Measures for security	At this time there is no alternative to the given security recommendations - all IP based fieldbus protocols are facing these problems. An extended version of Modbus with different security levels is in discussion.

9.15 EtherNet/IP

EtherNet/IP is the implementation of the CIP (Control and Information Protocol) for IP based networks

Name	EtherNet/IP
Description	EtherNet/IP Protocol
Port number	44818 (TCP), 2222 (UDP)
Security Rating	1 (1=insecure ... 5=secure)
Classification	3 (1=do not use ... 5=advisable)
Recommendation	restrict access to ports on border of production cells
Function	EtherNet/IP is a very complex port of the CIP automation protocol to IP based networks.
Usage	Up/Download of applications to PLCs , monitoring reading and writing variables (sensors/actors), controlling

Security	no authorization, no confidentiality, no integrity
Worst-Case	depends on used devices
Measures for security	At this time there is no alternative to the given security recommendations - all IP based fieldbus protocols are facing these problems. There are no plans of extended versions with security features in discussion.

9.16 EtherCAT

EtherCAT is an Ethernet real time technology with two variants: for hard real time applications the EtherCAT telegrams are transported directly in the data area of the Ethernet frame without using IP based protocols. This variant A is limited to one subnet and is hardly prone to IP security issues. Applications with routing requirements may use variant B, where the EtherCAT telegrams are transported within the data section of a UDP/IP datagram. In both variants, any IP based protocol can be used in addition. Since these protocols are transported by EtherCAT telegrams and relayed by the master, all security measures applied to the master protect the entire network.

Name	**EtherCAT**
Description	EtherCAT Protocol
Port number	Variant A: none; Variant B: 34980 (UDP)
Security Rating	2 (1=insecure ... 5=secure)
Classification	3 (1=do not use ... 5=advisable)
Recommendation	Use Variant B only if subnet routing is required. General IP security recommendations apply.
Function	A : Real time Control Network. B : EtherCAT/UDP provides access to EtherCAT segments via routers, e.g. in building automation applications.
Usage	Real Time Control, Industrial Automation, Building Automation

Security	Variant A: no IP security issues. Clear separation of mission critical real time protocol and other protocols. Variant B: no built in security measures, but use of dedicated protocol.
Worst-Case	depends on used devices
Measures for security	General security measures apply (e.g. password protection for configuration tool). Variant A: Little security concerns since IP is not used for mission critical purposes. Variant B: IP used for routing, but non IT protocols for control.

9.17 ETHERNET Powerlink

Name	**ETHERNET Powerlink**
Description	Real-Time Industrial Ethernet Protocol
Port number	No port assigned. Any IP-based protocol can be used with ETHERNET Powerlink
Security Rating	1 (1=insecure ... 5=secure)
Classification	3 (1=do not use ... 5=advisable)
Recommendation	
Function	Real-Time protocol for Industrial Automation.Isochronous channel for time critical data.Asynchronous channel for ad-hoc data. Any IP-based protocol and respective security claim appies.
Usage	Time-critical applications like in motion control

Security	Separated from non-real-time domains via router/firewall
Worst-Case	Depending on services used
Measures for security	Clear separation between real-time network domain and regular network domain.

9.18 RPC / DCOM

Protocol for using COM Objects over network.

Name	**DCOM**
Description	Distributed Component Object Model
Port-Nr	Dynamically assigned at run time (1 TCP / 1 UDP) SCM (DCOM´s Service Control Manager) TCP/UDP 135
Security Rating	1 (1=insecure ... 5=secure)
Classification	2 (1=do not use ... 5=advisable)
Recommendation	Due to several Design flaws in RPC it is not recommended to use DCOM.
Function	DCOM is a (Microsoft) solution for distributed computing. It allows one client application to remotely start a DCOM server object on another machine and invoke its methods. DCOM is language and platform independent.
Usage	DCOM is used to create networked applications built from components. Siemens' ProfiNet is also based on DCOM.

Security	• Because RPC (fully implemented in DCOM) has serveral design flaws it is possible to get full system access. • DCOM over non secure (e.g. https) tcp connection can be sniffed
Worst Case	Full system access if RPC is not patched.
Measures for security	• Use DCOM/RPC in closed areas • Block ports 135 from non trusted networks • Update RPC from Microsoft

9.19 LDAP

LDAP (Lightweight Directory Access Protocol) is used to access directories in portable form. Specified in RFC 2251-2256. The actual directory may store any form of information, most commonly user accounts. Vendors tend to store User information in databases and grant access over LDAP. Used for example by iPlanet Directory Server, Microsoft ADS, Novell NDS.

Name	LDAP
Description	Lightweight Directory Access Protocol
Port-Nr	389 LDAP 636 LDAPS / LDAP over SSL
Security Rating	5 (1=insecure ... 5=secure)
Classification	5 (1=do not use ... 5=advisable)
Recommendation	LDAP itself is not encrypted, so it may only be used in a private environment (e. g. VPN). Use of LDAPS is advised. The LDAP server needs to be protected by any means.
Function	Control access, authorization
Usage	Access to any object directory, most often user directorys.

Security	LDAP is secure and state of the art in protected environment
Worst Case	Server may be hacked. LDAP may be eavesdroped or modified in transit. LDAPS contains the risk of man in the middle attack
Measures for security	Server needs to be kept secure. LDAP should be used only in private networks

9.20 Kerberos

Kerberos is a generic authentication protocol.

Specification mainly in RFC 1510 and 1964.

Name	Kerberos
Description	authentication protocol
Port-Nr	UDP 88 for authentication TCP 4444, 749, 464 (setup dependant)
Security Rating	5 (1=insecure ... 5=secure)
Classification	5 (1=do not use ... 5=advisable)
Recommendation	The Kerberos server needs to be protected
Function	Authorizes users, applications, servers
Usage	Inside different applications / Operation Systems

Security	The Kerberos protocol itself is widely considered to be safe. There have been flaws in the implementation for different products. The Server needs to be protected.
Worst Case	Server may be hacked
Measures for security	Server needs to be kept secure

9.21 IPSEC

Encryption and Authentication Protocol

Name	IPsec
Description	IP Security Protocol
Port-Nr	UDP 500 Protocol 50 ESP Encryption Security Payload Protocol 51 AH Authentication Header
Security Rating	5 (1=insecure ... 5=secure)
Classification	5 (1=do not use ... 5=advisable)
Recommendation	Remote Access VPN and Site-to-Site VPN
Function	IPsec is a Layer 3 tunneling protocol Key management Protocol IKE Encryption protocol DES, 3DES, ADES Authentication Protocols SHA, MD-5 User authentication
Usage	Remote Access VPN and Site-to-Site VPN

Security	Authentication and encryption are using different protocols with open combinations. Open in order to use future protocols. Strong encryption. Scalability by using X.509 certificate authentication
Worst-Case	Theoretical weakness of SHA-1 as Hash Function or DES encryption
Measures for security	MD-5 as Hash Function 3DES Encryption X.509 Certification Authentication

9.22 PPTP

Tunneling Protocol for secure connections over insecure media.

Name	PPTP
Description	Point-to-Point Tunneling Protocol
Port-Nr	tcp 1723 Protocol 47 GRE Generic Routing Encapsulation Protocol
Security Rating	3 (1=insecure ... 5=secure)
Classification	3 (1=do not use ... 5=advisable)
Recommendation	Remote Access VPN and small Site-to-Site VPN
Function	PPTP is a layer 2 Tunneling Protocol Encryption Protocols MPPE Authentication Protocols PAP, CHAP UserAuthentication
Usage	

Security	CHAP Authentication MPPE with 128 bit key
Worst-Case	compromission of key management and Trojan Horses, Man in the middle Attacks
Measures for security	

9.23 L2TP / IPsec

Tunneling Protocol using IPsec

Name	L2TP / IPsec
Description	Layer 2 Tunneling Protocol using Ipsec
Port-Nr	udp 1701 Protocol 50 ESP Encryption Security Payload
Security Rating	5 (1=insecure ... 5=secure)
Classification	4 (1=do not use ... 5=advisable)
Recommendation	specially tunneling non IP Protocols
Function	L2TP is a layer 2 Tunneling Protocol Encryption Algorithm DES, 3DES PPP Authetication Algorithm PAP, CHAP User Authentication End Device Authentication
Usage	Remote Access VPN and small Site-to-Site VPN

Security	CHAP Authentication 3DES Encryption
Worst-Case	Theoretic Weakness of DES Encryption
Measures for security	

9.24 SOAP

Name	**SOAP**
Description	**S**imple **O**bject **A**ccess **P**rotocol SOAP is an XML syntax to exchange messages. It defines a set of rules for structuring messages that can performing remote procedure call’s RPC. It is not tied to any particular transport protocol, but HTTP is popular. It is not tied to any particular operating system or programming language, so the clients and servers can be running on any platform and written in any language as long as they can formulate and understand SOAP messages.
Port-Nr	protocol using HTTP, HTTPS, SMTP
Security Rating	depends on used transfer protocol
Classification	3 (1=do not use ... 5=advisable)
Recommendation	use point to point connection, do not use proxies.
Function	A SOAP server listens for requests. The requests containing the service name and any required parameters. The listener decodes the incoming SOAP request and transforms it into an invocation of the method. It then takes the result of the method call, encodes it into a SOAP message (response) and sends it back to the requester.
Usage	developing of distributed applications that exploit functionality published as services over an intranet or the internet. Useful to integrate devices, machines or plants into the company workflow.

Security	The SOAP standard does not define any security mechanism, but instead relies on application developers building appropriate security into their software. A number of web service security standards addressing confidentiality, integrity, and access control are under development or have already been released [MaNa03] The ability of SOAP to penetrate firewalls is perhaps its most controversial feature.
Worst-Case	opens a backdoor.
Measures for security	HTTPS allows data privacy for point to point between service requestor and service provider. Use encryption.

9.25 Remote control software

Name	Remote control software
Description	remote control software allows to view and interact with one computer (the "server") using a program (the "client") on another computer anywhere. cross platform solutions: - http://www.realvnc.com/what.html - http://www.tridiavnc.com/ - http://www.tightvnc.com/ - etc. solutions for windows based systems: - http://www.symantec.com/pcanywhere/ - http://www.radmin.com/products/default.html - http://www.dameware.com/ - http://www.deltasoft.hr/remote/ - http://www.s-inn.de/RemotelyAnywhere/ - etc.
Port-Nr	custom, depending on the used products
Security Rating	2 (1=insecure ... 5=secure)
Classification	2 ... 4 (1=do not use ... 5=advisable)
Recommendation	helpful tools to enlarge availability
Function	make it easy for helpdesk personnel to resolve server and workstation problems.
Usage	support and troubleshooting.

Security	access to the desktop generally allows access to your whole environment, so security is obviously important.
Worst-Case	unwanted access from intruders
Measures for security	add support for SSL or some other encryption scheme or tunnel it through something like SSH or Zebedee. Some tools (e.g. PcAnyWhere) have decent security functions, but are easily misconfigured so that these are not actually used.

9.26 NDDS

Service for development of distributed, real-time applications over network.

Name	**NDDS** (Network Data Delivery Service)
Description	Network-middleware that simplifies the development of distributed, real-time applications distributed by RTI (Real-Time Innovations; www.rti.com)
Port-Nr	Default : UDP-port 7400
Security Rating	(1=insecure ... 5=secure)
Classification	(1=do not use ... 5=advisable)
Recommendation	
Function	- using the operating system's standard IP stack - automatically manages communications channels - clients and servers can be started in any order - platform independent available on VxWorks, Windows, Solaris, and Linux.
Usage	One feature is the elimination of “real” network programming **-** Applications simply publish what they know and subscribe to what they need. NDDS takes care of all of the message addressing, data conversion, and delivery chores. All communications is anonymous; publishers don't need to know which nodes are subscribing to the data; subscribers don't need to know which nodes are publishing the data.

Security	
Worst Case	
Measures for security	

9.27 MAP/MMS

Several protocols for usage in factory-environment.

Name	**MAP** (Manufacturing Automation Protocol)
Description	Manufacturing Protocol
Port-Nr	
Security Rating	(1=insecure ... 5=secure)
Classification	(1=do not use ... 5=advisable)
Recommendation	
Function	- token-passing LAN similar to IEEE 802.4 - Transport-layer (OSI-4) protocol - on Application-layer *Manufacturing Message Specification* (MMS) is used, an object oriented interface (ISO 9506)
Usage	used for e.g. controlling automotive plants

Security	
Worst Case	
Measures for security	

9.28 RADIUS

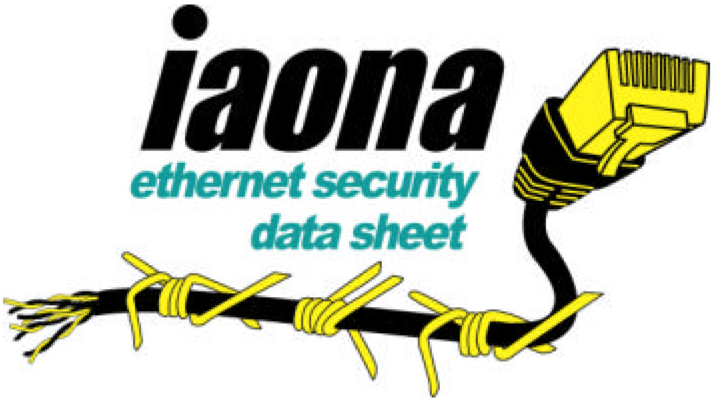
RADIUS provides authentication for remote users

Name	RADIUS
Description	RADIUS (Remote Authentication Dial-In User Service) is based on RFC 2865 and RFC 2866. NAS or other devices use RADIUS to talk to a server for authentication of incoming users. Since all communication protocol is behind a firewall, RADIUS is rated high.
Port-Nr	UDP ports 1812, 1813, earlier versions used UDP ports 1645 and 1646.
Security Rating	5 (1=insecure ... 5=secure)
Classification	5 (1=do not use ... 5=advisable)
Recommendation	protect RADIUS server holding accounting information
Function	control authentication, authorization and accounting
Usage	administration for remote access connections

Security	is secure state-of-the-art
Worst-Case	RADIUS server database may be hacked
Measures for security	protect server and keep behind firewall

10 Annex: IAONA SDS Logo

The IAONA Security Data Sheet Logo:



The logo can be found for download in the members area of IAONA.

11 References

[Bis03] Bishop, M.: Computer Security – Art and Science. Boston: Pearson Education Inc., 2003.

[Bre01] Brenton, C.: Active Defense: A Comprehensive Guide to Network Security. Berkeley, CA, USA: Sybex International, 2001.

[IAONA03] IAONA JTWG "Wiring Infrastructure": IAONA Industrial Ethernet Planning and Installation Guide. IAONA, Magdeburg 2003

www.iaona.org

[IndI06] IAONA Handbook Industrial Ethernet: IAONA, Magdeburg 2003

www.iaona.org

[Le03] Lessig, A.G.:Linux Firewalls. O'Reilly, 2003.

[Mai03] Maiwald, E.: Fundamentals of Network Security. Emeryville, CA, USA: McGraw-Hill/Osborne Media, 2003.

[MaNa04] Naedele, M.: IT Security for Automation Systems, in: R. Zurawski [Ed.]: Industrial Information Technology Handbook, CRC Press, 2004

[MaNa03] Naedele, M.: Standards for XML and Web Services Security, in: IEEE Computer, 4/2003

[MaNa03b] Naedele, M.: IT Security for Automation Systems. In: ATP-Automatisierungstechnische Praxis 5/2003, Oldenbourg Industrieverlag, 2003

[Schn04] Schneier, B: Secrets & Lies. John Wiley & Sons, 2004.

[Stev94] Stevens, W.R.: TCP/IP Illustrated, Volume 1; Addison-Wesley Publishing Company, 1994.

[THMC03] von Hoff, T., Crevatin, M.: HTTP Digest Authentication in Embedded Automation Systems. 9th IEEE Int. Conf. on Emerging Technologies and Factory Automation, ETFA 2003, Lissabon, Portugal, Sept. 2003