The IAONA Handbook
for Network Security

Draft / RFC 0.4

The IAONA Handbook for Network Security

DRAFT ! Version v0.4

Published by IAONA e.V.

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)
Fraunhofer IITB	Heike Schwingel Horner
ABB	Martin Naedele
Data Systems	Detlef Kilian
Fraunhofer CCNAT	Mr. Wagner
Innominate AG	Mr. Zilliger, Mr. Schmidt
iniNet AG VPI	Mr. Brügger
Hirschmann Electronics	Klaus Reister, Sven Fischer
KUKA Schweißanlagen	Mr. Beck
Pepperl + Fuchs	R. Rössling
Schneider Electric	Boris Süssmann
Trumpf Laser	Rainer Thieringer
University Bremen TZI	Jörg Ott
University Magdeburg	Mr. Tangermann
WAGO Kontakttechnik	Christoph Möller

Contents

1 General

1.1 Scope

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

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

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 - a down time of a few minutes can cost some thousands of Euros because it may take some hours to restart a complete production line - where a short breakdown in the office environment is equally disturbing, but the consequences are different.

1.2 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 guide, Security is used in the sense of "IT Security" and is concerned mainly with securing the hosts and network of the automation system. 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 these security objectives:

- **Data Integrity**
- **Authentication**
- Authorization (access control)
- Confidentiality
- **Availability**
- Auditability
- **Non-repudation**
- Third-party protection

The following paragraphs [MaNa04] give a detailed description of these items.

1.2.1 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.

1.2.2 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, that is, equipment or people may be harmed.

→ A user can be sure that his data was not modified, is complete and in order.

1.2.3 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 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.

→ The network and connected systems shall be able to transport data and respond to any requests within an expected time.

1.2.4 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.

→ What kind of access is allowed to a specific service or device ?

1.2.5 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 used for access control.

$\rightarrow$ Who is allowed to access a specific service or device ?

1.2.6 Non-repudiability

The non-repudiability 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.

$\rightarrow$ This covers that e.g. information from log files is true and cannot be denied.

1.2.7 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 the fact, 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.

$\rightarrow$ This covers that e.g. information from log files is complete and can be tracked.

1.2.8 Third party protection

The third party protection objective refers to averting damage done to third parties directly via the IT system, that is, damage that does not involve safety hazards of the controlled plant. The risk to third parties through possible safety-relevant failures of the plant arising out of attacks against the plant automation system is covered by other security objectives, most notably the authorization/access control objective. However, there is a different kind of damage only involving IT systems: The 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.

$\rightarrow$ A failure of a single device or service shall cause no harm to others.

1.3 Communication relations in an enterprise network

Before you can protect your network it is important to realize what communication relations exists in a company and which relations have to be protected. Therefore this section analyses a typical company network and explains the communication within.

The common architecture of larger company networks consists of different Intranets that communicate over the Internet as can be seen in Figure 1.1. 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.

The office network consists mostly of common PC technology equipped with Ethernet network interfaces used to fulfill common management tasks. The most common applications within this area are office applications of the ERP level.

The factory network represents the different production facilities within a branch and connects the different production units and production buildings. The data is produced by the Manufacturing Execution System (MES) or is used for controlling the devices within the factory network (protocols like EtherNet/IP).
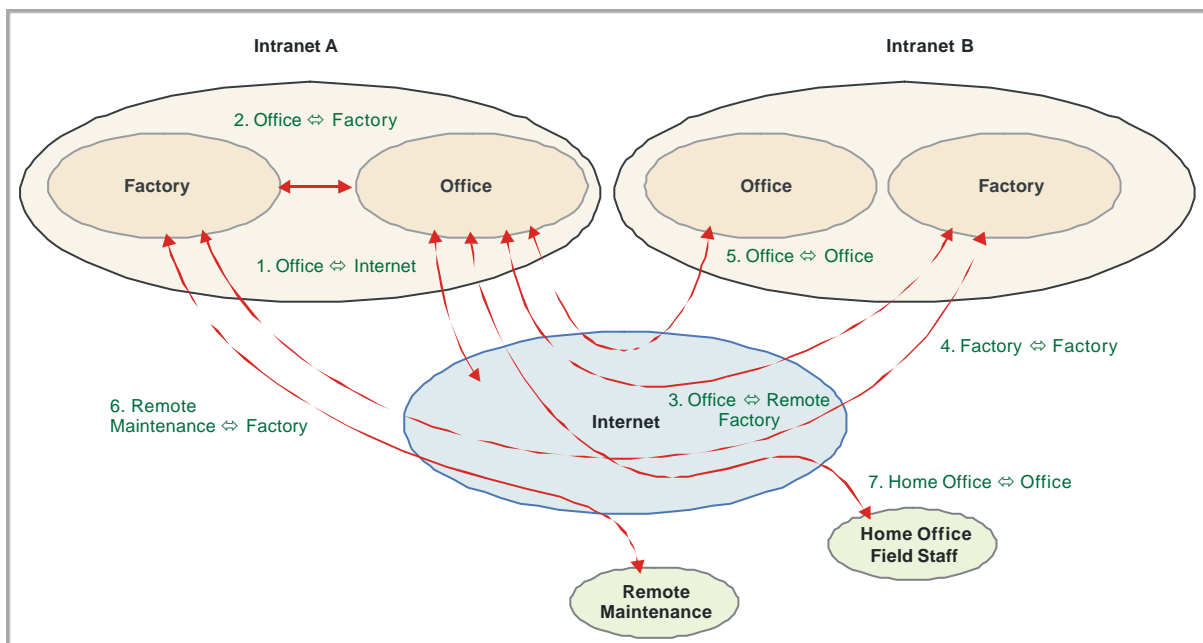
Figure 1.1: Communication relations of a company network

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, 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 further:

1. **Office ←→ Internet**
   The office PCs communicate with the Internet to access information resources that are located in this network e.g. accessing web servers (HTTP) or download files (FTP). These connections are non time critical.

2. **Office ←→ Factory**
   ERP (Office) and MES (Factory) communicate with each other for coordinating manufacturing processes. These connections are non time critical.

3. **Office ←→ Remote Factory**
   ERP (Office) and MES (Remote Factory) communicate with each other for coordinating manufacturing processes. These connections are non time critical.

4. **Factory ←→ Factory**
   To coordinate production processes between different production facilities, the MES of the facilities must communicate with each other. These connections are non time critical.

5. **Office ←→ Office**
   Office application must share data between the branches for example sharing documents or coordinating management processes.

6. **Home Office/Field Staff ←→ Office**
   Home Office workers and field staff members must access and share their data within the office network. This connections are non time critital.

7. **Remote Maintenance ←→ Factory**
   For remote maintenance manufacturers must access devices within the factory network.

1.4 Requirements of a factory level network

Though an standard for wiring office network is well established currently there exists no 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.
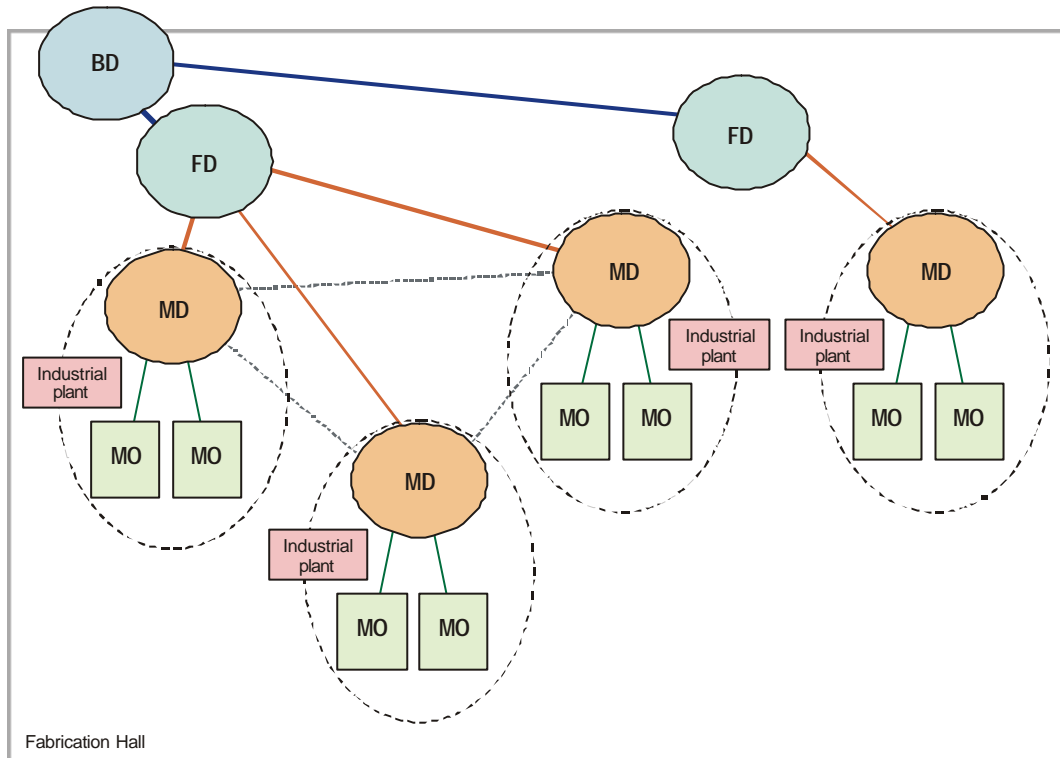
Figure 1.1: Fabrication hall with ring topology

The work resulted in the "IAONA Industrial Ethernet Planning and Installation Guide" which will be the base for the following description of the architecture and the special requirements of a factory level network.

As can be seen 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.

A factory hall is connected to the campus distributor via the building distributor (BD) which provides access to the company network to the floor distributors (FD). The machine units itself are connected via the machine outlets (MO) to the machine distributors. To provide fail save connectivity a ring topology is established which can bypass single failures of network connections.

Every distributor can be considered as an own subnetwork 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 subnetwork is used for control purposes of the machine units hard real-time requirements must be meet to guarantee secure operations. On the other hand it may be necessary to transmit data between different MD subnetworks e.g. in the case of work piece handover.

This results in three requirements:

1. 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.

2. The network traffic from outer networks must be restricted either to special persons or to special network nodes.

3. 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.

2 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 on 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.

2.1 Terminal Server
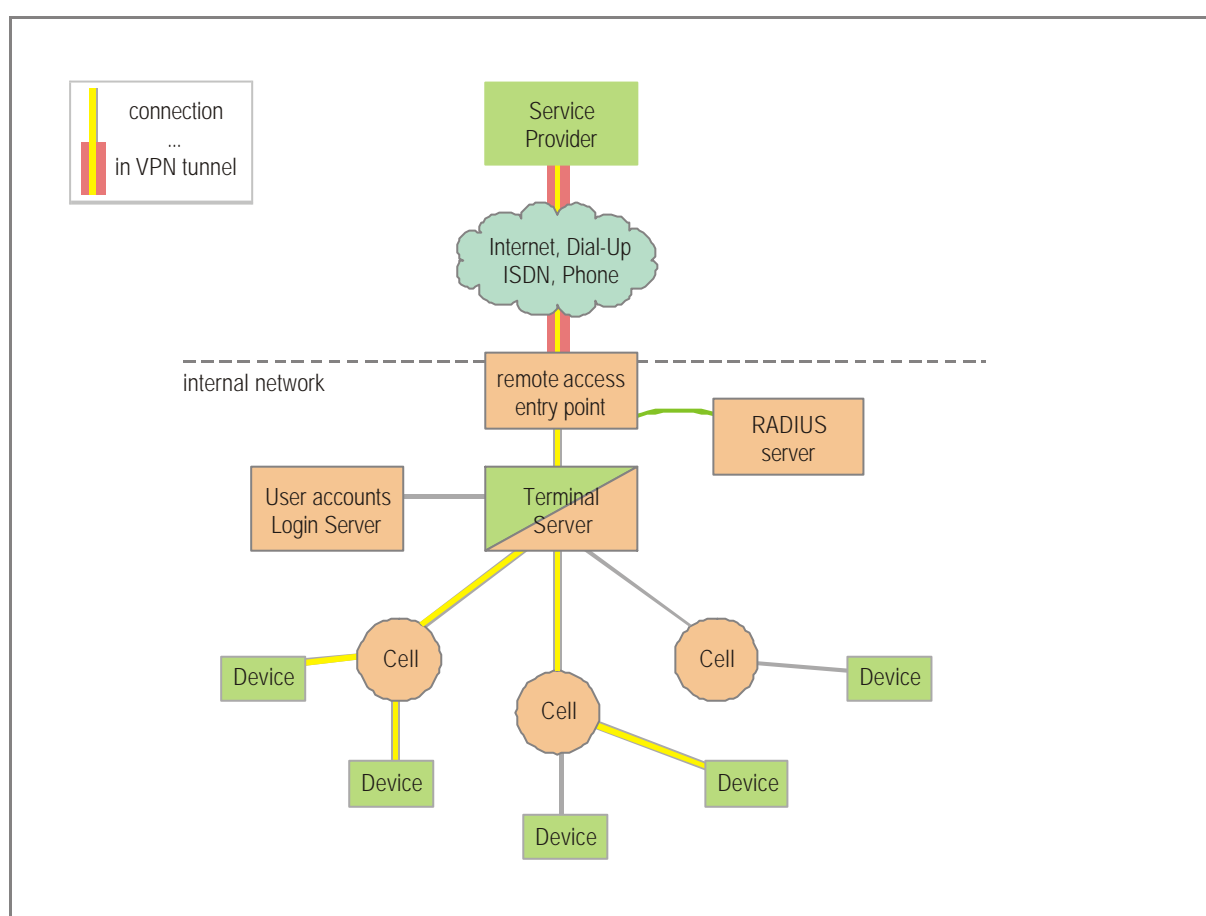
Case 1 : Security Gate as Terminal Server

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

2.2 Network Manager
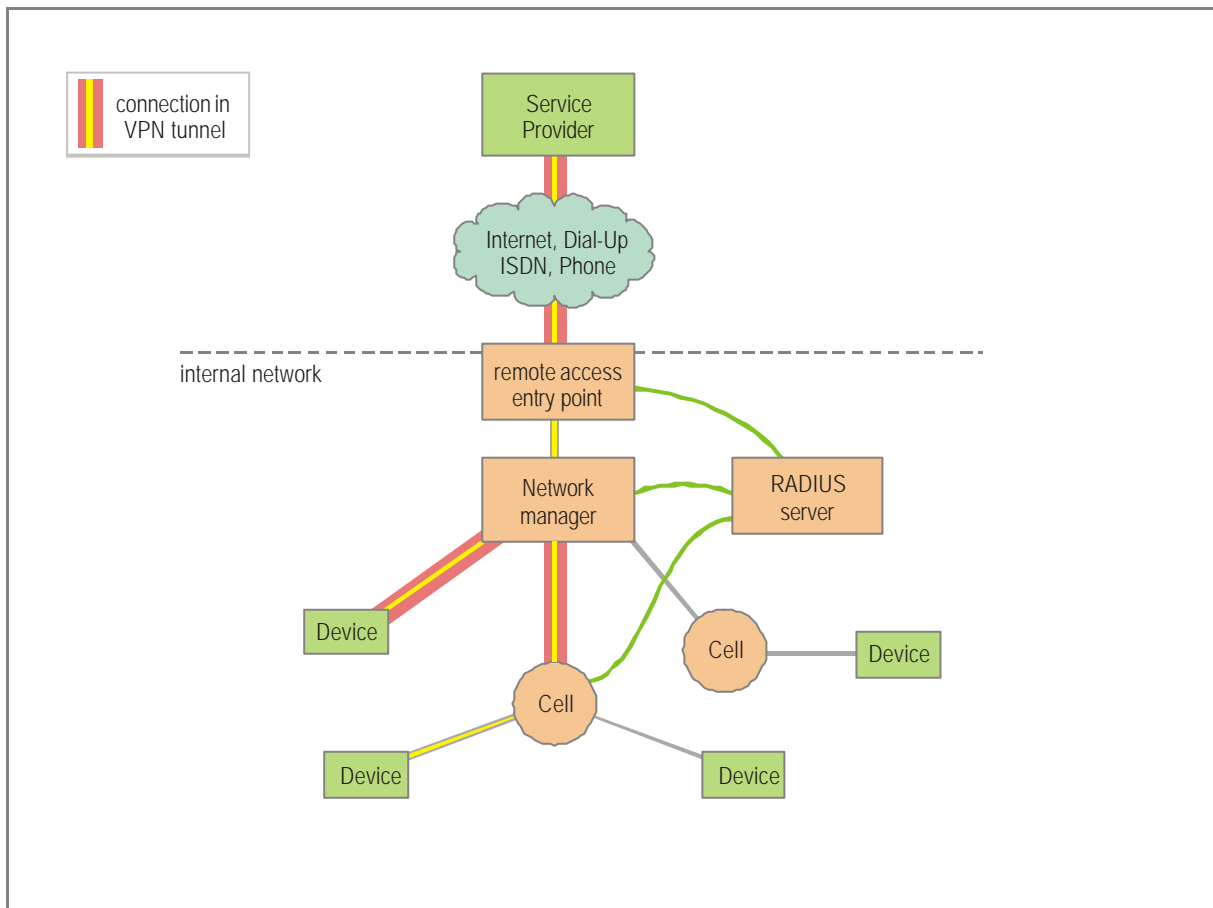
Case 2: Security Gate as Network Manager

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

- any physical access to the switch and its ports is not possible, a dedicated service network port is somewhere in each production cell.

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

3 Trusted Relations

While network structures are growing, there is also a growing number of manufacturers of devices, software and infrastructure products with the need to communicate. Advertising, selling and using these products is different from the IT world, where IT professionals are the persons to get in contact with each others – and they usually have excellent knowledge of security issues.

In contrast, in the automation industry, structures are quite different:

- Most device manufacturers are well-established with their fieldbus-based products and just changed the interface to ethernet and some protocol. Developers and Salesmen are often not aware of security issues in their products.

- Some other companies are coming from the IT world, moving their products into the automation industry. The pressure for fast market success may lead to compromises for security features.

- And least the customers and end users are confronted with a new line of problems, usually not right away, but after some time, after the first virus attack or a similar event. Unfortunately the most users have not enough knowledge about security and it is hardly possible to see what is inside ethernet based products.

Project managers, developers and salesmen need to speak a common language and have knowledge about security features. We call this a negotiation process, where both parties discuss their needs for security and how they can be solved.

These are recommendations for Device and Software Manufacturers and customers.

- use common services (=ports) whenever possible, e.g. try to avoid HTTP over custom ports or data tunneling, because this becomes hard to control for administrators.

- the user shall define his desired security level – for a device, network or application etc.

- deliver a "security note" for each device, that explains
  – which network ports are absolutely needed for productions purposes
  – which network ports are needed for service and maintenance
  – which network ports are optional

- rules for service and maintenance
  – who is allowed to access which devices
  – define access levels (installation, configuration) see VDI/VDE guideline 2187
  – direction of data flow (upload, download)
  – what needs to be done if a device is replaced (check policies, security-keys etc)

- establish administrative rules for both sides
  – explain how virus protection and detection works for your party
  – what needs to be done, when an employee is laid off ?
  – what needs to be done, when a laptop gets lost ? etc...

3.1 Definition of Security Terms

To ease the rating of security properties, this scheme addresses the levels of security for certain areas: the network itself, for devices, software services and applications – and user safety.

A customer can use this classification to define his needs – a manufacturer can describe his products and is able to consult his customers in a better way – this definition of security terms is supposed to help people to speak the same language.

3.1.1 Data Integrity

Keep data consistent, recognize change of data, concerns storage and transmission of data

* **none** *no or weak security mechanisms – e.g. temporary log files*
* **low-medium** *simple mechanisms are sufficient (checksum mechanisms), some failures are acceptable, failures can be compensated (buffered production), e.g. lost data packets are repeated but performance may drop*
* **high** *rare failures are acceptable, production loss will occur, data may be signed*
* **very high** *failures are not acceptable, severe damages (production loss and financial), data is signed.*

3.1.2 Availability

Access to devices and services, deliver data when needed, ensure delivery/response time

* **none** *doesn't matter if the device or service available*
* **low-medium** *backup for static data, restore may take some time, breakdowns are acceptable, no direct influence on production process (use buffers)*
* **high** *production is affected, manual recovery is possible within short time*
* **very high** *massive production loss may occur, automatic redundant systems (networks, devices)*

3.1.3 Confidentiality

Protect data against unauthorized access

* **none** *public available data, not protected at all*
* **low-medium** *basic mechanisms, data for internal use only, violation of this rule is acceptable and will not cause damages*
* **high** *confidential data, data channel is secured, must not accessed by unauthorized users, active protection measures, data loss will cause severe problems*
* **very high** *encrypted data (the data itself is secured), data loss will cause massive damages to the company.*

3.2 Definition of Categories

Risks and events caused by a device or service can be grouped in certain categories, which are

- **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 informations

- **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

3.2.1 Classification to Categories

The following paragraphs are explaining what behaviour may be acceptable for a certain category, depending on the desired security level. The details in these sections, especially downtimes, are only suggestions and may be discussed individually.

Security Level "**none**"	
affects production	- any effect on production / breakdown is possible - stop and restart time doesn't matter
user safety	no effects
affects privacy	no personal data present, all data is public
affects company	neutral
financial loss	not relevant
violation of contracts/laws	not applicable

Security Level "**low-medium**"	
affects production	- local, partial breakdowns are acceptable - downtime does not exceed 6 hours - loss may be compensated thru manual workers, buffering products, repeating of transmission etc.
user safety	any effect is not likely
affects privacy	personal data is present, access through other persons is possible and may be accepted, no loss of social state
affects company	only internal
financial loss	within budget / calculation
violation of contracts/laws	violation causes very limited damages

Security Level "**high**"	
affects production	• breakdown of a single system is acceptable • downtime does not exceed 30 min • loss may be compensated thru manual workers, buffering products, repeating of transmission etc.
user safety	• a failure may cause other systems to enter the safe state
affects privacy	• personal data may be accessed through other persons • it is still possible to track who and what was accessed
affects company	• a larger number of people is to know about the failure
financial loss	• exceeds budget / calculation
violation of contracts/laws	• may result in fines for breaking contracts

Security Level "**very-high**"	
affects production	• no breakdowns are acceptable • downtimes are not acceptable • loss cannot be compensated
user safety	• failures are likely to effect safety systems
affects privacy	• personal data gets lost, tracking not possible • loss of social state
affects company	• information about the failure is public
financial loss	• severe financial damages • threatens the company
violation of contracts/laws	• severe violations, may cause legal suits

3.2.2 Example

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

3.3 Template for Security Datasheet

Name of item _____

Description of item
- O   a device (any device, active and passive devices, switches)
- O   a production cell
- O   a network (infrastructure)
- O   _____

Device features

- O   Brief device description _____

- O   Operating System _____

- O   backup, replacement features / procedures
  _____

- O   firmware update possible

- O   external interfaces (FDD, keyboard, mouse, CD-ROM, USB etc)
  _____

- O   network interfaces (RAS, built-in Modem, Network Gateways)
  _____

- O   behaviour on power loss / network communication loss
  _____

Network features
- O   needs / provides DHCP
- O   manageable / SNMP
- O   MAC-address based authentication
- O   _____

Implemented Security features
- O   firewall, not configurable
- O   firewall, configurable
- O   virus protection
- O   data encryption
- O   intrusion detection
- O   robustness, stack overflow protection
- O   redundancy possible
- O   secure remote maintenance
- O   access control, user levels
- O   local user access possible
- O   supports user authentication, manageable
- O   _____

Service and Maintenance
- O   logging
- O   ready for remote maintenance
- O   requires local configuration
- O   requires remote configuration

Please describe used network ports and services

Security Rating	Name	needed for operation	service and maintenance	only optional
1	Modbus-TCP	exchange process data	---	---
1	FTP	---	Firmware Update	---
2	SMTP	---	---	used for error notifications
3	SNMP	send traps in case of warning or errors	---	---
3	DynDNS	may be used for to register URL for Web Access	---	---
4	SSH	---	diagnostic and setup	---
5	HTTPS	---	Web diagnostic, service and setup	---
.....				

4 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	unsecure mechanisms, no protection at all, information can be read with packet-analyzers
2	a minimum of security is provided, eg. 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, eg. 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 unsecure
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
FTP	(20) 21	File Transfer Protocol
FTPS		dto. secure
HTTP	80	Hypertext Transfer Protocol
HTTPS	443	dto.secure
SNMP	161, 162	Simple Network Management Protocol
DNS	53	Domain Name Service
DHCP	67, 68	Dynamic Host Configuration Protocol
SSH	22	Secure Shell
iPSEC	500	IP Security Protocol
SMTP	25	Simple Mail Transfer Protocol
TELNET	23	Terminal Emulation
TFTP	69	Trivial File Transfer Protocol
SOAP	80, 443, 25	Simple Object Access Protocol
RPC	135 + more	Remote Procedure Call
DCOM	135 + more	Distributed Component Object Model
DynDNS	110	use POP3 for dynamic DNS
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		Lightweight Directory Access Protocol
RADIUS	1812, 1813	Remote Authentication Dial-In User Service
PPTP	1723	Tunneling Protocols
L2TP	1701	Layer 2 Tunneling Protocol
Kerberos		network authentication
MODBUS	502	Modbus over TCP
Ethernet/IP	44818, 2222	Rockwell's Procotols
NDDS	7400	Real-Time middleware
PROFINet	135 + more	Siemens' Ethernet Procotol
MAP/MMS	*(?)*	Manufacturing Automation Protocols
Powerlink	*(?)*	EPSG Ethernet Protocol
EtherCAT	*(?)*	Beckhoff Ethernet Protocol
Safe Ethernet	*(?)*	HIMA Safety Ethernet Protocol
Custom-Ports	*(individually)*	*must be individually rated*
SQL-Server	*(individually)*	*(---)*
"SAP"-Services	*(?)*	*not sufficient data available*
Remote Access Services	*(individually)*	VNC, pcAnywhere, PC-Duo
File "Browser"	137-139, 445	NetBios over TCP

4.1 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=unsecure ... 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	block ICMP with a firewall (if possible)

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.

4.2 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=unsecure ... 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 Ethernetaddress – IP address Example: arpwatch (Linux)

4.3 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=unsecure ... 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

4.4 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=unsecure ... 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

4.5 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=unsecure ... 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

4.6 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=unsecure ... 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.

4.7 Telnet

Probably the most known service for interactive sessions.

Name	TELNET
Description	remote login protocol
Port number	23
Security Rating	1 (1=unsecure ... 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

4.8 SMTP

The most used mail transfer protocol.

Name	SMTP
Description	Simple Mail Transfer Protocol
Port number	25
Security Rating	1 (1=unsecure ... 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

4.9 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

4.10 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=unsecure ... 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

4.11 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])

TODO: differentiate between HTTP and HTTPS

4.12 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=unsecure ... 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.

4.13 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	2 (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.

4.14 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	2 (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.

4.15 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=unsecure ... 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 •

4.16 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=unsecure ... 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

4.17 PPTP

Tunneling Protocol for secure connections over unsecure media.

Name	PPTP
Description	Point-to-Point Tunneling Protocol
Port-Nr	tcp 1723 Protocol 47 GRE Generic Routing Encapsulation Protocol
Security Rating	3 (1=unsecure ... 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	

TODO: Usage and Measures

4.18 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=unsecure ... 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	

4.19 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.

4.20 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=unsecure ... 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.

4.21 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=unsecure ... 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	

4.22 MAP/MMS

Several protocols for usage in factory-environment.

Name	MAP (Manufacturing Automation Protocol)
Description	Manufacturing Protocol
Port-Nr	
Security Rating	(1=unsecure ... 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	

4.23 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=unsecure ... 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

5 IAONA Security Survey

This is an attempt to find out what kind of networking devices, infrastructures and services are existing today in the production environment.

Target Persons
Customers, Users - Line Builders, Machine Builders - Service Providers

We assume you are using an Ethernet network for your 'office world' and you are also networking your production units and devices. Please help us to find better solutions for your factory network and enhanced security.

Infrastructure

Is your 'production network' separated from your 'office network' ? (no link at all)	Yes	No

If 'No', what devices are coupling the networks	O	router
	O	firewall
	O	other _____

Are you using any hard- or software to restrict traffic between factory and office network ?	O	no
	O	planned for future
	O	yes _____

What kind of mechanisms will control your data flow between factory and office network ?	O	router, packet filter
	O	dedicated firewall
	O	other _____

What are your infrastructure components ?	O	Hubs
	O	Switches
	O	Routers

Do you have Internet access from within your production network ?	Yes	No

What are the devices in your production network ?	O	PCs	_____ %
	O	Sensors, Actuators	_____ %
	O	HMI	_____ %
	O	PLCs	_____ %
	O	Field IOs	_____ %
	O	Industrial Controls	_____ %
	O	Machines	_____ %

What operating systems are you using in your network ?	O	DOS	_____ %
	O	Linux	_____ %
	O	Win 3.11	_____ %
	O	Win 95/98/ME	_____ %
	O	Win NT	_____ %
	O	Win 2000	_____ %
	O	Win XP	_____ %
	O	OS/2	_____ %

O	VxWorks	_____	%
O	Win CE	_____	%
O	embed. Linux	_____	%
O	other _____		%

Communication

Do you require traffic between your office network and your production network ?

Yes   No

If 'Yes', which services are required

O   production planning data
O   CAD data
O   logfiles and statistics
O   other _____

Remote Access

Do you have a single remote access point or multiple (eg. modems)

Single   Multiple

How is your remote access used ?

O   only internal users
O   rarely, only few external access
O   service and support
O   intense use (service,maintenance)

Are you using a firewall for RAS users

Yes   No

Which kind of encryption are you using ?

O   none
O   SSL
O   SSH1
O   SSH2
O   IPSec (VPN)

What kind of authentication do you use ?

O   none
O   User / Password
O   RSA Token, Secure-IDs
O   Certificates (X.509)
O   other _____

Are you using any remote software

Yes   No

Which Software are you using

O   Pc-Anywhere
O   VNC
O   PC-Duo
O   Telnet
O   SSH
O   other _____

How often do you need or provide remote services ?

O   _____
(per day or week etc.)

Network Traffic

Are you using any fieldbus like protocol ?	O	NDDS
on your production ethernet	O	Profinet
	O	Ethernet/IP, CIP
	O	Modbus/TCP
	O	PowerLink
	O	EtherCAT
	O	other _____

Types of network communication	O	File transfer
in your production network	O	Web based Services
	O	PPS production planning systems
	O	any SAP service
	O	HMI
	O	OPC
	O	installing software updates
	O	SCADA (control software)
	O	SNMP

Which of the standard services are used	O	HTTP
in your network ?	O	SNMP
	O	Telnet
	O	SSH
	O	FTP
	O	SMTP
	O	POP3
	O	NetBios
	O	DHCP
	O	DNS
	O	other _____

Does your software uses custom ports for standard services (eg. HTTP over port 4711)	O	Yes	O	No

Can you rate the use of standard ports	O	_____ % standard ports
and custom ports ?	O	_____ % custom ports

Administration

On the RAS client side, are your customer datas (phone number, user, password etc) in any way protected or encrypted ?	Yes	No

Do you have a security policy ? That is a set of rules for certain cases (when a laptop gets lost or stolen, when an employee is laid off etc)	Yes	No

Are you using any administration tools	O	CA Computer associates
or network management systems ?	O	HP openView
	O	IBM NetView
	O	IBM Tivoli Manager
	O	other _____

6 References

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

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

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

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