VAN

FP6/2004/IST/NMP/2 - 016696 VAN

Virtual Automation Networks

Work Package 1

Requirements and Trend Screening

Task 1.1

State of the Art

Deliverable D01.1-1-V1

State of the Art and Trends in Safety, Security, Wireless Technologies and Real-time Properties

Document type	**:** Deliverable
Document version	**:** Final
Document Preparation Date	**:** 18.11.2005
Classification	**:** Public
Contract Start Date	**:** 01.09.2005
Duration	**:** 31.08.2009

Project funded by the European Community under the "Information Society Technology" Programme (2002-2006)

Rev.	Content	Resp. Partner	Date
1.0	Compilation of partner supplied files	BUT	18.11.05
1.01	Greyscale colour-matching fixed	BUT	18.11.05
1.02	Updated references	BUT/ifak	25.11.05
1.03	Updated chapter titles	BUT/Siemens	28.11.05
1.04	Updated Fig. 4-10, EPLSafety, references	BUT	9.12.05
1.05	Added conclusions into relevant chapters	BUT	24.06.06

Everybody please state revision index and short description of what has been done + partners involved and date.

Final approval	Name	Partner
Review Task Level	Petr Fiedler	BUT
Review WP Level	František Zezulka	BUT
Review Board Level	Axel Klostermeyer Peter Neumann	Siemens ifak

Executive summary

This document is the D01.1-1-V1 deliverable of the VAN project and reports the activity of the participants within WP1, T1.1, months 1 – 3.

The basic purpose of this deliverable is to show the state-of-the-art of the existing communication technologies with respect to the four main scopes of the VAN project: wireless, real-time, safety, security.

Chapter *Architecture* gives overall information on the status of communication technologies from the general point of view and further deals with particular technologies which could be incorporated into the open platform of VAN.

Chapters *Wireless Technologies*, *Real-time Technologies*, *Safety Technologies*, and *Security Technologies* cover the aforementioned main scopes. The chapters are organized in such a way that the general information on the current status of the particular scope is followed by selected technologies. These technologies are examples how to solve respective trouble spots. Sometimes they show what we should avoid.

Chapter *Previous European Projects* provides the document with results of the previous projects. These projects either tried to solve problems relevant to the VAN project or some of the results could contribute to the VAN project.

The document is complemented by abbreviation explanations in *Glossary*, the resources used in the text in *References*, and by tables including factual information enhancing the textual information of the aforementioned chapters in *Appendixes*.

This document is a result of cooperation of the parties: Aucoteam GmbH, Brno University of Technology (BUT), University of Magdeburg (CVS), Fidia S.p.A., ifak Magdeburg, Phoenix Contact, Schneider Electric, Siemens AG, and Teleport Sachsen-Anhalt GmbH (TSA).

Due to professional experiences and orientations of the participating parties, the main editorial competency of the respective chapters was given to ifak (*Architecture)*, BUT (*Wireless Technologies*), Siemens (*Real-time Technologies*), Phoenix (*Safety*), TSA (*Security*), and CVS (*Previous EU Projects*).

The document structure and compilation was performed by Brno University of Technology.

Contents

List of Figures

1 Introduction

Present automation architecture is dominated by intelligent field devices that are connected to various networks and fieldbuses. Often it is necessary to employ in one plant several different communication subsystems which meet specific requirements of various tasks found in such a plant.

At the office level of a company, many standardized technologies are used to handle the data and its exchange. To meet the growing requirements on flexibility of automation processes the whole variety of automation technologies would have to be further developed in parallel with the office solutions and they would not even be compatible after that.

By the overall aim of an easy data exchange between office and factory floor and the use of the high potential of well developed office (IST) technologies (including Internet and Web-based technologies) these office technologies conquer the factory floor. But these technologies and concepts do not reach industrial requirements and standards in areas as security, wireless, safety, and real-time.

Following these requirements an interconnection of all parts of the information system architecture (horizontal and vertical) of an enterprise has to be realized. As a result, flexible management structures handling the activities, e.g., commissioning, diagnosis, maintenance, and asset management have to be developed.

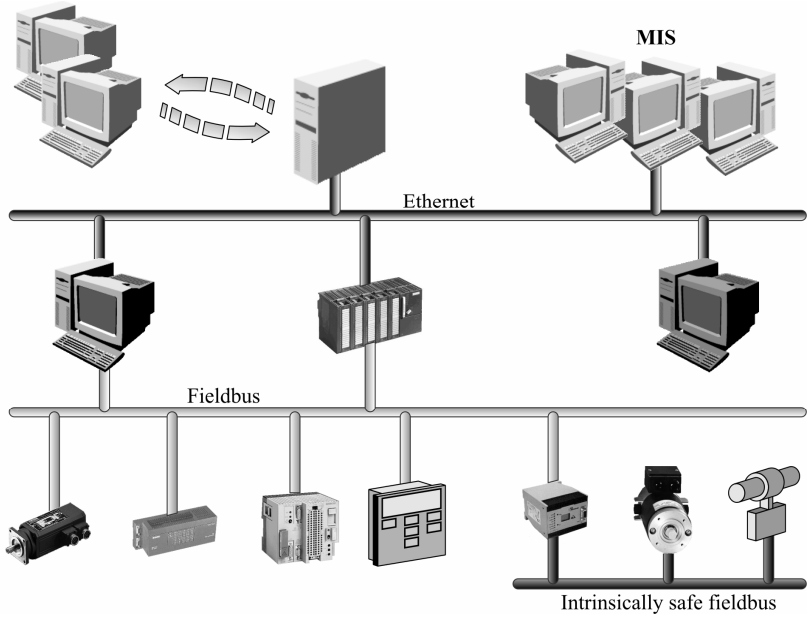

Fig. 1-1: Simplified communication architecture of a contemporary plant.

Automation tasks can be divided into two levels, the office automation and the process automation. The office automation is dominated extensively by American companies' effective solutions that can be used in heterogeneous networks. Comparable process automation solutions that would be capable of handling truly heterogeneous fieldbus systems are missing.

Today's industrial manufacturing is confronted with a high and further growing degree of fast changing, customised production. As a result flexible management structures handling the activities e.g. commissioning, diagnosis, maintenance, and asset management have to be developed. This requires a flexible and scalable company - internal data exchange and exchange with any other kind of involved remote companies. Within the process industry, the improvement of flexibility within the lifecycle of a process plant (about 25 years) is going on. Especially the engineering and asset management activities require the introduction of modern Web-based technologies to enable local and remote access to process data as well as parameters describing the features of installed devices. Following these requirements an interconnection of all parts of the information system architecture (horizontal and vertical, local and remote) of an enterprise has to be realised. The necessary research aims to provide the needed technologies to build up widely distributed, flexible, virtual automation networks.

Automation-technical practice goes through a paradigm change for some time: The steadily increasing influence of technologies and standards from the IT-world on the automatic control engineering cannot be ignored any more. Especially the engineering and asset management activities require the introduction of modern Web-based technologies to enable local and remote access to process data as well as parameters describing the features of installed devices.

In this context particularly Ethernet and the TCP/IP protocol suite are of high relevance for two economic reasons:

- It enables "vertical integration" over all levels (office level, supervisory level, field level) of an enterprise. In this way all in the network present data can be made available simply and without the need to use different communication media.
- The Ethernet (IEEE 802.3) as well as the TCP/IP protocol suite and Web-based technologies were already established as communication standards in the office environment. Therefore, there exist many "commercial of the shelf" (COTS) products and solutions that can be utilized in the field of industrial automation. Such synergy between an office solution and automation solutions causes gradual cost decrease of the final automation products. The conventional automation-only solutions are becoming uncompetitive.

The European project FP6/2004/IST/NMP/2 - 016696 VAN "Virtual Automation Network" has the goal to use heterogeneous networks for the optimal processing control as well as for the vertical integration between the office automation and the process automation. It has to address particular requirements of the process automation concerning:

- overall process control architecture,
- real-time requirements,
- specific aspects of wireless technologies,
- process safety and robustness,
- access protection (security).

As the requirements significantly differ from plant floor to office level, all the above mentioned aspects must be scaleable to meet vast range of possible control applications and automation solutions in various application areas. Moreover, the vertical integration can be extended from the on-site office-level to a remote access over the public wide area networks. A target scenario - an "Industrial System Environment" is shown in Fig. 1-2.

Data access and data exchange in automation hierarchies were so far usually accomplished over proprietary networks. Moreover, the communication infrastructure of industrial automation plants is subject to high security requirements.

At present, a change in the structure and the handling of automation systems takes place as the Internet technologies and mobile communication methods are enabling new services for automation domain. In particular, remote diagnostics, process adjustment and optimization, start-up assistance and general trouble-shooting activities can be performed over the public networks.

The remote access to the automation process over the public communications networks (Internet and portable radio, e.g. UMTS, Wireless LAN among other things) results in a reduction of the downtimes of automated plants and, thus, to substantial cost savings. Beyond that, a remote maintenance via public networks becomes compellingly necessarily when several plants should be handled by small amount of highly specialized experts.

However, at present in most cases operators demand a strict separation of the plant from public networks, so that unauthorized remote access over the Internet is not possible at all. The security solutions used over the public networks, e.g., Virtual Private Networks, do not meet all the requirements on real-time, safety and security that are needed to enable full remote access to the automation processes.

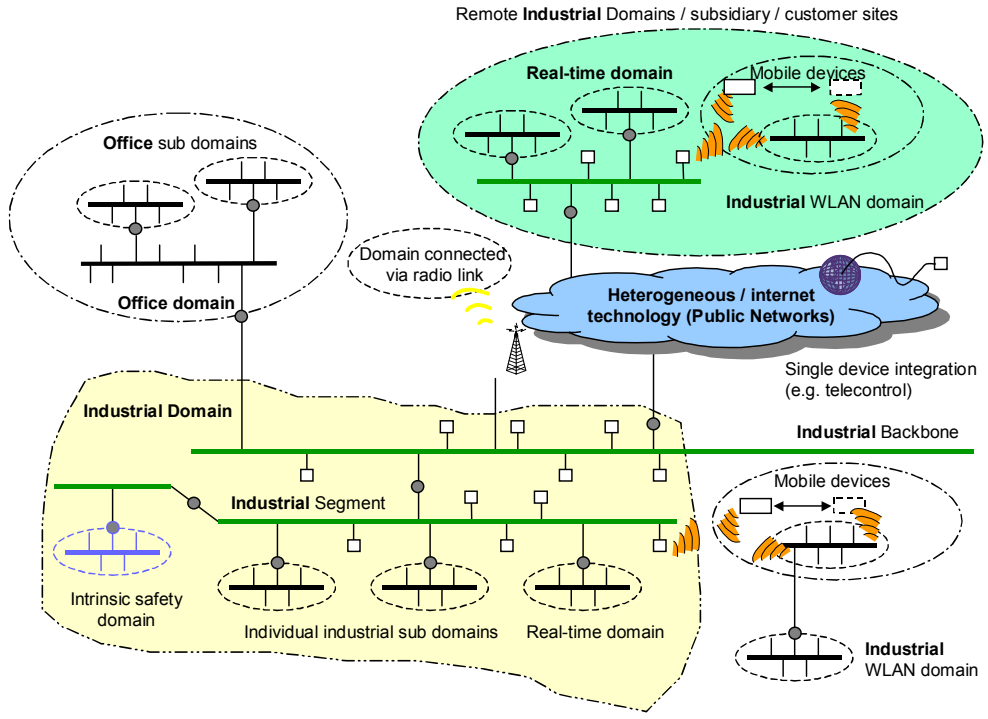

Fig. 1-2: Network consisting of local and wide area homogenous and heterogeneous networks.

Moreover, the present research and development of Internet-oriented technologies for purposes of industrial automation has led to more or less incompatible solutions. Heterogeneous networks consisting of local and wide area and wired and wireless communication systems will play an

increasing role in the future. However, there is not only a need for real- time, safe and secure communication. The desired context awareness leads to the usage of location-based communication services and context-sensitive applications.

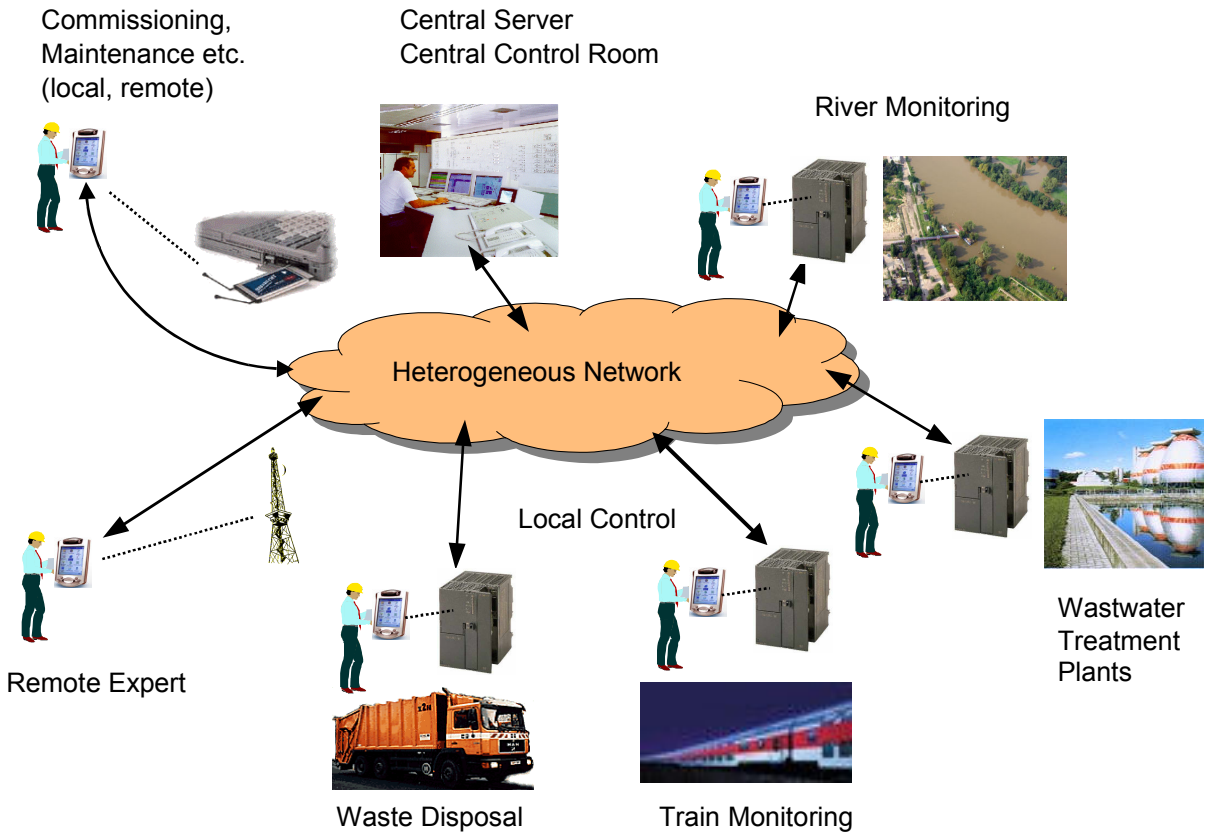

Fig. 1-3: Scenarios of distributed automation.

A Virtual Automation Network (VAN) is a heterogeneous network consisting of wired and wireless local Area Network, the Internet, and wired or/and wireless telecommunication systems. This means that geographically distributed application programmes co- operating to fulfil a control application are connected via this VAN accessed by remote connection endpoints. Worldwide distribution of Internet offers the Automation domain a good infrastructure but introduces many additional problems, which need to be solved.

The VAN project intends to provide innovative solutions, extensions and standards dedicated to industrial environments, to fill the existing gap between office technologies and industrial automation technology.

2 Architecture

2.1 Introduction

2.1.1 Motivation

For the last 20 years a lot of effort has led to the decisive usage of digital communications in distributed computer control systems within the factory as well as the process domain. The proprietary communication systems within SCADA systems were supplemented and partially displaced by the fieldbus systems and sensor bus systems. At the same time, Ethernet won the battle as the most used communication technology within the office domain resulting in low component prices caused by the mass production of these components. For the last five years and especially nowadays, there is a large community inventing the usage of Ethernet based communication systems to be used in the industrial automation domain, i.e. in the real-time and safety-critical world [ATV04, HL04, HJH02, TK04]. [Lin00, Fur03, Mar04] contain an overview regarding the real-time aspects. However, in contrary, fieldbus systems are the most important communication systems used in commercial control installations. Since these Fieldbus systems are widely used in the installed automation systems and will be used for new application projects in the industry without drastic changes, the following report does not touch these fieldbus systems. The project partners (in particularly Siemens, Schneider, Phoenix Contact, but also ifak) have deep knowledge as well as wide experience with the fieldbus technology. The actual activities within this field are the integration of the data objects of the fieldbus systems via gateways or proxies into the Ethernet-based systems. That implicates the ability to configure the field devices coupled by fieldbus systems and linked via gateways or proxies with Ethernet-based devices by a configuration and parameterization tool within the Ethernet-based system. These integration activities are going on and could be out of scope of this report. The main focus of this report lies on the communication technologies which are closed to the wired Local Area Networks and the wireless approaches which are suitable for the use in harsh environment as well as able to link the local area with the wide area. That means that not all thinkable local and wide area network technologies and not all wireless technologies have been analyzed. Instead of that, the project members selected a number of relevant legacy or ongoing systems for the analysis.

Future scenarios of distributed automation lead to desired mechanisms for geographically distributed automation functions due to various reasons:

- Centralized supervisory and control of (many) decentralized (small) technological plants,
- Remote control, commissioning, parameterization and maintenance of distributed automation systems,
- To include remote experts or external machine-readable knowledge for the plant operation and maintenance.

This means that heterogeneous networks, consisting of local and wide area as well as wired and wireless communication systems, will play an increasing role. However, there is not only a need for real-time, safe and secure communication. The desired context awareness leads to the usage of location-based communication services and context-sensitive applications. Thus, the functionalities offered by the entertainment electronics will influence more and more the complexity of the

communications approach within the automation domain. This section will mainly deal with the ongoing activities in the field of using Ethernet within factory automation.

The following problems have to be solved:

- Definition of real-time classes and guaranty of determinism,
- Behaviour of non real-time, soft real-time, and hard real-time Ethernet-based solutions,
- Functional safety concepts and mechanisms,
- Security concepts and mechanisms.

The analyzed communication approaches meet nowadays these requirements only partially.

2.1.2 Determinism in industrial communication and Real-time Classes

There are four basic media access principles used in the most common communication systems in automation [LON95]: Time Division Multiplexing (TDM), Token Bus, Token Ring and CSMA. Of these four principles the CSMA is commonly considered to be non-deterministic.

- Time Division Multiplexing - TDM protocols reserve time (time slot) for each node on the medium. Each node then transmits its data in its reserved time and the maximum amount to be transmitted is given by the size of the time slot assigned to the particular node. The maximum delay to access the media is determined by the number and size of time slots assigned to the nodes.
- Token Passing Protocols - Token bus and token ring systems circulate a 'token'. The 'token' is a message that grants the right to transmit on the medium. A node is allowed to hold the token for a restricted time. The access to the network is bounded by the maximum latency of the token to circulate the network. A weaknesses of token passing protocols is possible non-deterministic error recovery when a node is disconnected (the token-passing sequence has to be updated) or when a token is lost. Most protocols use a random (non-deterministic) method to recover tokens.

CSMA - based protocols - In the CSMA based systems a node that intends to transmit at first listens to the network. If no ongoing communication is detected then the node starts its transmission. The CSMA principle has many variants (e.g., non-persistent CSMA, p-persistent CSMA, CSMA/CD, CSMA/CR, etc.) The CSMA is fully deterministic if used as a Master-Slave system, however in such case the advantages of CSMA are lost. CSMA cannot be deterministic in peer-to-peer systems unless some deterministic algorithms are implemented above the CSMA. However, if the collision resolution algorithms are properly implemented and tuned according the intended application, the non-deterministic CSMA based protocol can be well suited for many control applications.

Real-Time Classes

Within the automation domain the real-time requirements are focused on the response time behaviour of data packets. Thus, there are three real-time classes guaranteeing response time:

- Class 1: soft real-time (scheduling of data traffic, normally on top of UDP/TCP): scalable cycle time; used in factory floor and process automation,
- Class 2: hard real-time (scheduling of data traffic, normally on top of MAC): cycle time 1…10 ms. Used for control,
- Class 3: isochronous real-time (with time/clock synchronisation and routing with time schedule): cycle time 250 μs…1 ms; jitter less than 1 μs. Used for motion control.

Additionally, there is a class “non real-time” which has not been considered here.

Within that chapter not all issues of real-time should be addressed, see chapter *Real-time Technologies*. The above defined real-time classes should be only used for the classification of

competing approaches within the maintenance phase of the fieldbus standard IEC 61158, starting in November, 2005.

2.1.3 Ethernet-based Local Real-time Approaches

2.1.3.1 A short Overview

The Local Area Networks (LAN) based on Ethernet-TCP (UDP)/IP has been standardised and widely introduced in the office domain and also in the automation domain, using Shared Ethernet as well as Switched Ethernet (star and tree topology). There are system-specific limits regarding the real-time behaviour, especially if the solutions use the TCP (UDP)/IP functionality and a middleware above TCP (UDP)/IP to schedule the (soft) real-time traffic (real-time class 1) and the non real-time traffic. [PW03] compares these approaches. There are many investigations regarding temporal behaviour related to Ethernet-TCP/IP based local networks; see, e.g., [PA05]. They include mainly the response aspect of data packet transmission, which is very important within the industrial automation domain. The synchronous video or audio stream transmission, supported by the infrastructure of LAN, is of secondary interest. In the industrial automation application, the data packet transmission with guaranteed response time has to have the highest priority.

A lot of research activities deal with a middleware on top of the MAC layer of Ethernet, scheduling the real-time and soft real-time / non real-time traffic, see, e.g., [AW03, ATV00, BLM03, CLM03, and CCL02]. [BSB00, DH03, GRD02a, GRD02b, Jas02, LL02, LH04, KSZ99, SKS02, WR04, XZY02] deal with the usage of Switched Ethernet in the automation domain (real-time class 2). [PA05] contains a rough overview of the methods and implemented systems. The investigated real-time mechanisms are very important for synchronous data transmission in the Motion Control area (real-time class 3). Examples of this category are described in later sections. Additionally, the 1394automation e.V. specified an approach based on IEEE 1394 transmission technology [Gor05], also offering a good dynamic behaviour for motion control (class 3).

Investigations have shown that at present the switched Ethernet itself is not the bottleneck of data transmission within local automation networks (for star topology as well as for line topology – line topology means: each control device assesses its own switch, and all traffic has to pass through many or all switches). The present bottleneck is the communication stack within the end devices [JN01a, JN01b, and Jas02].

The focus of this section is on local industrial communications using Ethernet-based approaches, especially the ongoing activities in the next generation of fieldbus systems based on this technology.

2.1.3.2 Local Soft Real-time Approaches

As mentioned above there are industrial approaches used in real-time automation applications. They are using shared and/ or switched Ethernet and TCP (UDP)/ IP mechanisms. They can be distinguished by different functionalities on top of TCP (UDP)/ IP as well as by their object models and application process mechanisms. The systems based on Ethernet-TCP/IP offer response time in the lower millisecond range. The systems are capable but not deterministic. The data transmission is based on the best effort principle. To use these systems within the automation domain, mechanisms are needed to monitor time limits, to use substitution values, to optimise the transmission (using records of many values within one MAC-PDU) as well as time and event-triggered data transmission. A few examples are:

MODBUS TCP/IP (Schneider). MODBUS is an application layer messaging protocol for Client/Server communication between devices connected via different types of of buses or networks. Using Ethernet as the transmission technology, the Application Layer Protocol Data Unit (A-PDU) of MODBUS (Function Code and Data) has been encapsulated into an Ethernet frame. The Connection Management on top of TCP/IP controls the access to TCP.

EtherNet/IP (Rockwell, ControlNet International, Open DeviceNet Vendor Association) uses a Common Industrial Protocol CIP [Eth01]. IP stands for Industrial Protocol (not for Internet Protocol). CIP represents a common application layer for all physical networks of EtherNet/IP, ControlNet and DeviceNet. Data packets are transmitted via CIP router between the networks. For the real-time I/O data transfer, CIP works on top of UDP/IP. For the Explicit Messaging, CIP works on top of TCP/IP. The application process is based on a Producer/ Consumer model.

High Speed Ethernet HSE (Fieldbus Foundation) [HSE01]. A Field Device Agent represents a specific Foundation Fieldbus application layer function (including Fieldbus Message Specification). Additionally, there are HSE communication profiles to support the different device categories: host device, linking device, I/O gateway, field device. These devices share the tasks of the system using distributed Function Block applications.

Interface for Distributed Automation IDA (MODBUS-IDA Group; Schneider) [IDA02]. The layer functions allow three types of communication channels: Client/Server Messaging for Engineering, data exchange for real-time traffic using real-time middleware (RTPS Wire Protocol) from RTI (Real-Time Innovations, 2002) over UDP/IPv4. The IDA concept has been used for the approach “MODBUS RTPS” [IEC65c341]. The RTPS protocol runs in a network of applications. There are two communication models for the data transfer: a Publish/Subscribe model for process data and a Composite State Transfer model for exchange of state information.

PROFINET (PNO PROFIBUS International, Siemens) [PRO03] uses for its object model CBA (Component Based Architecture) the DCOM Wire Protocol with the Remote Procedure Call mechanisms (DCE RPC) [OSFC706] to transmit the soft real-time data. An open source code and various exemplary implementations/portations for different operating systems are available on the PNO Website.

P-Net on IP (Process Data) [IEC65c360]. Based on the P-Net Fieldbus standard Type 4 [IEC61158] the Public Available Specification (PAS) contains the mechanism to use P-Net in an IP environment. Therefore, the P-Net PDUs are wrapped into UDP/IP packages, which can be routed through IP networks. Nodes on the IP network are addressed with two P-Net route elements. P-Net Clients (Master) can access Servers on an IP network without knowing anything about IP addresses.

All the mentioned approaches are able to support the office domain protocols, e. g., SMTP, SNMP, HTTP, some of them BOOTP, DHCP, for Web access and/or for Engineering data exchange.

The object models of the approaches differ:

- *EtherNet/IP* defines in the Common Industrial Protocol (CIP) specification the user layer including an Application Object Library (many standard objects of industrial devices) and Device Profiles (defining the device features),
- *HSE* [HSE01] is based on the Function Block technology [IEC61499] to design the distributed application as a Function Block network,
- *IDA and PROFINET (CBA)* define a user-friendly object background,
- *IDA* (MODBUS RTPS) [IDA02] defines an object-oriented common Runtime and Engineering model consisting of an Application Model (design of modular applications), an Engineering Model (description of the specific automation applications and their connections), a Process Model

(mapping the application model elements to the physical topology), a Presentation Model (description of the external behaviour of the application model elements) as well as an HMI Model (browser-based supervisory & control). The Engineering Model allows two views: the Functional view (representation of the hierarchical structure of the IDA system functionality), the Topological View (physical network structure including all segments and connected devices, routers, switches),

- *PROFINET CBA* [PRO03] also defines an object-oriented common Runtime and Engineering. It allows the pre-configuration of the automation application within the Engineering Tool and mapping it to the physical architecture easily using a powerful tool.

2.1.3.3 Ethernet-based Local Hard Real-time Approaches

As mentioned above the use of middleware concepts on top of TCP/IP leads to limits regarding real-time behaviour caused by the best effort features of TCP. That is why many investigations are directed to use a middleware concept on top of the MAC Layer. In academic and industrial research, different scheduling strategies and smoothing concepts are investigated [ATV00, HL04, HJH02, TK04,BLM03, CLM03, CCl02, KK00]. Following the results we can distinguish:

- Deterministic (but not isochronous) real-time behaviour enabling cycle times in the range of 1 to 10 milliseconds (real-time class 2). That fulfils the timing requirements of most industrial communications in a factory and can be implemented by software.
- Isochronous real-time behaviour (real-time class 3) enabling cycle times in the range of 250 microseconds to 1 millisecond and with jitters of less than 1 microsecond. That fulfils the timing requirements of motion control, especially for the synchronised operation of many distributed drives.

Deterministic real-time approaches (real-time class 2)

The first concept uses a middleware on top of the MAC layer to realise the scheduling and smoothing functions. The middleware is normally represented by a software implementation. Industrial examples are:

- PROFINET (PROFIBUS International, Siemens) [IEC65c359],
- Time-critical Control Network (Tcnet, Toshiba) [IEC65c353],
- Vnet (Yokogawa) [IEC65c352].

For the Ethernet-based *PROFINET IO* system (using the main application model background of the leading fieldbus PROFIBUS DP) the object model IO (Input/Output) has been established.

The Time-critical Control Network TCnet specifies in the Application Layer a so-called “Common Memory” for time-critical applications, and uses the same mechanisms as mentioned for PROFINET IO for TCP(UDP)/IP-based non real-time applications.

The Vnet supports up to 254 sub-networks with up to 254 nodes each. It realises in its Application Layer three kinds of application data transfer.

Isochronous real-time approach

Regarding real-time class 3, the following main examples are becoming part of the Fieldbus standard IEC 61158, Edition 4, in 2006:

- PowerLink (Ethernet PowerLink Standardisation Group EPSG, Bernecker & Rainer), developed for Motion Control [IEC65c352, Mei02].
- EtherCAT (EtherCAT Technology Group (ETG), Beckhoff) developed as a fast back plane communication system [IEC65c355].

- PROFINET IO/Isochronous Technology (PROFIBUS International, Siemens) developed for any industrial application [IEC65c359].
- EtherNet/IP with Time Synchronisation (ODVA, Rockwell Automation), an extension of EtherNet/IP [IEC65c361]
- SERCOS III, developed for Motion Control (IG SERCOS Interface e.V.) [IEC65c358].

Powerlink offers two modes: Protected Mode, Open Mode. *EtherCAT* distinguishes two modes: direct mode and open mode. *PROFINET IO/Isochronous Technology* uses a middleware on top of Ethernet MAC layer to enable high-performance transfer, cyclic data exchange and event-controlled signal transmission. The layer 7 functionality is directly linked to that middleware. The middleware itself contains the scheduling and smoothing functions. This means, TCP/IP does not influence the PDU structure. *EtherNet/IP with Time Synchronisation* uses, based on EtherNet/IP technology, the CIP Synch protocol to enable the isochronous data transfer. Since the CIP Synch protocol is fully compatible to standard Ethernet, additional devices without CIP Synch features can be used in the same Ethernet system. A *SERCOS III* network consists of Masters and Slaves. At the Application Layer two kinds of services are supported: AL services mapped onto TCP(UDP)/IP protocol suite; real-time services realised using five “Communication Phases” CP: from recognising the participating slaves by the master up to the validation of the transmitted data.

2.1.3.4 Standardisation

The maintenance phase of the fieldbus standard IEC 61158 starts in November 2005. As a result, the Edition 4 of that standard will be available in 2006. The different types of Ethernet-based industrial communication systems [IEC65c341, IEC65c360, IEC65c359, IEC65c353, IEC65c352, IEC65c356, IEC65c355, IEC65c361, IEC65c358] will become part of that standard. There will be none harmonised protocols. Some of these systems can run on the same cable, but are not interoperable. Thus, the normal case will be, that each system will work alone in a certain application by commercial reasons.

2.1.4 Safety in Automation

To minimize the risk of harming people, the environment, property and the like, some control loops must be shut down if the process experiences a problem or if the system fails [ISA02]. Safety related systems have to handle all kinds of faults.

By the IEC 61508-4 definition safety is freedom from unacceptable risk. Functional safety is a part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE (Electrical/Electronic/Programmable Electronic) safety-related systems, other technology safety-related systems and external risk reduction facilities.

A safety technology has grown up around the need to set target risk levels and to evaluate whether proposed designs meet these targets by they process plant, transport systems, medical equipment or any other application. There is no such thing as zero risk. This is because no physical item has a zero failure rate, no human being makes zero errors and no piece of software design can foresee every possibility.

The actual degree of risk considered to be tolerable will vary according to a number of factors such as the degree of control one has over the circumstances, the voluntary or involuntary nature of the risk, the number of person at risk in any one incident and so on. The IEC 61508 Standard is concerned with electrical, electronics and programmable safety-related systems where failure will affect people or the environment. The term safety-related applies to any hardwired or programmable system where

a failure, singly or in combination with other failures, could lead to death, injury or environmental damage.

Safety aspects of plant networks are addressed in chapter *Safety Technologies*.

2.1.5 Security in Automation Communication Systems

For traditional communication systems used in automation, use of an exclusively provided infrastructure, limited physical access to the transfer media and total isolation from the outside have been typical. However, in the VAN project secure communication over public networks is to be achieved.

The U.S. National Information Systems Security Glossary defines security as: “the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats”.

To achieve appropriate protection against such wide variety of threats the following elements of security have to be addressed in the VAN project:

- confidentiality;
- integrity;
- availability;
- accountability.

Security aspects of both automation and public communication technologies are addressed in the chapter *Security Technologies.*

2.1.6 Wireless Approaches

Wireless technologies can be divided into two subsections with respect to their use.

For automation purposes in plants, it is often required that a particular technology features real-time properties to ensure exact deadlines and jitters. Seeing the fact that factory floor is often strongly electromagnetically disturbed, errors occur more frequently. This can be avoided by massive data safety mechanisms with error detection and transmit repeat requests. However, this technique is contradictory to real-time requirements. Therefore, many local wireless technologies try to find a compromise to this contradiction.

Within the VAN project, connection of several local area networks is required. These connections are often provided by wireless connections. At this point the requirements are somewhat different from the previous case. As access to a public WAN is necessary, massive security methods are required. Real-time properties are usually not discussed at all.

2.1.6.1 Wireless Local Approaches

Bluetooth is a complete stack technology, based on radio transceivers with FHSS modulation. It is target predominantly for office purposes, e.g., headsets, device connection, PDU synchronisation, and so forth. The application layer offers different profiles which dedicates this technology for cable replacement purposes.

ZigBee is a home-area network designed specifically to replace the proliferation of individual remote controls. It is based on radio transceivers with DSSS modulation. ZigBee was created to satisfy the market's need for a cost-effective, standards-based wireless network that supports low data rates, low power consumption, security, and reliability.

nanoNET is a new standard for wireless networks, developed by Nanotron Technologies. It is based on chirp modulation and supports both TDMA and CSMA. nanoNET offers high flexibility and data rates as well as long range and low power consumption for many applications.

WiFi is another name for IEEE 802.11 (WLAN).It has become a wireless complementary technology to wired LAN. It if accepted due to its compliance with LAN technologies. It provides short-range, high data rate connections between mobile data devices and access points connected to a wired network.

2.1.6.2 Wireless Access to Wide Area Networks

GSM/GPRS is a combination of a mobile technology and a data bearer. GPRS stands for General Packet Radio Service. It provides packet transmission over GSM network. The data rate is quite low, however, the connection is available anywhere. Security issues are covered well. Provided services can be either public or private.

GSM/EDGE is enhancement of GPRS technology. It reaches higher data rates (up to 400 kbps).

UMTS is a 3G standard. It is broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates 2 Mbps theoretically. It offers a set of services to mobile computer and phone users no matter where they are located in the world.

WiMAX is a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL. WiMAX provides fixed, nomadic, portable and, eventually, mobile wireless broadband connectivity without the need for direct line-of-sight with a base station.

2.2 Selected Communication Technologies

Several communication technologies were chosen to introduce the solution of the abovementioned aspects. Parameters, which can be compared across technologies, are specified in *Appendix A*. Information provided within this section is mainly derived from the relevant standards and additional papers as [CEPNeum][Lar05][LL05][PW03].

2.2.1 EtherCAT Architecture

EtherCAT [IEC65C355] is a Real Time Ethernet technology, which was developed by Beckhoff in 2003 and is currently supported by the EtherCAT Technology Group (ETG). It aims to maximize the utilization of the full duplex Ethernet bandwidth. Medium access control is based on the classical Master/Slave principle.

Stack Architecture and Characteristics

EtherCAT distinguishes two modes of operation:

- Direct mode

  Using the direct mode, a Master Device uses a standard Ethernet port between the Ethernet Master and an EtherCAT segment. EtherCAT uses a ring topology within the segment. The medium access control adopts the Master/Slave principle, where the Master node (typically

the control system) sends the Ethernet frame to the Slave nodes (Ethernet device). One single Ethernet device is the head node of an EtherCAT segment consisting of a large number of EtherCAT Slaves. The Ethernet MAC address of the first node of a segment is used for addressing the EtherCAT segment. For the segment, a special hardware can be used. The Ethernet frame passes each node. Each node identifies its sub-frame and receives/sends the suitable information using that sub-frame. Within the EtherCAT segment the EtherCAT Slave devices extract data from and insert data into these frames. The EtherCAT Slave devices process the incoming frames directly and extract the relevant user data, or insert data and transfer the frame to the next EtherCAT Slave device. The last EtherCAT Slave device within the segment sends the fully processed frame back. This frame is returned to the Master device as response frame. EtherCAT uses in the direct mode a direct communication between a Master device and an EtherCAT segment without switches. Thus, there is no need for direct addressing of nodes. For less time-critical data traffic the data section of an UDP datagram can be used (via IP routing). On the Master side any standard UDP/IP implementation can be used.

- Open mode

  Using the open mode, one or several EtherCAT segments can be connected via switches with one or more Master devices and Ethernet-based “Basic Slave” devices. Each segment can be addressed using a “Segment Address Slave” device (the head station of the segment.).

  The technical background of EtherCAT is 100Base-TX and -FX Ethernet used within an EtherCAT segment and between Master devices and Slave devices. Within EtherCAT segments Low Voltage Differential Signals (LVDS) (IEEE 803-3ae-2002) can also be used.

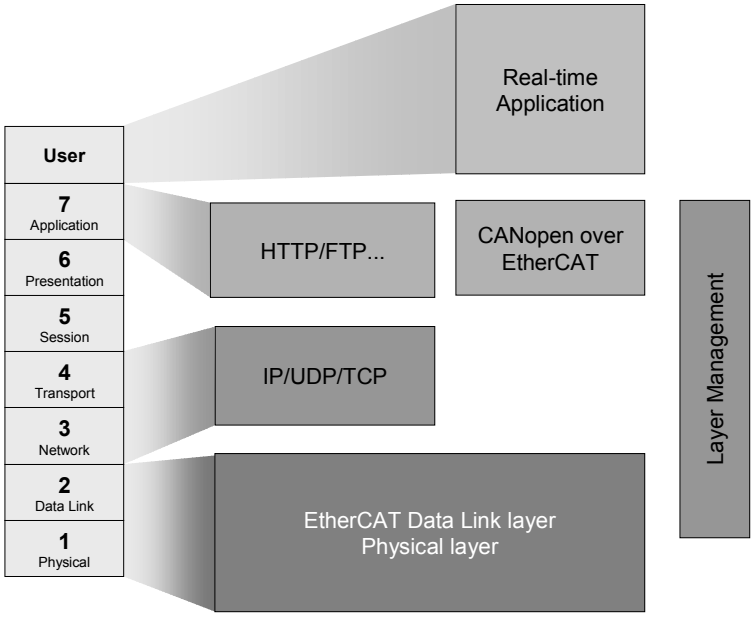

Fig. 2-1: EtherCAT Slave Node Architecture

The Application Layer follows the CANopen model. There is an Object Dictionary and the handling of service data and process data objects. In addition EtherCAT has been designed to feature standard IP-based protocols such as TCP/IP, UDP/IP and all higher protocols based on these (HTTP, FTP, SNMP etc.).

The protocol is realised by an EtherCAT state machine. To enable isochronous data transfer the Precision Clock Synchronisation Protocol [IEC61588] is used.

From the architectural point of view an EtherCAT node can be modelled as described above.

2.2.2 Ethernet for Plant Automation (EPA) Architecture

Ethernet for Plant Automation (EPA) [IEC65C357] was developed by the Chinese Zhejiang Supcon Company as a trade name and introduced into the standardisation process. Actually it is not supported by a registered user group.

Stack Architecture and Characteristics

EPA is an approach for TCP/IP or UDP/IP based deterministic communication for distributed applications, which supports a time slot mechanism. This mechanism is realized through a special EPA Communication Scheduling Management Entity (ECSME), which in fact is an extension of the Data Link Layer [LAR05].

Data transfer is divided into two phases:

- Periodic message transfer (deterministic communication between distributed function blocks in slow real-time based on time sliding within the MAC layer)
- Non-periodic message transfer (normal IT traffic and process communication over TCP/IP or UDP/IP)

The synchronization mechanism of the distributed clocks is based on IEEE1588.

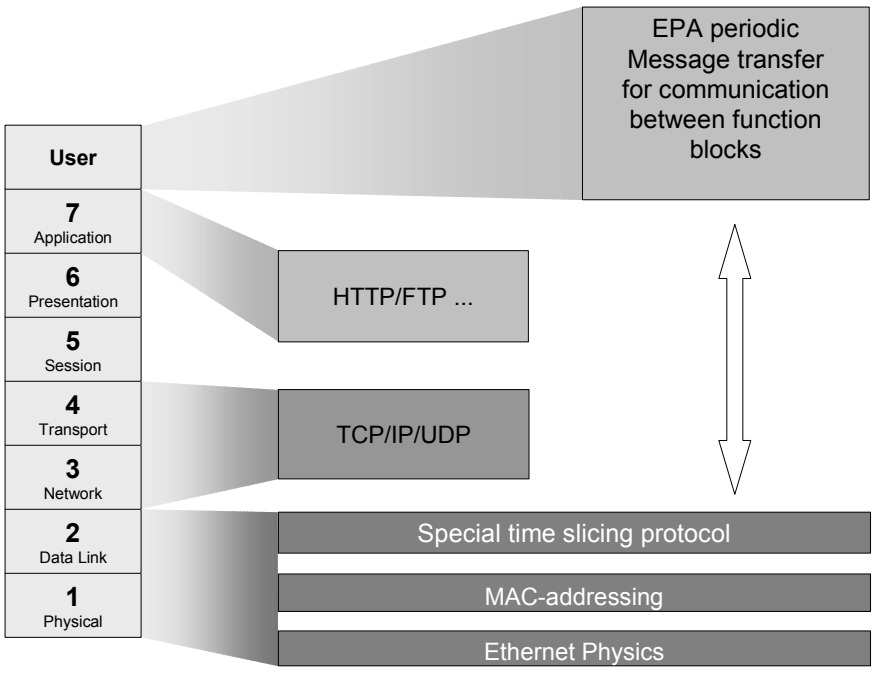

Fig. 2-2: EPA Architecture

2.2.3 Ethernet Powerlink (EPL) Architecture

Ethernet Powerlink [IEC65C356] is a strict deterministic, isochronous real-time protocol which is based on standard Fast-Ethernet. The protocol defines isochronous time slot procedure to assign the right to send data to the bus. The Powerlink manager is a station responsible for assigning the time slots for the other stations; there is exactly one Powerlink manager on the bus. Other stations are called Powerlink Controllers and can send data only when requested by the manager. The bus cycle is divided into isochronous phase and an asynchronous phase.

During the isochronous phase every node broadcasts (EPL broadcast) its data, which will be received by any other node directly, without the need for a supervising node to serve as a relay station. Thus direct peer-to-peer communication with maximum speed and flexible publish/subscribe relationships between all nodes are possible.

The asynchronous phase is using IP-frames and is therefore absolutely transparent to any standard TCP/IP or UDP/IP communication. These facts offer optimum throughput and efficiency but also ensure transparency for existing TCP/UDP/IP applications to ETHERNET Powerlink nodes.

Stack Architecture and Characteristics

Ethernet Powerlink distinguishes between Real-Time domains and non Real-Time domains. This separation matches typical machine and plant concepts. It also satisfies the increasing security demands to prevent hacker attacks on the machine level or harm through erroneous data communication on higher network hierarchies. Hard Real-Time requirements are met within the Real-Time domain. Less time critical data is routed transparently between the Real-Time domain and non-Real-Time domain using standard IP frames. A clear boundary between a machine and factory network prevents potential security flaws from the very beginning while keeping full data transparency.

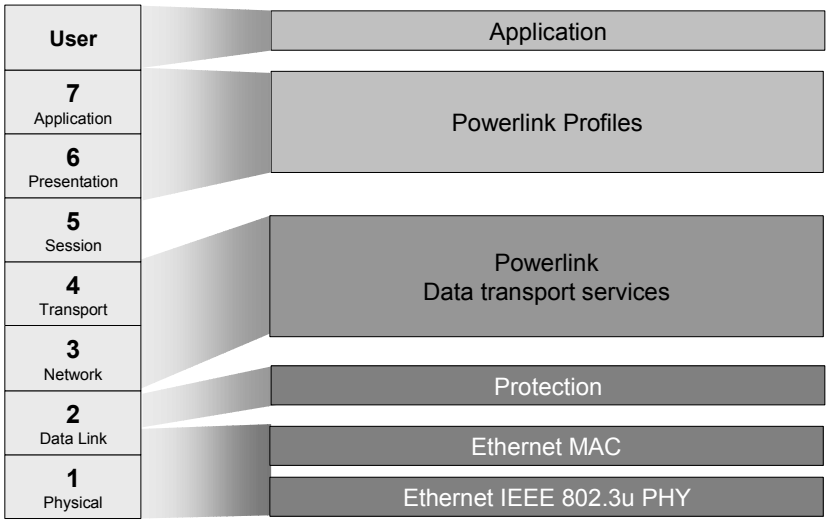

Fig. 2-3: Ethernet Powerlink Architecture

In order to provide a flexible and proven solution for the application layer, ETHERNET Powerlink has been combined with the well known and widely deployed CANopen family of communication and

device profiles. The EPSG and the CiA (CAN in Automation) has founded a joint technical working group, which has achieved the adaptation of CANopen's DS301 and DS302 communication profiles to ETHERNET Powerlink [POW02].

Now every ETHERNET Powerlink device is described by a standardised Device Model with its central element, the Object Dictionary, containing a list of descriptions of all data, parameters and functions of the device that can be accessed or controlled remotely via Ethernet.

Furthermore, all configurable communication parameters are listed in the Object Dictionary. By means of the Object Dictionary each data of a device can be easily accessed from any device of the network by a unique 24-bit reference, consisting of a 16-bit index and a 8-bit sub-index.

For describing an ETHERNET Powerlink device, a standardised file format exists in form of an XML-based Electronic Data Sheet (EDS) according to ISO 15745-4.

2.2.4 Ethernet Industrial Protocol (EtherNet/IP) Architecture

EtherNet/IP (IP means Industrial Protocol) [IEC65C361] defines an open industrial standard which combines the classical Ethernet with a special industrial protocol. This standard was elaborated jointly by ControlNet International (CI) and the Open DeviceNet Vendor Association (ODVA) with the help of the Industrial Ethernet Association (IEA). Rockwell Automation is the main producer for controllers, I/O devices, drives, and HMIs.

Stack Architecture and Characteristics

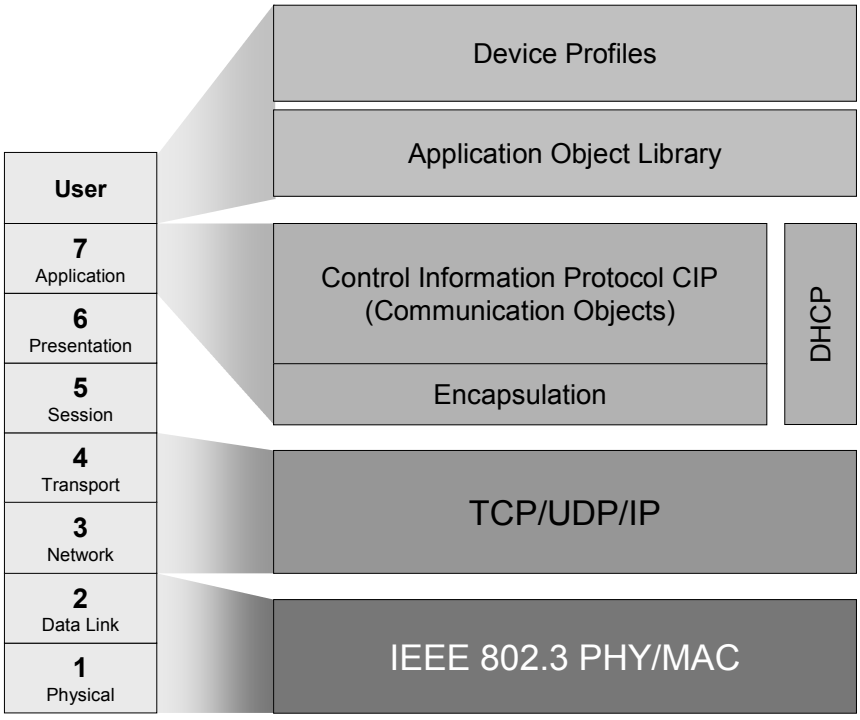

Fig. 2-4: EtherNet/IP Architecture

EtherNet/IP uses the *Common Industrial Protocol (CIP)*, which represents a common application layer for all physical networks of EtherNet/IP, ControlNet and DeviceNet. Data packets are transmitted via

CIP router between the networks. The application process is based on a Producer/Consumer model. CIP is a well-defined object-oriented protocol and defines the transport of I/O data, configuration data, and diagnostics over a normal Ethernet network. The mapping of the CIP services onto the TCP/IP protocol is enclosed by the Encapsulation Protocol.

The *CIP object model* defines all data as real objects which consist of attributes and methods. The CIP specification contains a lot of common objects and some for the specific networks DeviceNet, ControlNet, and EtherNet/IP. Every device has to support a mandatory set of the common objects, for example the Identity Object. Further objects, implemented into the device, determine the special device type.

CIP is a connection-based protocol and distinguish between Explicit Message Connection and Implicit Message Connection.

The *Explicit Message Connection* works on top of TCP/IP and is used for generic, multi-purpose communication between two devices. The Explicit Messages Connection always requires a source address, a destination address, and a connection ID in each direction. Explicit messages are event-oriented and will be triggered by the application.

The *Implicit Message Connection* works on top of UDP/IP and is used for the real-time I/O data transfer between a producer and one or more consumers. The messages are produced cyclically by a producer on a pre-defined schedule base.

CIP provides several options for the *device configuration*. These are the printed data sheet, parameter objects and parameter object stubs, an electronic data sheet (EDS), a combination of an EDS and parameter object stubs, or a configuration assembly in combination with any of these methods.

EtherNet/IP with Time Synchronisation uses on the basis of EtherNet/IP technology the *CIP Sync* protocol to enable the isochronous data transfer. Since the *CIP Sync* protocol is fully compatible to standard Ethernet, additional devices without CIP Sync features can be used in the same Ethernet system. The CIP Sync protocol uses the Precision Clock Synchronisation Protocol [IEC61588] to synchronise the node clocks using an additional hardware function. CIP Sync can deliver time - synchronisation accuracy of less than 500 nanoseconds between devices, which meets the requirements of the most demanding real-time applications. The jitter between Master and Slave clocks can be less than 200 nanoseconds.

2.2.5 Fieldbus Foundation High Speed Ethernet (FF HSE) Architecture

High Speed Ethernet (HSE) has been developed on the initiative of the Fieldbus Foundation. This organization was founded in 1994 and counts about 200 members worldwide. The development of HSE has been started within the second half of the 90th with the intention to use Ethernet as system bus for FF-H1-Fieldbus segments. H1-subnets are integrated through H1 Links [IEC61158].

FF HSE distinguishes between different device categories

- Host Devices,
- HSE Linking Devices,
- HSE I/O Gateway,
- HSE Field Devices.

Each device is dedicated to realize application processes following the approach of FF Function Blocks. To operate Function Block application processes necessary infrastructural components have been defined. The FF HSE specification contains:

- System Architecture,
- System management,
- Network management,
- HSE Presence,
- H1 Bridging,
- FDA Agent,
- Redundancy,
- Communication profiles.

Stack Architecture and Characteristics

The HSE stack architecture and its relation to the ISO 7-Layer model is represented within the figure below. In addition to the FF HSE layer 7 communication service the specification contains user layer functions (Application Processes – AP). Such an Application Process describes that part of a distributed application, which is executed within an individual device. Within the HSE context this considers functions for executing Function Blocks, Network Management and System Management. The lower protocol layers, down the transport layer, are based on the Internet standards TCP/IP [STE94] and UDP/IP [STE94].

The FF specification defines the following Application processes:

- The Function Block Application Process (FBAP) is an application process, which supports execution of Function Blocks like PID-controller or Analogue Input. Access to Function Blocks is done based on object descriptions (OD). All accessible objects are represented/abstracted through a Virtual Field Device (VFD).
- The System Management (HSE System Management Kernel (HSE SMK)) is an application process to manage basic information and functions of a HSE device. Information accessible via the bus system is represented through a so called Management Information Base (MIB).
- The Network Management Agent (NMA VFD) is used to manage communication relationships between different application processes. They are called Virtual Communication Relationships (VCR).
- Another application process is the HSE Management Agent (HMA). This HMA contains a DHCP-Client, a SNTP-Client and a SNMP-Agent. The Internet standards used are DHCP [RFC1541], SNTP [RFC2030] and SNMP [RFC1157].
- The HSE LAN Redundancy Entity (HSE LRE) is an application process, which realizes switching between redundant interfaces.
- The H1 IF Bridge is an application process, which co-ordinates the routing of data between different FF H1 fieldbus interfaces.

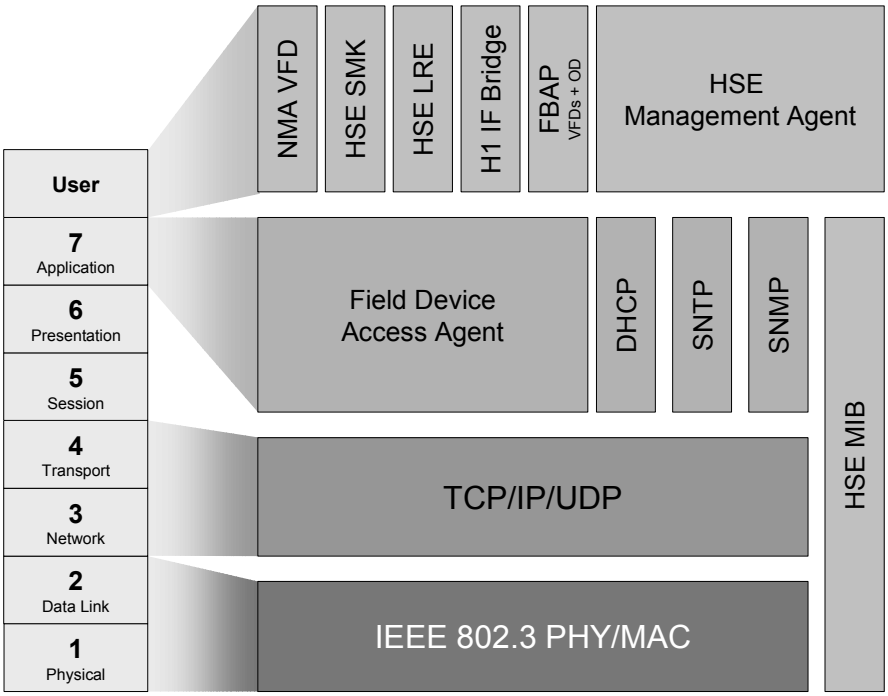

Fig. 2-5: HSE Architecture

These application processes highlight that FF HSE also defines, beside the process related applications, infrastructure needed to operate a system. The data transfer on the transport layer is based on the Internet Standards IP, UDP and optional TCP. The Field Device Access (FDA) Agent is the specific FF Layer 7 and defines the communication protocol and services to support the different applications – it provides special services for System Management Kernel and VFD access. SMK services are transferred via UDP whereas VFD services are transferred via UDP or optional TCP. This part of the HSE architecture, which contains the Internet standard protocols from Ethernet to SNMP, is called HSE Presence.

2.2.6 JetSync Architecture

JetWeb is a complete Ethernet based system solution provided by the Jetter AG for the realization of automation projects including field devices, controller, programming and visualisation/SCADA. Only TCP/IP is used for all underlying communication, also for synchronisation of motion systems. This way, modular organization and servicing of plants have been simplified, and connectivity to the Office/ERP has been provided. Transparent access to each device, visualisation and operation via Web-browser has become possible, as well as alarm messages sent by the plant as e-mail or SMS. Since 2003 there is cooperation with Lumberg to extend the range of available products. At the SPS/IPC/DRIVES 2002, Jetter AG introduced the JetSync technology with its specific products. This technology serves for synchronizing axes with the help of Ethernet and TCP/IP.

Stack Architecture and Characteristics

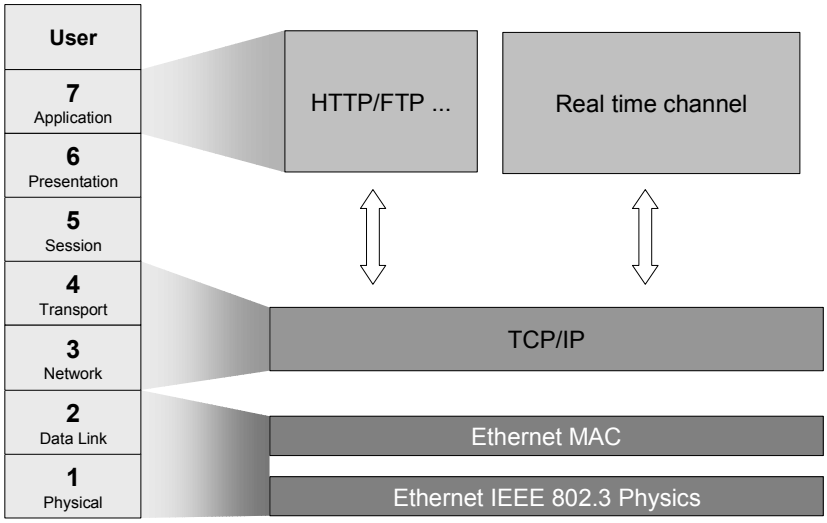

Fig. 2-6: JetSync Architecture

JetWeb/JetSync are based on a standard Ethernet controller together with a standard TCP/IP stack. It enables the use of standard components and infrastructure. It is possible to use standard application protocols like HTTP and FTP.

Commissioning and programming of all controllers and all automation functions is accomplished using one engineering tool and one programming language. JetWeb completely integrates motion technology into the control system.

With the help of JetWeb, motion systems can also be synchronized via standard Ethernet and TCP. For this purpose, the JetSync solution has been developed. It is based on standard protocols and special hardware is not required. Standard IT components, such as switches, are used. The synchronizing of axes by means of Ethernet-TCP/IP with jitter smaller than 10 µsec is possible. There is no restriction of network participants. Asynchronous (TCP/IP) communication can also be applied in runtime, e.g. for access to the Web server in the field device. JetSync contains an error management, e.g. for synchronized and controlled ramping-down of drives (within 1 ms). Network analysis tools and measuring devices belonging to the office-world can also be applied together with TCP/IP; arbitrary direct access to individual devices, e.g. to their embedded homepage, is possible any time. Further, any PC can be connected to any free port which means it will have got access to the entire network, interfaces not being required.

The technological background of the solution based on Ethernet-TCP/IP, developed by Jetter, is a procedure of synchronizing clocks in pulse-generator accuracy [Lar05]. User data will then be transferred in asynchronous mode and given a time stamp. This is based on the Precision Clock Synchronisation Protocol IEC61588 [IEC61588]. With the help of the synchronized information on time, these data will then be synchronized towards the respective sampling instant.

Jetter and Lumberg provide a complete range of JetWeb/JetSync enabled products: controllers, motion control systems, visualization systems, user guidance with HMI, programming software (for controlling, operating, managing data, and driving).

2.2.7 Modbus/TCP Architecture

Modbus has been developed by Schneider Electric starting in 1979. Currently it is supported by the Modbus-IDA user group. It is an open and widely used network protocol in the industrial manufacturing environment, which is implemented in different devices in order to transfer discrete/analogue I/O and register data between control devices [IEC65C35541]. It's also a common denominator between different manufacturers.

Stack Architecture and characteristics

Considering Ethernet based Modbus protocol one has to distinguish between the classical “Modbus messaging on TCP/IP” and the “Real-Time Publish-Subscribe” (RTPS) Wire Protocol.

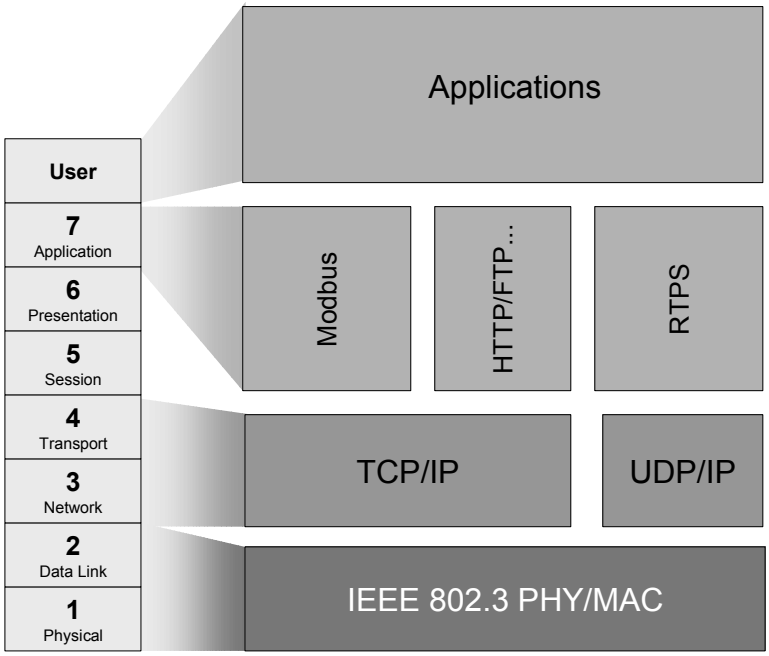

Fig. 2-7: Modbus/TCP and RTPS Architecture

Modbus

Modbus is a protocol based on application layer messaging, which in fact is located at layer 7 of the ISO model. Communication between devices is based on the classical Client-Server communication model. It is currently implemented using:

- TCP/IP over Ethernet,
- Asynchronous serial transmission over a variety of media (wire: EIA/TIA-232-E, EIA-422, EIA/TIA-485-A; fibre, radio, etc.),
- MODBUS PLUS, a high speed token passing network.

Modbus protocol defines a simple protocol data unit (PDU) independent from the underlying layers. The mapping of Modbus to different underlying layers may require the introduction of additional fields

within the application data unit (APDU). Regarding this deliverable only the Modbus on TCP/IP version is relevant.

Typically a Modbus on IP network is composed of different types of devices:

- MODBUS TCP/IP Client and Server devices and
- Interconnection devices like bridge, router or gateway for interconnection with different sub-networks.

Real-Time Publish-Subscribe (RTPS) Wire Protocol

According to the protocol definition Real-Time Publish-Subscribe Wire Protocol is designed to be based on the UDP/IP lower level protocol. That means the reception of data published is not confirmed by the subscriber. The RTPS protocol targets the following goals [IEC65C341]:

- plug and play connectivity in terms of discovery and integration of new applications and services,
- performance and quality-of-service properties to meet real-time requirements,
- reliability and timeliness oriented configuration,
- extensibility of the protocol while guarantying interoperability,
- fault tolerance to allow the creation of networks without single points of failure,
- type-safety to prevent application programming errors from compromising the operation of remote nodes.

RTPS provides two main communication models:

- the publish-subscribe protocol, which transfers data from publishers to subscribers and
- the Composite State Transfer (CST) protocol, which transfers state.

  The Composite State Transfer (CST) protocol transfers Composite State from CSTWriters to CSTReaders. It is handled as a state synchronization protocol.

2.2.8 P-Net on IP Architecture

The development of the P-Net communication was started in 1983 by Proces-Data. Later on the fieldbus protocol became part of the IEC 61158 standard (Type 4) [IEC61158] and the P-Net User Organisation was formed. P-Net was proposed by the Danish national committee to become the IEC/PAS 62412 specification.

Stack Architecture and characteristics

P-Net on IP is based on the P-Net Fieldbus standard Type 4 [IEC61158] and contains the mechanism to use P-Net in an IP environment [IEC65C360]. Therefore, the P-Net PDUs are wrapped into UDP/IP packages, which can be routed through IP networks. Nodes on the IP network are addressed with two P-Net route elements. P-Net Clients (Master) can access Servers on an IP network without knowing anything about IP addresses. [IEC65C360] defines replacements within and additions to [IEC61158]. An important section is dedicated to the definition of the routing mechanisms.

The resulting protocol architecture is described below.

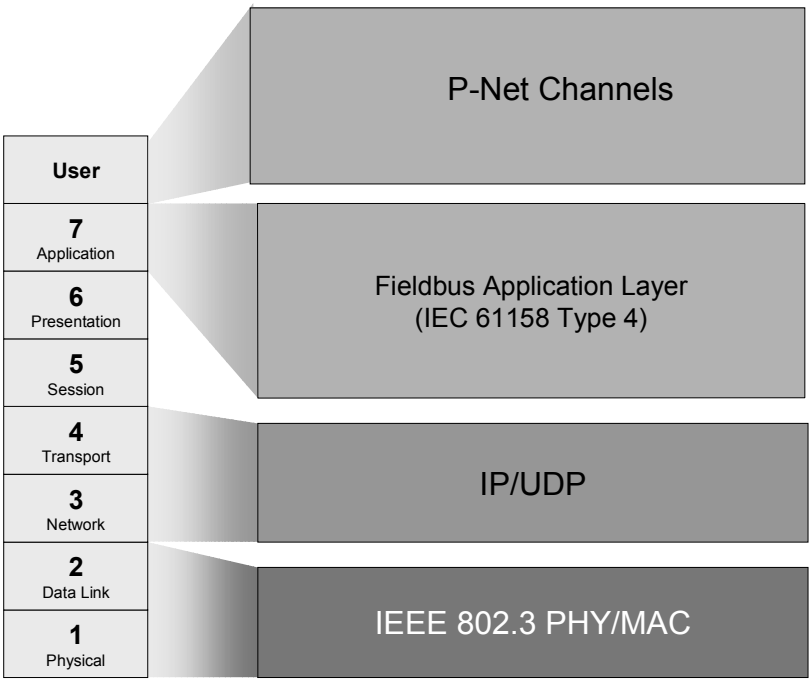

Fig. 2-8: P-Net on IP Architecture

The architecture of the P-Net protocol is based on:

- The MAC and LLC sublayer is based on ISO/IEC 8802-3.
- The Network Layer is based on the Internet standard RFC 791 (IP, Internet protocol) and its amendments and successors.
- The Transport Layer is based on the Internet standard RFC 768 (UDP, User Datagram Protocol) and its amendments and successors.
- The application layer is the same as defined within IEC 61158 Type 4

2.2.9 PROFINET Architecture

PROFINET [IEC65C359] is an industrial Ethernet standard for automation. PROFINET comprises with CBA, an architecture for the distribution of control intelligence and with PROFINET IO the integration of distributed I/O devices and I/O drives. The standard was elaborated jointly by the PROFIBUS user organisation (PNO) and Siemens. Siemens is the main producer for PROFINET products like I/O controllers and I/O devices. Since 2004 the INTERBUS Club also supports the PROFINET technology as the most comprehensive concept.

Stack Architecture and Characteristics

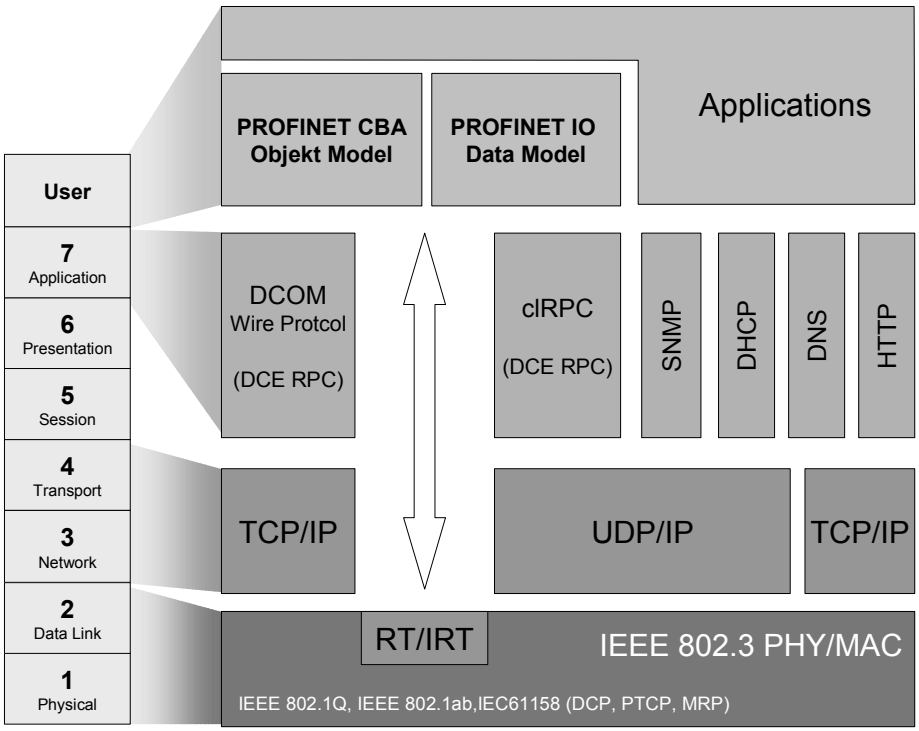

Fig. 2-9: PROFINET Architecture

PROFINET CBA (Component Based Architecture) is effective in distributed automation plants. The component model describes the autonomous modules of machines or plants as technological modules. A distributed automation system developed on the basis of technological modules simplifies the modular design of plants and machines, thus considerably simplifying the reuse of plant and machine parts.

PROFINET on the basis of a component model is described via a PCD (PROFINET Component Description). It is XML-based and can be created using either the Component Generator of a manufacturer-specific configuration tool or the PROFINET Component Editor.

The engineering of distributed automation plants differentiates between the programming of the control logic of the individual technological modules (manufacturer-specific configuring tools) and the technological configuration of the overall plant, which determines the communication relationships between the technological modules.

There is a common engineering defined for PROFINET CBA. With a manufacturer spanning engineering tool only the communication relationships between the modules will be defined via graphical lines. Together with performance information these connection information will be transferred into the devices in a defined way. The establishment of loaded connection information is then realised by the devices.

PROFINET CBA uses the DCOM Wire Protocol with the Remote Procedure Call mechanisms (DCE RPC) [OSFC706] to transmit the soft real-time data. The packets are prioritized as specified in IEEE

802.1p to guarantee an optimal performance. The highest priority is used for the soft real-time data. Exemplary implementations of PROFINET CBA for different operating systems are available as source code on the PNO Website.

The Ethernet-based *PROFINET IO* system defines an object model IO (Input/Output) which is using the main application model background of the fieldbus PROFIBUS DP. The PROFINET IO service definition and protocol specification [IEC65c359] covers the communication between programmable logical controller PLC systems, supervisor systems, and field devices or remote input and output devices.

In general, PROFINET IO distinguishes between three device types: an IO controller, which represents mainly a PLC, an IO device, which represents mainly field devices and remote IO devices, an IO supervisor, which represents a diagnosis, HMI or commissioning tool, and real devices may be composed of several instances of the above mentioned basic device types.

The PROFINET IO specification is a combination of own layer definitions and several other standards. On top, the PROFINET IO application process PROFINET IO AP has been defined. The PROFINET IO application layer providing the PROFINET IO specific services and protocol follows it. PROFINET IO uses IETF and OSF standards for the OSI Middle Layers, which has been empty in most known fieldbus architectures. PROFINET IO uses the Internet Standards IP [RFC791] and UDP [RFC768, RFC791] defined by the Internet Engineering Task Force IETF. Furthermore, the connectionless distributed communication environment remote procedure call clRPC [OSFC706], available from the Open Software Foundation OSF, defines the basis for context management and generic read or write services. Between the application layer and data link layer a glue layer for hard real-time scheduling, referred to as PROFINET IO link layer mapping protocol machine PNIO LMPM, has been specified. It is responsible for the precedence and timeliness of provider/consumer IO data and alarm data, which bypass the OSI Middle Layers. The lower layers comply to the IEEE standards [IEC8802] with different physical media.

PROFINET provides a fair mechanism to restrict the transmission performance of each device. The transmission of frames is divided into different cycles at the local interface. A typical value for a cycle is one millisecond, the range can be configured. The data to be transmitted are ordered by the priorities cyclic real-time data, acyclic real-time data, non real-time data.

PROFINET IO/Isochronous Technology uses a middleware on top of Ethernet MAC layer to enable high-performance transfer, cyclic data exchange and event-controlled signal transmission. The layer 7 functionality is directly linked to that middleware. The middleware itself contains the scheduling and smoothing functions. That means: TCP/IP does not influence the PDU structure. A special Ethertype is used to identify real-time PDUs (only one PDU type for real-time communication). That enables an easy hardware support for the real-time PDUs. The technical background is a 100 Mbps full duplex Ethernet (switched Ethernet). PROFINET IO adds an isochronous real-time channel to the RT channels of real-time class 2 option channels. This channel enables a high-performance transfer of cyclic data in an isochronous mode [JSW04]. The time synchronisation and node scheduling mechanism is located within and on top of the Ethernet MAC Layer. The offered bandwidth is separated in a bandwidth for cyclic hard real-time and soft/non real-time traffic. This means, within a cycle there are separate time domains for cyclic hard real-time, for soft/non real-time over TCP/IP traffic, and for the synchronisation mechanism. The cycle time should be in the range of 250 ms (35 nodes) up to 1ms (150 nodes) when simultaneously TCP/IP traffic of about 6 Mbps is transmitted. The jitter will be less than 1µs. PROFINET IO/IRT uses switched Ethernet (full duplex). Special 4 Port (followed by 2 Port) switch ASIC has been developed and will allow the integration of the switches into the devices (nodes) substituting the legacy communication controllers of the fieldbus systems.

2.2.10 SERCOS III Architecture

SERCOS (SErial Real-Time COmmunication System) has been developed by an industrial consortium in co-operation with ZVEI and VDM in the 1980s. Marketing, further technical development work and standardisation activities are under responsibility of the IGS (Interest Group SERCOS interface) which was founded in 1990.

After SERCOS interface has been approved as international standard in 1995 (IEC 61491), further development steps took place within the second SERCOS generation, e.g. increasing of transfer rate. SERCOS was originally developed as drive interface but supports also I/O modules.

The third version, SERCOS III [IEC65C358] has been designed for Industrial Ethernet.

Stack Architecture and Characteristics

Real-time behaviour and determinisms will be achieved by using time-slot mechanisms (Time Division Multiplex Access or TDMA) and hardware synchronisation. The time-slots allow for transmission of time-critical and non-critical data in alternation.

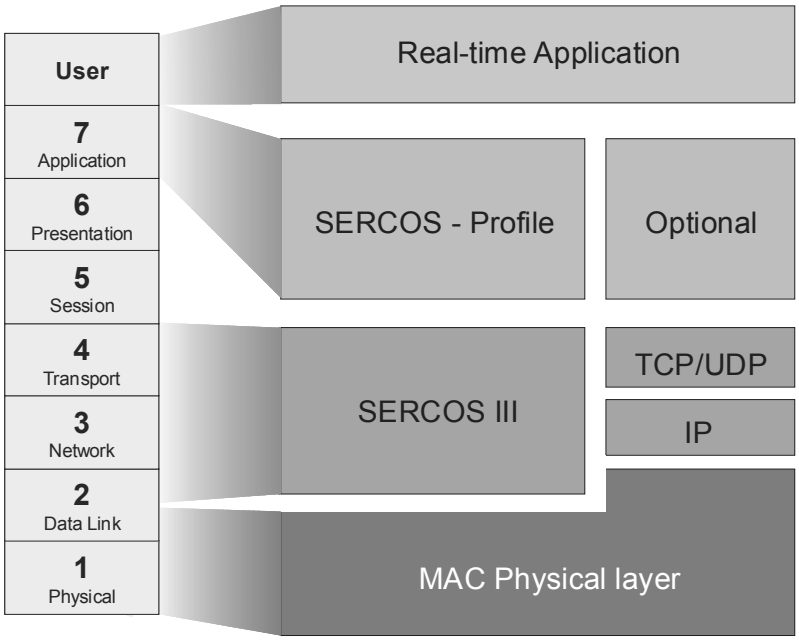

Fig. 2-10: SERCOS III Architecture

To ensure hard real-time requirements in spite of the Ethernet use, SERCOS III uses an additional, collision-free real time channel parallel to the standard IP channel. In this collision free real time channel the SERCOS defined telegrams are transmitted. For this the SERCOS III sets up directly on the MAC Layer. An IP channel can be optional configured parallel to this real time channel, in which Ethernet telegrams or IP based protocols like TCP/IP or UDP/IP can be transmitted. The cycle times, as well as the partitioning of the cyclic channel and the IP channel can be adjusted to the specific requirements of the application.

SERCOS III uses a flexible hardware solution. The basis is the development of a SERCOS core (SERCOS III IP), with which the FPGA-based SERCON100 communication controller is realized. In addition, manufacturers of components and systems are able to integrate the SERCOS III hardware functionality and their own logic components in one common FPGA.

SERCOS III is currently in the implementation phase. First soft drivers and a starter kit are available.

(For real time related features please see chapter 4.)

2.2.11 TCnet Architecture

The Ethernet based Time-critical Control Network (TCnet) was developed by Toshiba based on ISO/IEC 8802-3. TCnet was proposed by the Japanese national committee to become the IEC/PAS 62406 [IEC65C353] specification.

Stack Architecture and Characteristics

TCnet was designed to provide predictable time deterministic and reliable time-critical data transfer and means, which allow co-existing with non time-critical data transfer over the ISO/IEC 8802-3 series communications medium. This is to support of cooperation and synchronization between automation processes on field devices in real time application system. This focus resulted in a protocol architecture as described below.

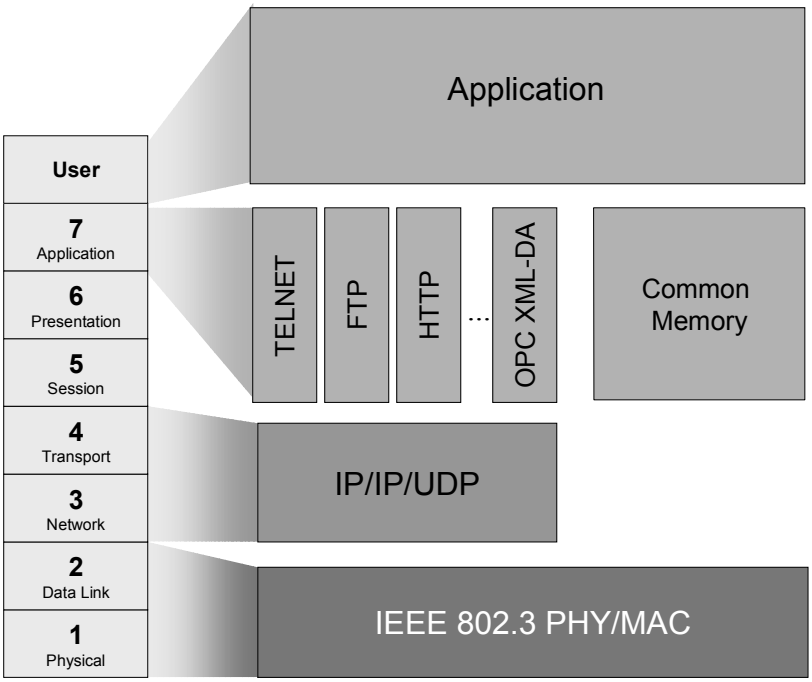

Fig. 2-11: TCnet Architecture

As can be seen within the Fig. 2-11, main protocol parts can be distinguished:

- the common Physical and Data Link layer (with specific scheduling extension) based on ISO/IEC 8802-3,

  The Scheduling mechanism in the Data Link Layer follows a Token Passing mechanism. The Target Rotation Time depends on the desired cycle time. After a SYN frame, broadcasted to all TCnet nodes, each node can send its data within a preset time (holding the transmission right). The data to be transmitted are ordered by priorities (high-speed cyclic data, medium-

speed cyclic data, sporadic message data, low-speed cyclic data). At the end of the holding time the node transfers the transmission right to the next node.

An extended Data Link Layer contains the Scheduling functionality.

- a part dedicated to regular ISO/IEC 8802-3 based applications using Application layer protocols like TELNET, FTP, HTTP, OPC XML-DA etc.,
- a part dedicated to support time-critical applications with Common Memory.

  The Common Memory is a virtual memory used and globally shared by the participating nodes as well as the application processes running in each node. It provides a temporal and spatial coherence of data distribution. The Common Memory is divided into numbers of blocks with several size of memory. Each block is transmitted to the member nodes using multicast services, supported by a node publisher. A cyclic broadcast transmission mechanism is responsible for refreshing the block data. Therefore, the Common Memory consists of dedicated areas for each node's transmitted data to be refreshed. Thus, the application program of a node has a quick access to all (distributed) data. The Application Layer protocol (FAL) consists of three protocol machines: FSPM FAL Service Protocol Machine, ARPM Application Relationship Protocol Machine, DMPM Data Link Mapping Protocol Machine.

2.2.12 Vnet/IP Architecture

Vnet/IP [IEC65C352] is a real-time plant network system for the continuous process automation. It is based on the 1-Gbps Ethernet. Vnet/IP was developed by the Japanese company Yokogawa. This system also has been put forward to the IEC for approval as a new international standard.

Stack Architecture and Characteristics

Vnet/IP integrates both control and information networks in its architecture without interference from the other. Thereby two kinds of communication are distinguish one for non-critical and one for time-critical applications. Non time-critical data for engineering and maintenance are sent using the TCP/IP protocol. The time-critical control data are sent using the UDP protocol. Using RTP communication cycle times in range of milliseconds can be achieved.

Vnet/IP has to implement the following requirement [DANY05]:

- It is essential to ensure that the real-time communication is not affected by other traffic,
- The reliability is not compromised by redundancy an environmental resistance technology,
- The security needs to be provided against cyber attacks and other network-related threats.

The Vnet/IP stack architecture contains a new Real-time & Reliable Datagram Protocol (RTP). This protocol is a specific real-time transport layer for control applications using the UDP/IP channel.

Vnet/IP adopts technologies for transmission scheduling priority control, and high-speed response. Transmission scheduling is used for the transmission of a large amount of packets by multiple transmitting stations at one time in order to prevent data delays. Priority control is used to prioritize packets with important data according to its priority order. High-speed response from UDP/IP stack is used to recover quickly from transient communication errors.

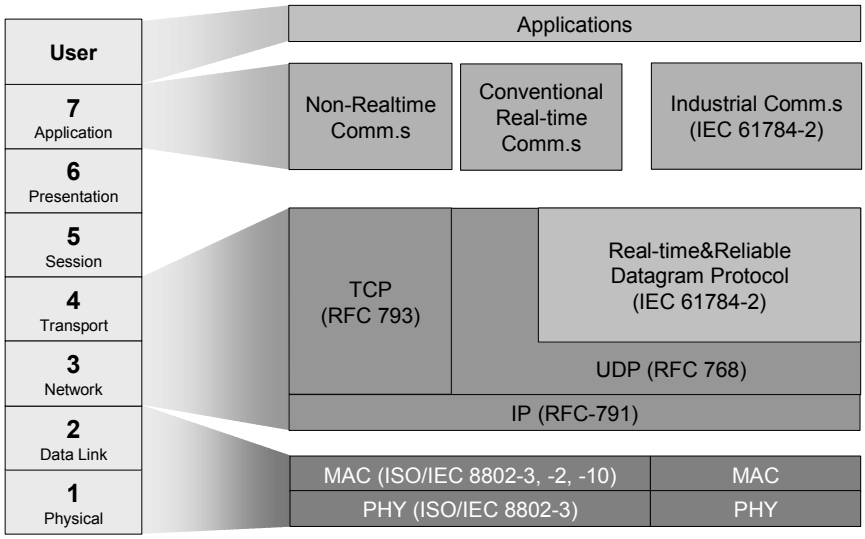

Fig. 2-12: Vnet/IP Architecture

Vnet/IP offers high reliability by using a dual network redundancy with two networks which are independent from each other. When the main network goes down the other network is immediately activated.

Vnet/IP is open for standard internet technologies. Beside the control communication standard protocols, such as FTP and HTTP can perform simultaneously for handle engineering and maintenance data.

The Vnet supports up to 254 sub-networks with up to 254 nodes each. It realises in its Application Layer three kinds of application data transfer:

- One-way communication path used by an endpoint for Inputs or Outputs (Conveyance Paths): unidirectional Application Relationship (AR). To realise bi-directional ARs (for transactions between communication endpoints), two of these Conveyance Paths have to be established.
- Trigger Policy. There are two types: user-triggered type requests the earliest opportunity for transmission of the A-PDU by the Data Link Layer; network-scheduled type supports the A-PDU transmission according to a schedule configured by the management.
- Data transfer using a buffer model or a queue model (Conveyance Policy). For the buffer type, the AR endpoints have a single buffer. Old data will be replaced by new data. For the queue model type, queues at the connection endpoints are used, ordered by a FIFO principle without overwriting of transmitted data.

2.2.13 Bluetooth Architecture

Bluetooth was originally developed for low-cost wireless short range communication with Personal Computers and laptops (e.g. wireless keyboard, mouse) as well as for wireless audio transmission with telecommunication devices such as fixed and mobile phones (e.g. wireless headsets).

The specification was developed by the members of the Bluetooth Special Interest Group. The lower layers (physical layer and MAC layer) were introduced into the IEEE802.15.1 standard. The first

version of the standard can be considered as mature. The number of products for home and office applications increases.

So Bluetooth became interesting also for automation applications in recent years. The physical layer is used by ABB in its Wireless Interface for Sensors and Actors (WISA). An I/O-solution for industrial applications using the Bluetooth Human Machine Interface (HMI) profile is offered by Phoenix Contact.

The standardisation of Bluetooth and IEEE802.15.1 is being continued. E.g. the planed scatter networks (communication between several star topologies) are not standardized yet.

Stack Architecture and Characteristics

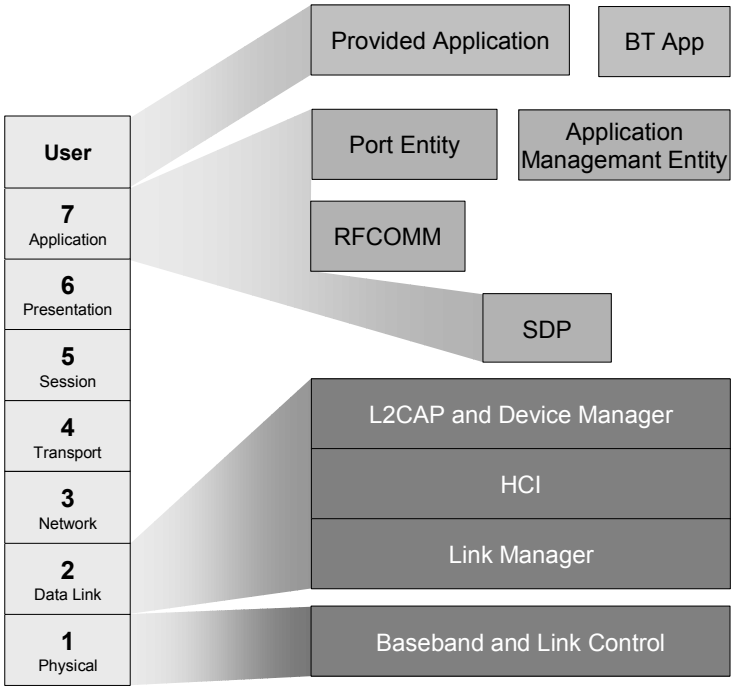

Fig. 2-13: Bluetooth Architecture

The standard IEEE802.15.1 specifies in its physical layer part a Frequency Hopping Spread Spectrum (FHSS) procedure using 79 channels of 1MHz between 2400 MHz and 2483.5 MHz. The frequency channels have to change 1600 times per second which assures a robustness against narrow band users and multipath propagation. On the other hand radio nodes in FHSS systems require a noticeable time to synchronise to the hopping sequence. Depending on the transmission power two classes of devices are possible allowing coverage of up to 10m, respectively up to 100m. However, system which promise greater coverage are known.

Bluetooth defines a star topology (piconet) with one master and up to 7 active slaves. Further slaves may be hold in a stand-by mode to minimise the activation time. Several types of services are provided offering different transmission rates. Asynchronous connections with asymmetric transmission of maximum 723.2 kbps downstream and 57.6 kbps upstream are possible as well as symmetric transmissions of maximum 433.9 kbps downstream and upstream.

The Bluetooth SIG specified security functions to support e.g. data integrity and privacy as well as service discovery functions to support plug and play like behaviour. Furthermore, several application profiles are defined e.g. for LAN access, serial port behaviour, cordless telephony and file transfer.

2.2.14 Wi-Fi Architecture

The Wi-Fi standards (IEEE 802.11x) define lower OSI layers only. As there is no standardized Application layer, these technologies are described in chapter **Chyba! Nenalezen zdroj odkazů.**.

2.2.15 Wireless Interface for Sensors and Actuators (WISA) Architecture

The Wireless Interface for Sensors and Actuators (WISA) is an interesting proprietary solution based on the physical layer of IEEE802.15.1. It was developed mainly by ABB to get a solution for wireless realtime communication between several sensors/actuators and a master station. Included in the concept is a wireless power supply as well. Cordless manufacturing automation is the addressed application area of WISA.

Stack Architecture and Characteristics

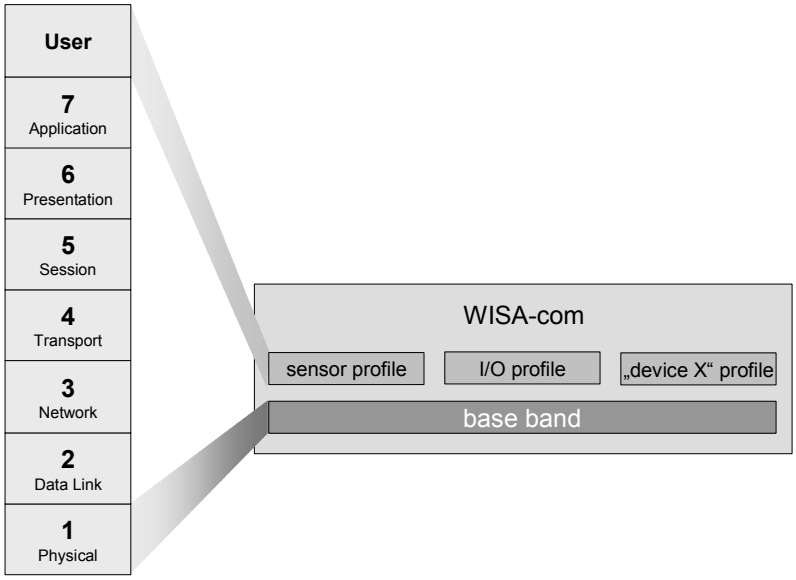

Fig. 2-14: WISA Architecture

Corresponding to the underlying IEEE802.15.1 physical layer the transmission takes place using the frequency hopping spread spectrum (FHSS) schema in the 2,4GHz band. The media access is a tailor-made solution of ABB and combines Frequency Division Multiple Access (FDMA) and Frequency Division Duplex (FDD) with Time Division Multiple Access (TDMA). It allows a high number of devices with a high density using a star topology. Up to 3 master stations in one and the same area providing up to 120 slave stations each are possible. For WISA a maximum message transmission delay of 15 ms is specified.

The power supply concept comprises low power devices, power saving communication protocols and an cordless, electro magnetic power supply.

2.2.16 ZigBee Architecture

ZigBee is a wireless specification targeting low cost, low power and low data rate communication mainly for sensor networks. The intended application area includes building automation (heating, lighting, air-conditioning), remote control units, metering but also toys and industrial control systems.

The physical and link layers the ZigBee technology utilize the IEEE 802.15.4 standard. It defines the protocol and interconnection of devices via radio communication in a personal area networks. The standard uses CSMA/CA access supports both star and peer-to-peer topologies. The media access is contention based; however, time slots for time critical data can be allocated by the PAN coordinator. The IEEE 802.15.4 standard specifies an 868/915 MHz DSSS physical layer and a 2450 MHz DSSS physical layer. The 2450 MHz band supports an over-the-air data rate of 250 kbps, and the 868/915 MHz bands support over-the-air data rates of 20 kbps and 40 kb/s respectively. There are 16 channels in the 2450 MHz band, 10 channels in the 915 MHz band, and 1 channel in the 868 MHz band. In Europe, only the 868 MHz and 2450 MHz shall be used. The 2450 MHz band is the only worldwide band allocated for unlicensed usage without any limitations on applications and transmits duty cycle. It provides up to 1 W transmit power in spread spectrum modes in the United States, up to 100 mW in Europe, and up to 10 mW/MHz in Japan. The 2450 MHz band has been selected as the primary IEEE 802.15.4 band. New physical layer solutions are being developed currently in the IEEE802.15.4a standardisation group, these activities include low speed ultra wide band technology.

Stack Architecture and Characteristics

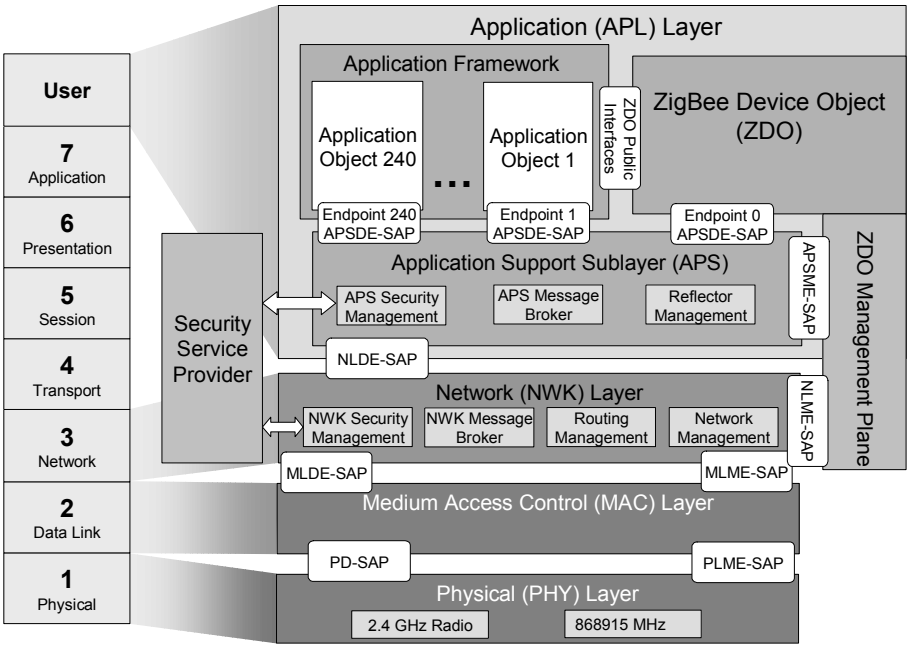

Fig. 2-15: ZigBee Architecture

Above the IEEE 802.15.4 the ZigBee standard defines a network layer (NWK). The responsibility of the NWK layer includes mechanisms to join and leave a network, application of security to frames, routing of frames and inter-device route discovery and maintenance. The ZigBee network layer (NWK) supports star, tree and mesh topologies. In a star topology, the network is controlled by the ZigBee coordinator. The ZigBee coordinator is responsible for initiating and maintaining the devices

on the network. All other devices (end devices), directly communicate with the ZigBee coordinator. In mesh and tree topologies, the ZigBee coordinator is responsible for starting the network and for choosing certain key network parameters, however the network may be extended through the use of so called ZigBee routers. Tree networks may employ beacon-oriented communication.

The ZigBee application layer (APL) consists of Application Support Sublayer (APS), Application Framework (AF) and ZigBee Device Objects (ZDO). The responsibilities of the APS sublayer include maintaining tables for binding and forwarding messages between bound devices. The responsibilities of the ZDO include defining the role of the device within the network (e.g., ZigBee coordinator or end device), initiating and/or responses to binding requests and establishing a secure relationship between networked devices. The ZDO is also responsible for device and service discovery.

Two different device types can participate in the ZigBee network; a full-function device (FFD) and a reduced-function device (RFD). The FFD can operate in three modes serving as a PAN coordinator, a star coordinator (router), or an end device. An RFD is intended for applications that are extremely simple. The RFD can operate as end device only.

The ZigBee standard is suitable for networking of low-power (incl. battery powered) low-cost embedded devices. The standard defines extensive security mechanisms to guarantee suitable security for commercial automation applications.

The major shortcomings are the use of unlicensed ISM band, which is shared with Bluetooth, Wi-Fi and other technologies, and limited range due to high-frequency low power physical layer. The major advantage over other contemporary wireless technologies is support for large wireless networks consisting of hundreds of devices, good security and existence of automation device profiles.

2.2.17 General Packet Radio Service (GPRS) Architecture

GPRS is an additional data bearer service of GSM. It provides packet-switched data transmission within GSM and packet-access to data networks. It also provides effective utilization of the scarce radio resources and is ideally suited for bursty data transmissions. It enables instant, anywhere and anytime-wireless access to IP based networks such as the public Internet and Local Area Networks.

It has been standardised by the ETSI, while the 3GPP has taken over this task now. Several new MAC and PHY layer features have been included to the GSM specifications.

Stack Architecture and Characteristics

GPRS involves overlaying a packet based air interface over the existing circuit switched GSM network. This gives the user an option to use packet-based data services, where GPRS radio resources are used only when users are actually sending or receiving data. FDMA/TDMA multiple access technique is employed. GPRS support nodes (GSN) support the use of GPRS in the GSM core network via the Gn interface and support the GPRS tunnelling protocol. The two key variants of the GSN are the GGSN (Gateway GSN) and the SGSN (Serving GSN). The GPRS Core Network provides mobility management, session management and transport for Internet Protocol packet services. The core network also provides support for other additional functions such as charging and lawful interception. GPRS fully enables Mobile Internet functionality by allowing inter-working between the existing Internet and the new GPRS network. Thus, for a normal user, GPRS looks like any normal IP network and in principle, all IP applications work on top of GPRS. With GSM, data transfer rates around 10 kbps can be achieved, whereas GPRS can cater to data rates of up to 170 kbps. However, in practice, data rates around only 50 kbps have been attained.

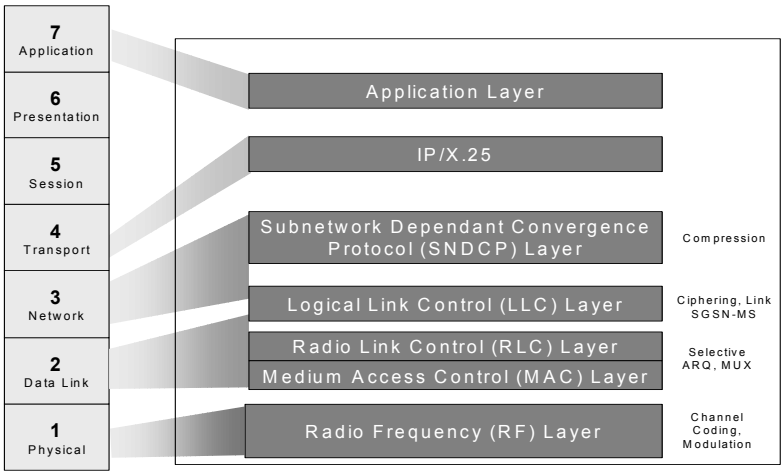

Fig. 2-16: GPRS Architecture

EDGE is introduced within the existing specifications and descriptions rather than by creating new ones. Due to the minor differences between GPRS and EDGE, the impact of EDGE on the existing GSM/GPRS network is limited to the base station system (BSS) only. The base station is affected by the new transceiver unit capable of handling EDGE modulation as well as new software that enables the new protocol for packets over the radio interface in both the base station and the base station controller. The core network does not require any adaptations. Due to this simple upgrade, a network capable of EDGE can be deployed with limited investments and within a short time frame.

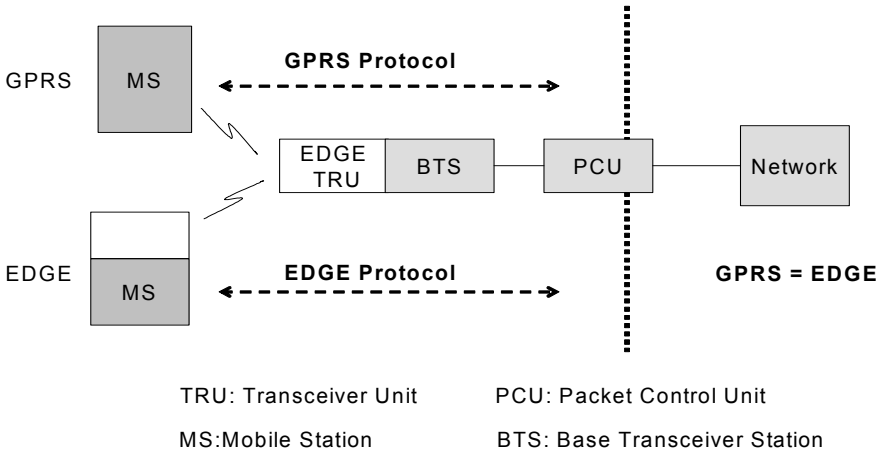

Fig. 2-17: EDGE Architecture: GPRS + changes on BSS

2.3 Conclusion

The architecture of communication technologies for automation application has been optimized with respect to control application requirements. The most of the requirements stem from the need to have deterministic communication, i.e. well defined time-domain properties. Taking advantage of both the high speed data transfers and broad market recognition of standard Ethernet the automation world has adopted Ethernet in the form of so called industrial Ethernet. Ethernet based industrial communication solutions enable easy co-existence of time-critical and non-critical (best effort) data transfers. However, to enable such co-existence while guaranteeing real-time behaviour, the industrial Ethernet communication stack shows significant differences from the office Ethernet. The stochastic media access method (CSMA) of standard Ethernet has to be eliminated for the time-critical data. Various solutions have been developed, however most of these solutions more or less adhere to protocol architecture shown in the simplified figure below.

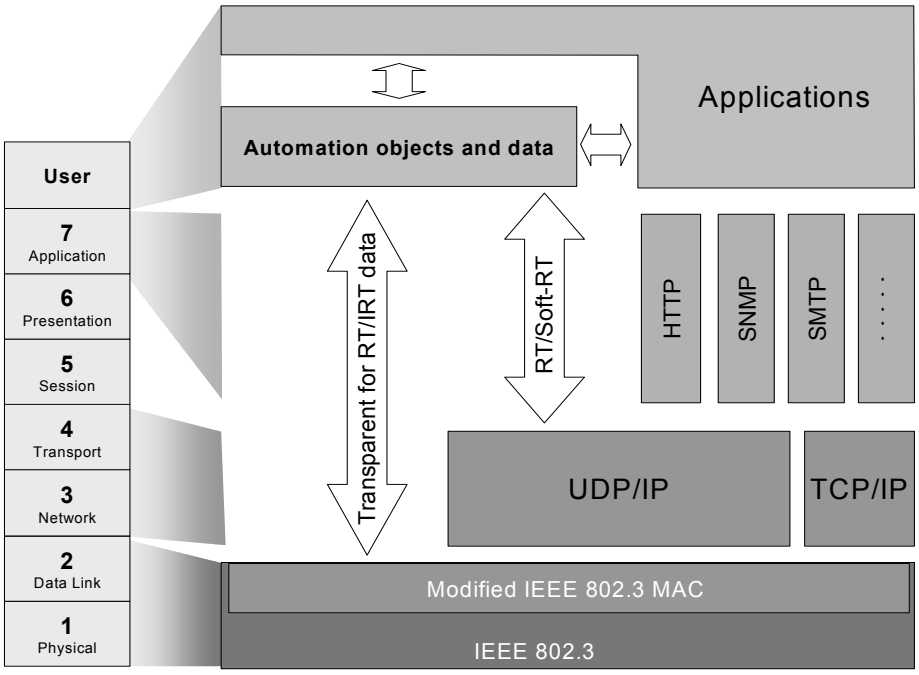

Fig. 2-18: Architecture

Hard real-time and isochronous real time communication requires modified IEEE 802.3 MAC to realize deterministic or isochronous media access. Moreover, the time-critical communication is based on IEEE 802.3 frames only and does not utilize the IP/UDP/TCP stack at all. Less time-critical communication may use UDP/IP stack for automation data too, however the real-time is guaranteed only within single LAN, where all the active network devices either support the modified IEEE 802.3 MAC or use only IEEE 802.3 PHY (e.g. HUBs).

The wireless commercial and industrial solutions follow totally different principles and philosophies, the wireless physical layer has consequences at the upper layers. For this the wireless protocol stacks enormously differ form the wired ones as there are, among other, huge differences induced by unmatched flexible topologies of wireless networks. Integration of wired and wireless communications for automation application will be extremely challenging as there are heterogeneities not only at the application layer. There are principal differences at all the layers.

3 Wireless Technologies

3.1 Introduction

3.1.1 Motivation

The main idea for the use of radio communication is the same as in home and office applications which is the benefit of mobility and the saving of costs for installing the communication infrastructure. The financial outcome is remarkable e.g. if otherwise an automation concept cannot be implemented. For example, in mobile robotic systems, autonomy is growing and multi robot systems and co-ordination with unmanned air vehicles is becoming a reality. Thus, transmission links capable of monitoring the behaviour of all the robots and transferring the video taken by observation systems are certainly required. As traditional hertzian spectrums and frequencies are nearly full, wireless technologies and multiplex provided by these ways can offer an alternative to this crucial problem in developing cooperation between robots and coordination with manned vehicles.

This is a reason why the turnover with wireless components in automation increases significantly. The turnover was 117 Million US$ in 2002 in Europe. For 2006, a turnover of 422 Million US$ is forecasted. The growth rate will be increased from 28.2 % to 50.6 %. However, a progress in standardisation for automation applications was mentioned as an important precondition. The intention of the proposed project is to contribute to a standardised integration of radio implementations into the whole lifecycle of automation software systems.

Automation device and system manufacturers as well as manufacturers of radio components will benefit from the results of the project.

The comprehensive approach of the project ensures that radio implementations are no longer expensive special solutions without any relation to automation systems but integrated parts of them.

The idea of this proposal has been supported by a number of companies which are active in the working group (FA5.21) of the German VDI/VDE society for measurement and automation (GMA) which deals with radio communication in automation. Even if they are not directly involved in the proposed project they are very interested to use the results in future product concepts.

The foundation of the Wireless Industrial Network Alliance in the United States in 2003, with objectives similar to that of the mentioned working group in Germany, emphasises the relevance of the above described activities.

To assure the market position in particular for small and medium enterprises in Europe, the above mentioned goals have to be met. The planned formal description of the methods and models is a suitable measure for ongoing standardisation activities.

Consortium members are active in a number of relevant working groups which deal with radio communication and industrial communication e.g. the Institute of Electrical and Electronics Engineers (IEEE), the International Electrotechnical Commission (IEC), the Zentralverband der Elektrotechnik und Elektronikindustrie (ZVEI), the German Commission for Electrical, Electronic and Information

Technologies of DIN, and VDE (DKE) the German VDI/VDE-Society. Regular contact with these panels increases the acceptance of the latest standardisation followed in this area.

3.1.2 Integration of Wireless Technologies into Embedded Automation Components

3.1.2.1 Different Views on the Integration of Radio Based Communication

Automation systems are more and more determined by software. More capable microcontrollers and matured communication technologies allow one to adapt the architecture of automation systems to the architecture of production systems even better. This development results in distributed automation systems, which represent software-intensive distributed systems consisting of devices/components which are embedded systems. A new quality of this development is initiated by the demand for more flexible production systems as well as by the demand to integrate mobile and movable parts of the production system. Adequate solutions for such kinds of automation systems are based on wireless communication. That is why the interest in radio based communication in industrial automation is growing. The developments in the field of digital radio communication (mobile communication, wireless LAN, Bluetooth, short range devices) offer interesting features. However, the specific requirements of industrial automation do not belong to the design criteria of these technologies.

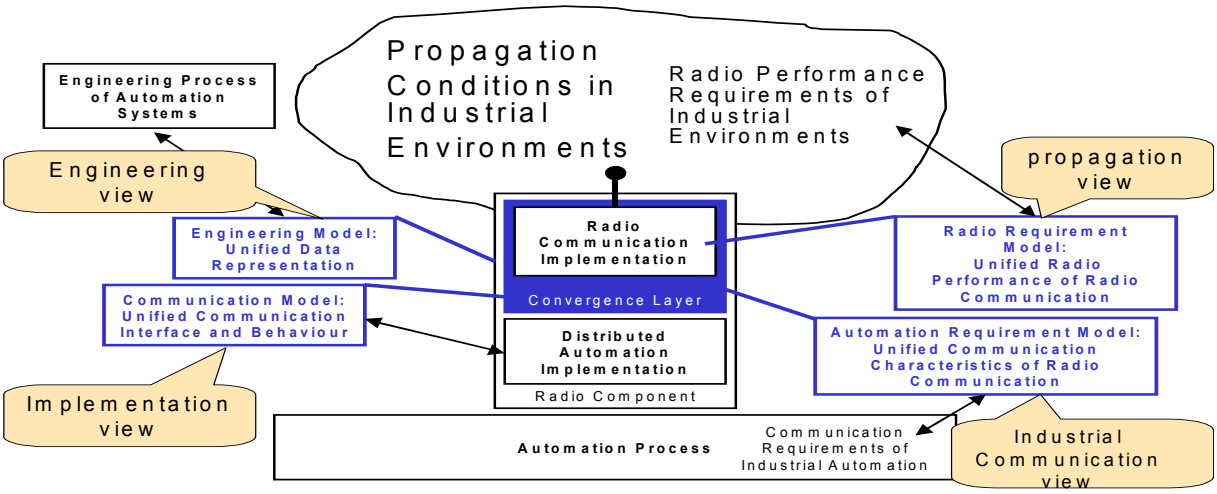

Fig. 3-1: Different Views.

Thus, the manufacturers of automation components and systems as well as system integrators are responsible for the integration of available radio implementations into automation components and systems. Fig. 3-1 illustrates the different perspectives of the integration of radio based communication software into industrial automation systems focussing on a single distributed component. It is obvious that the problem in an entire distributed automation system with gateways between wired and wireless communication systems is much more complex.

The largest effort requires a connection between the automation software and software, and firmware modules of the radio systems.

3.1.2.2 Integration of Radio Technology into Automation

Subject of these activities is the development of an unified communications software for different radio communication technologies and its integration into the lifecycle of Distributed Automation software systems. This unified communication software (allocated to a specific “Convergence Layer”) will enable the integration of different radio communication components into automation components running in a Distributed Automation software system (Fig. 3-2).

The integration has to take into consideration the various influences as there are propagation conditions, specific industrial communication requirements (real-time, safety, security), implementation conditions (i.e. limited resources), and engineering aspects.

The main goal is the development of a methodical and technical basis to support the integration. This includes:

- an automation requirement model which covers the automation system oriented description to be able to evaluate radio communication implementations according to the specific communication requirements of industrial communication;
- a software integration model of a convergence layer which covers the specialities of different radio communication implementations and provides a unified interface to the automation application software;
- a software engineering model which covers the specialities of different radio communication implementations and provides a unified interface to the engineering of automation application software.

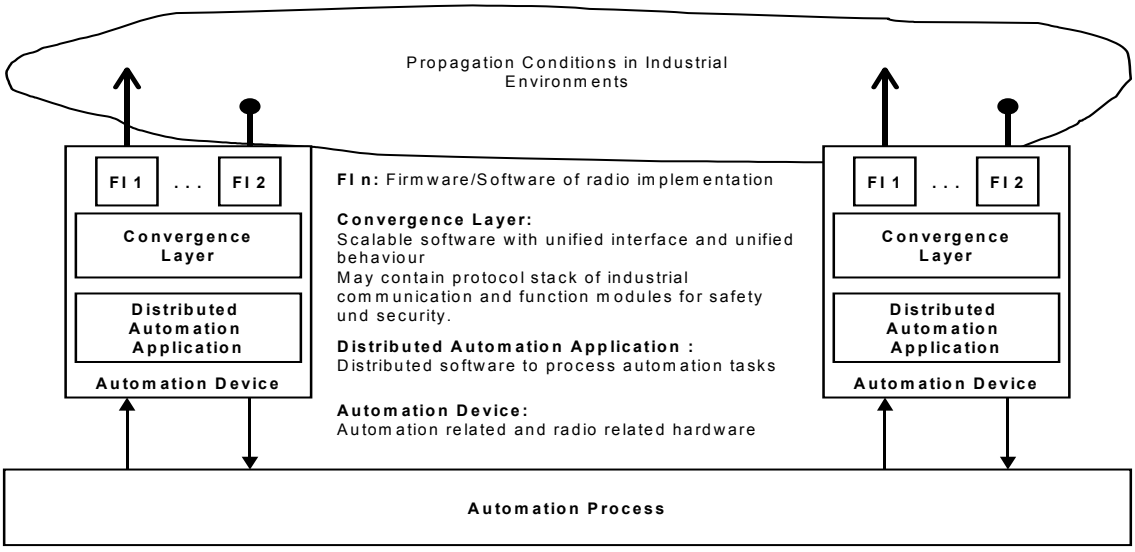

Fig. 3-2: Position of the Convergence Layer within Automation Applications.

The implementation of the intended methods and models is the precondition to select an appropriate radio communication target driven and based on facts. Independent of the radio technology (e.g. Bluetooth, DECT, GSM, SRD, UMTS, WiMAX, WLAN, ZigBee, UWB), the integration into automation systems can be achieved quickly without remarkable efforts. The convergence layer implementation will consist of modules, which contain functions important for industrial automation (e.g. considering safety, security or QoS requirements) and will be adjusted to the radio communication. Therewith,

scalable software is available to meet the requirements of automation systems (incl. engineering) and radio communication.

For automation devices and system manufacturers (e.g. ABB, Siemens, Schneider), the effort to integrate radio implementations into distributed automation system software will be decreased. On one hand, the choice of the suitable radio technology or radio implementation will become more transparent. The automation requirement model enables a comparison of radio implementations concerning the usage in automation. On the other hand, the integration of radio implementations into automation devices, which are software dominated and part of distributed automation software, will become easier. Because of the software integration model, special adaptations by the manufacturer are no longer necessary if different applications require different radio technologies. But also in the light of rapidly developing radio implementations (short innovation cycles) without respect to automation applications, the software integration model is necessary to save investments in automation software. The automation software may be kept unchanged even if a new generation of radio implementations arises. Furthermore, the type of interface is no longer a criterion of decision but the characteristics of the radio technology or implementation. Therefore automation devices, which provide mobility and flexibility to automation systems, can be offered with lower costs. Furthermore, the software engineering model enables the integration of radio implementations into the entire lifecycle of distributed automation software systems including design, configuration, commissioning, maintenance, and diagnosis. This contributes to a remarkable growing of productivity.

The project results open up a new market for radio component manufacturers: the market of automation applications. On one hand, they will get a clear picture on the requirements in distributed automation systems. The requirement model shows which information must be provided by the automation device, by the system manufacturer, and in which form. Based on the software integration model, the convergence layer may be implemented in a goal-oriented way and completely tested. Time-consuming adaptations are not necessary any more. On the other hand, special tools for commissioning and maintenance are not necessary. The software engineering model ensures that tools of the automation area can be used.

Software integration models and software engineering models contribute to the growing productivity concerning the ability of configuration and scalability of software in distributed automation systems.

3.1.2.3 Connection to Communication Systems in the Automation Domain

Fieldbus Systems

Legacy fieldbus systems are broad distributed over the world and used in many applications of the Industrial Automation. There are approximately 25 Million nodes in use headed by PROFIBUS (12 Mio) and Interbus (7 Mio.). Thus, it should be very important to bridge the gap between the wireless and the wired technologies by specific network components or by integration of wireless components into the fieldbus-enabled automation devices.

The following fieldbus systems will come into question for deeper investigation:

- PROFIBUS
- Interbus
- DeviceNet
- CANopen
- Hart

- CCLink

Ethernet-based Communication Systems

Nowadays much effort is directed to introduce the Ethernet-based transmission technologies into the field area/real-time domain. Main examples are:

- PROFINET IO
- IDA Modbus
- EtherNet/IP

Thus, it should be very important to bridge the gap between the wireless and the wired technologies by specific network components or by integration of wireless components into the Ethernet-enabled automation devices. The above-mentioned Ethernet-based systems will come into question for deeper investigation and an interesting topic would be transmission of Switched Ethernet via wireless components.

3.1.3 Specific Properties of Wireless Devices/Systems

3.1.3.1 Specific QoS Requirements

Since there is an economic interest to widely introduce the radio-based technologies, the inventors have to guarantee that the automation domain-specific requirements can be fulfilled.

3.1.3.2 Real-time

There are different levels of real-time behaviour within a network used in the automation domain depending on the level of the enterprise network. In contrast to a high priority of stream transmission, in the industrial automation application the data packet transmission has to have the highest priority

The usage of wireless wide area networks within the automation domain has to be investigated just as the uninterrupted commercial availability.

In the local area, the wired communication systems fulfil the requirements of all the real-time classes, mostly implemented in specific devices for each class. The specific properties of a radio channel limit the ability to use wireless devices in a few hard real-time applications.

3.1.3.3 Safety

There is a need to meet defined Safety Integrity Levels (SIL, see IEC 61508), e.g. Residual Error Probability <= 10^{-7} errors/h for SIL 3. The communication part requires a residual error probability of <= 10^{-9} errors/h for SIL 3 (1% of 10-7; the other 99% is required for sensors, PLCs, and actuators etc.).

The background has to be mapped to Wireless Networks. Investigations are necessary on how wireless networks can be extended for the transfer of safety-related data in automation systems.

Investigations are also necessary on how to enable a radio communication channel for high safety level and high availability. Desired results are mapping of safety layers of wired fieldbus systems on the wireless automation devices.

3.1.3.4 Security

Today's automation islands are relatively secure against attacks. In the case of Internet and wireless communication usage, the attack probability is growing.

3.1.3.5 Location Awareness

The usage of Information Technologies within the life cycle of an automation system is becoming broader. The engineering in the various phases (design, development, manufacturing and commissioning of automation devices and systems, maintenance of the system) is becoming more efficient using formal methods to develop information models and description languages (describing the features of the components for all the mentioned phases) and computer aided wireless tools to handle these features. An important requirement is a context-sensitive offer of the needed information at these tools. Since the needed database is distributed through the decentralised automation system (connected by the heterogeneous network) it also requires location-based services. The recent approaches use web technologies to organise access to the remote data. Since the remote access raises the probability of attacks to the system, the security becomes more important. Additionally, a unified data structure describing the features of the installed devices has to be standardised. At the moment, there are various profiles in the fieldbus domain. These profiles have to be mapped to the heterogeneous networks.

3.1.3.6 Available Frequencies

The use of frequencies for wireless communications in industrial automation focuses on non-specific Short Range Devices (SRD). The use of frequencies by SRD is not fixed to a certain technical standard. Table 3-1 depicts the allowed frequency bandwidths and their parameters.

Frequency in MHz	Max. Channel Bandwidth / Channel Raster in kHz	Max. Equivalent Emitted Radio Power (ERP) / Max. Magnetic Field Strength	Relative Frequency Using Time
c) 26.957-27.283	No limitations	42 dB A/m in a distance of 10 m or 10 mW	No limitations
d) 40.660-40.700	No limitations	10 mW	No limitations
e) 433.050-434.790	No limitations	10 mW	No limitations
f) 868.000 - 868.600	No limitations	25 mW	< 1.0 %
g) 868.700 - 869.200	No limitations	25 mW	< 0.1 %
h) 869.300 - 869.400	25	10 mW	No limitations
i) 869.400 - 869.650	25	500 mW	< 10 %
j) 869.700 - 870.000	No limitations	5 mW	No limitations
k) 2400-2483.5	No limitations	10 mW	No limitations
l) 5725-5875	No limitations	25 mW	No limitations

Table 3-1: Available frequencies

These frequencies can also be used by other wireless applications, e.g. for RFIDs, ISM applications, and WLAN applications. There is no guaranty for a minimum quality of the radio transmission.

Nowadays, the frequencies in the range 433.05 ... 434.79 MHz, 868 ... 870 MHz and 2400 ... 2483.5 MHz are preferably used. The Ultra Wide Band technology (UWB) uses very large bandwidths (500 MHz and above).

3.2 Selected Wireless Technologies

The following technologies represent the state-of-the-art in wireless communication technologies. The introduced technologies may have appeared in the chapter *Architecture.* However, this chapter stresses the pertinent properties and solutions of these technologies.

3.2.1 Lower Layer Standards

3.2.1.1 Wireless Local Area Networks (WLAN - IEEE802.11)

Wi-Fi (Wireless Fidelity)

- Target: wireless access to the Internet without technical problems.
- Focus: home and office communications, up to now: no interest in industrial domain.
- Lower Layers: standards family IEEE 802.11. Basic Requirement/Precondition: Interoperability of radio components. Wi-Fi Alliance will guarantee the interoperability by rigid certification.
- Higher layers: Internet protocols.
- Status: certification of home and office products is now state-of-the-art.

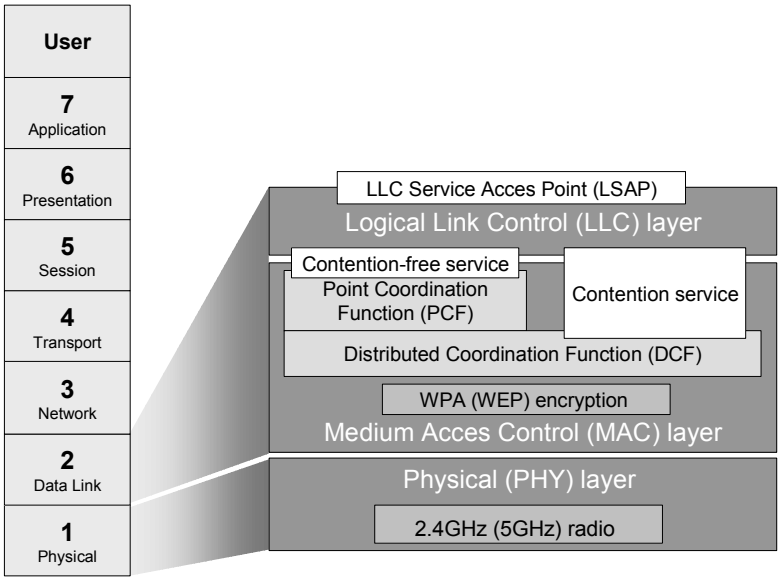

Fig. 3-3: WLAN Architecture

A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wired networks (which use IEEE 802.3 or Ethernet). Wi-Fi networks operate in the ISM bands (2.4GHz, 5GHz), offer speeds up to 54Mbps (IEEE 802.11g standard), and has support for QoS (Quality of Service) with managed levels for data, voice, and video applications (IEEE 802.11e standard). The

access to a medium is stochastic, based on the CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) principle.

Wi-Fi networks support two modes – “Ad Hoc” and “Infrastructure”. The ad hoc mode allows stations to spontaneously form a wireless LAN, i.e. all stations communicate directly with each other in a peer-to-peer manner. In the infrastructure mode, the network consists of an Access Point (AP), with each client communicating through it. Thus, the AP can coordinate access to a shared medium among all stations and can ensure a support for QoS.

Wi-Fi networks provide support for a Wi-Fi Protected Access (WPA2) security technology, which is a replacement of a less secure Wired Equivalent Privacy (WEP).

An AP built into a typical Wi-Fi router might have a range of 45m indoors and 90m outdoors.

The Wi-Fi technology is still under development. It is supposed that a new standard, which can offer speeds up to 100Mbps, will be adopted in 2006 [WiFiAlnc].

IEEE 802.11.a

- Up to 54 Mbps
- 5150 ... 5350 MHz, 5470 ... 5725 MHz
- Modulation: Orthogonal Frequency Division Multiplexing (OFDM)
- Range: max. 50 m
- Additional amendments: IEEE 802.11h

IEEE 802.11.b

- 11 Mbps
- 2400 ... 2483.5 MHz
- Modulation: DSSS
- Physical Layer interoperable with all 802.11 standard devices
- better Signal to Noise Ration (SNR)
- Max. 50 m (indoor)
- Max. 3 independent channels with 22 MHz bandwidth each

IEEE 802.11.g

- 54 Mbps
- Modulation: OFDM, Complimentary Code Keying (CCK), Packet Binary Convolution Coding (PBCC)

3.2.1.2 Wireless Personal Area Networks (WPAN - IEEE 802.15)

IEEE 802.15.1

- Physical Layer and Data Link Layer standards of Bluetooth Spec. 1.1

- 2400 ... 2483.5 MHz
- Modulation: Frequency Hopping Spread Spectrum (FHSS) using 80 channels with 1 MHz each
- Synchronisation delay for new devices

IEEE 802.15.3

- High data rates, min. 20 Mbps
- 2400 ... 2483.5 MHz, in discussion: 57 ... 64 GHz
- Physical layer for UWB (also 802.15.3a)
- In discussion: alternative Physical Layer

IEEE 802.15.4

- Physical Layer and Data Link Layer for ZigBee
- Low data rates: 20 kbps, 40 kbps, 250 kbps
- Frequencies: 868 ... 868.6 MHz (Europe), 902 ... 929 MHz (USA), 2444 ... 2483.5 MHz

IEEE802.15.4a

- Physical Layer and Data Link Layer for nanoNET
- 2.45 GHz ISM band, 80 MHz Bandwidth
- Modulation: Chirp Spread Spectrum
- Up to 2 Mbps data rate over 60 m indoors
- Max. 800 m outdoor
- Low Power Consumption
- Receiver sensitivity: -92 dBm @ BER=10-3
- Media access: CSMA/CA and TDMA
- Higher Layer Implementations available

3.2.1.3 Wireless Metropolitan Area Networks (WMAN, MBWA)

IEEE 802.16

Wireless Metropolitan Area Network

- Small range transmission: last mile between user and broadband networks, world-wide wireless access to broadband networks
- Frequencies: 3.4 ... 3.6 GHz, 5725 ... 5850 GHz, 25 ... 2690 GHz,
- Data rate: target: 70 Mbps over 50 km, realistic: 20 Mbps over 600 m,
- Status: IEEE 802.16 and 802.16.2 available, standardisation has not been finished, no products yet in the market.

WiMAX

Worldwide Interoperability for Microwave Access: Synonym of IEEE 802.16

- Target of the WiMAX Forum:
  - Conformance of radio components with IEEE 802.16 standard;
  - Interoperability of the radio components.
- Status: test specifications under development, WiMAX components for Laptops: announced for 2006, problems: high costs

WiMAX, commonly known as the IEEE 802.16 standard, is a wireless metropolitan area network (MAN) capable of providing a wireless alternative to cabled networks for last mile point-to-multipoint broadband access and connecting 802.11 hotspots to the Internet. It can provide a service area range of up to 50 kilometers, has cost and time advantages compared to cabled equivalents, and is designed for latency-sensitive video and voice services. WiMAX forum focuses on creating a single interoperable standard from IEEE 802.16 and ETSI HiperMAN standards, with a non-optional MAC structured to support multiple PHY specifications. System profiles in 2.4 GHz, 5.8 GHz unlicensed bands and 2.5 GHz, 3.5 GHz licensed bands are planned [EMSW02].

Physical (PHY) and media access control (MAC) layers form the main constituents of the air interface. The IEEE 802.16 standard considers a common MAC layer combined with PHY specifications depending on the spectrum in use. Protocol layering is as shown in the Fig. 3-4.

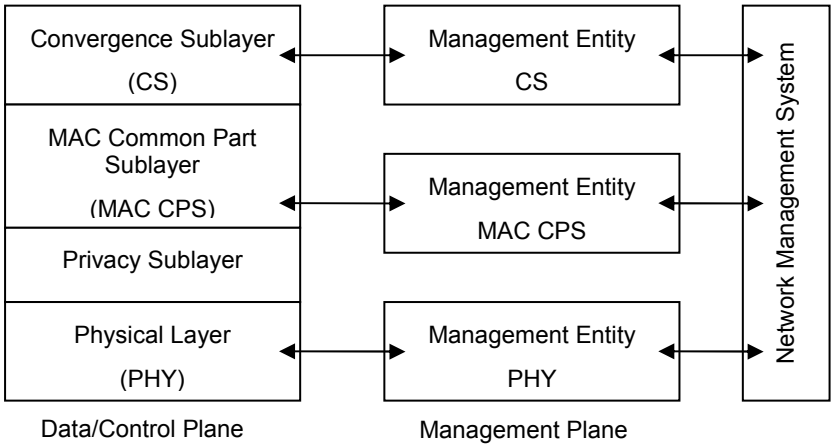

Fig. 3-4: IEEE 802.16 Protocol Layers

The original 802.16 specification, completed in December 2001, is designed for the 10-66 GHz range (short wavelength) fixed-mode operation, where multi-path is negligible and line-of-sight (LOS) is necessary. Channels are typically 25-28 MHz wide and data rates are in the range of 120 Mbps, making it suitable for small-office-home-office (SOHO) applications.

The IEEE 802.16a standard, approved for the 2-11 GHz range in January 2003, provides broadband wireless access (BWA) to fixed, portable and nomadic devices, without needing direct LOS with the base station. Major changes to the PHY layer with the inclusion of OFDM, and significant enhancements to the MAC layer have been carried out, along with an optional Mesh topology enhancement to the MAC. Enhanced features such as advanced power management techniques, interference mitigation/coexistence and multiple antennas have been added. Data rates of up to 268

Mbps per base station are achievable, making it possible to support hundreds of businesses and thousands of homes with T1 and DSL type connectivity respectively.

In general, the MAC supports a point-to-multipoint architecture with a central base station (BS) handling multiple independent sectors simultaneously. On the downlink (BS to SS), TDM is used for data transfer, whereas TDMA is used on the uplink. An advanced radio-link control (RLC) layer is also included to manage PHY transitions from one burst profile to another, along with the traditional power control and ranging functionalities.

Unlike no QoS support in 802.11 standards (with CSMA/CA MAC), 802.16 has QoS built into its dynamic TDMA-based MAC. The 802.16 PHY uses a 256 FFT vs. 64 FFT used by 802.11 and the channel sizes are flexible in 1.5-20 MHz range, unlike the 20 MHz fixed channels in 802.11.

On the data rates front, the IEEE 802.16 was originally designed for a bit rate of 5 bps/Hz with peak rates up to 100 Mbps in a 20 MHz channel. Compared with IEEE 802.11 Wi-Fi's bit rate of 2.7 bps/Hz (54 Mbps in a 20 MHz channel), this is a big leap forward, which has been made possible by an enhanced air interface design. The 802.16a is capable of providing an average performance of 70 Mbps in a single RF channel, with peak rates of up to 268 Mbps in a range up to 50 km, made possible by the spectral efficiency of OFDM.

ETSI HiperMAN is the European MAN standard being developed by ETSI. It shares the same PHY and MAC with the IEEE 802.16a, making it possible to have a single global wireless MAN standard, as being planned by the WiMAX Forum [WiMAXFrm].

IEEE 802.20

Mobile Broadband Wireless Access (MBWA)

- large range: mobile access to broadband networks (allowed distance: 15 km, allowed set of nodes: 250 km/h)
- Data rate: min. 1 Mbps
- Status: standardisation has not been finished, no products

3.2.2 Wireless Telecommunication Standards

3.2.2.1 GSM (Global System for Mobile Communications)

An ETSI Standard for Mobile Radio Communication Systems (Mobile communication standard of the 2nd generation)

- Frequencies: 900 MHz, 1800 MHz in Europe; 1900 MHz in Northern America
- TDMA – Time Division Multiple Access
- Data Rate: max. 9.6 kbps

3.2.2.2 GPRS (General Packet Radio Service)

- Packet-oriented
- Data Transmission with Channel Grouping
- Data rate: 53.6 kbps, not available all the time

GPRS uses packet switched resource allocation, in which resources are allocated only when data is to be sent or received. It incorporates flexible channel allocation mechanism in which 1 to 8 time slots can be allotted to a user. Active users share the available resources. Uplink and downlink channels are reserved separately. Also, GPRS and circuit switched GSM services can use the same time slots alternatively [Hei99].

Typical applications of GPRS include standard data-network-protocol based applications such as WWW, FTP, Telnet, conventional TCP/IP and X.25 based applications, P2P applications such as toll road system, train control system and P2M applications such as weather and road traffic info, news and fleet management. It also supports web browsing, E-mail, WAP, E commerce and many more.

3.2.2.3 EDGE (Enhanced Data Rates for GSM Evolution)

EDGE is a radio based high-speed mobile data standard. It is the next step in the evolution of GSM and IS-136 technologies. The objective of the new technology is to increase data transmission rates and spectrum efficiency and to facilitate new applications and increased capacity for mobile use.

EDGE can be introduced in two ways, either as a packet-switched enhancement for general GPRS, known as EGPRS, or as a circuit-switched data enhancement called enhanced circuit-switched data (ECSD). It is capable of offering data rates of 384 kbps, and beyond. With EDGE, operators can deliver multimedia and other broadband applications to mobile phones. A new modulation technique and error-tolerant transmission methods, combined with improved link adaptation mechanisms, make these EDGE rates possible. This is the key to increased spectrum efficiency and enhanced applications, such as wireless Internet access, e-mail and file transfers. The data speeds provided by the various coding schemes of EDGE reduce as the distance from the base station increases. Therefore, the existing network structure has an impact on the economic viability of EDGE. The larger cells found in rural areas provide more opportunity for greater variations in transmission rates, while indoor environments, where signal strength is less predictable, also pose a problem.

In addition to GMSK (Gaussian minimum-shift keying), EDGE uses 8-PSK (8 Phase Shift Keying), as illustrated in Fig. 3-5 below, for its upper five of the nine modulation and coding schemes. EDGE produces a 3-bit word for every change in carrier phase. This effectively triples the gross data rate offered by GSM. EDGE, like GPRS, uses a rate adaptation algorithm that adapts the modulation and coding scheme (MCS) used to determine the quality of the radio channel, and thus the bit rate, and robustness of data transmission. It introduces a new technology not found in GPRS, called incremental redundancy, which, instead of retransmitting disturbed packets, sends more redundancy information to be combined in the receiver, thus increasing the probability of correct decoding.

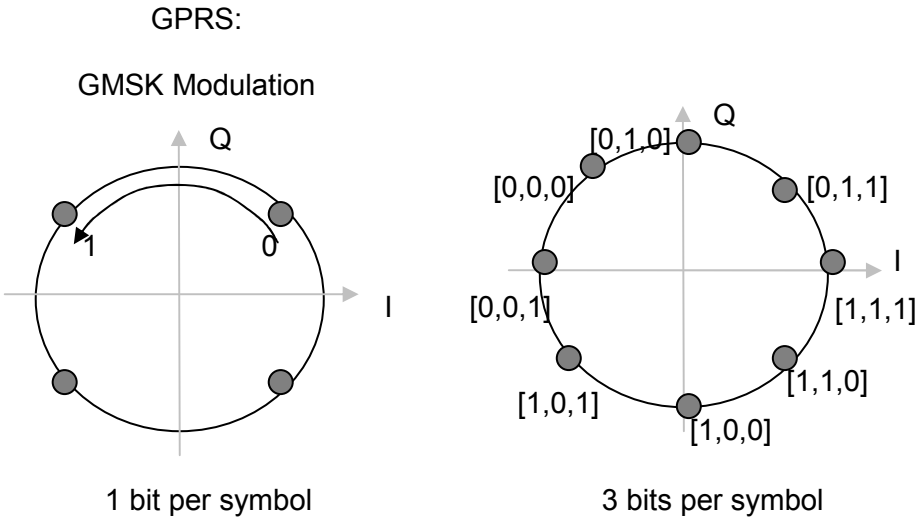

Fig. 3-5: I/Q diagram depicting benefits of EDGE modulation.

The next evolutionary step for the GSM/EDGE cellular system includes enhancements of service provisioning for the packet-switched domain and increased alignment with the service provisioning in UMTS/UTRAN (UMTS terrestrial radio access network). These enhancements are currently being specified for the coming releases of the 3GPP standard. Based on EDGE high-speed transmission techniques combined with enhancements to the GPRS radio link interface, GERAN will provide improved support for all the QoS classes defined for UMTS: interactive, background, streaming and conversational. By doing so, a new range of applications, including IP multimedia applications, are likely to be adequately supported.

3.2.2.4 UMTS (Universal Mobile Telecommunications)

- large bandwidth,
- CDMA access method
- Data rates:
  - 144 Kbps for mobile user (max. speed: 500 km/h)
  - 384 Kbps with limited mobility in macro and micro-cellular suburban outdoor environments, at a maximum speed of 120 km/h
- 2 Mbps for quasi-stationary operation
- Status:
  - Influence of the Standards IEEE 802.16 (WiMAX) and IEEE 802.20 on the market penetration of UMTS products is unclear
  - The UMTS products will displace the GSM, GPRS, HSCSD products regarding data transmission possibly within the next ten years

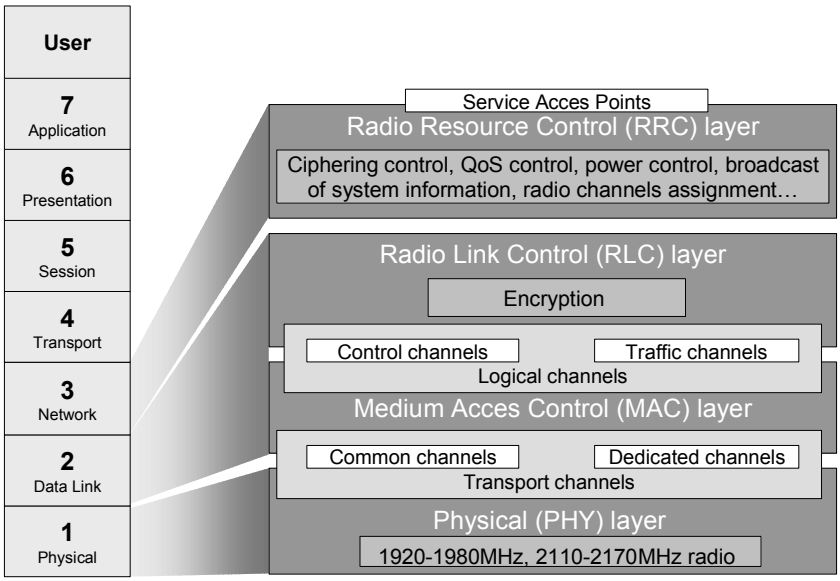

Fig. 3-6: UMTS Architecture

UMTS is a 3G mobile communication technology based on Wideband Code Division Multiple Access (WCDMA), and Time Division CDMA (TD-CDMA) technology. The technology offers high throughput, real-time services, and end-to-end QoS, and is designed to deliver pictures, graphics, video communications, and other multimedia information as well as voice and data to mobile wireless subscribers [3GPPSpec].

The UMTS technology supports authentication of UE, and 128-bit ciphering.

The technology suffers from high costs and lack of any significant consumer demand.

3.2.2.5 DECT (Cordless Phones)

Digital Enhanced Cordless Telecommunications (DECT): Standard of the European Telecommunications Standards Institute (ETSI) dealing with the air interface of cordless telephones.

- Point-to-point connection between a Fixed Port (FP) and a Portable Port (PP) using a combined Frequency Multiplex and Time Multiplex method
- 24 time slots: the first 12 for the transmission of FP to PP (downlink), the second 12 for transmission in the opposite direction (uplink)
- Data safeguarding by Cyclic Redundancy Check (CRC), Forward Error Correction (FEC) and Automatic Repeat Request (ARQ)
- Frequencies: 1.88 GHz till 1.90 GHz
- Sender Performance: 250 mW
- distances: 50 m (indoor), 300 m (outdoor)
- Higher data rate: using DECT Packet Radio Service (DPRS):
    - Using 23 of the 24 slots on a middle frequency are available: 552 Kbps net in one direction

  - Using the DQPSK Modulation than the net data rate can be increased to 1.3 Mbps
  - Using D8PSK Modulation the net data rate can be increased to 2 Mbps
- Status:
  - Broad use of products, mostly in the home and office domain, but also in the industrial domain (limited use)
  - Long-term, survey-able technology

3.3 Conclusion

Common wireless communication standards designed for commercial application do not define any automation application layer. These standards can be used as a communication channel for VAN automation data. As these wireless standards have been designed for commercial applications, the automation specific aspects are not addressed within these standards.

Safety over wireless links has to be extensively studied within WP5. At present there exists very few information regarding functional safety over wireless links. The major challenge in this field represents the fact that the safety system must not excessively activate the safety function (because of some RF interference) and at the same time the probability of “failure on demand” has to be provably kept within defined limits.

Some of the wireless standards define Quality of Services (QoS), however for automation purposes more detailed information regarding real-time properties is needed. To guarantee applicability in hard-real time automation applications common metrics for wired and wireless communication have to be defined. To be able to achieve homogeneous integration of wireless and wired channels within VAN, the real-time performance and reliability of wireless links has to be studied in more detail. Within WP4 a common metrics for definition real time properties of a communication links shall be developed. Within the WP3 the metrics have to be evaluated and applicable wireless standards have to be investigated as for the chosen metrics.

Each of the wireless standards is predestined to different kinds of applications and application areas. However to enable integration of wireless standards within single VAN platform, the wireless technologies have to be investigated from the automation perspective in more detail using single methodology for all communication standards.

4 Real Time Technologies

4.1 Introduction

4.1.1 Motivation

Industrial communication systems must be able to satisfy very strict demands, since a misdemeanour of the communication system can lead to a malfunction of the complete production system and by this to high economical loss in form of downtimes or even mechanical collisions and destructions up to personal injuries. The following chapters will give a general overview and idea about what has to be understood under (industrial) real-time and then offer a deeper insight into the real-time aspects and methods of industrial Ethernet. Industrial Ethernet was chosen as wireless technologies today are not able to fulfil real-time requirements in an industrial sense and correspondingly there does not exist any content to be written down here; most of the conventional fieldbuses are phase-out models in industrial environments (due to the latest developments in Ethernet technology) and correspondingly need not to be described in detail in a future oriented research project as VAN either.

4.1.2 Real Time Capability - What is Real Time?

First it will be clarified what real time capability comprehends and which different real time capabilities can be classified in general; a second step comprises special aspects of process industry.

4.1.2.1 General Aspects

If a system is able to react under all operating conditions to all events correctly and within the expected time constraints, then it is real time capable. Accordingly, if a communication system meets all time requirements for data exchange of the components of a certain application, it is – related to this application – real time capable.

Determinism is a word that is very closely linked to real time capability. Determinism describes the exact predictability of a system's time behaviour. If it is possible to exactly predict the temporal behaviour of a system in all of its states, then the system is strictly deterministic.

On principle real time demands can be distinguished into two categories. The first category merely requires a maximum time (deadline) until an action has to be executed and completed. This is the requirement for "timeliness". The second one requires a certain specified time or time grid at which an action or co-ordinated actions has/have to be completed – in the latter case it is also a fault, when the action is completed earlier, this is the requirement for "synchronisation". The deviation that can be tolerated in this context is called "jitter". Formally, such time-constraints can be represented by the use of time/utility functions. Time/utility functions express the utility of executing and completing a certain action as a function of the point of time when the action is executed and completed. The utility values express the relative importance of an action.

According to Douglas Jensen´s Time/Utility Function Model of real time the first category timeliness implies that the utility of completing an action is fully given (value 1) from time zero until a certain

deadline. The other category synchronisation implies, that the utility of executing an action is only given within a small window of time around an allocated execution time (deadline). The time window is determined by the acceptable jitter of the deadline.

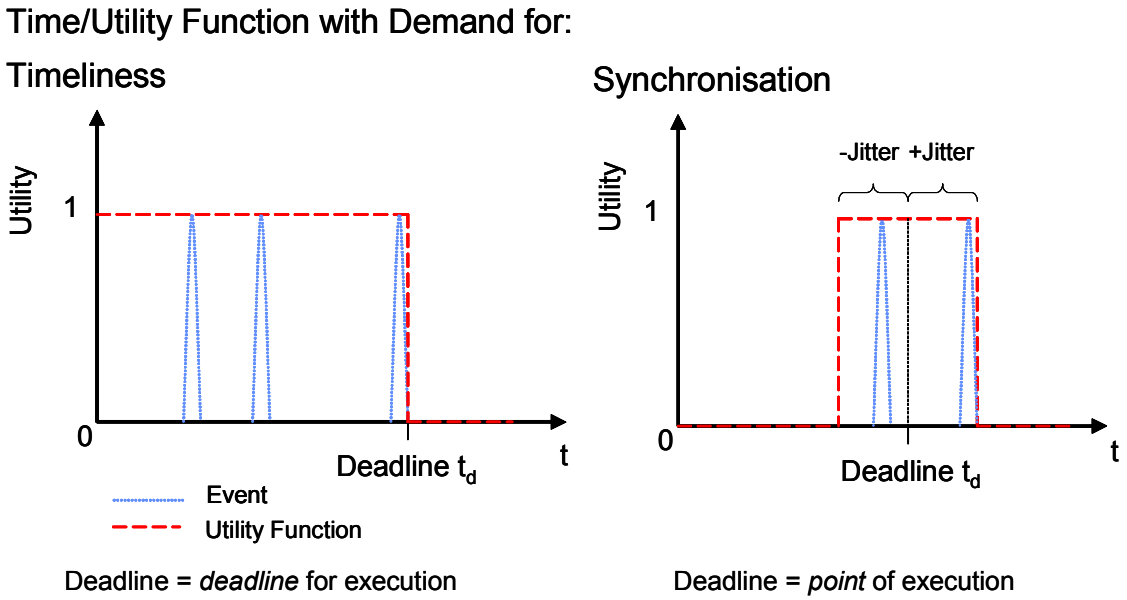

Fig. 4-1: Timeliness and Synchronism

For performing the first category (the requirement for timeliness) Standard Ethernet according to IEEE 802.3 can be an appropriate protocol for a broad range of applications. The second category, the requirement of synchronisation, can generally not be guaranteed by standard Ethernet. This is due to the fact that a not acceptable jitter in the transmission duration can be caused by non predictable delays in packet buffer queues. [Mes03]

4.1.2.2 Special Aspects of Process Industry

In the process industry the time constraints depend on the kind of process control task. These process control tasks are defined as follows:

- Process stabilization: Compensation of correctable disturbances with the aim of holding the process parameters constant at specified values
- Process optimization: Determination and setting of control variables so as to optimize a specified criterion while complying with specified restrictions
- Safety control (Process securing): Compensation of uncorrectable disturbances with the aim of preventing unacceptable process states and product qualities or of minimizing their consequences

For the process stabilisation and the process optimisation we have soft time constraints. For the safety control we have hard time constraints. The definition of process control tasks must be done by comparing the disturbance amplitude D_z and frequency f_z for each control object. An analysis of this kind is done for the dominant disturbance in each control problem. Fig. 4-2 shows that closed

regions can be defined in the D_z-f_z plane, in which safety control (process securing) optimization and stabilization are to be performed.

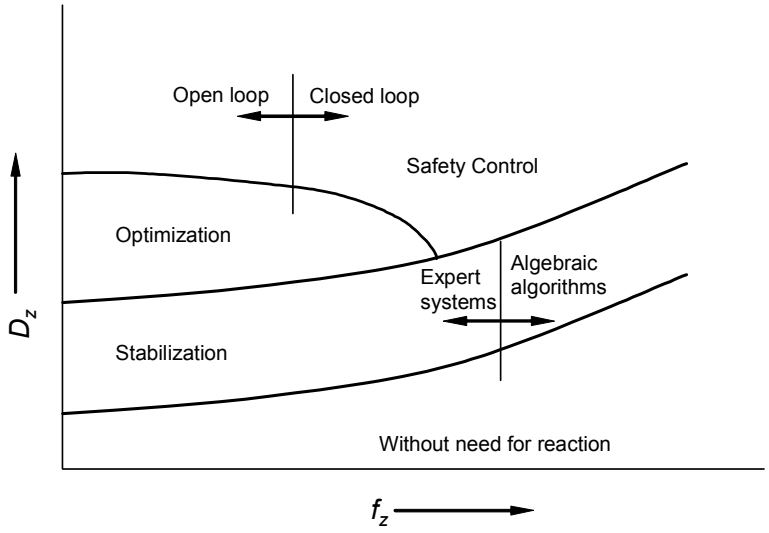

Fig. 4-2: Relationship between automation tasks and properties of the disturbances

Fig. 4-2 also shows, as a function of f_z , the trend in the use of expert systems and mathematical algorithms (conventional process control) as well as the use of consultative (assistant) systems (open loop) and automatic systems (closed loop). In this way, it is possible to identify a certain number of standard situations to which a particular control task applies. Expert systems are especially well-suited to the solution of process securing tasks, since as a rule there are no mathematical models for large disturbance amplitudes (emergencies), although a certain amount of empirical knowledge exists.

In the process industry each process control task has a specific Time/Utility function. Fig. 4-3 shows the time/utility function for safety control. The Fig. 4-2 shows the time/utility function for process stabilisation and process optimisation. [Bal05]

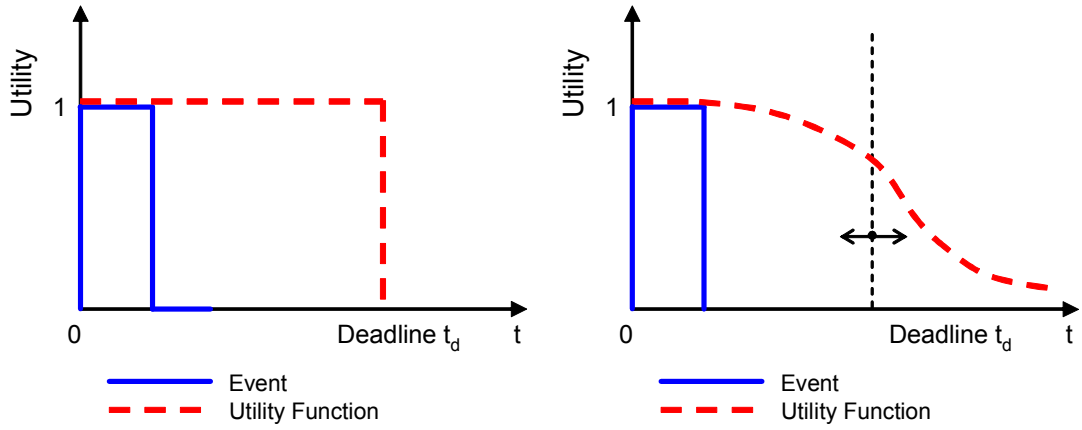

Fig. 4-3: Time/Utility Function for Safety with Demand for Timeliness Hard Real time constraints (on the left), Soft Real time constraints (on the right)

4.1.3 Time Behaviour of Ethernet

Ethernet as physical layer is due to its transmission speed superior to conventional field bus systems. In addition, there is its fast development and high development potential as an open world-wide used standard. For transmitting a packet of maximum size (1522 Bytes) Fast Ethernet needs about 120 µs.

Ethernet was originally based on CSMA/CD (Carrier Sense Multiple Access / Collision Detection). An end device wishing to send data checks the transmission medium. If the network is not being used by another device, it starts to transmit. As illustrated in the Fig. 4-4 below it is possible that several devices detect the network to be free and simultaneously start to send data.

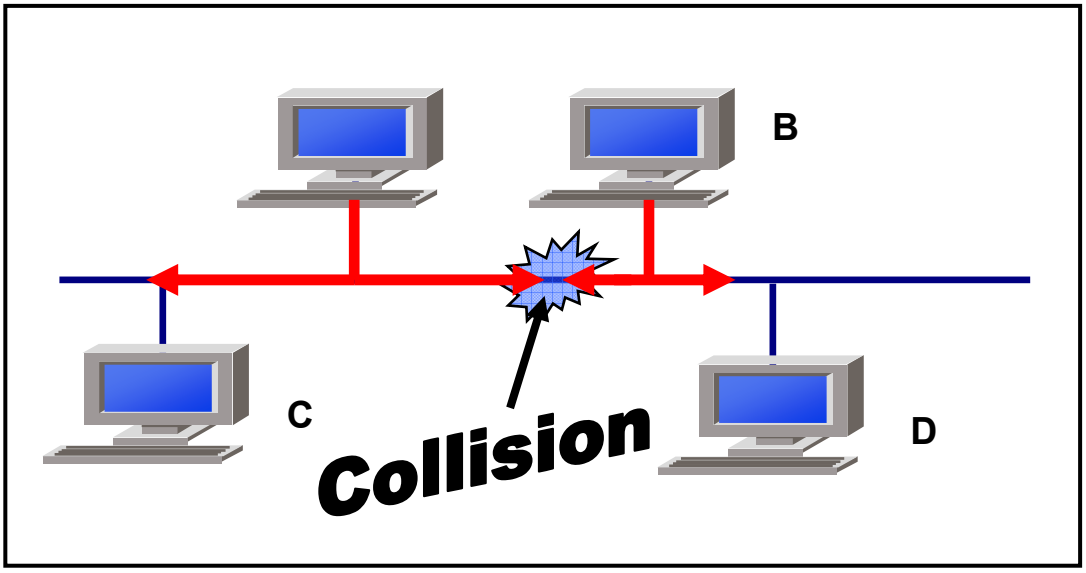

Fig. 4-4: Collision in Conventional Ethernet

This collision will be detected by the devices and all of them will stop transmitting. They will each try again after a random period of time. In this way there is a very high likelihood that the collision will not re-occur. This access technology is intrinsically not deterministic, since access to the network is based upon statistical probability. This behaviour has resulted in Ethernet TCP,UDP/IP's reputation as being unsuitable for real time applications.

However, only using Ethernet, together with the TCP/IP suite causes compatibility to the office world. Since just the TCP/IP stack causes delays in a range of 100µs and has to be considered twice for each transmission, it is the biggest brake in the system; therefore communication engineers often try to bypass this stack for real-time communication, as shown by the examples in subchapter 4.1.4. Thus, the functionality of layer 3 and 4 is not available with such a bypassed stack. Since hard real-time communication happens *within* and not *in-between* subnets, the functionality e.g. of IP to interconnect subnets is also not needed. Furthermore, the reliable transmission behaviour of TCP is even detrimental for real-time communication. The compatibility to the office world is kept, if the TCP/IP stack remains in parallel within the devices for non real-time communication. Hence, the Ethernet driver must be able to distinguish between real-time and non real-time data packets.

Because of the on principle event triggered data transmission, the state of an Ethernet net can not be predicted for each moment, but under consideration of the communication rise of the single stations of a net, at least a maximum transmission time can be calculated.

While Ethernet was originally designed with a data transmission rate of 10 Mbps, since 1995 there has been a standard for 100 Mbps (Fast Ethernet). In 1998 1000 Mbps (Gigabit Ethernet) was standardized and in 2002 a 10 Gbps standard was issued. Today most Ethernet terminal devices do support transmission rates of both 10 and 100 Mbps, Gigabit and 10 Gigabit Ethernet are already established for use in backbone applications. The IEEE 802.3 group is now discussing a 100 Gigabit Ethernet standard.

With each decoupling in the transmission speed, the transmission time for a single packet is reduced by factor ten. On a 10 Mbps network it takes about 1.2 ms to transmit the maximum Ethernet frame size of 1522 bytes. Using Fast Ethernet this time is only about 120 µs, with Gigabit Ethernet only 12 µs and with 10 Gigabit Ethernet only 1.2 µs.

4.1.3.1 Collision Avoidance

Basic resume for the use of Ethernet in automation is the avoidance of collisions in the net. This means it may not happen that several stations send data at the same time on the bus because the resulting retransmission attempts caused by a collision cause swaying and unpredictable time behaviour. Collision avoidance can be achieved on the one hand by dedicated full duplex connections by means of switches and the full duplex mode and on the other hand by realising a cyclic bus communication technology. Usually cyclic communication technologies base on the master-slave principle, where the master manages the bus access rights and allocates it cyclically to each single slave. The first variant can be realised with standard components, with the second variant the question is in which communication layer the cyclic method is realised. Further issues which shall be dealt with in this context are prioritisation according to IEEE 802.1p, segmentation of the network, and problems caused by broadcasts.

Switching and Cyclic Methods

Modern networks based on Ethernet are mostly built using only switching (star distributor) technology. In contrast to CSMA/CD there is no shared medium, in which end devices must compete for access. Instead each end device is assigned a full duplex connection to the switch. As a result there is no contention for access to the transmission medium and each node of the network can send data independently from the activities of other nodes.

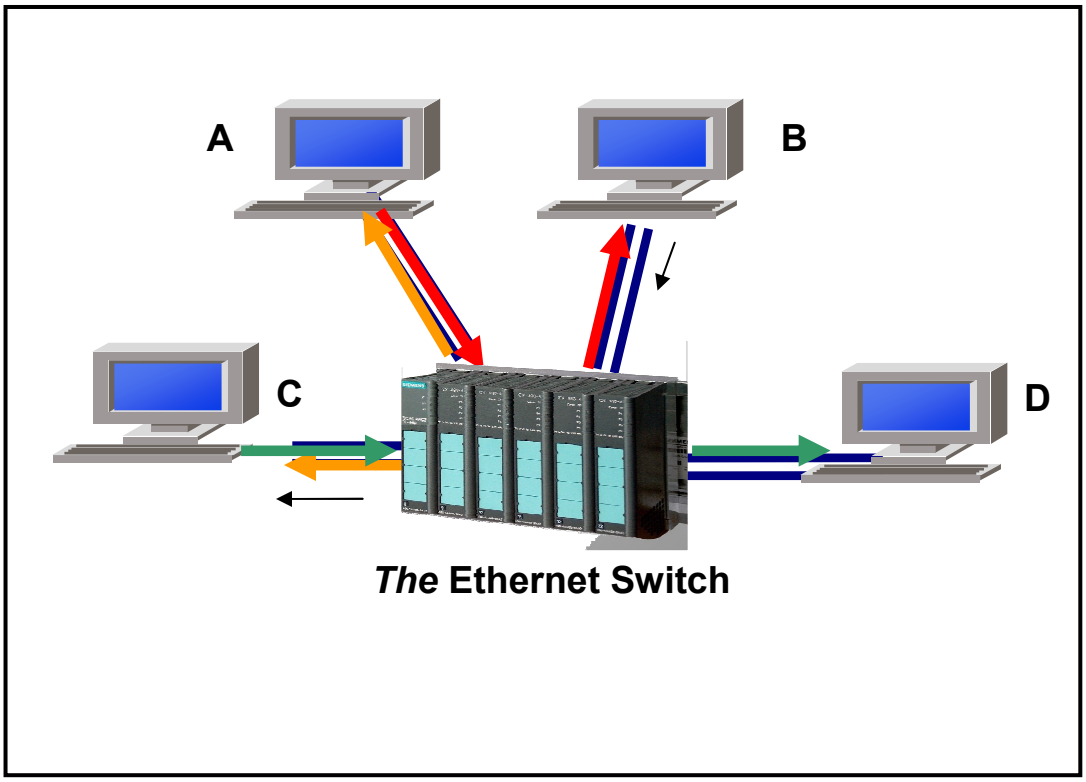

Fig. 4-5: Collision Prevention by Using a Switch

Correspondingly, the communication of two devices in a switched network occurs over at least one switch, whereas each station is at exactly one port of the switch. A switch is able to serve several ports at the same time. If a switch is able to serve all ports at the same time – assumed that there is input and output traffic on all ports – it is called “non blocking”. Thus, switches can accomplish the communication of several communication pairs at the same time. Only if several stations want to send at the same time to the same target station, the switch has to buffer data packets at the output port of that target to be able to send the packets successively. This kind of buffering is called “queuing”.

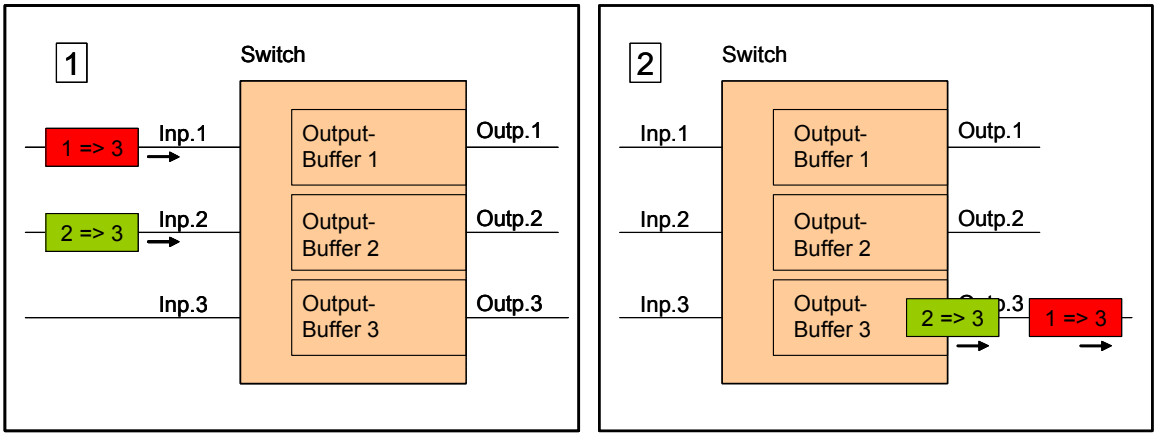

Fig. 4-6: Queuing Effect

Since queuing causes non constant delays – it is not known in advance, when queuing appears – it enlarges the network jitter. Using cyclic technologies, queuing obviously can not occur, because always only one station in the system is in the send mode. On the other hand this also shows that with cyclic methods on Ethernet the advantageous features of today's Ethernet – concerning the independent simultaneous communication of several stations - are not useable.

With cyclic communication the received data are processed immediately by the receiver or at the start of a cycle. The time behaviour of each station and therefore the fulfilment of the demand for synchronism directly depends on the delays and delay fluctuation of the just before preceded communication.

If a cyclic method is not wanted and instead the efficiency of an event triggered communication shall be applied, the above described queuing with its resulting fluctuation in the communication has to be accepted. To still be able to meet demands of synchronism, it is possible to decouple the time behaviour of a station from the communication by adding a timestamp to the transmitted data or instructions. The timestamp fixes the time of validity or execution. The prerequisite is that all stations have a common time base. For that purpose the clocks of the single stations have to be synchronised. Basic condition is, of course, that the communication has to be finished in any case right before the timestamp expires, therefore the communication has to be much faster than the required reaction time pattern of the application. This is shown in Fig. 4-7.

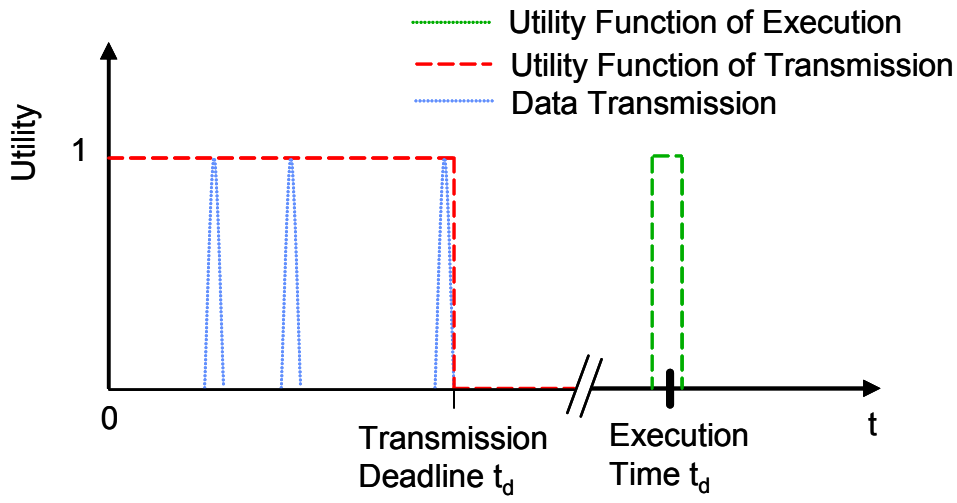

Fig. 4-7: De-Coupling of Communication and Execution

Prioritisation according to IEEE 802.1p

An important enhancement that Ethernet offered a couple of years ago is a layer-2-prioritisation mechanism, standardised by the 802.1p working group. An additional field, known as tag, is added to the Ethernet frame. The tag contains information about the priority of the data.

Switches used within an automation network should support this function. But not all products do support the full range of priority levels and do only distinguish between 2 or 4 priority levels. Each transmission port of a switch that supports IEEE802.1p has a separate queue for each supported priority level. Data packets of a higher priority queue are always transmitted before those in a lower priority queue.

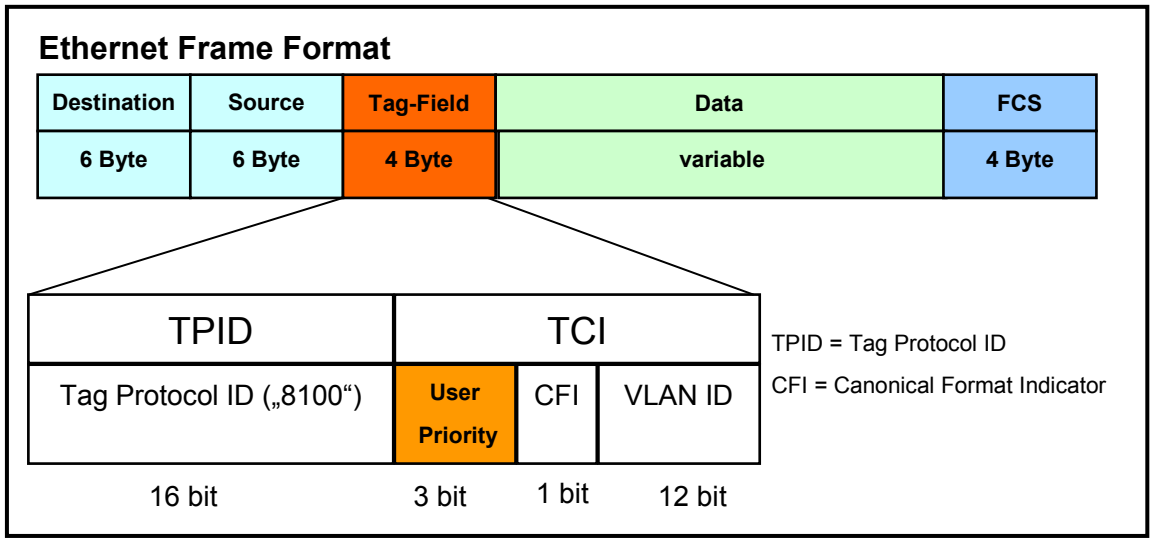

Fig. 4-8: Priority Tag according to IEEE 802.1p

The real-time communication rise can usually be quantified; if in parallel prioritisation according IEEE 802.1p is used to distinguish between real-time and non real-time traffic, it is possible to include the queuing in a worst case calculation. For this it has to be assumed that a non real-time data packet of maximum length was just started to be sent to the same target station. So the real-time data packet with the highest priority has to wait until this transmission is finished before it can be transmitted itself.

Normally prioritisation within the real-time cell ensures that the cyclic data traffic is favoured over the low prioritised traffic. However, it is possible that traffic from outside the real-time cell, also marked with the same high priority, is transmitted into the cell. To prevent this, some switches support the ability to manually adjust the priority of data traffic for specific ports. If the port to the rest of the network is configured with a lower priority, then incoming traffic can not disrupt the cyclic data traffic.

Real Time Behaviour by Segmentation

In addition to control data which require real time communication capability, data with different load profiles and characteristics normally use the network as well. For example, visualisation data, software updates, e-mail traffic, office applications, and Internet data traffic. For this reason the network must be meticulously designed, including segmenting those parts of the network where real time behaviour is necessary.

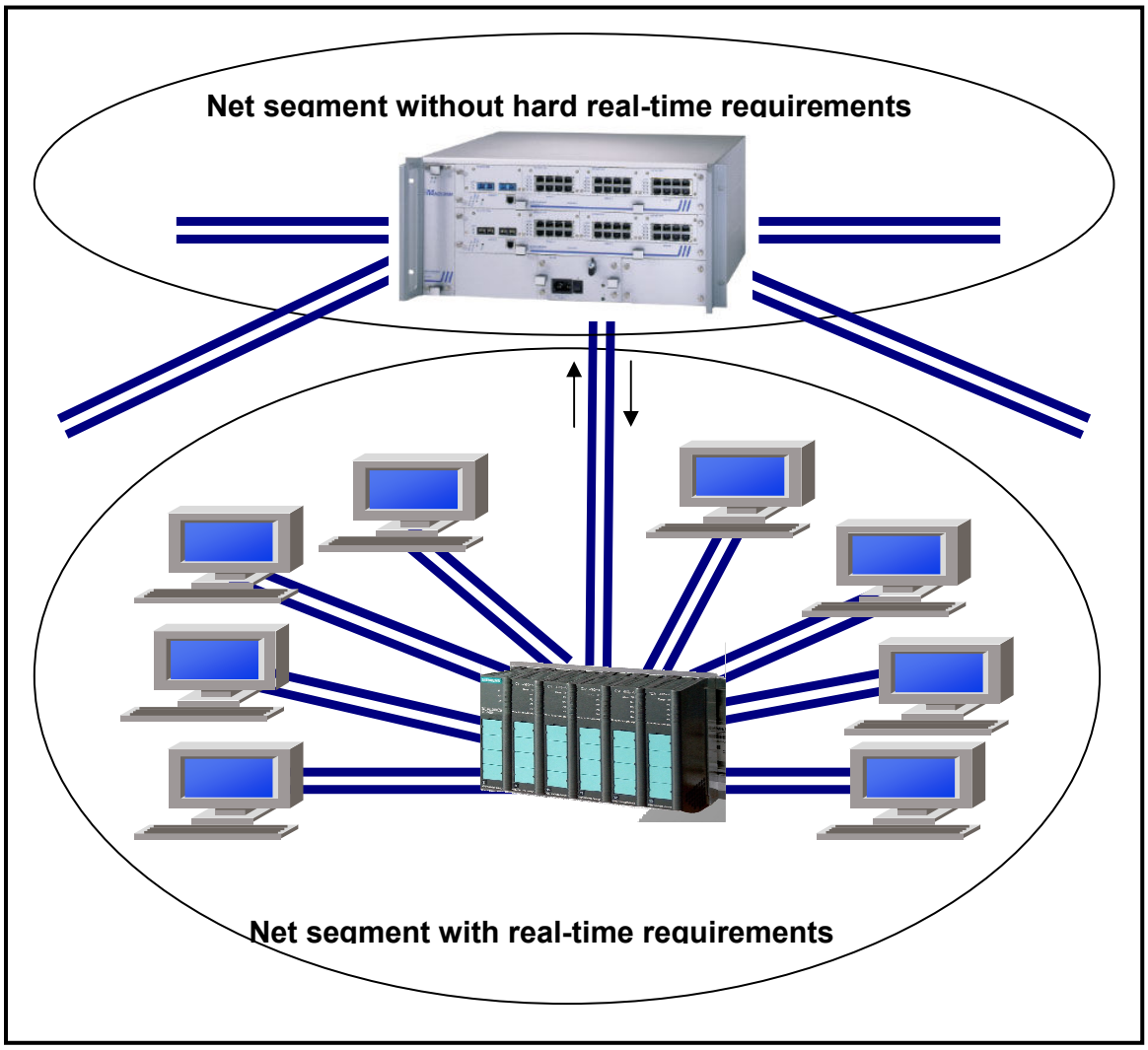

Fig. 4-9: Net Segmentation

The terminal devices that require real time behaviour should be linked over as few switches as possible. Inevitably, the more switches there are between two terminal devices, the higher the “worst case” throughput and queue time. With backbones or other instances where there are no factors limiting real time performance, the individual segments are commonly connected in a ring structure.

In addition, the interface between a real time segment and the rest of the network must be precisely controlled. Since the data traffic from the general network can adopt any load profile, it must be monitored and restricted when entering a real time segment. To prevent the real time segment from being overloaded, the amount of data traffic entering this segment must be limited. An effective way to achieve this is to configure the inter-segment link to 10 Mbps, while all devices on the real time segment communicate at 100 Mbps. Further segmentation, as well as access control, can be accomplished by the use of routers and firewalls.

Problem Area Broadcasts

The number of broadcast frames in a network is also a contributing factor to network overload. On the one hand broadcasts stress the terminal devices, because the devices have to examine each broadcast. On the other hand, depending on the switch architecture, broadcasts place an additional load on the switches. This is because a broadcast frame has to be duplicated for each output port of the switch. To counteract the negative effects of broadcasts, some switches offer a function known as a Broadcast Limiter. This limits to a pre-defined threshold the number of broadcasts transmitted each second.

4.1.3.2 TCP or UDP

TCP (Transmission Control Protocol), a layer 4 protocol of the Ethernet TCP/UDP/IP protocol suite, is a connection based protocol. It establishes a virtual connection at the beginning of the communication process, and closes the connection down when the communication process has finished. As a result loss of data can be detected and the lost data can be automatically re-transmitted. TCP also ensures that the transmitted data remain in the correct sequence.

In contrast to this, UDP (User Datagram Protocol) is connection-less. The data packets sent are absolutely independent from each other. For real time applications UDP is normally used as the layer 4 protocol, since re-transmission and real-time capability are contradictory demands. UDP is easier to tolerate in industrial automation applications as in case of a single transmission failure (with a complete loss of data) it would lead to a refreshing with current data with the next transmission. On the opposite, TCP would repeat the transmission with the outdated data until it was successful.

4.1.3.3 Bottleneck TCP, UDP/IP Protocol Stack

In most cases data transmission bottlenecks are not caused by the network infrastructure, but by the protocol stacks which are generally a component of the applied real time operating system. Investigations of typical real-time operating systems showed that stacks, as used today, have relatively high throughput times. Measurements with 400 MHz Pentium systems e.g. showed times around 200 µs, with a jitter of less than 10 µs. Test of other systems showed throughput times fluctuating around five times this level. Consequently, no narrower indexes concerning the time behaviour can be assumed. Of course with more powerful CPUs and lower CPU workload, the process times are shorter. In specific cases a statement about the time behaviour of the stack should be requested from the provider of the operating system being used. Meanwhile there are operating system and network stack provider, who have improved their products concerning network time behaviour.

If protocol stacks are realised in hardware, the network protocol software is completely removed from the CPU. It is handled in a separate chip, which is located between the CPU and Ethernet chips. In this way the throughput of layer 3 and 4 is clearly improved compared with any software implementation and becomes absolutely independent from all other operations.

From the network perspective, further improvement will be achieved, if terminal devices communicate using Gigabit Ethernet. Even if today the price of Gigabit Ethernet confines its use to backbones or possibly large server systems, the progress in semiconductor technology will dramatically reduce the costs within the next few years. This shows clearly, how automation benefits automatically today and

in future from the international further development of Ethernet as an open communication standard. In addition, features as prioritisation, (data) rate limiting, and rate shaping (smoothing of the load profile), will find wider acceptance and spreading.

4.1.4 Generic Architectures of Ethernet-based Automation Protocols

From the above considerations in principle three generic architecture variants for real time capable Ethernet based communication protocols can be derived.

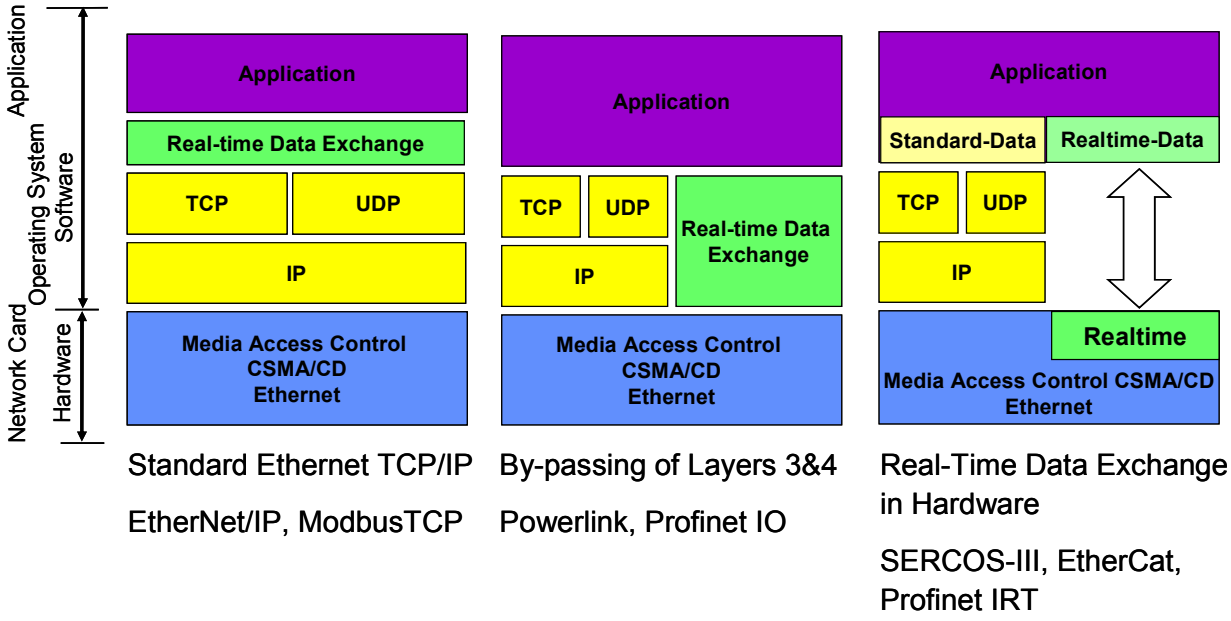

Fig. 4-10: Ethernet-based Real Time Architectures

In the Fig. 4-10 three variants of placement of the real-time scheduling mechanism are shown. Allocation of these scheduling mechanisms in different layers leads to different real-time classes, for definition of real/time classes please, see section 4.1.5. Placement of the real-time scheduler on top of the TCP leads to a soft real time or non real-time only. By passing the layers three and four, class 2 (hard real-time) can be reached. If the scheduling is performed at layer two, which is mostly implemented in HW, it provides an additional functionality and as such is able to guarantee hard real-time. If additional synchronization mechanisms are available, then isochronous hard real-time can be guaranteed.

In the architecture presented on the left side of the Fig. 4-10 both the exchange of non time critical data and the real time data exchange are carried out over the standard TCP/UDP/IP stack. The architecture in the middle and the right hand architecture realize a bypassing of the TCP/UDP/IP stack for the real time data exchange, whereas the realisation of the real time data exchange can be distinguished between soft- and hardware implementations.

The time until user data can be really processed in the application or physically converted, also depends additionally on the respective organizational structure (e.g. the object model) of the single automation protocol. Further influencing factors that depend on the respective automation protocol

are e.g. the used physical and logical network topology, the multicast and broadcast ability – as a possibility to send the same datagram at the same time to several receivers - or the kind of data exchange: message oriented or summation frame method as well as the underlying hierarchical system. [Mes03][LL05].

4.1.5 Real Time Classes

Having a look at Local Area Networks, especially in the Ethernet domain, there are three *real-time classes* guaranteeing response time:

Class 1: soft real-time (scheduling on top of UDP/TCP): scalable cycle time; used in factory floor and process automation (local and wide area domain).

Class 2: hard real-time (scheduling on top of MAC): cycle time 1…10 ms. Used for control (local domain).

Class 3: isochronous real-time (with time/clock synchronisation and routing with time schedule): cycle time 250 µs…1 ms; jitter less than 1 µs. Used for motion control (local domain).

Additionally, there could be seen a virtual fourth class, of course, the class “non real-time”.

The international standardisation activities regarding the above mentioned classes are concentrated in IEC SC65C WG 11 “Real-time Ethernet”. Approaches of various user organisations are established there as Public Available Specifications PAS. These PAS have not been harmonised yet.

Using Wide Area Networks, the stock of existing communication technologies becomes broader:

- all appearances of the Internet (mostly with best effort quality of services)
- public digital wired telecommunication systems (ISDN, DSL etc.)
- public digital wireless telecommunication systems (GPRS-based, UMTS-based)
- private wireless telecommunication systems, e. g. trunk radio systems.

Using these technologies within the automation domain there are many private protocols over leased lines, tunnelling mechanisms etc. Most of the Radio Networks can be used in non real-time applications, some of them in soft real-time applications (but industrial environments and ISM Band limit the corresponding possibilities).

- The usage of wide area networks within the automation domain in the VAN sense is new and has to be investigated just as the uninterrupted commercial availability.
- Since the Internet or other telecommunication systems are general-purpose communication systems, the infrastructure and business model preconditions for the selection of requested QOS within a spectrum of available communication services of various providers have not been investigated suitably and have to be developed.
- This means, in analogy to the “switched” Ethernet in LANs, a WAN switching mechanism has to be developed for this selection, i.e. choosing dynamically the network type and/or network provider, which guarantees the required QOS. [Neu05]

4.1.6 IEEE 1588 Clock Synchronisation for Ethernet

The IEEE 1588 standard defines a protocol for the synchronisation of real time clocks in measurement - and automation systems. This protocol is very suitable for the application in Ethernet networks and enables the realisation of highly precise synchronisation tasks in the sub-microsecond range. For this reason there are busy activities at present in the integration into several Ethernet based automation protocols. Even strictly deterministic protocols will be extended with the IEEE 1588 protocol.

The intention of this subchapter is to give an insight into and overview of the IEEE 1588 standard. The IEEE1588 defines a protocol (PTP – Precision Time Protocol) for the precise synchronisation of distributed clocks in measure and control networks in close relation with network communication, local computing and distributed objects [IEEE1588]. The protocol especially, but not exclusively, considers the use of Ethernet as underlying network technology and is suitable to synchronise also heterogeneous systems in the sub microsecond range.

4.1.6.1 IEEE1588 History

In the last years a number of academic and commercial organisations developed techniques for synchronising clocks in devices typically used in measurement and control applications. Public discussion of the standardisation of such a technology occurred between engineers developing technologies and standards applicable to distributed systems in industrial automation, the IEEE 1451 family of standards [IEEE1588-2]. In November 2000 the interest was sufficient enough to warrant forming a committee and seeking sponsorship for a standardisation activity on clock synchronisation. The initial committee's first meeting was held in April of 2001 and it was decided to seek sponsorship from the Institute of Electrical and Electronics Engineers (IEEE) Technical Committee on Sensor Technology of the Instrumentation and Measurement Society which had also sponsored, along with the National Institute of Standards and Technology (NIST), the IEEE 1451 activity. The committee membership included engineers from the automation, robotics, test and measurement, and time keeping industry as well as representatives from NIST and the US military. The committee decided to submit a formal application to the IEEE which was approved on June 18, 2001.

A first draft of the standard was produced by the committee, which was submitted according to the usual IEEE rules for ballot in April of 2002. The draft passed the first ballot but there were a number of helpful comments submitted by the reviewing balloters. The committee incorporated these suggestions and resubmitted the standard for a second ballot which passed in May of 2002. The committee has submitted this final balloted version to the IEEE Standards Board Review Committee for final approval. On September 12, 2002, the draft was approved as an IEEE standard by the review committee. The publication of the standard took place three month later in November of 2002. Since then the IEEE 1588 is available at its homepage (http://ieee1588.nist.gov/) as pdf file and hardcopies can be ordered, too.

Technical basis for the standard was a technology of the company Agilent which was spun off from the test and measurement department of the Hewlett-Packard Company in 1999. The measurement of many parameters in extensive, spatially distributed respectively separated systems could not be realised with the usual classical centralised approaches. Therefore a technology was developed in which the single gauging stations got a clock, were networked, and the clocks distributed in the network were synchronised among each other. [Jen02]

When sampling single values, each one is provided with a time stamp which represents the point of time of the measurement. For a later analysis the different values can be merged easily and exactly.

The technology was integrated by Agilent into the Vantera gauging systems. The precision of these systems was around 200 ns.

4.1.6.2 Time Stamps for Automation

The principle to use time stamps to synchronise local real time clocks can also be transferred to the control of processes. The achieved independence of the execution precision of synchronised control commands from possible fluctuations in the network communication makes this technology interesting especially for the use in Ethernet based systems, as by using it, Ethernet TCP/IP can be applied without basic changes for networking within highly precise control systems. The achievable precision exceeds those of present systems based on field busses. Additionally there is the huge advantage of Ethernet TCP/IP as a general network technology through all levels of an enterprise.

4.1.6.3 System Components

A 1588, respectively PTP system consists of several nodes, all representing a clock. The clocks are connected with each other via a network. On principle there are two kinds of clocks: ordinary clocks and boundary clocks. The difference between them is that an ordinary clock has a single PTP port and a boundary clock has more than a single PTP port. From the network view a clock can be in either one of the general states: slave clock, master clock, or grand master clock.

A simple system consists of slave clocks and one master clock. If there are several potential master clocks, the active master clock will be determined according to a best master clock algorithm. All slave clocks permanently compare their own clock characterisations with that of the current master clock, if there are e.g. new clocks added to the system or the current master clock is suddenly disconnected, then the other clocks realise this and a new master will determine itself. If several PTP subsystems need to be connected with each other, the connection should exclusively be realised by a boundary clock. Exactly one port of the boundary clock works as a slave port, this port is connected to the subsystem that provides the time for the whole system. Therefore the master clock of this subsystem is the grand master clock for the whole system. The other ports of the boundary clock work as master ports, since over these ports of the boundary clock the messages for the synchronisation of the connected subsystems will be sent. The port of a boundary clock appears to the connected subsystem as if it would be an ordinary clock.

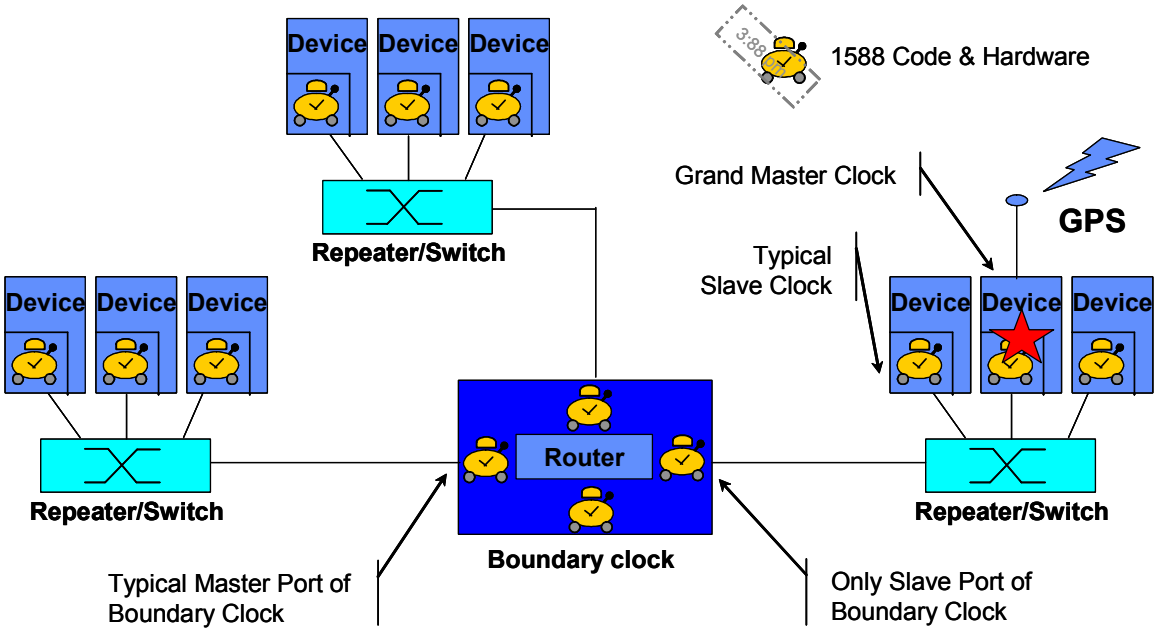

Fig. 4-11: IEEE 1588 System

The basic principle of the synchronisation consists in the time recording of the send and receipt time of special messages and in adding a corresponding timestamp to the respective messages. With this time recording the receiver can calculate its clock deviation and the delay in the network.

4.1.6.4 Specified Time Messages

For that, beside management messages, the PTP protocol defines four types of messages that are sent per multicast: a synchronisation message, briefly named Sync, a message followed at the Sync, briefly named Follow_Up, a delay request message, briefly named Delay_Req, and a reply to the Delay_Req, briefly named Delay_Resp. The reaction of a clock on the receipt of such a message depends on the current state of that clock.

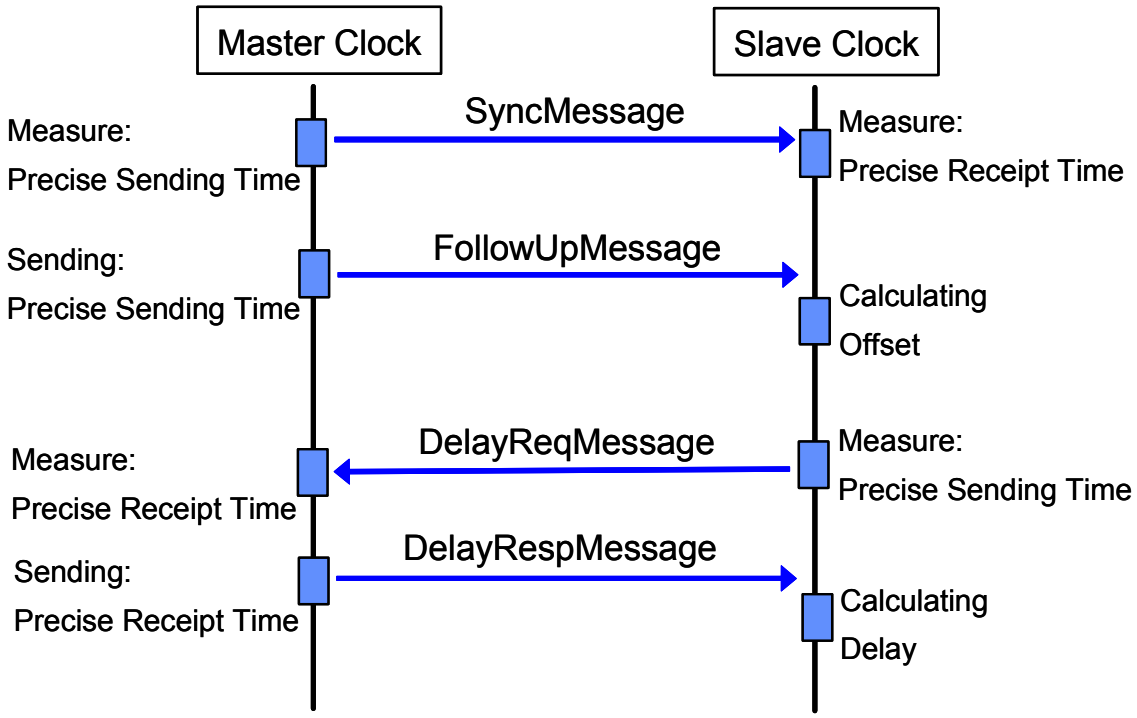

Fig. 4-12: IEEE 1588 Clock Synchronisation

The Sync message is sent periodically (typically every 2 seconds) by the clock that is in the master clock state. It also contains the clock characteristics of the sender that are needed for the best master algorithm. First of all the Sync message contains a timestamp which - as precise as possible – specifies the estimated sending time of that packet. Since the estimated sending time has to be integrated into the packet before it is really sent, the real sending time can differ from the estimated one. Because of that, the precise sending time of a Sync message is measured and sent in a following Follow_Up message. The receiver of a Sync message records its precise receipt time. Using the precise sending time contained in the Follow_Up message and the precise receipt time, the deviation of the slave clock from the master clock can be calculated and the slave's time can be corrected accordingly. However, the determined deviation still includes the transmission delay of the network. For determining this transmission delay the Delay_Req message is used.

A Delay_Req is sent from a slave clock after the receipt of a Sync message. Equivalent to a Sync message the sender records the precise sending time and the master clock as the recipient records the precise receipt time. The precise receipt time is sent within a Delay_Resp message to the sender of the belonging Delay_Req, where the according transmission delay can be calculated and considered for the next calculation of the clock deviation.

The precision of the synchronisation - the synchronisation jitter – strongly depends on the kind of realisation of the time stamp implementation and the detection of the time messages. A pure software implementation can achieve a precision in a millisecond range. An implementation in hardware achieves a jitter below 1 µs.

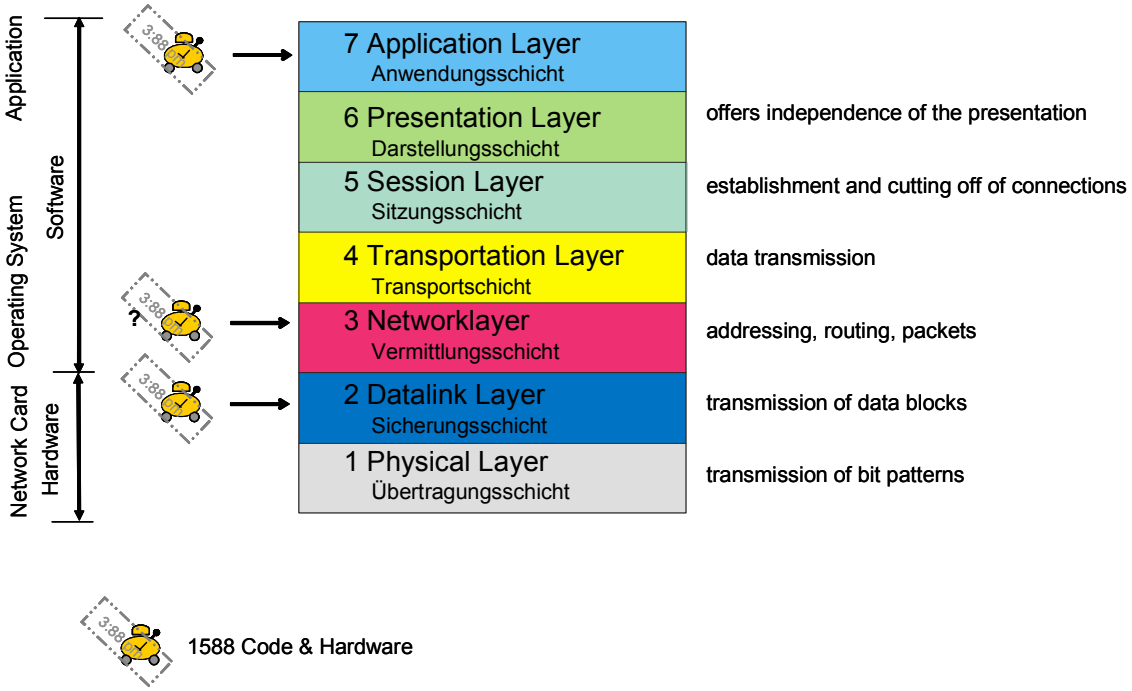

Fig. 4-13: Implementation of IEEE 1588

4.1.6.5 IEEE 1588 Task Groups

To push and co-ordinate the further development of the standard three task groups were founded at the IEEE 1588 workshop in September, 2003.

In detail these are:

- The User Requirements Task Group, dealing with the topic: requirements of the users and the acceptance of IEEE 1588 and related topics as formation of a user group, relationship to other standards, and enablers as design tools;
- The Technical Extensions Task Group, dealing with the topic: technical extensions or modifications of IEEE 1588 and related topics as influence of tagged frames and ipv6, non-UDP implementations, redundancy and fault tolerance, and simplified versions of IEEE 1588;
- The Conformance and Interpretation Task Group, dealing with the topic: conformance and handling of IEEE 1588 interpretations and related topics as certification procedures or test sets, reference implementation, and plug-fests.

Further information about the task groups can be found at the homepage http://ieee1588.nist.gov.

4.1.6.6 Comparison with other Synchronisation Protocols

The main difference between IEEE1588 and other well known synchronisation protocols that are applicable to Ethernet TCP/IP networks as SNTP (Simple Network Time Protocol) or NTP (Network Time Protocol) is that PTP is designed for networks in a rather stable and secure surrounding. Therefore PTP is obviously slimmer and requires only a minimal use of network and computing resources. By this PTP focuses on relatively localised and networked systems with few subnets and relatively stable components, co-operating within a frame of well defined tasks as it is typical for

industrial automation and measurement environments. Unlike this the synchronisation protocol NTP aims on autonomous systems widely dispersed on the Internet with the need to specify security aspects. Also GPS (Satellite based Global Positioning System) is designed for autonomous, widely dispersed systems.

PTP has the outstanding ability to define its network structure for the time synchronisation by itself, by setting ports e.g. of redundant network paths into a passive state for the PTP protocol. In opposite to SNTP respectively NTP the timestamp can be preferably realised in hardware and not only at the application layer. This enables PTP to perform a precision in the sub-microsecond range. At the same time PTP is designed so modular that it is also possible to integrate it with less effort into low-end devices. [Mes04]

4.2 Selected Technologies with Real-time Properties

Several technologies possessing real-time properties were chosen to introduce the solution of the abovementioned real-time aspects. Parameters, which can be compared across technologies, are specified in *Appendix B*.

4.2.1 Real-time aspects of AS-interface

AS-interface is a simple modern sensor-actuator bus operating on the master/slave principle. Although the transmission speed is quite low (167 kbps) the bus cycle is relatively short due to extremely short messages (request:14 bits, response: 7 bits). Each message contains up to 4 data bits.

The Master-slave principle guarantees deterministic operation; each bus cycle consists of a data exchange phase, an inclusion phase and a management phase. The duration of the data exchange phase depends on the number of slaves; there are approx. 154 μs needed for each slave. The approximate bus cycle can be calculated as $T_{cycle} = n * 154\ \mu s$, where n = (“number of slaves” + 2).

For transfer of analog data up to 7 bus cycles are needed. For high speed I/O operation single slave may occupy more than single address.

Length of each phase might slightly differ due to detection of errors and management operations, the worst case jitter can be estimated as less than 3 ms even if every message gets repeated once during the bus cycle.

Neither internal nor external clock synchronization is available.

4.2.2 Real-time aspects of Ethernet

A scheme known as carrier sense multiple access with collision detection (CSMA/CD) governs the way the computers share the channel. Originally developed in the 1960s for the ALOHAnet in Hawaii using radio, the scheme is relatively simple compared to token ring or master controlled networks.

When one computer wants to send some information, it obeys the following algorithm:

1. Start - If the wire is idle, start transmitting, else go to step 4
2. Transmitting - If detecting a collision, continue transmitting until the minimum packet time is reached (to ensure that all other devices detect the collision) then go to step 4.
3. End successful transmission - Report success to higher network layers; exit transmit mode.
4. Wire is busy - Wait until wire becomes idle

5. Wire just became idle - Wait a random time, then go to step 1, unless maximum number of transmission attempts has been exceeded
6. Maximum number of transmission attempt exceeded - Report failure to higher network layers; exit transmit mode

This works similarly to a dinner party, where all the guests talk to each other through a common medium (the air). Before speaking, each guest politely waits for the current guest to finish. If two guests start speaking at the same time, both stop and wait for short, random periods of time. The hope is that by each choosing a random period of time, both guests will not choose the same time to try to speak again, thus avoiding another collision. Exponentially increasing back-off times (determined using the truncated binary exponential backoff algorithm) are used when there is more than one failed attempt to transmit.

Ethernet starts out fast, with micro-second-level response times, when it runs alone under good conditions. However, Ethernet-based networks usually begin to bog down, to multiple milliseconds and longer, for many of the same reasons that strain capacities of all communication, automation and/or control networks.

Data gathering and transmission problems at the device and I/O level; inefficient switching, too many devices, and poorly coordinated traffic on the network itself; and error-checking and translation hurdles at upper-layer communication levels, such as TCP and UDP, can steal precious slices of time from Ethernet-based networks. These delays can prevent Ethernet from bringing its well-known advantages to discrete, motion control, and other higher-speed applications.

4.2.3 Real-time aspects of EtherCAT

Communication is formed by a token bus. Seeing the fact that FastEthernet cards are full-duplex, the physical architecture resembles token ring. One EtherCAT frame periodically passes through all the stations in the given cluster, while each station can read data from segments belonging to particular devices and fill data into an assigned segment. An EtherCAT network claims to be synchronous, which meets the requirements of IRT applications.

According to the exchange method, no packet losses are possible unless a failure occurs. Latencies are precisely given for each node in the network thanks to the fact that accepting and passing a packet is a matter of the hardware solution in the EtherCAT card. Thus, latency on one slave device is only a few ns.

The master device can calculate the propagation delay from the latency of the circulating packet and carry out synchronization whose jitter is below 1 μs. Synchronization in a vast factory floor is performed externally according to IEEE 1588.

The whole stack is placed within the card hardware; hence, latencies do not depend on the latencies caused by the CPU computing. The update time for 1000 IOs is 30 μs. Communication with 100 servo axes takes 100 μs. Ethernet services of higher layers are also permitted on EtherCAT hardware. This is provided by protocol tunneling.

Potential risk is represented by tolerating of Ethernet-based services, which can cause lowering of the network performance.

4.2.4 Real-time aspects of EtherNet/IP

EtherNet/IP (IP=Industrial Protocol) is the implementation of the CIP (Common Industrial Protokol) on Ethernet TCP/UDP/IP. CIP and is a quite complex object oriented specification. EtherNet/IP

cosequently sets on standard Ethernet and thus also uses commercial Ethernet components and bases on the typical star topology.

The communication in general is message oriented on a producer/consumer base.

All connections in a CIP network can be divided into Explicit Messaging Connections - these are non cyclic, point to point messages - and Implicit (or I/O) Messaging Connections.

- Explicit Messaging Connections provide generic, multi-purpose communication paths between two devices.
- Implicit Messaging Connections provide dedicated, special purpose communication paths between a producing application object and one or more consuming application objects.

The exchange of the implicite messages (I/O data) in EtherNet/IP is running via UDP and may also be used for scheduled communication between controllers.

The implicite messages can be sent as unicast or – and that is the usual case - as multicast.

Multicast IP addresses are treated like broadcast addresses by ordinary (layer 2) switches. This means that all multicast frames will be sent to all nodes in the subnet even though only few nodes consume these messages. To avoid a “flooding”, it is recommended to use switches that support IGMP snooping. With this feature enabled, multicast messages will only be sent to those devices that have joined a multicast group.

CIPSync and CIPMotion

For really time critical communication with a high demand as synchronisation as needed for coordinated motion with sub-microsecond action jitter EtherNet/IP in its above described original form can not be used due to non precise predictable transmission times and jitters. Since without any further measures the action jitter in a node is a direct result of the message jitter. To overcome this restriction in its applicability an extention of the CIP Specification is under development that is called CIPSync and CIPMotion. CIPMotion defines new CIP objects that will provide the capability necessary for high performance, closed loop drive operation It bases on the IEEE1588 - a protocol for the highly precise synchronisation of distributed clocks in automation.

The key technology used for CIP Motion over EtherNet/IP includes:

- IEEE-1588 time synchronization services (CIP Sync) with hardware assist
- Time-stamped cyclic data telegram
- QoS (Quality of Service) support as defined in the IEEE 801.2q standard
- Use of managed switches and full duplex operation to provide collision free data transfer
- UDP/IP support for Cyclic data transfer
- UDP/IP support for Acyclic data transfer
- TCP/IP support for explicit messaging

So CIP Sync defines a set of time services that have been added to CIP which are used to link IEEE 1588 time synchronization into the CIP object model and therefore EtherNet/IP. It is fully compliant with the IEEE-1588 “Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems” (for more details see IEEE 1588 subchapter). Using the hardware assist mode, the 1588 services provide nanosecond clock resolution, and +/- 100 nanosecond clock synchronization across distributed controls, drives, and other devices on EtherNet/IP.

At the moment CIPMotion is under development a specification or draft is not publicly available yet.

4.2.5 Real-time aspects of Ethernet Powerlink

Powerlink cycle

The protocol works isochronously, i.e., the data exchange between the stations occurs cyclically, repeating in a fixed interval (*Powerlink cycle*). The Powerlink cycle time can be configured in the manager.

The following time periods exist within one cycle. Start, cyclic, asynchronous and idle.

- Start period: Start-of-Cyclic frame is sent, necessary data preparation, etc.
- Cyclic period: Processing of all active stations.
- Asynchronous period: End-of-cyclic frame is sent. Non-cyclic communication (configuration, diagnostics, TCP/IP, etc.) precedes here.
- Idle period: Remaining time period between the completed asynchronous period and the beginning of the next cycle. During this time, all network components "wait" for the beginning of the following cycle. The duration of the period can also be 0, i.e. implementation cannot start from a fixed Idle period!

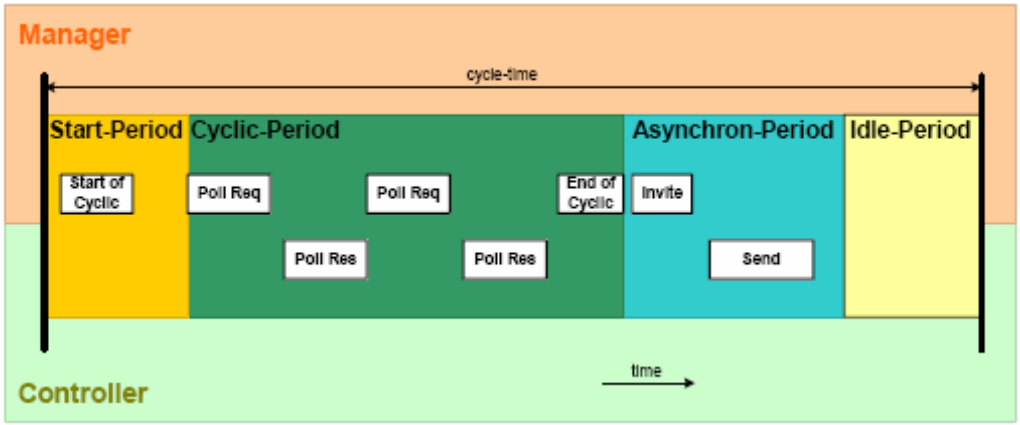

Fig. 4-14: Powerlink Cycle

The network must be configured so that the preset cycle time is not exceeded. Adherence to the cycle time is monitored by the manager. If a cycle time violation occurs, the manager continues at the next valid cycle start position, i.e. one (or more) cycles is (are) lost.

Transfer protection

Transfer disturbances are detected by the Ethernet CRC-32. This is sufficient for detecting transfer errors. All data transfers are unconfirmed, i.e. there is no confirmation that the data has been received. To maintain deterministic behaviour, protecting the cyclic data (PollRequest and PollResponse) is not necessary or desired. Asynchronous data must be protected in higher protocol layers (a respective proposal is still being specified).

Communication classes – prescaled stations

Powerlink supports communication classes which determine the cycles in which stations are to be operated.

- Class 1 - cyclic: These stations are in each Powerlink cycle which is being used.
- Class 2 - prescaled: Only one limited number is processed by these stations in each cycle (limit can be configured).

The number of stations processed per cycle is determined by the number of class 1 stations plus the (configured) maximum number of class 2 stations per cycle. Example: 2 cyclic stations (1 and 2), 2 prescaled stations (3 and 4), one class 2 station per cycle configured.

Performance

Ethernet Powerlink offers outstanding real-time performance and timing precision on standard Ethernet networks. It is by far the fastest software-only Real-Time Industrial Ethernet system on the market. Other real-time Ethernet approaches need special proprietary hardware chip support (ASIC) to come close to ETHERNET Powerlink's performance. The following application example should give an impression about ETHERNET Powerlink's real-time capabilities:

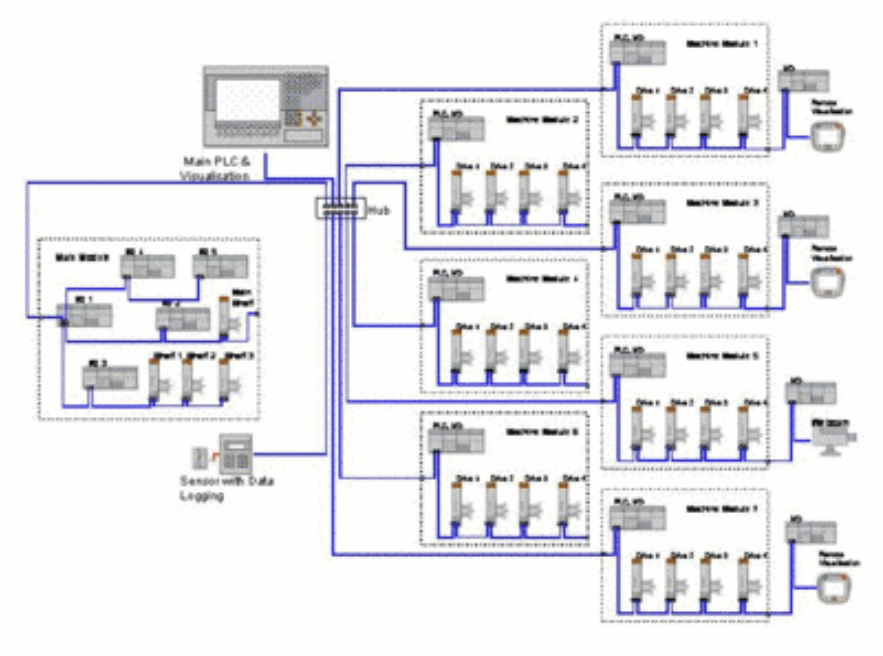

Fig. 4-15: Powerlink Topology

Parameter	Value
Total Devices	53
Drives	32
IO Nodes	16
Analog I/Os (2 Bytes)	320 (160 IN, 160 OUT)
Digital I/Os	4096 (2048 IN, 2048 OUT)
Remote Visualisation	3 Devices
Web Cam	1 Device
Data Logger	1 Device
Calculated Cycle Time	992 µs w\o Multiplex ,400 µs with Multiplex
Asynchronous Bandwidth (1 Maximum Frame/Cycle)	1.5 MBps (@ 992 µs cycle) 3.75 MBps (@ 400 µs cycle)

Table 4-1: Powerlink Parameters

4.2.6 Real-time aspects of INTERBUS

In bus systems, distinction is made between various access methods and physical transmission methods used. In addition to the bus systems commonly used in electronics and computer technology, the two systems illustrated below play a key role in automation technology.

Summation Frame Method - Master/Slave Structure

INTERBUS is a bus system working according to the summation frame method that uses only one protocol frame for messages from all the devices. In this master/slave access method, the bus master acts as the coupling to the higher-level control or the bus system.

The method provides a high level of efficiency during data transmission and enables data to be sent and received simultaneously (full duplex operation). With this data transmission method, INTERBUS ensures constant and predictable sampling intervals for set-points and real time control values. In summation frames, which consist of the header, the loop-back word, and data save and end information, data from all the connected I/O devices is grouped together in a block. Additional information that is required is transmitted only once per cycle.

In practice, this method can be described as a register, which is formed by the devices that are connected in a ring system. In INTERBUS this consists of a number of binary memory cells, which push digital information from cell to cell to clock pulses. Each device has a certain number of buffers assigned to a preset number of cells for different tasks, e.g., data input and output for the process.

Additional registers monitor the data transmission for errors. An INTERBUS device contains three registers that are connected in parallel. I/O data is transferred using the data register. The type of INTERBUS device is defined in the identification register. This enables the bus master to identify the devices and the bus topology, as well as to carry out addressing.

Data is saved using the CRC16 register (cyclic redundancy check), where correct data transmission is checked.

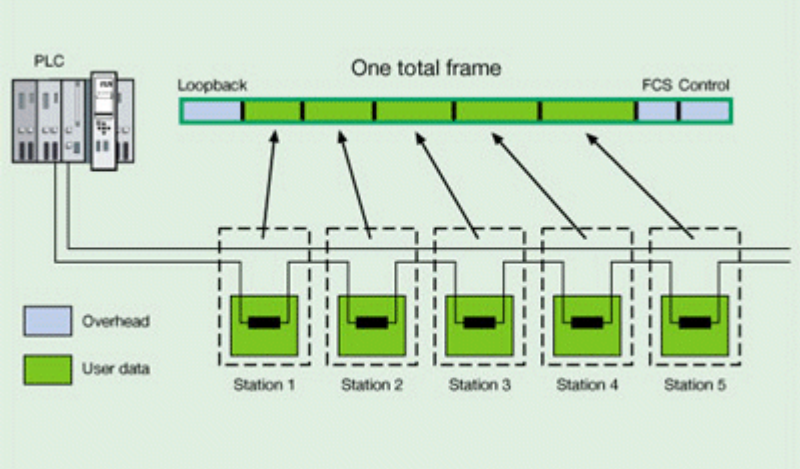

Fig. 4-16: Physical transmission method - summation frame method

The cycle time, i.e., the time required for I/O data to be exchanged once with all the connected modules, depends on the amount of user data in an INTERBUS system. The cycle time increases linearly with the number of I/O points, because it depends on the amount of information to be transmitted. A certain amount of time is needed for each bit. Because the summation frame has a set length, the cycle time also remains constant. In INTERBUS, the deterministic method of operation is provided by the summation frame method, which is essential for fast controllers.

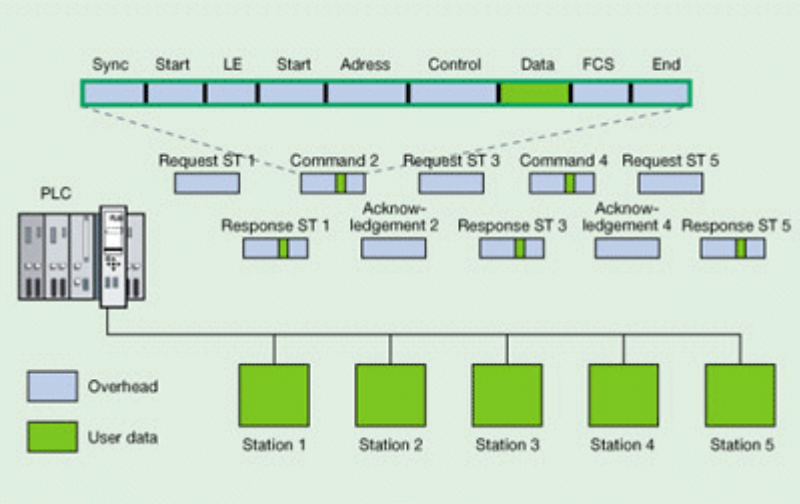

Fig. 4-17: Linear structure for message-based transmission

Cycle Time and Calculation

Process data that is to be sent to I/O devices is stored in the output buffer of the master in the physical order of the connected output stations. During data output, process information in the form of

input data is simultaneously returned to the input buffer of the master. Once the entire summation frame has been sent and simultaneously read in again, all output data is correctly positioned in the individual devices.

The data is made available to the host as defined by the user. A network is established by connecting all the devices, whose length and structure corresponds exactly to the structure of the user data field in the summation frame telegram. The amount of user data for the summation frame method is over 60%. Bus access conflicts do not occur due to the master/slave structure. This means that potential error sources are avoided from the outset.

PCP Transmission

To transmit parameter data simultaneously as well as time-critical process data, the data format must be expanded by a certain time slot. In several consecutive cycles, a different part of the data is inserted in the time slot provided for the addressed devices. The PCP (*Peripherals Communication Protocol*) software performs this task. It inserts one part of the telegram in each INTERBUS cycle and recombines it at its destination.

The parameter channels are activated if necessary and do not affect the transfer of I/O data. Longer transmission time for parameter data that is segmented into several bus cycles is sufficient for the low time requirements that are placed on the transmission of parameter information.

Transmission Reliability

The bus master ensures transmission reliability by using the loop-back word. This unique bit combination is executed in a calculated number of bus system cycles. If it has returned to the master input buffer after this time, the ring is closed. Data is saved according to the CRC16 method. This information is attached to the data, and evaluated by the receiver.

Determinism

An important feature of INTERBUS is determinism, i.e., the guaranteed time in which cyclic data transfer is carried out between spatially distributed devices. The summation frame method also ensures that the process image for all devices is consistent, because all the input data originates from the same point of scan time and all the output data is accepted by the devices simultaneously.

Optimum EMC Behavior

Unlike other bus protocols, the physical transmission speed of INTERBUS lowers the component and cabling costs while improving electrical noise immunity. INTERBUS provides high data throughputs without compensating for the protocol overhead by increasing transmission speeds, and noise susceptibility, which is common for conventional message-based systems.

4.2.7 Real-time aspects of ModbusPlus

ModbusPlus is a proprietary specification and is used for communication between individual PLCs in a system. It is based on cyclic token passing between devices. The jitter of 200 ns is outstanding in comparison with other technologies. The communication timing can be calculated with exact formulas introduced in *Appendix B*.

4.2.8 Real-time aspects of PROFINET IO

The Ethernet-based communication at PROFINET can be scaled. It has three performance levels:

1. TCP, UDP and IP for non-time-critical data, such as parameter assignment and configuration,

2. Real-Time (RT) for time-critical process data used in the field of factory automation and

3. Isochronous Real-Time (IRT) for particularly sophisticated demands, as for Motion Control applications.

These three performance levels of PROFINET communication cover the entire spectrum of automation applications. Key features of the PROFINET communication standard include the following:

- Coexistent use of real-time and TCP-based IT communication on a single line
- Standardized real-time protocol for all applications, for communication between components in distributed systems as well as between the controller and the decentralized field devices
- Scaleable real-time communication from performant to high-performant and time synchronized

The characteristics of the scaleable and standardized communication basis are one of the key strengths of PROFINET. They ensure consistency right through to corporate management level and fast response times in the automation process.

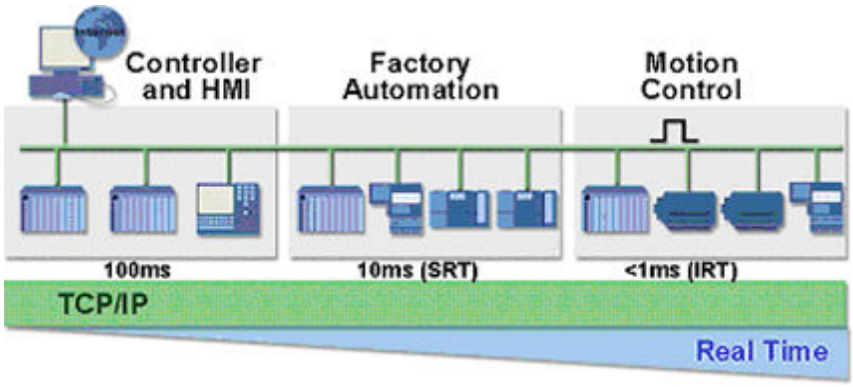

Fig. 4-18: The Ethernet-based communication for PROFINET can be scaled

With PROFINET IO the UDP/IP-based RPC is used at startup for the initiation of data exchange between the devices, parameter assignment of the distributed field devices and diagnostics. Due to the open and standardized RPC protocol, HMI stations and engineering systems (IO-Supervisors) can also access PROFINET IO-Devices.

The RT communication is then used for the transmission of IO data and alarms. The IRT communication is finally used in sufficient for Motion Control applications. These require update rates of around 1 ms with a jitter accuracy for the consecutive cycles of 1µs for up to 100 nodes. To meet these demands, PROFINET has defined the time-slot-controlled transmission method IRT on the Layer 2 Protocol for Fast Ethernet.

4.2.9 Real-time aspects of SERCOS III

SERCOS III is based on the established real time mechanisms of the SERCOS interface and continues to work on the principle of cyclic data transfer with an exact time pattern (time slot mechanism). The synchronization is hardware-based performed on FPGA technology. With a clear Master-Slave hierarchy. The application was originally focused on reliable motion control as drive interface. The portation of the SERCOS interface to Ethernet increases the transmission speed from 16 Mbps to 100 Mbps. The logical topology is a ring that can be physically realised as double ring or as a simple ring (line structure). The double ring structure offers a redundant data transfer or/and redundancy respectively fault tolerance in case of a broken line. The ring structure also enables a slave to slave communication. Since SERCOS III does not use the star topology of the standard Ethernet no hubs or switches are needed, each device owns 2 Ethernet ports. Fig. 4-19 below shows the composition of the communication cycle.

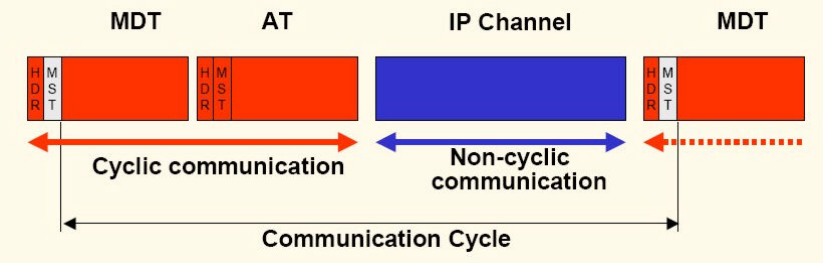

Fig. 4-19: Sercos III communication cycle

For hard real time requirements a collision free real time channel is used. The cyclic data are embedded in one standard Ethernet frame released by the master, transmitted from slave to slave in the ring and at the end sent back to the master. As with all summation-frame like technologies the efficiency (the relation of user data to header data) is high. The transmission of none real time data is organised in a separate, parallel time channel within the communication cycle.

The minimum cycle time is 31.25 µs with a Jitter <1 µs and can be achieved with up to 8 drives and allocated 8-byte cyclic data each. One master (motion control) can be connected to a ring with a maximum number of 254 slaves (e.g. drives) and (also via switches) to further controllers.

For the future it is also planned to define a profile for the synchronization and communication between motion controls to synchronise different real-time segments (rings). Likely this could be also IEEE1588 based.

4.2.10 Real-time aspects of Bluetooth

Asynchronous data exchange is carried out on a request/response basis, if asynchronous communication is required. In such a case, control checksums at different levels are added and the stack takes care of errorless transfer. ARQ (*Auto repeat request*) is employed. Deadline for 50 bytes can reach dozens of ms. Jitter can reach 50 ms. Asynchronous data transfers are suitable for slow diagnostics, configuration, large data block transfers (programs).

If voice (synchronous) data transfer is employed, the data safety methods are restricted to accelerate the transfer. Data are not re-sent if errors occur. The bit rate is limited to dozens of kbps.

Each of these two data transfer paradigms is bound to a profile. The profiles can be bypassed by using HCI protocol.

4.2.11 Real-time aspects of GPRS

To deal with both packet- and circuit-switched data, GPRS incorporates three new entities in its network, namely, packet control unit (PCU), serving GPRS support node (SGSN) and gateway GPRS support node (GGSN). These are interconnected with each other and with the existing GSM network elements via a series of interfaces which support both traffic as well as signalling connections. The PCU, shown in Fig. 4-20, ensures that the packets are of the correct size for transmission (segmentation), determines Quality of Service (QoS) measurements, and allocates radio channels.

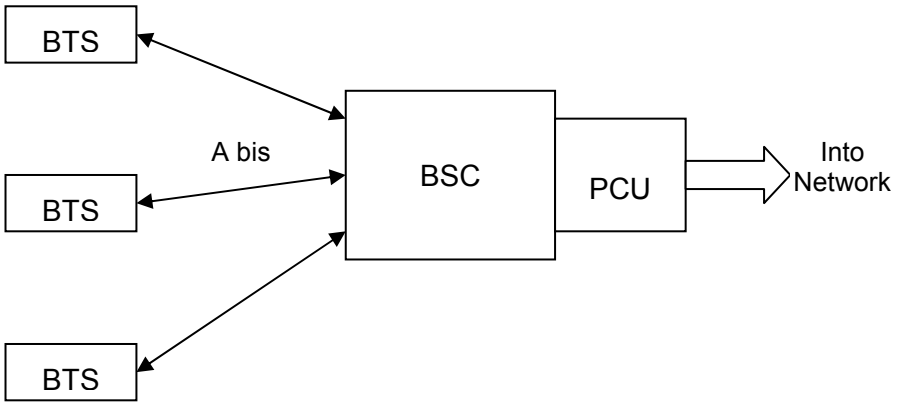

Fig. 4-20: Packet Control Unit in GPRS.

Data Transmission

All the physical aspects of the GPRS air interface, namely, the radio channels used, the modulation scheme, and the multiple access method, all have a defined structure and format. Three types of channels are used: radio channels (defined by frequency), physical channels (defined by timeslots) and logical channels (defined by function).

The time structure on which the GPRS air interface is based is a frame containing 8 timeslots over a period of 4.62 ms. This structure repeats, giving each mobile station an opportunity to transmit or receive information for 0.577 ms every 4.62 ms. Each physical channel consists of one out of eight timeslots on a carrier. Use of a physical channel requires transmission and reception of short burst of data with periodicity equal to frame length i.e., one every 4.62 ms. The GPRS network supports 52-frame multi-frames.

Data transmission is via a full-duplex system consisting of uplink and downlink bands, making use of a combined FDMA-TDMA multiple access system.

Burst	Burst	Burst	Burst	Burst	Burst	Burst	Burst	Burst

Fig. 4-21: GPRS Frame Structure.

3t	57 data	1f	26 synch	1f	57 data	3t	8.25 guard

Fig. 4-22: GPRS Traffic Channel Slot Structure.

On top of the physical channels, a series of logical channels are defined to perform a multiplicity of functions, e.g., signalling, broadcast of general system information, **synchronization**, channel assignment, paging, and payload transport.

Quality of Service

The QoS requirements of typical mobile packet data applications are very diverse (e.g., real-time multimedia, Web browsing, and e-mail transfer). Support of different QoS classes, which can be specified for each individual session, is therefore an important feature. GPRS allows the definition of QoS profiles using parameters such as service precedence, reliability, delay, and throughput.

The service precedence is the priority of a service in relation to another service. There exist three levels of priority: high, normal, and low. The reliability indicates the transmission characteristics required by an application. Three reliability classes are defined, which guarantee certain maximum values for the probability of loss, duplication, mis-sequencing, and corruption (an undetected error) of packets.

The delay parameters define maximum values for the mean delay and the 95-percentile delay. The latter is the maximum delay guaranteed in 95 percent of all transfers. The delay is defined as the end-to-end transfer time between two communicating mobile stations or between a mobile station and the Gi interface to an external packet data network. This includes all delays within the GPRS network, e.g., the delay for request and assignment of radio resources and the transit delay in the GPRS backbone network. Transfer delays outside the GPRS network, e.g., in external transit networks, are not taken into account. The throughput specifies the maximum/peak bit rate and the mean bit rate.

Using these QoS classes, QoS profiles can be negotiated between the mobile user and the network for each session, depending on the QoS demand and the current available resources. The billing of the service is then based on the transmitted data volume, the type of service, and the chosen QoS profile.

Class	**Probability for**			
	Lost packet	**Duplicated packet**	**Out of sequence packet**	**Corrupted packet**
1	10^{9}	10^{9}	10^{9}	10^{9}
2	10^{4}	10^{5}	10^{5}	10^{6}
3	10^{2}	10^{5}	10^{5}	10^{2}

Table 4-2: GPRS Reliability Classes

Class	**128 byte packet**		**1024 byte packet**	
	Mean delay	**95% delay**	**Mean delay**	**95% delay**
1	<0.5s	<1.5s	<2s	<7s
2	<5s	<25s	< 15s	<75s
3	<50s	<250s	<75s	<375s
4	Best effort	Best effort	Best effort	Best effort

Table 4-3: GPRS Delay Classes

Latency and Jitter

Latency is the time taken for data packets to pass through the GPRS bearer, normally measured as a round-trip time. Jitter is the variability in this time. In GPRS, there are a number of factors contributing to the overall latency. These include: the mobile station (MS), radio resource procedures, the effective data throughput and the GPRS core network nodes.

Mobile station delay is the time taken by the MS to process an IP datagram and request radio resources. This includes the delay from the PC to MS, and the MS processing time. This delay is typically less than approximately 100 ms, with the possible exception of the processing associated with establishing the initial uplink radio channel. The time taken depends on the MS, and hence the supplier.

Radio resource procedures are the major source of delay in GPRS. In order for the MS to be capable of sending or receiving data, radio resource known as a temporary block flow (TBF) must be made available to the user. If a TBF is currently active, then the MS may use it hence minimising the delay. However, if no TBF is established, then the MS and the network must exchange signalling messages in an attempt to establish a TBF. The time taken to successfully achieve an active TBF will depend on the availability of radio resources and will be different for the uplink and downlink directions. Once established, the TBF will generally remain active for as long as data is made available to the layer (i.e. for as long as there are LLC frames to transmit).

Effective data throughput (over-the-air delay) is the rate at which the user data is physically transmitted between the MS and the SGSN over an active TBF. The delay associated with this throughput is directly related to the size of the IP datagram being sent. Smaller packets cause less delay. The delay is proportionally reduced when multiple timeslots are used. The effective throughput is also dependent on the number of re-transmissions resulting from hostile radio environments (i.e. the RLC Block Error Rate). The time taken to re-transmit the erroneously received information will affect the quantity of the delay.

Core network delay occurs as packets transit through the SGSN and the GGSN. These nodes effectively operate as IP routers and as such will have a relatively low impact on the overall latency. However, under high load conditions, the transit delay may increase.

The maximum speed of a GPRS connection is the same as that of a modem connection in an analogue wired telephone network, about 4–5 kBps (depending on the phone used). Latency is very high: a round-trip ping being typically about 600–700 ms and often reaching one second round trip time. GPRS is typically prioritised lower than speech, and thus the quality of connection varies greatly.

4.2.12 Real-time aspects of EDGE

EDGE is a superset to GPRS and can function on any network with GPRS deployed on it. The idea behind EDGE is to eke out even higher data rates on the current 200 kHz GSM radio carrier by changing the type of modulation used, whilst still working with current circuit (and packet) switches. Hence, the features described above for GPRS hold good, in general, for EDGE as well. In addition to GMSK, EDGE uses 8-PSK for its upper five of the nine modulation and coding schemes (MCS). EDGE produces a 3-bit word for every change in carrier phase. This effectively triples the gross data rate offered by GSM. EDGE, like GPRS, uses a rate adaptation algorithm that adapts the MCS used to determine the quality of the radio channel, and thus the bit rate, and robustness of data transmission. It introduces a new technology not found in GPRS, *incremental redundancy*, which, instead of retransmitting disturbed packets, sends more redundancy information to be combined in the receiver. This increases the probability of correct decoding.

4.2.13 Real-time aspects of UMTS

Communication in the UMTS technology is based on 10 ms radio frames. Each frame is divided in to 15 timeslots, where each timeslot can be reserved for uplink or downlink and assigned to different users. Within each 166.7 μs timeslot, different users can communicate using spreading codes on the same carrier (WCDMA technology).

The UMTS technology provides four different QoS classes:

- Conversational class which is used in telephony speech, Voice over IP and conferencing tools between two (groups of) users; defines stringent and low delay and time relation between entities (samples, packets),
- Streaming class, which represents one way transport such as watching real-time video or listening to radio; defines time relation between entities (samples, packets),
- Interactive class, which is applied when a machine or a user requests data from a remote server (web browsing); this class is characterized such that the recipient is expecting the requested data in a certain time period,
- Background class, which is applied when a machine or a user requests data from a remote server (email sending, SMS); this class is characterized such that the recipient is not expecting the requested data in a certain period.

The UMTS bearer supports the following attributes: QoS class, maximum bit rate, guaranteed bit rate, delivery order, maximum Service Data Unit (SDU) size, SDU format information, SDU error ratio, residual bit error ratio, delivery of erroneous SDUs, transfer delay, traffic handling priority and Allocation/Retention Priority. Attributes for all QoS classes are shown in the next table (taken from 3GPP TS 23.107 specification).

Traffic class	Conversational class	Streaming class	Interactive class	Background class
Maximum bit rate (kbps)	< 2 048	< 2 048	<2 048 - overhead	<2 048 - overhead
Delivery order	Yes/No	Yes/No	Yes/No	Yes/No
Maximum SDU size (octets)	≤ 1502	≤ 1502	≤ 1502	≤ 1502
Residual BER	$5\cdot10^{-2}$, 10^{-2}, $5\cdot10^{-3}$, 10^{-3}, 10^{-4}, 10^{-6}	$5\cdot10^{-2}$, 10^{-2}, $5\cdot10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$4\cdot10^{-3}$, 10^{-5}, $6\cdot10^{-8}$ (value is derived from CRC)	$4\cdot10^{-3}$, 10^{-5}, $6\cdot10^{-8}$ (value is derived from CRC)
SDU error ratio	10^{-2}, $7\cdot10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-1}, 10^{-2}, $7\cdot10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-3}, 10^{-4}, 10^{-6}	10^{-3}, 10^{-4}, 10^{-6}
Transfer delay (ms)	≤ 100	≤ 250		
Guaranteed bit rate (kbps)	< 2 048	< 2 048		
Traffic handling priority			1, 2, 3	
Allocation/Retention priority	1, 2, 3	1, 2, 3	1, 2, 3	1, 2, 3

Table 4-4: UMTS Classes

4.2.14 Real-time aspects of Wi-Fi

Communication in the Wi-Fi network is based on the client/server principle using CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Real time properties come from the standard IEEE802.11e which offers two modes of operation - Enhanced Distributed Coordination Function (EDCF) and Hybrid Coordination Function (HCF). HCF mode is supported only by networks with a dedicated Access Point (AP).

With EDCF, high priority traffic has a higher chance of being sent than low priority traffic: a station with high priority traffic waits a little less before it sends its packet, on average, than a station with low priority traffic. There are no real guarantees of Quality of Service (QoS).

The HCF works as following – the interval between two beacon frames (each beacon is usually sent every 100ms) is divided into two periods, the CFP and the CP. During the CFP, the AP controls the access to the medium. During the CP, all stations function in EDCF mode. The AP can coordinate the traffic in any fashion it chooses. Moreover, the stations give info about the lengths of their queues for each Traffic Class (TC). The AP can use this info to give priority to one station over another. All stations can send multiple packets in a row, for a given time period selected by the AP. During the CP, the AP may choose to resume control of the access to the medium by sending CF-Poll packets to stations. With the HCF, things like bandwidth control, fairness between stations and classes of traffic can be configured within the AP.

The reaction time in the *Appendix B* is estimated as the minimum time that one station has to wait to access the medium. Time required to transfer the smallest packet is ~250 µs (200 µs preamble +~50 µs time for collision avoidance and sending a packet).

4.2.15 Real-time aspects of ZigBee

Communication on ZigBee is based on the client/server principle. RT is provided by optional use of the beaconing mode[1]. Beacon signals are transmitted by the network coordinator in constant intervals, delimiting a superframe consisting of 12 timeslots. Out of these 12 timeslots, a defined number of contention-free timeslots can be reserved for cyclic RT data. Hence, these timeslots are dedicated for peer-to-peer communication

This principle is the cornerstone of standing up to QoS requirements. Furthermore, packet loss is prevented by sending acknowledgement frames which signal successful packet reception. The MAC packet payload and the header are used for MIC (Message Integrity Code) calculations with 4, 8, or 16 octets. The MAC packet also provides freshness counts to ensure that the packet is up-to-date, which prevents replay attacks.

Clock synchronization of RT mode is provided by coordinator Beacons which delimit the superframe structure. Synchronization is performed by MAC messages. The synchronization method is proprietary.

[1] Beaconing is a term to describe a packet broadcast which is used by an awakening node to advertise or solicit an interaction between two or more nodes.

The ZigBee specification claims that the enumeration of a new slave takes 30 ms which makes the responsiveness of a new node in the network very fast.

The basic drawback is the throughput limited to 250 kbps, which in future, and even today, is a potential risk within fast communication. Furthermore, developers claim that this technology is suitable for applications with very low duty cycles with adequate power source (non-rechargeable batteries). RT performance would have to be considered, if the network load increases. Finally, higher layers of the ZigBee stack are still under development and need trend screening.

4.3 Conclusion

Real-time characteristics of communication systems used in automation range from the order of microseconds (isochronous real-time systems) to the order of seconds (GPRS). The required time-domain parameters of automation communication system depend on utility function of the controlled systems. The utility function can be described by deadline and jitter. Consecutively the real-time parameters of communication systems can be described as latency (delay) and a jitter. For strictly deterministic communication systems there are guaranteed latency and jitter parameters. However for stochastic systems these parameters, which define Quality of Services) are either undefined or defined in a stochastic way using averages and quantils (e.g. 95% percentile delay for GPRS).

In the field of industrial automation the real-time control is being performed using real-time networks with appropriate real-time properties. However the hard real-time control is being achieved within single LAN. Inter-LAN or WAN communication based on TCP/UDP/IP stack is considered to be at best soft-real-time due to the best effort bases of the interconnected communication systems.

Within VAN WP4 the real-time parameters of communication system have to be investigated with the aim to enable uniform classification of various communication links. Also investigation of real-time features of various interconnecting devices and solutions has to be investigated to enable to evaluate, classify and validate real-time properties of LANs, inter-LANs and WANs. Real-time application requirements have to be taken into account when designing the RT classification too. The classification will enable engineering of automation solutions utilizing real-time control within LANs, multiple LANs with inter-LAN real-time data exchange, or even over WANs.

An important part of real-time control is clock synchronization. For deterministic automation systems the clock synchronization algorithms are well established. However it is necessary to deeply investigate clock synchronization algorithms that enable inert-LAN or WAN synchronization of local clocks while matching the requirements of automation applications. Uniform VAN clock synchronization method will enable broad range of VAN features including synchronized event executions, data-logging, diagnostics, remote post-mortem analysis etc.

5 Safety Technologies

5.1 Introduction

5.1.1 Motivation

The development of safety networks represents a major step forward in the overall migration of safety applications. Similar to its everyday counterpart, a safety network is a fieldbus system that connects devices on the factory floor. It consists of a single cable that allows for quick connect/disconnect of replacement devices, simple integration of new devices, easy configuration and communication between the devices, delivery of diagnostic data (as opposed to just on/off status updates), and a wealth of other features to help workers maintain a safety system more efficiently. But unlike standard networks, which also provide this functionality but are designed to tolerate a certain number of errors, a safety network is designed to trap these errors and react with pre-determined safe operation.

Companies can choose to deploy a safety network for the significant wiring savings and ease-of-installation, or they can use it to their full advantage by capitalizing on the network's diagnostic capabilities, enhancing the underlying performance of the manufacturing process. When an error occurs today, for example, a hardwired safety system responds by shutting off the power to all the PLC outputs — essentially shutting down the entire application. Regardless of the problem, the response of the system is the same. This reaction negates a hazardous situation, but at a substantial cost. Once an entire application is powered down, it takes a significant effort to get it up and running again — time and energy that equates to significant profit loss and broken commitments to customers.

With a networked system, on the other hand, the safety controller can make a narrower decision as to what needs to be shut down and what can continue operating. If, for instance, a misaligned safety sensor is impacting a robotic arm in a cell located at the far end of the facility, the shutdown can be limited to that particular cell. Not having to cut power to an entire area or machine when a safety event occurs translates into greater productivity. The key to this ability is the advanced diagnostics designed into the controller, networks and I/O devices, as well as both firmware and application software-level response to those diagnostics.

At first it may seem risky to rely on communications and software to change a system's behaviour in such a way. However, the protocol inherent in a safety network takes measures to ensure a high level of integrity within the application. These measures, such as message redundancy and cross checking, ensure that safety messages are reliably transmitted from one device and received at another in the predetermined time and with the integrity of the data content maintained.

5.1.2 EN 954-1 Standard

EN 954-1 is a European Standard developed by the European Committee for Standardization (CEN) [EN 954-1] and was first released in November 1992. [FAA01] The standard was developed for the safety of machinery and is titled "Safety of Machinery, Safety related parts of control systems". The

standard has two parts: Part 1: General principles for design, and Part 2: Validation, testing, fault lists. The standard makes numerous references to the EN 292-1:1991 standard for basic terminology and methodology. EN 954-1 sets out a procedure for the selection and design of safety measures. The procedure contains the following 5 steps:

- Hazard analysis and risk assessment,
- Decide measures to reduce risk,
- Specify safety requirements to be provided by the safety related parts of the control system,
- Design, and
- Validation.

EN 954-1 also provides a list of typical safety functions:

- Stop,
- Emergency stop,
- Manual reset,
- Start and restart,
- Response time,
- Safety related parameters,
- Local control functions,
- Fluctuations, loss and restoration of power sources,
- Muting, and
- Manual suspension of safety functions.

Categories that define the behaviour of the safety related parts of the control system are specified in the EN 954-1 standard. The categories are B, 1, 2, 3 and 4 with category B being the lowest with no special measures for safety, and Category 4 being the highest where no single fault shall lead to loss of safety and the single fault shall be detected. An Annex provides guidance for the selection of categories. The EN 954-1 standard should be used for the development of low complexity safety-related systems for the machinery.

EN 954-1 states that, to meet the requirements of category 4, “a single fault in the control system shall not lead to a loss of the safety function”, and that “the single fault is detected at or before the next demand upon the safety function.” If this is not possible, “an accumulation of faults shall not lead to a loss of the safety function.” In other words, it must be possible to manage a variety of potential faults. The security of the bus system is based primarily on a safe communications protocol, which includes security mechanisms such as CRC checksums, echo mode, connection/addressing tests and time monitoring. The ISO/OSI reference model is an internationally recognised method of representing the functionality of complex communications systems. Functions are divided into a layer model with seven different functionalities.

5.1.3 IEC 61508

IEC 61508 — the International Electrotechnical Commission (IEC) standard for functional safety in programmable electronic systems — defines the functionality of safety networks. This seven-part standard [IEC61508] defines the requirements of a safety system to comply with the appropriate safety integrity level (SIL).

Recently introduced, IEC 61508 redefined the way safety systems are assessed, switching from a prescriptive rules based approach to a goal-oriented approach. This change has been instrumental in allowing the development of advanced safety control systems and, in particular, in the growing use of safety networks as an alternate to hardwired circuits. Prior to IEC 61508, a vendor demonstrated that its components and solutions were designed in accordance with block diagrams prescribed by the assessors. Now users and vendors together perform risk assessments to examine potential failures, documenting the consequences and probability of occurrence. This analysis determines the SIL that must be achieved by the protective system, which in turn defines the maximum allowable Probability of Failure on Demand (PFD).

The top-most integrity level (SIL 4) is applied to such critical equipment as that used on aircraft and in nuclear power plants. SIL 3, meanwhile, is the highest-level found in traditional manufacturing and process applications.

Safety Integrity Level	**Mode of Operation** Average Probability of Failure on Demand – per Hour	
	Low Demand	High Demand or Continuous
SIL 4	$> 10^{-5} < 10^{-4}$	$> 10^{-9} < 10^{-8}$
SIL 3	$> 10^{-4} < 10^{-3}$	$> 10^{-8} < 10^{-7}$
SIL 2	$> 10^{-3} < 10^{-2}$	$> 10^{-7} < 10^{-6}$
SIL 1	$> 10^{-2} < 10^{-1}$	$> 10^{-6} < 10^{-5}$

Table 5-1: IEC 61508 Safety Integrity Levels

With this goal-oriented approach, the end result is more important than the equipment used to achieve it. So essentially, the new standard questions whether a system is safe rather than if it “looks” safe. Once this determination has been made, the decision of whether to use a network is the same as deciding on networks in standard applications, such as improved diagnostics, lower cost or the need for a distributed system.

5.1.4 Possible Transmission Errors

During the communication a lot of transmission errors can occur. In the following lines they are mentioned. In the next chapter measurements are described, which can avoid these transmission errors.

Repetition

Due to an error of a bus participant, old, non-up-to-date messages are repeated at an incorrect point in time. This may cause a dangerous situation in a receiver (e.g. access door closed although it is already open).

Loss

Due to an error of a bus participant, a message is deleted (e.g. request for safe stop).

Insertion

Due to an error of a bus participant, a message is inserted. (e.g. release of a safe stop)

Incorrect sequence

Due to an error of a bus participant, the sequence of messages is changed.

Example: Before going to a safe stop, a safe reduced speed is to be selected. If the messages are swapped, the machine is running instead of going to a safe stop.

Remark: Bus systems may contain elements that store telegrams (FIFOs in repeaters, routers etc.) that may alter the sequence.

Message corruption

Due to an error of a bus participant, or due to errors on the transmission medium, messages are corrupted.

Delay

The transmission line is overloaded by the data exchange that occurs during normal operation. A bus participant causes overload by sending incorrect messages so that a service associated with a message is delayed or impeded.

Coupling of safety relevant and non-safety relevant messages:

Due to an error of a bus participant, safety relevant and non-safety relevant messages get mixed up.

5.1.5 Description of Error Abatement Measures

The following chapter lists measures that serve to overcome transmission errors.

Consecutive number

A consecutive number is appended to each message that is exchanged between sender and receiver. This consecutive number may be defined as an additional data field containing a number that changes in a predetermined way from one message to the next.

Time stamp

In most cases, the content of a message is only valid at a particular point in time. The time stamp is e.g. a date that is appended to a message by the sender. There are relative time stamps, absolute time stamps and dual time stamps.

Time expectation (time-out)

During the transmission of a message, the receiver checks whether the delay between two messages exceeds a predetermined value. If this is the case, an error has to be assumed.

Reception acknowledgement

The message sink sends a message on the content and the reception of the original message back to the source. As an example, a reception acknowledgement may repeat the data to allow the sender to check the correct reception.

Remark: Some bus systems use the terms like “echo” and "acknowledgement" as synonyms.

Identification for message sender and receiver

Messages may have a uniform sender and/or receiver identifier that describes the logical address of the safety related participant (authenticity).

Data integrity assurance

The data integrity assurance is a fundamental component to reach the required safety level. Various pragmatic concepts are being discussed that may all lead to the required category (according to EN 954-1) or the required Safety Integrity Level (according to IEC 61508).

Redundancy with cross check

For this method, sender and receiver have dual channels. The message is sent twice in independent transmissions. In addition to this, the transmitted messages are cross-checked for validity over the bus or over a separate connection within the dual channel sender/receiver unit. If a difference is detected, an error must have taken place during the transmission, in the processing unit of the sender or the processing unit of the receiver. When redundant media are used, then there must be safeguarding by suitable measures (e.g. diversity, time skewed transmission) against failure due to a common cause.

Different data integrity assurance systems for safety relevant (SR) and non-safety relevant (NSR) data.

If safety relevant (SR) and non-safety relevant (NSR) data are transmitted via the same bus, different data integrity assurance systems or encoding principles may be used (different CRC algorithms, different generator polynomials) to make sure that NSR messages cannot influence any safety function in an SR receiver.

5.1.6 Selecting a network

Now that the IEC standards framework no longer excludes safety networks, several vendors and/or organizations are rapidly developing multiple networks to meet the expected demand from end users. Due to the general nature of guaranteeing safety, these networks will most likely share basic features, such as fulfilled safety requirements, pre-determined safety states, determinism and dual-CPU designs.

Most importantly, safety networks must be designed to recognize and to handle all possible transmission errors (above mentioned).

Second, safety networks must be designed to allow devices to enter a pre-determined safe state when a communication error occurs. A safe state for one device, such as the swinging robotic arm, could be immediate “power off.” The safe state for an exhaust fan, meanwhile, could be “power on” ensuring harmful substances cannot accumulate and if present are dispersed.

Third, a safety network must be deterministic to ensure all safety messages are transmitted in a predefined and predictable amount of time. A safety network allows customization for each device to have its own periodic response time. This is scaleable to a single device or a chain of associated safety devices. From this, safety devices have guaranteed expectation of message delivery. Some safety messages include a timestamp, which is checked to ensure that it arrives within the defined time expectation. Safety messages arriving beyond the time expectation will cause the affected connection and associated device(s) to go to its safe state.

5.1.7 Safety Loops

When dealing with multiple networks, it is important to consider how safety loops are closed. There are two approaches for closing a loop between an input and output device. The first is the controller-centric approach, which mandates that all safety loops go through a safety PLC. The second is the safety network controller approach, which doesn't require a safety PLC to be part of the safety loop. The latter method could be categorized as a conventional relay replacement and is typically used for very tight loop closures. Both approaches have advantages and are not mutually exclusive, which means manufacturers can use a combination of both.

5.1.8 Safety Engineering

The programming of "Safety Logic" and parameterization of "Safety Devices" has to be safe in every stage and depends on the target system. Typically the engineering system (ES) should contain special protective measures to prevent failures as soon as possible. Some typically measures are:

- safe editors (input of data, variables, code, parameters);
- safety data storage (e.g. additional CRC);
- diverse 2-channel compiler (depends on target architecture);
- checks of plausibility as soon as possible to prevent user errors;
- checks of strictly recommended separation of safe and non-safe parts of code, variables, parameters;
- checks of consistency and completeness of program and parameter sets as good as possible;
- special additional checks of download of program and parameters.

5.2 Selected Safety Technologies

Several safety technologies were chosen to introduce the solution of the abovementioned safety aspects. Parameters, which can be compared across technologies, are specified in *Appendix C*.

5.2.1 AS-Interface Safety at Work

Safety at Work [ASISafe] is a safety concept based on the AS-Interface standard [ASI] for the implementation of applications for safety machines and plants. By using this interface is possible to implement the wiring of a plant up to control system category up category 4 according to EN 954-1 and SIL3 according to IEC 61508.

AS-Interface Safety at Work can be used in vast variety of safety applications, including robotics, conveyor systems, handling systems, airport carousels and further. The AS-Interface Safety at Work System allows safety components to be easily integrated into standard AS-Interface networks.

Safety and standard components work in parallel on the same cable. The AS-Interface master considers the safety slaves like all other slaves and incorporates them into the network. The high safety level is guaranteed due to special safety slaves and a safety monitor. Safety-related actuators are being controlled by the safety monitor. There is no need for safety version of AS-Interface master. The safety slaves encode information “Stop not actuated” into a 8 x 4 bit code sequence that is unique for each safety slave.

The code sequence is transmitted in standard slave responses so transmission of the code sequence requires 8 bus cycles. The safety monitor listens to the slave responses and compares each safe slave response with the teached-in reference values. The code sequences are defined so that any error on an input of the safe slave results in breach of the sequence. Breach of the code sequence results in action of the safety monitor.

The number of safety devices (monitors and safety slaves) on a bus is limited to 31.

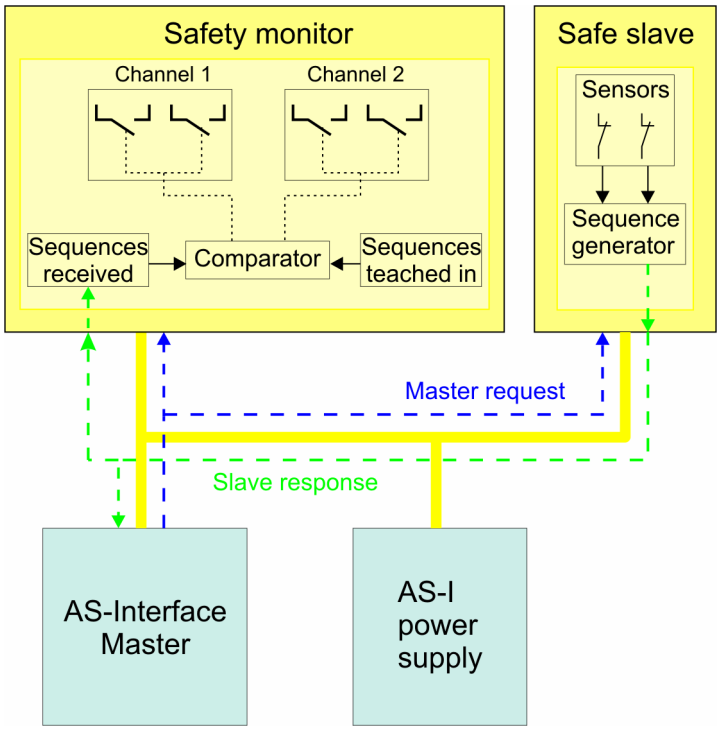

Fig. 5-1: Safety at Work

5.2.2 CIP Safety

The ODVA [ODVA] defined a safety protocol that is media-independent. Safety extensions to the Common Industrial Protocol (CIP) – on which DeviceNetsafety™ is based – can be applied to other CIP-based networks like ControlNet™, EtherNet/IP™ and other future technologies [CIPSafe]. This allows for the seamless transfer of safety I/O messages from any point in the multi-segment architecture to one or more points in the same architecture using either point-to-point or multi-cast connections.

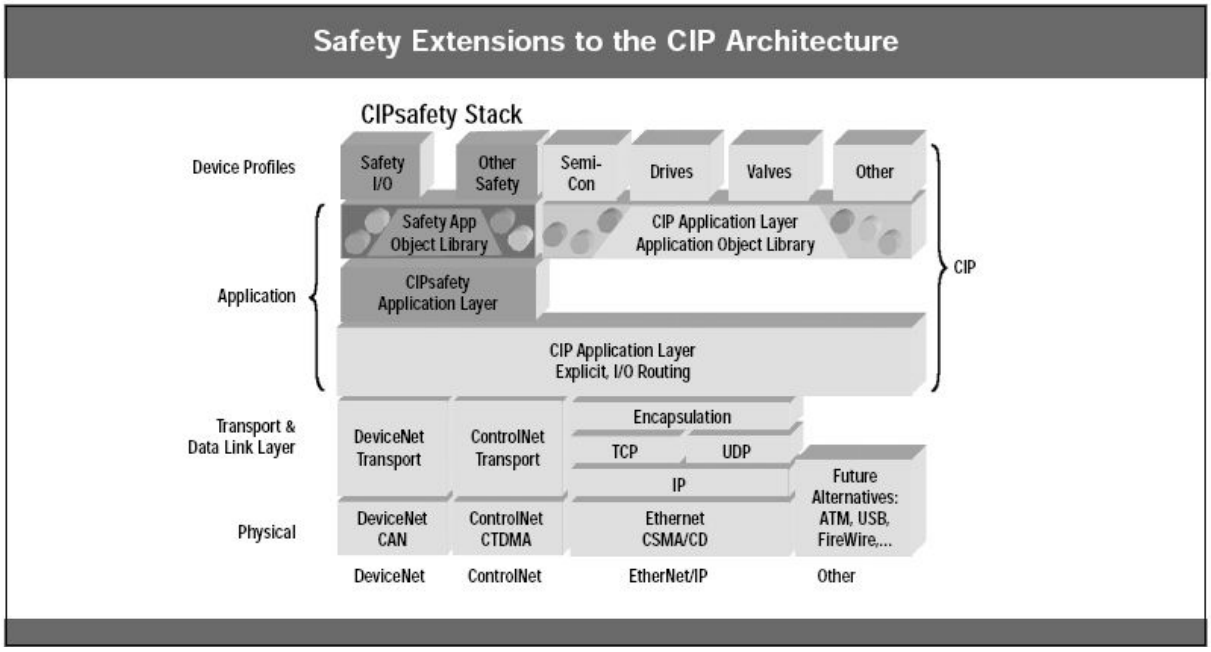

Fig. 5-2: CIP safety extension

Main features of CIP Safety

In addition to the producer/consumer architecture, which allows devices to synchronize for precise system performance, DeviceNet has following attributes:

- Robust media, which has been tested in high noise and other challenging environments;
- Automatic checking for duplicate node addresses;
- Built-in retries at the data-link layer;
- Priorities established by configuration;
- Bit error rate of $\leq 10^{-7}$ under stress (i.e., approximately one error transmitted every 150 years on a fully loaded system);
- Error counters for each connection to the network;
- Connection based messaging so both producer and consumer can identify data failure.

Standard DeviceNet media and topology requires no changes when used in safety implementations. That means DeviceNet users can continue to use existing wiring to implement a safety system by adding DeviceNetsafety devices to the existing network. End users will be able to integrate standard and safety controls on a single network. The DeviceNetsafety Protocol ensures that standard devices do not interfere with the function of the safety devices and vice versa.

Because CIPsafety is an extension of standard CIP, it automatically inherits the bridging and routing capabilities of EtherNet/IP, ControlNet and DeviceNet.

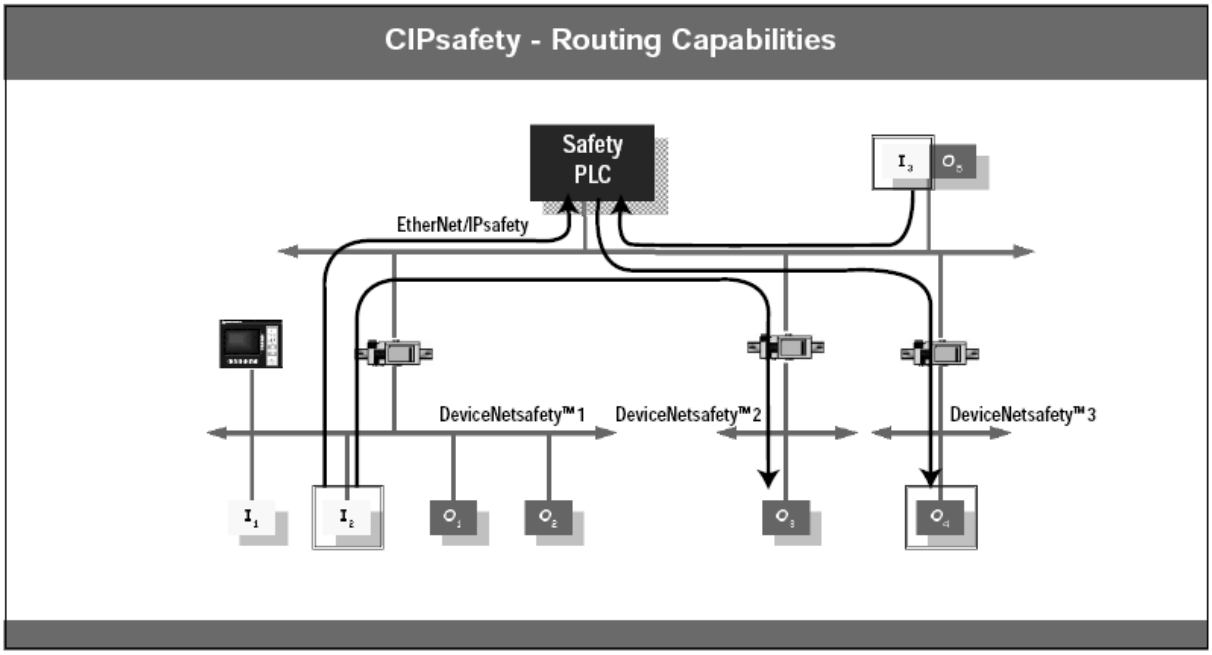

Fig. 5-3: Routing capabilities of CIPsafety

5.2.3 EPLsafety

EPLsafety, designed by EPSG (Ethernet Powerlink Safety Working Group), is defined as a bus-independent safety extension for ETHERNET Powerlink - it defines an autonomous frame, which can in principle be inserted into other standard protocols than Powerlink. This safety frame is for example compatible with CAN messages, so the compatibility with CANopen model is kept. EPLsafety allows both publish/subscriber and client/server communication. Safety relevant data is transmitted via an embedded data frame inside of standard communication messages. EPLsafety defines uniform telegram format for different data purposes (payload data, configuration, time synchronization), each EPLsafety node recognizes automatically the data purpose of the telegram. Measures to avoid any undetected failures due to systematic or stochastic errors are an integral part of the safety protocol.

The safety related data frame allows data transfer capacity between 0 and 249 byte net data. By using a specific structure any systematic and most of the stochastic failures can be detected. Using two-byte information on consecutive time, watchdog and addressing information, failures like repetition, wrong sequence, insertion, loss and masquerading can be detected. Besides the techniques to avoid systematic failures, following measures to identify stochastic failures are available: CRC checksum, comparison of redundant data of two subframes, timestamp, and comparison of received address with an internal address or address in look-up table [WRA05].

The residual error probability is less than $5.234 \cdot 10^{-20}$ per frame for peer-to-peer transmission at a bit failure rate of 1 in 10^3. To guarantee that a valid frame is distinguished from frames, which contain invalid data or are delayed, the validity of data can be checked with CRCs and the delay can be checked by comparison of the time of each frame from the producer, the local time of the consumer, and the time difference between producer and consumer. For this reason a time synchronisation mechanism is defined. [EPS05].

The EPLsafety supports sub-networks within one safety-domain, complex network architectures with safe and non-safe sub-nets with own domains are allowed [EPS04]. There can be up to 1023 safety related devices in one safety domain. In total there can be up to 1023 safety domains.

EPLsafety is in conformance with IEC 61508. The protocol fulfils the requirements of SIL 3, and within specific architectures also SIL 4. Error detection techniques have no impact on existing transport layers.

5.2.4 IDA Safety

The IDA Application

An IDA-safety-area is always separated by gateways or bridges from “the rest of the world”. All safety functions only take place in this quite well defined area. The following figure shows a typical safety-network-area for safety applications (Fig. 5-4):

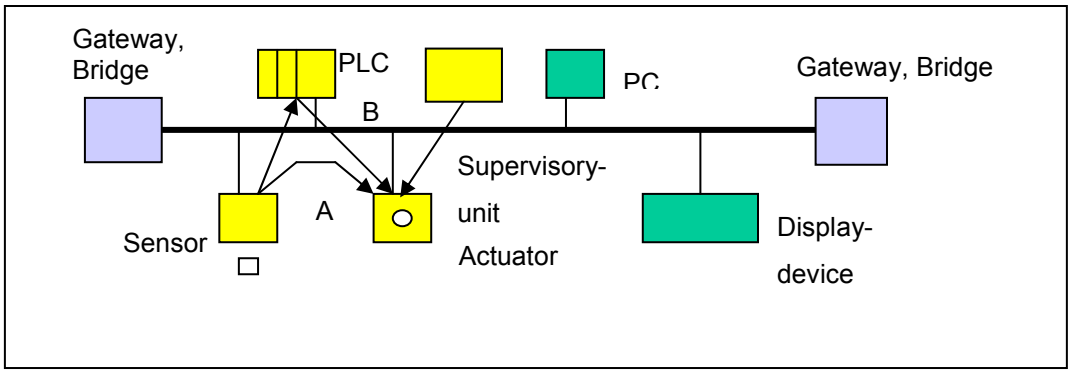

Fig. 5-4: Typical safety network with safety-network-area

The calculation of the reaction time and the failure rate only is valid for this safety-area. But it is also possible to communicate between two or more safety-areas. For that purpose safety related and non-safe data can be transmitted via the gateways or bridges. The data-format for such communication sequences are identical to the safety-format, which is used in the safety-area, but the reaction time depends on the topology of the whole system.

It is a main principle, that all IDA-components have the opportunity to communicate directly without a PC or PLC [IDA]. So it becomes possible, to build up a system with distributed intelligence (A: direct communication from sensors to an actuator).

But the safety-data-format and the necessary services also support the usage of PLCs, PC or other supervisory-controllers (B: communication by the usage of PLCs, PCs or supervisory units). If the structure of distributed intelligence is used, an actuator has to be updated by one or more sensors. In this case, the actuator has to contain the safety-program in order to react in the expected way. The next figure (Fig. 5-5) gives an example of such a communication, where 3 sensors transfer data to 1 actuator.

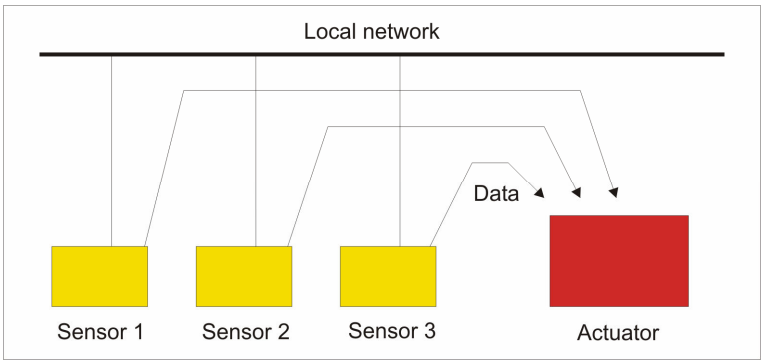

Fig. 5-5: Example of safety communication

A safety related actuator is build up with an internal watchdog. If a valid information is missing or if there is a fault on the local area network, the actor has to reach a safe state. If the actuator gets the right information in time, the watchdog will be reset.

For the priority purpose the system should work with a transmission speed of 100 Mbps. „Twisted pair“ and „fibre optics“ are preferred media. It is highly recommended to use switches to avoid collisions.

The IDA Safety Data Format

In order to meet the requirements of SIL 3, a data format is specified below, which ensures a high level of error detection probability. The format provides the actual safety data with additional information.

The entire data format is therefore part of the data information of the remaining data width (in addition to IP, UDP, and RTPS).

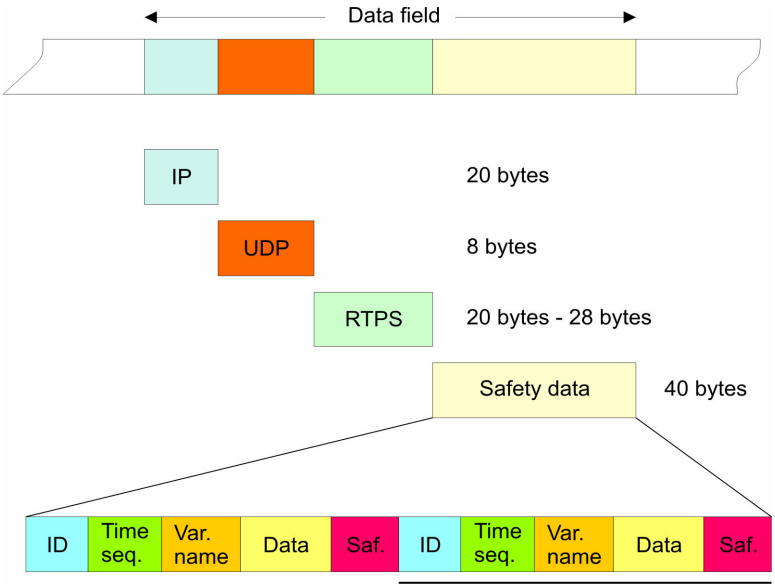

Fig. 5-6: Internal structure of the data field for safety data

As shown in the figure, the IDA Safety data information consists of two data blocks, which have the same structure. The second data block (underlined) contains all the data in inverted form. In addition to the data itself, each individual block contains the variable name and the incremental time code with sequential number. The data record also contains an ID code and a safety sequence[IDASafe].

5.2.5 Interbus Safety

Method of Operation

INTERBUS-Safety profile is based on the Standard INTERBUS communication system [IBClub].

INTERBUS-Safety uses the existing conveyance path for cyclic transmission of data (for process data). This is in principle a master slave concept with a physical ring topology and logical one-to-one relationships between one master and each of its slaves. The data is transmitted via a PDU - commonly known as summation frame - in which each slave fills in its input data and takes out its output data.

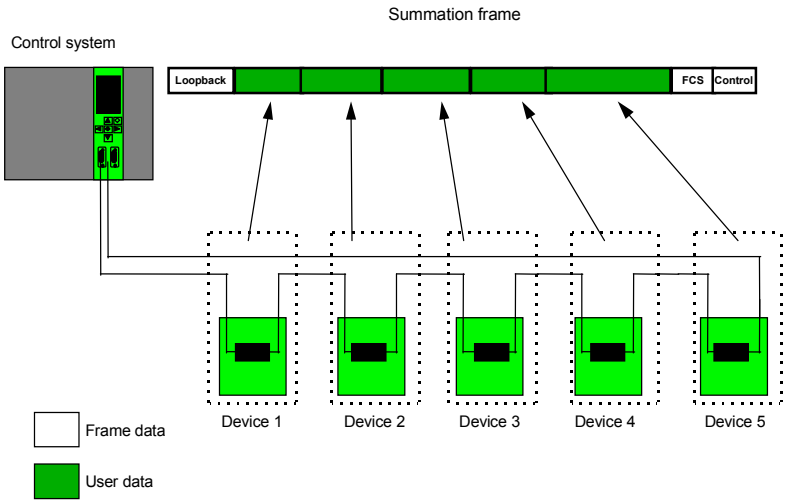

Fig. 5-7: Interbus summation frame

The INTERBUS-Safety layer provides the following measures to realize its safety sublayer:

- consequence numbering;
- time expectation;
- sender/receiver information;
- cyclic redundancy checking for safety data integrity (CRC 24).

Consequence numbering uses the range from 001 to 111 without 000. The sender/receiver information consists of 7 bits so that up to 126 slaves can be integrated in the system. At a maximum 14 bits of safety data can be transmitted from the master to each slave and from each slave to the master within a single data cycle. A separate watchdog timer in each slave ensures a worst case reaction time for each safety function and can be widely parameterized. The watchdog timer can be adjusted for each output signal of a slave.

The safety relevant data (14 bits) and the safety code (consequence number, time information, sender/receiver information, CRC: 24 bits) for each safety relevant slave will be integrated in the summation frame and consists of 6 bytes.

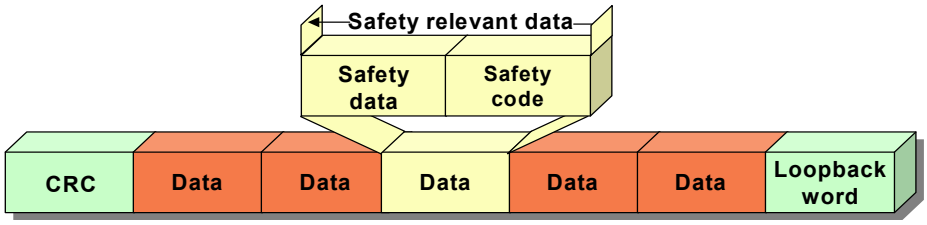

Fig. 5-8: Integration of the safety relevant data in the summation frame

With a transmission speed of 500 kbps or 2 Mbps, extensive diagnostic features, and easy operation, INTERBUS, which is certified according to IEC 61158, forms the basis of the safety bus system. As the INTERBUS master, the controller board uses an integrated safe control system. In addition, safe components have been developed based on standard IP67 and standard IP20 modules. The Safety profile has been integrated into the INTERBUS protocol for the transmission of safe data and parameters. Safety components and standard components can thus be operated via one bus cable. The INTERBUS controller board with integrated safe controller is the basic unit in the system. It processes all safety-related inputs and confirms them to the standard control system by setting an output or resets the output. This method of operation is similar to contact-based safety technology and is referred to as an enabling unit. The enable is programmed with pre-approved blocks such as emergency stop, two-hand control or electro-sensitive protective equipment in "SafetyProg" Windows software, which is compatible with IEC 61131. The amount of programming required is reduced considerably through the use of blocks and the enable principle.

The safe input and output components form the interface to the connected I/Os. They control, for example, contactors or valves and read the input status of the connected safety sensors, including intelligent sensors. The user uses the parameterization function to select the settings for the I/O components such as clock selection, sensor type, and signal type. This means that numerous safe I/O devices are available that are already used by the user. The INTERBUS Safety system meets safety functions up to Cat. 4 according to EN 954 and SIL 3 according to IEC 61508. Depending on the application, the user can choose to use either a "one-cable solution with integrated safety technology" or a "two-cable solution", where one bus cable is used for standard signals and the other for safety signals. It is important to note that all the bus properties are still available and that there are no additional requirements for a "two-bus solution".

User Advantage

The major user advantages of the INTERBUS Safety system can be summarized as follows:

- Very short response times;
- Optimum integration, i.e., safe and non-safe devices can be used in the same network;
- Easy operation from planning to maintenance;
- User-friendly and precise diagnostics with prophylaxis properties;
- High level of system availability;
- Robust system response to external influences;

- Use of existing I/O components;
- Safety buses can be retrofitted without any problems;
- Highest level of safety up to SIL 3 according to IEC 61508 and Cat. 4 according to EN954;
- Comprehensive project and service support.

5.2.6 PROFIsafe

PROFIsafe safety measures are realized in software and simply added as Safety Layer to the devices on top of the PROFIBUS layer 7 (ISO/OSI model) with no change to the other layers. The safety layer is responsible for the communication of safety relevant user or process data (safety application) besides the unchanged existing standard application for non safety critical functions, like e.g. diagnosis. Safety devices are connected to the same single transmission line as standard devices and communicate with an additional safety controller or a combined standard/safety-controller. Thus PROFIsafe uses a single-channel transfer.

The safety data are packed in the PROFIBUS telegram frame as supplement to the standard data, thus forming the PROFIsafe frame, which is passed completely unmodified from a (safety) sender to a (safety) receiver no matter what kind of transmission system is used. The safety measures are encapsulated in the communicating devices thus forming a 'black channel'. On this basis, safe communication is performed by:

- the standard transmission system PROFINET IO and Profibus DP;
- additional safety transmission protocol on top of this standard transmission.

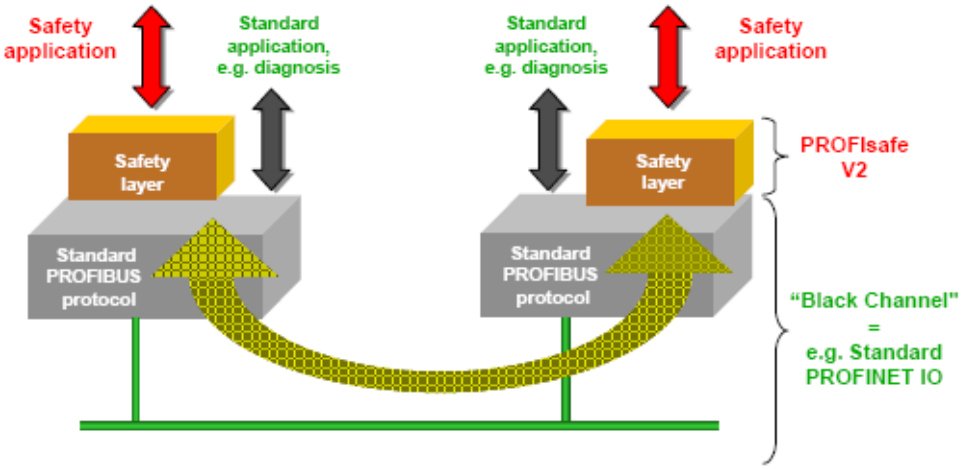

Fig. 5-9: Architecture of the PROFIsafe technology

The standard transmission system includes the entire hardware of the transmission system and the related protocol functions (i.e. OSI layers 1, 2 and 7 according to Fig. 5-9).

Safety applications and standard applications are **sharing** the same standard **PROFINET IO** or **PROFIBUS DP** communication systems at the same time [PNO].

The safe transmission function comprises all measures to **deterministically discover** all possible faults / hazards that could be infiltrated by the standard transmission system or to keep the **residual error (fault) probability** under a **certain limit**. This includes

- Random malfunctions, e.g. due to EMI impact on the transmission channel;
- Failures / faults of the standard hardware;
- Systematic malfunctions of components within the standard hardware and software.

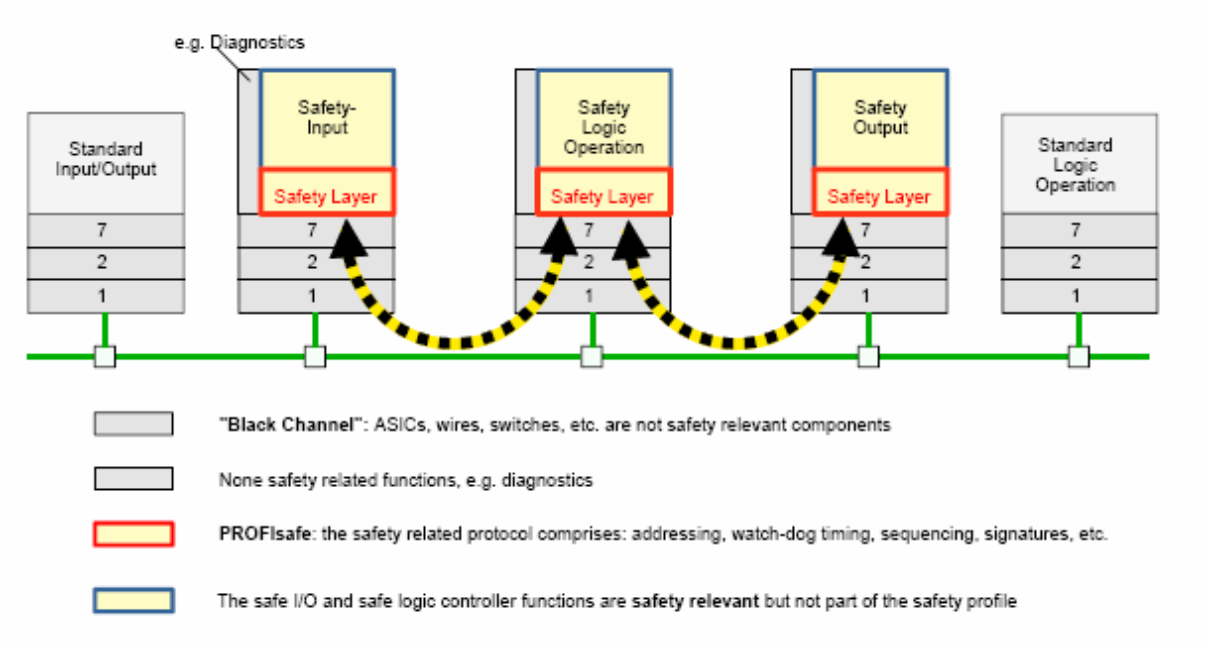

Fig. 5-10: Principle of safe transmission functions

This principle delimits the certification effort to the "safe transmission functions". The "standard transmission system" does not need any additional certification.

5.3 Conclusion

The most VAN relevant functional safety standard, the IEC 61508, defines safety categories denoted as SIL1 to SIL4. The SIL level required for a given application is determined by risk assessment, documenting failure consequences and probability of occurrence. The highest SIL level found in traditional manufacturing and process applications is the SIL3.

The communication systems being part of the safety systems have to be engineered to fulfil safety requirements. This includes determinism and fail-safe designs, i.e. safety networks must be designed to recognize and to handle all possible transmission errors. Also the safety networks must be designed to allow devices to enter a pre-determined safe state when a communication error occurs. Moreover the safety communication network must be fully deterministic to ensure all safety messages are transmitted in a predefined and predictable amount of time.

The needed reaction time of the safety system is dependent on the given application; however without deterministic real-time communication system engineering of safe application is not possible. At present the safety systems use single industrial LAN for the safety functionality. The real-time

classification of interconnected communication systems (performed within WP4) might enable design of safety systems that are not limited to a single LAN.

Usually the safety extensions of industrial networks are based on a “black channel” principle, where only safety-related devices have to conform to safety standards. Standard (nonsafety) components share the network with safety devices to reduce the costs. Having a VAN domain spreading across multiple LANs, if the VAN platform guarantees sufficient real-time parameters of the “black channel”, it would be possible to create a safety system utilizing safety components connected to multiple LANs.

6 Security Technologies

The intended use of the outcomes of the VAN project implies a sufficiently high degree of security of the communication channels and may require new approaches and solutions. In the following chapter after an introduction on what security in this context actually is a list of technologies will depict the available technical solutions to achieve security mainly in the office domain, starting from principle technological means to their application. We focus on technologies here being aware that security systems are mainly complex concepts instead of simple technical appliances. The concepts will be further discussed in WP2.

6.1 Introduction

6.1.1 Motivation

The use of an exclusively provided infrastructure together with impossible physical access to the transfer media and total isolation may provide a certain degree of security. Unfortunately the reality confronts us with the need to interoperation, integration, cost reduction and compliance to standards.

In the VAN project communication over public networks is to be achieved. We will be facing networks that may be used by an unknown number of other users at the same time, we will not have complete control over all parts of the infrastructure and political, commercial, viral or even purely reasons of challenge may cause malicious influences to our communication needs we have to be aware of.

6.1.2 Definition

To define security is a goal that very seldom yields a practically measurable benchmark. One still used approach defines security as achieved when the effort to break a system is higher than the commercial result (win) of an attack. This is no longer suitable in modern IT systems because:

- Automated attack mechanisms reimburse the effort invested once by multiple times
- Many attacks use systems broken into merely as springboards to a more rewarding attack by opening doors or simply providing resources such as bandwidth or computation power
- Many attack motives do not follow rational or commercial reasoning but rather political, religious or even sportive goals

When talking about an attack in this context there is not necessarily a human being involved. We also use this term in the case of self reproducing agent based attack networks (botnets and worms) and for any natural influence to the system with the same effect.

We especially have to understand that security – especially in technical environments – is not a state but a continuous process.

This guides to a more strict definition which in principal covers every security risk. If an attacker has complete knowledge of the system and still has no way of maliciously influencing this system then it is to be considered as save. This ideal state of security then covers all random threats as well: if there is

any random event that has negative effects then an attacker could know it and use it so we have to deal with it like above and iteratively add it to the list of possibly attacks. Needless to say that this principle forbids “security by obscurity” from the start.

This assumption is known as the paranoid approach or also as Shannon’s maxim (the enemy knows the system) or Kerckhoff’s principle.

In practical situations not every threat can be dealt with, but one first step is that all issues are known. Typically a priorisation based on the risk (defined as the product of probability of the attack times the damage expected) will then allow to select which effort is acceptable to deal with a specific threat.

6.1.3 Security tasks

For any communication systems a set of up to seven basic tasks can be defined [KT98]

Authentication:	Sender is authorized to send this message
Access Control:	only to the communication partner relevant information is accessible
Availability:	no interruption within service level agreement
Integrity:	data arrives at the recipient unchanged as sent
Confidentiality:	content of the message is only accessible for the sender and recipient
Non-repudiability:	the message is bindingly liable for the sender, it has been sent
Privacy:	sender requests that its identity stays unrevealed (no known application in AT)

Any attack against a communication system will apply one of the four basic mechanisms or sometimes a combination of them:

Interception:	passive reading, information gain, possibly undetected
Modification:	catch, change and send information
Interruption:	communication loss, also denial of service
Fabrication:	spoofing of sender, abuse of identity, replay attack

The combination matrix of these two dimensions provides a concise framework for all security related aspects of any communication technology [AJ04].

6.1.4 Security Techniques

6.1.4.1 Encryption

Cryptography is the field concerned with linguistic and mathematical techniques for securing information, particularly in communications. One main application of it is the task to encrypt user data (or in the VAN environment especially automation data) to an unreadable form, making it impossible to be used without the knowledge of a key.

The technical solutions are based on the fact that the computational effort to break the code must be substantially higher than its usage. In communication systems they usually make a key that may even have been found useless as they frequently change the key so that only past messages from a short time frame are decipherable. [BS96]

Two principles are used: the symmetric systems have knowledge of a common key/secret and use it on both sides of the channel. These systems usually are fast and easy to deploy but require additional effort for the exchange of keys in order to reconfigure the secret occasionally. The asymmetric systems or public key systems work based on a pair of keys, of which one may be publicly known and freely distributed. New advantages in public keys are the use of elliptic curves that may offer efficiency gains over other schemes.

In automation there is one speciality that affects the use of symmetric and asymmetric systems: public key encryption only works between two partners in a communication whereas symmetric encryption allows for encrypted broadcast messages to be distributed to many receiver stations at once.

Only one encryption scheme is shown to be mathematically considered to be secure, the one time pad. However, it is not practically feasible in automation and is like all ciphers susceptible to human engineering.

The use of encryption mainly addresses the tasks of confidentiality but also provides integrity checking as changes of encrypted communications are often indecipherable and hence recognised as broken integrity.

6.1.4.2 Digital Signatures

Digital signatures make use of the same mathematical basics as public key encryption but the tasks they are aimed at are integrity, non-repudiation and authorisation checks. In other words it is possible with digital signatures as with natural signatures to verify that a message or document has been sent by the correct sender and not has been tempered with.

Signatures normally make use of digital fingerprinting (see there) and then apply an encryption to the fingerprint (hash value) using the private/secret key of the sender. This encrypted information is then attached to the file or message who's content is then signed. As only the public key decrypts this signature a newly calculated fingerprint and the decrypted signature are verified. This requires the fingerprinting algorithm to be publicly known amongst the systems and to be strong, meaning that collisions (two messages produce the same hash) are unlikely and the generation of a file that produces a given hash is computationally expensive.

6.1.4.3 Digital fingerprinting

The check if the integrity of an information given usually requires additional redundancy information. Well known functionalities in technical communication systems are CRC and error correction measures. These are usually distributed within the message or stream. Fingerprints mostly apply to higher amount of information checked at once.

Mathematically these make use of a hash function which produces different values even when small changes to the original message are applied. Broadly speaking, a cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable. By that "I pay 100€" should produce a totally different hash than "I get 100€" or "I pay 500€".

Fingerprinting is most commonly used to distribute the fingerprint on a separate distribution channel, making it harder for an attacker changing both, the message and the fingerprint accordingly, or by applying encryption and so digitally sign the original document.

In various standards and applications, the two most-commonly used hash functions are MD5 and SHA-1; however, as of 2005, security flaws have been identified in both algorithms.

Also, there are known attacks like the birthday attack which use the theoretical possibility of collisions (different files produce the same hash), but have rather academic importance up to now.

6.1.4.4 Public Key Infrastructures

PKI is the term generally used to describe a centralised key management system which has the primary task to distribute the public part of a key pair in asymmetric cryptographic algorithms.

PKI rely on the fact that there is a trusted third party running a certification authority (CA) which certifies the integrity of a given public key by digitally signing it. All members of the communication network know the public key of this CA and hence can verify this signature. The check of a signature does not require a connection to the CA in the moment of checking [PG02].

One specific option a PKI can offer is the management of revoked certificates, making it possible to invalidate formerly accepted certificates. This requires a connection to the PKI at checking time as the digital signature of a certificate itself still appears as valid.

Another alternative to the centralised approach of a PKI is the so called web of trust. This usually relies on the directive “a friend of my friends is my friend” which immediately shows its weaknesses in an automation environment: one compromised node may yield access to the whole communication system. In a PKI special care has to be applied to the security of the certification authority, leaving no weak spot in the field.

6.1.4.5 Packet filtering

Public communication channels today usually are shared media and contain packets that may be addresses to the intended target systems even though they are of malicious nature.

Many attacks to a system are complicated and use weaknesses that would burden the target device with the need to verify the correctness of the offered piece of information in many aspects. As this is not desirable, possible or commercially feasible this task is to be delegated and centralised.

At the perimeter of a system or separate subsystem dedicated devices observe every packet searching either for attributes (like wrong addresses or ports), known attack patterns and behavioural (heuristic) abnormities and react on these communication attempts. Usually the reaction includes denial of these attempts, logging and sending alarms up to complete reconfiguration of the affected communication systems. We should however be aware that an expensive reaction on a cheap attack is an easy way to cause the denial of service.

As with the background noise in public networks the usual way to treat unwanted communication attempts is to drop these and leave evidence for further statistical or forensic analysis.

Most firewall solutions offer different levels of packet filtering, either treating every single packet or using the knowledge about related communication parts (statefull inspection).

6.1.4.6 Application layer gateways

Some attack patterns cannot be identified by observing the communication channel itself because the malicious nature may be obvious to only the receiving application. The SQL statement “drop from customers” is correct in terms of SQL and may be transferred with all correct CRC, address and port checking but still may not be desirable to be executed.

Because of that technical means are installed at the periphery of systems allowing for descent checking of communication content before it enters the processing chain. These application level

gateways (ALG) decode the communication stream (may also be part of the cryptographic chain) and check the resulting communication requests against a white list of allowed actions.

ALGs do not make the correct management and rights structure of the actual application unnecessary but apply a second line of defence and usually are implemented on an alternative technical basis than the target system, avoiding weaknesses to be present in the operational and in the guarding system.

ALGs may become important in the VAN project if they are integrated in communication gateways together with VPN functionalities allowing for a rights-based administration in the communication path.

6.1.4.7 VLAN switching

One way to implement the security concept of structuring infrastructures (as discussed in WP2) is to create logical sub domains of networks on the same physical device. Virtual LANs (VLANs) are a means of isolation of traffic, flexible restructuring and effective bandwidth management.

The application of VLANs rather than physically isolated networks has been discussed as a security threat continuously because the implementation usually allows to abuse MAC addresses or to completely overload certain internal tables of a switch which changes the operational mode to a fully transparent, hub like behaviour. Most of these attacks are dealt with in actual operating system versions and patches, but they show that any sufficiently flexible and user friendly system without sophisticated and strict management can be abused. [HM02]

6.1.4.8 Host intrusion detection / Anti virus software

One major task of security systems in the office domain is ensuring operational security in the communicating nodes. Even though huge efforts are spent to not let malicious information enter a protected communication system or network the need to protect applications and operation systems from attacks performed locally or entering the system the trojan way or simply by the means of end to end encryption is undeniable.

For communication nodes in an automation networks the threats to be compromised by malicious software become more important with the increase in complexity, local intelligence, the use of standard technologies (eg. Java) and modular upgrade mechanisms.

We have to be aware that not only transferring and running of executable code changes the behaviour of a system but also modifications of configuration files. These can be achieved by known weaknesses like format string vulnerabilities or attacks against network based auto configurations.

Host intrusion detection systems (HIDS) usually compare actual fingerprints of system and configuration files with a securely stored information base, making changes obvious. Complementary systems try to identify content in files hitherto unknown to the system as malicious by comparing known attack pattern (virus signatures) or analysing its behaviour (typical system calls a virus would make).

VAN devices in most cases will not have the computing power to perform extensive self assessments but the implementation of a certificate based verification for operating systems and centralised reporting of checksums for system files will be viable ways to improve security significantly.

6.1.4.9 Network intrusion detection systems

Network intrusion detection systems are like HIDS part of a complete fraud management system but concentrate completely on the ways of communication and the content transferred if applicable.

Normal operational traffic in a communication system follows a specific pattern as far as used protocols, transmission frequencies, packet content and traffic volume are concerned. Changes in these patterns and also the recognition of already known malicious sequences in header and payload of transfer protocols have to be observed, identified and reported in order to take appropriate measures.

Intrusion detection systems (HIDS and NIDS) are likely to create so called false positives so the recognition level and the correlation with other historical and present events have to be adapted to specific needs. Heuristical, cooperative, statistical and neural approaches are being developed to increase the ratio between correctly identified attacks on one hand and those attacks not recognised and falsely identified normal traffic on the other.

6.2 Selected Security Technologies

Several technologies possessing some security features were chosen to introduce the solution of the abovementioned security techniques. Parameters, which can be compared across technologies, are specified in *Appendix D.*

6.2.1 Bluetooth Security

Authentication is implemented using a symmetric passkey, a random number, and Bluetooth Device Address. Authentication challenge comprises a randomly generated number which is used together with passkey and BD address for a result generation. Result is sent back to the claimant and verified.

Due to very slim topology possibility, access control is not implemented.

Integrity is assured by HEC (Header Error Check), FEC (Forward Error Correction) 1/3, FEC 2/3, ARQN (Automatic Repeat Request), SEQN (Sequential Numbering), CRC (Cyclic Redundancy Check), and Data whitening.

Confidentiality is assured by encryption. Stream cipher is generated from an encryption key, Bluetooth address, random number, and clock.

Implementation needs 32-bit microprocessor.

6.2.2 Ethernet Security

Since entire communication happens on the same line, each information, which was sent by a communication node, is received by all others. This fact can be used by protocol on higher layers, in order Broadcast to send messages to all attached systems. With TCP/IP for example the ARP protocol uses such mechanism for the dissolution of the Layer-2-Addresses.

On the other hand Unicast messages (those for exactly one receiver) are received likewise from all attached computers. Most Ethernet connected devices must constantly filter out information, which is not intended for them. This is a security gap of Ethernet, since a participant with bad intentions can intercept the entire data traffic on the line.

In modern, larger installations almost exclusively Switches are used. The security lack is reduced by the mechanism of a switched environment, but not totally resolved. A possible attack on a switched Ethernet is the ARP Spoofing or MAC Flooding

Ethernet itself does not support any Authentication Principle and Encryption Algorithms. Plain Ethernet hence is not acceptable for security applications.

Methods of the "Security in depth" are needed, "zone models" can be used. Possible divisions in zones can be:

- expresses zone → with access outward,
- middle zone → Operator functions as a "mediator" inward and outside (e.g. VPN gateway),
- internal zone → actual automation function, extremely secured

In the zones individual Security functions of the Office world can be used, but also additional, automation-typical Security functions will be necessary.

6.2.3 LonWorks Security

Authentication on LonWorks is carried out using symmetric passkey. Nodes, which need to communicate via an authenticated connection, obtain equivalent 48-bit keys during installation phase. When the receiver obtains a message during run-time, and the authentication is required, the receiver asks the sender for an authentication code. Meanwhile, the receiver calculates the authentication code from the 48-bit key, part of the message and a random number. The sender shall calculate the authentication code in the same manner and passes the result to the receiver. Receiver compares the results. If the results are equal, the message is accepted.

6.2.4 OPC Security

OPC client-server communication is performed over DCOM, which requires authentication. This authentication is overtaken from MS Windows login, which requires NTDomain, NTlogin, NTPassword. Security of OPC servers is scaleable; the administrator can choose the authentication level.

6.2.5 Security Aspects in GSM Technologies

Security functionalities of GSM/EDGE and GPRS are almost equivalent, with the distinction that SGSN handles them in GPRS. In addition, GPRS uses a new ciphering algorithm optimized for packet data transmission.

Security in GSM revolves around two features: authentication, and ciphering. A set of parameters called Triplet is generated by the Authentication Centre (AuC) and consists of a cipher key Kc, a random number RAND and a signed response SRES.

Security is implemented in three systems:

1. SIM: involves IMSI, TMSI (P-TMSI in case of GPRS), PIN, authentication key Ki, ciphering key Kc, ciphering key generation algorithm 8 (A8), and authentication algorithm 3 (A3)
2. Handset: involves ciphering algorithm 5 (A5) (GEA in case of GPRS)
3. Network: A3, A5, A8; Ki and IDs stored in AuC

AuC is a database of identification and authentication information for subscribers. It is responsible for generating RAND, RES and Kc which are stored in HLR/VLR (SGSN in case of GPRS) for authentication & encryption processes.

A3 is used with inputs Ki and RAND to calculate SRES. It's a trapdoor algorithm, which means that it's relatively easy to calculate SRES knowing Ki and RAND but extremely hard to calculate Ki knowing RAND & SRES. This is significant, since both SRES and RAND are passed over the air interface before entering the ciphering mode. A8, also a trapdoor algorithm, uses Ki and RAND to calculate Kc. In the authentication procedure, the network sends SRES to the MS, where it's passed to the SIM card. A3 is stored on the SIM card, as is Ki, and the SIM card calculates SRES. The SRES

is returned to the network and the authentication is valid if the network SRES equals the mobile SRES.

Ciphering is employed over the air interface following the authentication procedure so as to provide security for voice and data traffic. In GSM, A5 is used with Kc and the current TDMA frame number to generate a ciphering code. The cipher key is different in the uplink and downlink directions. The TDMA frame number changes approximately every 4.6 ms & is not repeated for about 3.5 hours, making it difficult for the cipher code to be cracked. However, ciphering is optional in some countries & forbidden in others. There are several versions of A5, with A5.0 indicating no encryption, A5.1 being the most widely used & A5.3 the newest one based on Kasumi.

GPRS Encryption Algorithm 3 (GEA3) is used in GPRS for ciphering. Both A5/3 and GEA3 are based on the 3GPP ciphering algorithm (F8).

Some of the known threats to GSM security include:

- SIM card cloning;
- Fake base station;
- Reuse of Kc every 3h58';
- Attack on the signalling network elements such as AuC and HLR;
- Breaking of A5/1 and so on.

Some of these threats can be countered by employing measures such as increase of key lengths, use of public algorithms, mutual authentication between the mobile terminal and the network, and provision of end-to-end security. Recent major updates have resulted in a significant improvement, from no protection on the wired part in GSM to the provision of tunnelling, private IP, firewalls and encryption up to SGSN in GPRS.

6.2.6 UMTS Security

The UMTS technology supports mutual authentication between User Equipment (UE) and Base Station (BS) by shared knowledge of a 128bit secret key (K) stored on the UMTS Subscriber Identity Module (USIM) and in the Authentication Centre (AUC). Since authentication is based on challenge/response principle, the key is never exposed to an eavesdropper. After the authentication, the Cipher Key (CK) and the Integrity Key (IK) are known to both sides. A set of algorithms used in the authentication process is known as MILENAGE. Each algorithm of the MILENAGE set is based on the AES encryption algorithm.

The USIM module, located in UE, performs both authentication and ciphering of transferred data (the secret key K is not known by UE). For ciphering of user data, the ciphering algorithm f8 is used. This algorithm generates a key-stream, which is bit-to-bit added to a plaintext to obtain a cipher-text. The input parameters to the f8 algorithm are the CK (128 bits), a time depended input (32 bits), the bearer identity (5 bits), the direction of transmission (1 bit) and the length of the key-stream (16 bits). On the recipient side, the same key-stream is generated and the plaintext is obtained from the cipher-text in the same way.

The UMTS technology supports authentication of the data integrity of signalling messages. This is ensured by computation of 32bit Message Authentication Code for Integrity (MAC-I). The MAC-I is computed on both sender and recipient sides by the f9 algorithm. Inputs to the algorithm are the IK (128 bits), the sequence number (32 bits), a random value (32bits), the direction of transmission (1 bit), and the message.

Both of the key-stream algorithm f8 and the integrity algorithm f9 are based on the KASUMI block cipher.

The UMTS technology also ensures user identity confidentiality, which is based on Temporary Mobile Subscriber Identity (TMSI). The effective level of confidentiality is ensured by regularly changing temporary identities.

6.2.7 WiMAX Security

WiMAX Forum (the Worldwide Interoperability for Microwave Access Forum) is a non-profit corporation formed by equipment and component suppliers, including Intel Corporation, to promote the adoption of IEEE 802.16 compliant equipment by operators of broadband wireless access systems. The 802.16 standard, amended in 2003 by the IEEE to cover frequency bands in the range between 2 GHz and 11 GHz, specifies a metropolitan area networking protocol that will enable a wireless alternative for cable, DSL and T1 level services for last mile broadband access, as well as providing backhaul for 801.11 hotspots.

The 802.16a standard specifies a protocol that among other things supports low latency applications (designed for voice and video) probably suitable for automation applications, provides broadband connectivity without requiring a direct line of sight between subscriber terminals and the base station (BTS) and will support hundreds if not thousands of subscribers from a single BTS.

Worldwide Interoperability for Microwave Access (WiMAX) is the common name associated to the IEEE802.16a/REVd/e standards. These standards are issued by the IEEE 802.16 subgroup that originally covered the Wireless Local Loop (WLL) technologies with radio spectrum from 10 to 66 GHz.

Recently, these specifications were extended below 10 GHz:

- In January 2003, the IEEE approved 802.16a as an amendment to IEEE 802.16-2001, defining (Near) Line-Of-Sight capability,
- Mid 2004, IEEE 802.16REVd, which should be published under the name IEEE 802.16-2004, will introduce support for indoor CPE (NLOS) and nomadicity through additional radio capabilities such as antenna beam forming and OFDM sub-channeling,
- Early 2005, an IEEE 802.16e variant introduced support for mobility.

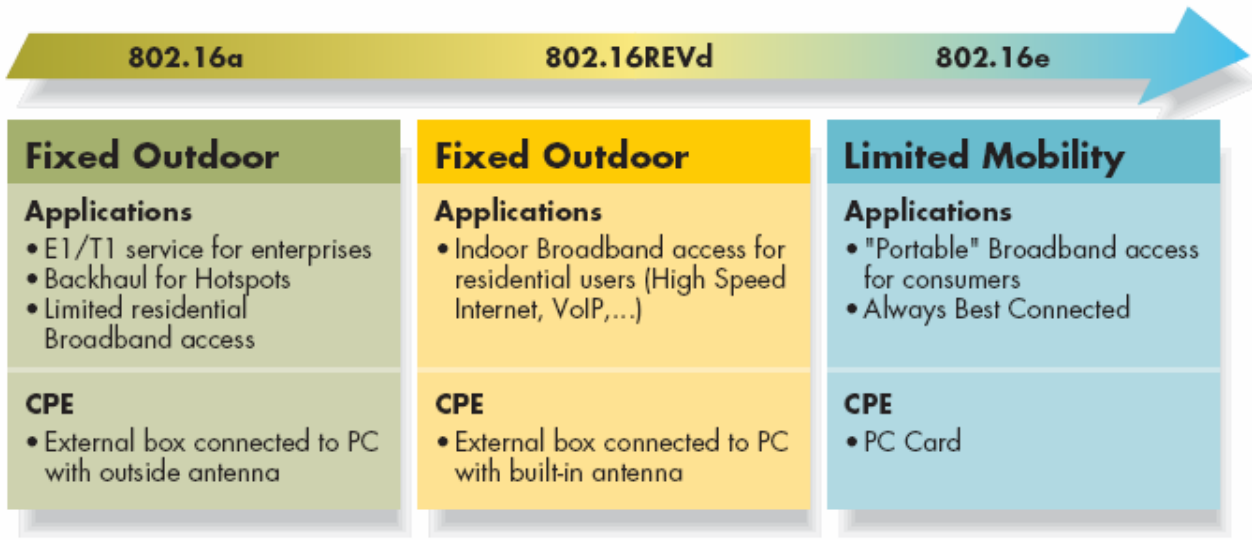

Fig. 6-1: IEEE 802.16 variants

Restrictions are:

- 75 Mbit/s is achievable with a 20 MHz channel. Regulators will often allow only smaller channels (10 MHz or less) reducing the maximum bandwidth, and concurrent use of frequency bands by different vendors of automation equipment will effectively apply further limitations
- 50 km is achievable only under optimal conditions and with a reduced data rate (a few Mbit/s). Typical coverage will be around 5 km with indoor CPE (NLOS) and around 15 km with a CPE connected to an external antenna (LOS), typically less in industrial and automation environments
- Mobility will target only urban usage, with up to 60 km/h vehicle speed to maintain optimum throughput performance.

The technological security solutions are implemented in the media access control layer and can be extended by the layers above that. The following measures are provided:

- Privacy Sublayer — IEEE 802.16's privacy protocol is based on the Privacy Key Management (PKM) protocol of the DOCSIS BPI+ specification but has been enhanced to fit seamlessly into the IEEE 802.16 MAC protocol and to better accommodate stronger cryptographic methods, such as the Advanced Encryption Standard [IEEE802.16].
- Security Associations — PKM is built around the concept of security associations (SAs). The SA is a set of cryptographic methods and the associated keying material; that is, it contains the information about which algorithms to apply, which key to use, and so on. Every SS establishes at least one SA during initialization. Each connection, with the exception of the basic and primary management connections, is mapped to an SA either at connection setup time or dynamically during operation.
- Cryptographic Methods — currently, the PKM protocol uses X.509 digital certificates with RSA public key encryption for SS authentication and authorization key exchange. For traffic encryption, the Data Encryption Standard (DES) running in the cipher block chaining (CBC) mode with 56-bit keys is currently mandated. The CBC initialization vector is dependent on the

frame counter and differs from frame to frame. To reduce the number of computationally intensive public key operations during normal operation, the transmission encryption keys are exchanged using 3DES with a key exchange key derived from the authorization key[RSA98].

- The PKM protocol messages themselves are authenticated using the Hashed Message Authentication Code (HMAC) protocol with SHA-1. In addition, message authentication in vital MAC functions, such as the connection setup, is provided by the PKM protocol.

The implemented security mechanisms are mainly susceptible to malicious activities against the availability of transmissions. Normal Transmissions stay confidential and can be considered as authenticated.

However, the small size of frequent data transmissions in the automation domain, their often predictable content and similar specific attributes of automation data in theory allow for a range of attacks like pre-computed birthday attacks, replay attacks and some ciphertext attacks.

6.2.8 Wi-Fi Security Solutions

WEP

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

WEP specifies a shared secret 40 or 64-bit key to encrypt and decrypt the data. With WEP, the receiving station must use the same key for decryption. Each radio NIC and access point, therefore, must be manually configured with the same key.

WEP combines the keystream with the payload / ICV (32-bit integrity checksum value), which produces ciphertext (encrypted data). WEP includes the IV (Initialization Vector) in the clear (unencrypted) within the first few bytes of the frame body. The receiving station uses this IV along with the shared secret key supplied by the user of the receiving station to decrypt the payload portion of the frame body.

The ICV is a check sum that the receiving station eventually recalculates and compares to the one sent by the sending station to determine whether the transmitted data underwent any form of tampering while intransient. If the receiving station calculates an ICV that doesn't match the one found in the frame, then the receiving station can reject the frame or flag the user.

WEP is vulnerable because of relatively short IVs and keys that remain static. The issues with WEP don't really have much to do with the RC4 encryption algorithm. With only 24 bits, WEP eventually uses the same IV for different data packets. The WEP ICV is based on CRC-32, an algorithm for detecting noise and common errors in transmission. CRC-32 is an excellent checksum for detecting errors, but an awful choice for a cryptographic hash. Better-designed encryption systems use algorithms such as MD5 or SHA-1 for their ICVs.

The frequent changing of IVs also improves the ability of WEP to safeguard against someone compromising the data.

WPA

Wi-Fi Protected Access (WPA) is a security technology specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11i. This technology supports better security mechanisms than Wired Equivalent Privacy (WEP) in the following points:

- Mutual authentication by IEEE802.1x – Extensible Authentication Protocol (EAP),
- Support for Temporal Key Integrity Protocol (TKIP) that offers dynamic change of 128-bit encryption keys of the WEP technology, which prevents attacker to obtain enough messages encrypted by the same key to recover it,
- Support for a message integrity by Michael Message Integrity Check (MIC) algorithm.

The IEEE 802.11i standard also defines Wi-Fi Protected Access2 (WPA2) technology, which is backward compatible with WPA and which provides better security than WPA, but it is more difficult for an implementation. The WPA2 extends the WEP technology by:

- Mutual authentication by IEEE802.1x – Extensible Authentication Protocol (EAP),
- Stronger data encryption based on Counter Mode (CTR), that uses the 128-bit Advanced Encryption Standard (AES) algorithm,
- Support for message integrity by the Cipher Block Chaining Message Authentication Message (CBC-MAC) algorithm.

The Wi-Fi device, using the WPA (WPA2) technology, can be configured to support either Pre-Shared Key (PSK) (the same authentication mechanism as in the WEP technology) or to perform an authentication by the EAP, which requires an authentication server and which is more secure.

Similarly as in the WEP technology, both WPA and WPA2 frame contain the 48-bit Initialization Vector (IV) in its unencrypted part. This IV is a part of an encryption/decryption key.

6.2.9 ZigBee Security

ZigBee technology is intended for low-cost low-power devices based on 8-bit microcontrollers. The computing power and memory available on ZigBee devices is very limited. ZigBee is intended also for building control including building security systems so security mechanisms are supported.

The security is based on a set of encryption keys that are used at the Medium Access Control Layer, Network Layer and the Application Layer. All layers share the same keys. Keys can be either pre-installed or acquired via network. For secured networks the ZigBee defines a Trust Center, which is a device trusted by devices within a network. The Trust Center distributes the keys for purposes of end-to-end applications and network configuration management.

In general two primary security modes for the Trust Center are defined – a Commercial mode (higher security) and Residential mode (lower security). The two modes differ in key management. In the residential mode static keys are used, which leads to reduced security. Network key updates are not supported in the residential mode.

In the Commercial mode the keys are being updated during network runtime. In secured networks, the devices have to authenticate themselves before joining the network. The ZigBee standard defines four security levels for unencrypted communication and another four security levels for encrypted communication. The four levels differ in the length of message integrity code (0 to 128 bit) used during communication. The high security configuration uses 128 bit message integrity code and AES encryption with 128 bit key. The main vulnerability lies in key distribution in case that the keys are not pre-installed. For commercial applications Commercial mode with pre-installed keys and runtime key updates is recommended. For VAN the ZigBee might be an inspiring technology as for implementation of cost efficient advanced security technologies into field devices.

6.3 Conclusion

The traditional industrial communication systems used at the plant floor use little or no security mechanisms. The industrial Ethernet solutions are based on single LANs, where the real-time communication is isolated from the IP based traffic so no strong security has been implemented into the present industrial Ethernet communication systems. However, as the VAN intends to enable communication across LANs and even WANs security has to be addressed within the VAN platform.

However as the implementation of security into automation devices might conflict with other requirements (real-time and determinism, integration of legacy devices, cost of new devices) a “zone model” of scaleable security shall be investigated in more detail.

The automation environment has specific requirements on communication systems used for real-time data exchange. These requirements together with security threats found at both the plant floor and WAN environment have to be investigated in more detail to define scaleable security architecture that would provide state-of-the-art security for the automation data, while meeting the automation specific needs. Moreover within the WP6 an access rights management system will heave to be investigated as multiple access rights have to exist within VAN applications.

On the contrary, all the wireless communication systems define security mechanisms, however some of them have been found week in the past. One of the challenges within WP6 will be integration of various security solutions found in wireless systems into the VAN platform as each of the wireless systems use different kind of security architecture with different strengths and weaknesses. On the other hand the wireless systems, especially the more complex ones, might provide an inspiration for design of good security architecture.

Major challenge within WP6 will be integration of scaleable security architecture into the VAN architecture; the different security zones might require totally different security approaches because of dissimilar threats, needs and requirements found there.

7 Previous European Projects

7.1 Overview

Regarding the Architecture of Ethernet based communication systems the following European projects could be interesting for the VAN project:

- TORERO: Total life cycle web-integrated control [TOR02]
- PABADIS: Plant automation based on distributed systems [PAB04]
- REMPLI: Real-time Energy Management via Power Lines and Internet [REM05]
- OCEAN: Open Controller Enabled by an Advanced real-time Network [OCE05]
- PROTEUS (EUREKA/ITEA) - a generic platform for e-maintenance [PROT05]
- SIRENA (EUREKA/ITEA): Service Infrastructure for Real time Embedded Networked Applications [SIR05]

7.2 TORERO

7.2.1 General Information

- Research project funded by the EU (5th FP), IST-2001-37573
- Duration: 33 month, July 2002 – March 2005
- Work Packages:
    - 6 technical work packages
    - 3 Management work packages
- Consortium:
    - 3 Research institutions: Politecnico di Milano / Italy, Industrial Systems Institute / Greece, CVS@IAF Univ. of Magdeburg / Germany
    - 4 Industrial partners: Machining Centers Manufacturing S.p.A / Italy, Fraba Posital GmbH / Germany, LENZE Drive Systems GmbH / Germany, ALTEC S.A. / Greece
- Coordination: CVS@IAF Univ. of Magdeburg / Germany
- Information: www.uni-magdeburg.de/iaf/cvs/torero
- Achievements: Specification of a DCS including architecture and methodology, Prototype implementations + industrial demonstrator

7.2.2 Technical Achievements

- Architecture of a Distributed Control System (DCS)
- Development and implementation of a new type of control device (TORERO Device = TD)
- Methodology of the DCS: Development and implementation of an engineering tool (TORERO IDE = TIDE)
- Hardware independent programming of the control application using IEC 61499 based Function Blocks
- Application of Plug-and-Play capabilities in the field device level (UPnP)
- Semi-automatic allocation of the control application to the underlying hardware
- Web based engineering and maintenance
- Prototype implementation in a demonstrator system: Real TD (Fraba Encoder), Virtual TD (PC based), TIDE (Eclipse based), and several demonstrator plants
- Integrative approach to cover the whole life cycle of a DCS

7.2.3 Introduction

In the near future, the Distributed Control System – consisting of networked intelligent field devices – will be connected via an industrial Ethernet network, providing a seamless integration of all levels of the automation pyramid, ranging from the ERP (Enterprise Resource Planning) and MES (Manufacturing Execution System) level down to the field device level. In the course of this, the adoption of Internet related technologies in the field device level will be supported. A DCS will have direct access to the company Intranet and the Internet, assuming that appropriate security mechanisms are applied. This will open up new ways for managing the DCS via the company Intranet / Internet.

One the one hand, the Internet can be used for Web based Management, which is already state of the art in the field of automation.

On the other hand there is the usage of the Internet for engineering/maintenance purposes and re-configuration processes in the case of device replacement. Such functionalities, adapted to DCS, are still under development although this is state of the art in the office world.

In this respect, the research project TORERO aims at specifying a DCS, which is called TORERO system, consisting of a new type of Internet connected and web based engineered field device (TORERO Device, TD). Such a Java based device provides plug-and-play capabilities to increase the flexibility of the DCS with respect to (re-) configuration and maintenance and also to support the minimization of down time in case of device replacement.

Based on this infrastructure and in connection with Software Servers (TORERO Software Servers, TSSs) and an Integrated Development Environment (TORERO IDE, TIDE), the total life cycle of the DCS, ranging from the engineering phase and managing of the system during runtime, to the maintenance / re-configuration phase and termination of the system will be supported.

Results interesting for the VAN project

The TORERO project focuses on distributed control applications using an Ethernet based communication infrastructure. There is none direct influence to the protocol architecture itself. The

TORERO project developed a web-based engineering methodology for the management of the different features of distributed control devices (including their communication and plug-and-play features) covering the complete life cycle. That could be the focus on using TORERO results within the VAN project. Furthermore, the prototype implementation of the Engineering Tool (TIDE) which is based on the open source platform ECLIPSE and the usage of UPnP in automation could be of interest for VAN.

7.3 PABADIS

7.3.1 General Information

- Research project funded by the EU (5th FP), IST-1999-60016
- Duration: 38 months, December 2000 – January 2004
- Work Packages:
  - 5 technical work packages
  - 4 Management work packages
- Consortium (EU):
  - 4 Research Institutions: Vienna University of Technology / Austria, University of Marburg / Germany, Association pour la recherche et le development des methodes et processus industriels / France, CVS@IAF Univ. of Magdeburg / Germany
  - 6 Industrial partners: IMS GmbH / Germany, Phoenix Electronics GmbH / Germany, Jetter AG / Germany, ALTEC S.A. / Greece, A. Hatzopoulos S.A. / Greece, P2I Engineering / France
- Consortium (IST non Europe):
  - Switzerland: University of Geneva (CUI), PebbleAge S.A., Zurich University of Applied Sciences (ZHW), SIG Pack Systems AG
  - Canada: University of Calgary, PsiNaptic Inc.
  - USA: Sun Microsystems, Inc., aJile Systems, Inc.
- Coordination: CVS@IAF Univ. of Magdeburg /Germany
- Information: www.pabadis.org
- Achievements: Specification of a agent and PnP based distributed architecture for flexible automated manufacturing systems, Prototype implementations + demo

7.3.2 Technical Achievements

The PABADIS project is one step towards the use of distributed systems in (plant) control. Based on the use of plug-and-participate and mobile as well as residential software agent technologies a control system is designed which enforces the use of distributed intelligence and therefore enables horizontal as well as vertical flexibility in plant, product, and device management.

The main advantages of the PABADIS control system in contrast to existing centralized control systems are the following:

- Effort reduction, improvement of reuse, and partial automation in field control design In PABADIS the function of field control systems can, abstractly speaking, be reduced to product processing. The presently existing logistical functions of control devices needed for product handling over machine borders in PABADIS are shifted to the intelligent product agents which are more flexible with respect to product handling. Hence, the design of field control devices becomes more efficient and potentials for reuse are enlarged or opened. The design and integration of control devices in a PABADIS system is simplified by the use of co-operative manufacturing units (CMU). A CMU contains a set of functions in the field of automation and/or logical calculation. This is the only thing really needed to be programmed by the device vendor. The correct use of CMU in the PABADIS system is ensured by residential agents (RA) staying at the interface between CMU and product agents. The design of the part of the CMU control system and of the interfacing RA is automated. Hence, a device vendor has not to undertake too much effort in creating a PABADIS feasible device.
- Creation of horizontal flexibility on the field device level

  The integration of a new or an updated CMU (and with it a new or an updated device) in a PABADIS system can be done in a plug-and-participate fashion. Hence, no further effort is needed with respect to system updating, if a change in the CMU structure of the system appears. This is ensured by the use of JINI technology and the automatic function provision to the system by RA with the help of the JINI lookup service. This feature of CMU results in an improvement of system flexibility with respect to the production environment.
- Improvement of vertical flexibility in the product handling field

  The used system of mobile agents for product description and handling improves the system flexibility with respect to product processing. Each mobile product agent (PA) contains all required data for product processing and a set of methods for automation and logical function access. These methods are identical for each agent and each CMU by using pre-designed interfaces between PA and RA as well as between RA and CMU function. Here, the use of XML descriptions of required and offered functions co-operates with the named methods to ensure the correct use of different product processing functions of the CMU. The mentioned set of data of the PA also enables a soft change in the product program of a PABADIS company by only changing this data set. There is no further effort in changing the control system in this case.
- Improvement of MES and SCADA system flexibility

  The MES system in the PABADIS plant is based on mobile as well as on residential software agents. These agents will ensure for example the scheduling and resource allocation in the case of PA and RA or monitoring functions in the case of plant management agents (PMA). All MES functions can be incorporated in the PABADIS system. The use of software agents encapsulates the algorithms used of the solution of MES functions. Hence, a system redesign or discrimination between different parts of the system with respect to products, CMUs or regions can be achieved by changing agent methods in the moment of the agent creation. The SCADA functions are also realized by the use of agents in co-operation with special dedicated SCADA-CMU. The above mentioned flexibility is also given in this case.
- Easy ERP system integration and automated ERP system update with respect to system shifts

All common ERP systems can be integrated into a PABADIS system. This is due to a special interface between ERP and the PABADIS community. Based on this interface the use of single order management is enforced by the PABADIS system. By use of the JINI lookup service the PABADIS community is able to monitor system changes for the ERP system and can enforce the integration of new machine abilities in the ERP by the evaluation of the capability description of the CMU.

- First step to an ontology of distributed automation systems

  Throughout a detailed ontology is outside of the scope of PABADIS the used XML descriptions in the capability description of the CMU, the work order description of the PA, and the ERP-agency-interface are a first step to create such ontology for distributed automation systems.

Last but not least the used infrastructure of a PABADIS plant is a key factor for its effective use. This is especially true for the used agent system, the plug-and-participate-technology, the used communication system, the programming environment, and the control technology.

7.3.3 Introduction

The PABADIS approach focuses on automation using distributed systems. In fact, the aim is to dissolve the MES layer and divide its functionality into a centralized part that can be attached to the ERP system and a decentralized part that can be implemented by partially mobile software agents. This effectively comes down to reducing the hierarchy to two layers. From the communications point of view, this approach both necessitates and supports the current trend in industrial automation to flatten the network hierarchy and to use IP-based networks down to the control level. Briefly, PABADIS aims at creating a plug-and-participate environment which allows producing companies to simply plug in a new machine and use it without major changes within the legacy systems to make job control more flexible by augmenting “conventional” (mainstream) ERP functionality with intelligence inherent in software agents.

The baseline vision of the project is that every work piece has an agent “attached to it” carrying the necessary product information and moving through the plant the same way the work piece does. In fact, every production system needs two main ingredients: the actual physical work piece and information. If we consider a single piece production system, most of this information is tightly connected to the individual product, such as

- production sequence and schedule,
- machine-related production data,
- status of the processing,
- general administrative information about the order.

In addition, there is information associated with the entire production system, such as

- overall resource use,
- overall production schedule,
- machine status information,
- quality control information.

The system-wide scheduling and resource planning data should of course be consistent with the product-specific data sets, hence they can be compiled or deduced from each other. Traditionally,

these data are generated by the ERP system in a strictly centralized fashion. Detailed planning and adjustments to the overall scheduling are subsequently done by the MES. With a view to the information distribution sketched above, it seems reasonable to largely remove the planning functionality from the ERP and distribute it on the level below among the “products” that can independently keep track of their processing needs and status. This requires the introduction of an information-oriented “alter ego” for each product, and software agents are a suitable approach for it.

PABADIS uses object-oriented models and object-oriented software technology to describe and perform automation tasks. The work piece is seen as an object that has all necessary information regarding its production somehow embedded or attached. It seems natural to use an intelligent Software Agent for such a purpose. Software agents are the real-world manifestation of object-oriented and distributed functionality. The combination of software agents and physical instances (like machines or the work piece in our case) is sometimes also referred to as “holon”, however, PABADIS prefers to stay with the term “agent” since in contrast to the main use of the term “holon” for intelligent machines PABADIS intends to put intelligence also into the product by appropriate agents.

7.3.4 Results interesting for the VAN project

The PABADIS project defines requirements for the used communication systems, but does not specify new communication functionality. The requirements were mainly related to the application of plug-and-participate as well as agent-systems (including mobile agents) within industrial networks on the shop-floor level.

There is a follow up project of this project named Pabadis’Promise.

7.4 Pabadis’Promise

General Information

- Research Project funded by the EU (6th FP), FP6-IST-016649
- Duration: 36 month, September 2005 – August 2008
- Work Packages:
  - 8 technical work packages
  - 1 Management work packages
- Consortium (EU):
  - 4 Research Institutions: Austrian Academy of Science / Austria, Politecnico di Milano / Italy, ARMINES Ecole des Mines d’Ales / France, Industrial Systems Institute / Greece, and CVS@IAF, Univ. of Magdeburg / Germany
  - 6 Industrial Partners: SAP AG / Germany, Siemens AG / Germany, Identec Solutions AG / Austria, Machining Centers Manufacturing S.p.A. / Italy, CR Fiat, Business information Technologies / Italy, Defi Systems / France and Advanced Concepts Engineering S.A. / Greece
- Coordination: CVS@IAF, Univ. of Magdeburg
- Information: www.pabadis-promise.org

7.4.1 Technical Achievements

The ongoing research project PABADIS'PROMISE will develop a new architecture to overcome restrictions and limitations of currently existing approaches for distributed manufacturing systems. This will be reached by introducing new concepts and technologies such as:

- Architecture and methodology for on the fly design of manufacturing control systems based on plug-and-participate of resources and for on the fly design of order related control applications based on predefined resource related control building blocks on the resource side and order related building blocks on the product side; both encapsulated in embedded Real-Time agents.
- A minimum-size, embedded, and Real-Time agent system for factory control, providing access to order data during the whole production process and, thus, the maximum flexibility with regard to additional customer wishes/ changes even during manufacturing.
- New generation of control devices enabling the definition, design and control of sets of fine grained basic control functions running on it to control the machinery as such, the communication paths, the security mechanisms and so on as resource related control building blocks – without any relation to the products produced and enabling the integration of this control function blocks on-the-fly in order related control applications during the runtime of the device and the underlying manufacturing resource.
- RFID tags for order and product data transmission - attached to the products, enabling the migration of embedded Real-Time agents.
- Building blocks for a new generation of Enterprise Resource Planning Systems dedicated to handle most flexible manufacturing systems with direct access to the filed control level will be developed.
- An ontology based product and process description language for the complete integrated data flow of the overall control system.

The intended results of PABADIS'PROMISE will enable a most flexible, adaptable, and efficient control of manufacturing systems covering the necessities of future manufacturing. The results can be used as a whole but also independent of each other to improve future European manufacturing systems.

The new control design architecture, the products related to this architecture and the new emerging manufacturing ontology will have different impacts.

The impact on manufacturing systems in general can be subsumed by improving production efficiency, improving the ability to integrate customer requirements until its ultimate deadline defined by the realization of production steps and by new emerging products and services. These new products and services will emerge in the fields of control devices, specialized design tools and its application, ERP system add-ons, RFIDs, and services based on the application of building block design strategies.

The complete range of companies within the manufacturing sector and all sectors related to the design, development, and implementation of manufacturing systems will be effected by the PABADIS'PROMISE project. At least one market leader of the effected markets is involved in the project as a participant. Smaller companies and SMEs will be enabled to apply the project results with respect to the mentioned economical effects. Here the integration, application, and finally market of specialized knowledge of SMEs will be improved.

7.4.2 Introduction

Future manufacturing systems will have to face new requirements to react on upcoming dramatic changes in technological, environmental, economic, and social terms as described in an EC evaluation study for the developments within the next 20 years. European manufacturing will be more and more driven by a turbulent industrial environment which is characterized by an aggressive economic competition on a global scale, more educated and demanding customers, and a rapid pace of change in process technology. Thus, future manufacturing will require high flexibility/adaptability and speed with respect to organization of production and supply-chain management and require an increasing amount of services and inter-company collaboration. These requirements especially concern control and networking of embedded control systems of manufacturing enterprises at ERP (office), MES (factory control) and production level. In the last years several approaches for future manufacturing systems such as HMS and PABADIS were developed, making remarkable advances in enhancing the flexibility of production systems by using distributed and agent based systems. Nevertheless, the industrial application of these concepts is still in the fledgling stages due to the required comprehensive paradigm change on all levels of a manufacturing systems and problems of more practical nature with respect to an economic reasonable use of technologies such as agent systems. To overcome these problems and make the next steps towards a wide industrial usage, future projects have to face up the ongoing technological development in the information technologies and increase the applicability of the basic concepts under real industrial conditions.

Taking these requirements into account and building on top of the PABADIS architecture, the PABADIS'PROMISE project extends the idea of distributed control to an innovative architecture which incorporates both resource and product.

To overcome the existing drawbacks of limited flexibility and interoperability, within a number of research activities new architectures were developed. Some of these concepts such as PABADIS (see above) break the monolithic architecture on the MES layer by using agent and plug-and-participate technologies, other introduce a distributed control architecture on the field level by collaborating function block systems (in approaches like CORFU, TORERO) or cover both areas such as HMS.

These systems shows in principle the applicability of agent based distributed architectures in flexible manufacturing systems. Nevertheless there are still open problems in terms of a practical application and industrial acceptance. Implementations have to be costly tailored to the specific needs of implemented demonstration systems and even the generic PABADIS-architecture has limitations especially with respect to the interaction between MES and control level. The application of agents on the field level is still cost intensive with respect required resources and here especially the mobility of product related agents is problematic in terms of networking capabilities of devices and system reliability. The generic approach enables the integration of a wide range of control devices following different concepts, but also limits the interaction with the control application to a simple parameterization.

Therefore the PABADIS'PROMISE architecture will carry this distribution trend beyond current boards by including distributed manufacturing sites with border crossing ERP interaction, stringent connection of order data and material, and an improved field control flexibility by on-the-fly and on demand order related control application design. The incorporation of new technologies such as RFIDs and agent systems tailored to the specific needs of field control systems will enable reasonable implementations of these new concepts.

7.4.3 Results interesting for the VAN project

For the application in real industrial networks the agent based system of Pabadis'Promise has to consider many network aspects that are investigated in VAN as security, real-time and public/private wide area networks for cross-company connections. Thus the VAN architecture will give a remarkable support for the future related agent communication in industrial networks.

7.5 REMPLI

7.5.1 General Information

- Research project NNE5-2001-00825, funded by the EU under the "Energy, Environment and Sustainable Development" Programme (1998-2002)
- Duration: 36 month, Start: 01. 03. 2003
- Work Packages:
  - 7 technical work packages
  - 2 Management work packages
- Consortium:
  - 4 Research institutions: Institute of Computer Technology at the Vienna University of Technology, Vienna, Austria; LORIA (Laboratoire Lorrain de Recherche en Informatique et ses Applications) Nancy, France; The Polytechic Institute of Porto (IPP), Portugal; Advanced Control Systems Laboratory at the Department of Engineering (ELDE), Technical University of Sofia, Bulgaria
  - 3 Industrial Partners: TCE TeleControlExpert GmbH, Germany; iAd Gesellschaft für Informatik, Automatisierung und Datenverarbeitung mbH, Nuremberg, Germany; Toplofikacia Sofia EAD, Sofia, Bulgaria
  - 2 Authorities: Ministry for Energy and Energy Resources (MEER), Sofia, Bulgaria; DENE (Agência para a Energia), Alfragide, Portugal
- Coordination: Institute of Computer Technology at the Vienna University of Technology / Austria
- Information: www.rempli.org

7.5.2 Technical Achievements

A communication infrastructure consisting and connecting of:

- low-voltage segments which cover groups of energy consumers (for example, a segment can span across one staircase of apartments within a living block)
- mid-level voltage segments between the primary and secondary transformer stations
- TCP/IP (or IEC 60870) based network connecting the primary transformer stations and the SCADA Server(s) and Billing Server(s) of the utility company

- TCP/IP communication over the Internet between some of the Utility Company's Servers and clients that need to access the data.

Primary applications of the REMPLI project will be

- meter reading and
- remote control.

7.5.3 Introduction

The goal of the REMPLI project is to create a solution that allows for saving energy in large-scale energy distribution networks: private households within a certain district or town, large production environments, etc. The intended scope of applications is not limited to electrical energy only; other kinds of supplies (heat, water, gas, and the like) are intended to be covered as well.

The basis of the system is a power line communication (PLC) infrastructure that allows to access metering and control equipment remotely. The primary usage of this infrastructure is the remote meter reading and remote control. However, the communication platform is open to various kinds of add-on services.

The communication infrastructure typically consists of:

- Low-voltage segments which cover groups of energy consumers (for example, a segment can span across one staircase of apartments within a living block),
- mid-level voltage segments between the primary and secondary transformer stations
- TCP/IP (or IEC 60870) based network connecting the primary transformer stations and the SCADA Server(s) and Billing Server(s) of the utility company,
- TCP/IP communication over the Internet between some of the Utility Company's Servers and clients that need to access the data.

The proposed architecture implies using a cascaded powerline communication system in the most general case. However, there can be situations where the communication on the mid voltage level is already based on IP networks. In the more typical case, communication both at mid-voltage and low-voltage sides is Master/Slave based. The REMPLI MV-LV Bridge between two parts of the cascade (comprised of interconnected high-voltage slave and a low-voltage master) is installed at the secondary transformer station.

The transition between PLC and TCP/IP (or IEC 60870) communication environments is carried out by the REMPLI Access Point, installed at the primary transformer station. Apart from gatewaying between two different networks, the Access Point also performs a number of application-specific tasks, such as data concentration, logging, failure detection, various maintenance procedures, etc.

The SCADA server obtains data from the relevant REMPLI Access Point over private TCP/IP or IEC 60870 communication lines. On the other side, it accepts requests from the SCADA clients, which implement the actual visualization and control functions. These clients are the end-terminals for human operators from utility companies.

The other side of the communication infrastructure is primarily comprised of Nodes, each coupled with a low-voltage PLC slave. The Node is installed at the consumer site, e.g. inside apartment, and has a number of metering inputs (such as S0, for electrical energy meters). A node can also be equipped

with relays that allow switching off and on electrical/heat/gas/water supply for a particular consumer, upon respective control commands from the utility company.

The universal communication infrastructure, based on the PLC, as well as the open architecture of the access points, allow for integrating various kinds of add-on services, such as security alarms, demotic control. This infrastructure is a base to implement solutions for energy savings in huge energy distribution networks; from the top of a distribution network down to the private household. The communication infrastructure relies on approved power line communication technology, IP-based private networks and communication devices equipable with intelligent functionality

The primary application within the REMPLI project will be

- meter reading and
- remote control,

but the system is open to add-on services. This services can be achieved by extended functionality of the central SCADA system in the same way as they can be realized using the local decentralized intelligence of the new devices. Some additional functions like

- loss detection,
- ground circuit detection,
- automatic transformer control,
- load balancing
- automatic billing
- prepayment

can be realized with a finer resolution then it is possible today.

The project focuses on the mentioned application functionality

7.5.4 Results interesting for the VAN project

The Rempli project addresses remote monitoring using power link for the last mile. The technology to be developed should be interesting for WP 7, in particular in the sense of telematic systems. There should be an influence to the protocol architecture as well as the management concepts.

7.6 OCEAN

7.6.1 General Information

- Research Project funded by the EU (5th FP), IST-2001-37394
- Duration: 36 month + 3 months extension, August 2002 – October 2005
- Work Packages:
    - 5 technical work packages
    - 1 Management work package

- Consortium:
  - 5 Research Institutions: Universitaet Stuttgart / Germany, Rheinisch Westfaelische Technische Hochschule / Germany, Katholieke Universteit Leuven / Belgium, Fundacion Fatronik / Spain, Consiglio Nazionale delle Ricerche / Italy
  - 5 Industrial Partners: Fidia S.p.A. / Italy, HOMAG Holzbearbeitungssysteme AG / Germany, Fagor Automation, S. Coop / Spain, OSAI S.p.A. / Italy, Goratu Maquinas Herramienta, S.A. / Spain
- Coordination: Fidia S.p.A.
- Information: http://www.fidia.it/english/research_ocean_fr.htm
- Achievements: definition and realization of a "Distributed Control System Real-Time Framework" (DCRF) for numerical controls + definition and realization of a component based open numerical control reference architecture for machine tools + industrial demonstrators

7.6.2 Technical Achievements

- The "Distributed Control System Real-Time Framework" (DCRF) is a standardized communication platform real-time capable in distributed hardware environments, able to host numerical control components in distributed open platforms. It is based on standardized communication systems and delivered as open source. The DCRF provides a real-time communication API. This framework is to be coupled with standardized interfaces enabling the integration of external real-time critical and non real-time critical control components. The most innovative aspects of the DCRF are:
  - the DCRF is real-time capable in contrast to former approaches like OSACA, OPC, etc. This ability is crucial for distributed control systems.
  - The DCRF enables a flexible composition and reconfiguration of control systems with manufacturing task specific functionality on the basis of a common communication platform. In fact at the moment there is no software tool able to make a high-quality software engineering design for such a complex system as a numerical control. The result is a scalable, portable and flexible framework.
  - The DCRF is offered as open source, which helps to gain a wide propagation easily, especially for SMEs that do not have resources to develop a control platform by themselves.
  - New generations of control systems can be built upon the DCRF which will simplify the design and implementation of distributed real-time controls.
  - The DCRF is not limited to control systems for machine tools but it can rather be applied to various purposes in the field of control systems (e.g. chemical industry, packing machine industry, plastic machine industry, ...).
- The OCEAN project defined an extended component based open numerical control reference architecture for machine tools, not delivered as open source but whose standardized interfaces for motion control components are publicly available. In fact the results achieved within former research projects were not flexible and granular enough as the monolithic software blocks of the control system remained almost the same. In order to take advantage of open control systems it was necessary to extend the existing reference architecture and to

decompose the monolithic blocks into components with clearly defined interfaces, described in standardized IDL format for RT CORBA. These specifications were published for further input and implementation by users in the field of control techniques. Thus it is now possible to integrate additional functionality and third party software just using the standardized interface description, without any need of adapting interfaces.

- The key innovative features are:
  - Non-ambiguous interfaces have been specified in a reference architecture that will enable an interoperability of control systems and additional components that can be supplied by third parties.
  - Existing reference architecture have been extended with components which are not covered yet by any standard; the modeling of the single control components and the definition of their interfaces is for sure one of the most innovative aspects of the OCEAN project.
  - Conventional monolithic control systems can now be opened for the integration of additional functionality.
  - User interfaces for specific machining tasks or for an individual adaptation depending on the skills of the operator can be substituted in the control system on the basis of DCRF interfaces.
  - The integration of third party software with standardized interfaces will now allow the reuse of software in different control systems which will result in shorter time to market periods, reduced software development costs and more stable software applications.

7.6.3 Introduction

The approaches for standardized communication platforms which have been made in the field of process automation and open controls in the past years (e.g. OSACA, OMAC, OPC) own the common disadvantage that they are not real-time capable in distributed hardware environments. This lack represents a major constraint as there are many applications which need real-time capability, e.g. fast process controls based on high performance DSP hardware or PLCs on separate embedded hardware which have to communicate with the CNC in real-time. The first main objective of the OCEAN project was therefore the definition and realization of a real-time capable framework called “Distributed Control System Real-Time Framework” (DCRF) which is able to host control components in distributed open platforms and provides a real-time communication API.

Another major obstacle for the transfer e.g. of OSACA results into industry can be identified in the complex and not easy to use communication infrastructure that was developed in the course of the research project due to the lack of available alternative solutions at that time. In the meantime new standardized communication systems have been developed outside the automation world (e.g. CORBA, RT-CORBA) which were analyzed systematically and scientifically refined for usability in a DCRF. These communication systems are used world-wide and are improved continuously. This is possible due to the Open Source philosophy which represents a further important aspect of this project. In order to facilitate the development and production of competitive products by reducing software development time and costs, the DCRF was based on open source components and is available as open source itself at the end of the project. The basic idea was to continue the approach of OSACA by adopting its benefits and realizing a fundamental improvement on the basis of newly available technologies. This strategy promises a broad industrial acceptance of open control technologies based on the DCRF.

7.6.4 Results interesting for VAN project

OCEAN created a framework potentially to become a standard for communication among software components in a Real-Time environment. This sets the basis for a standardisation of open architecture Numerical Controls.

This standard was totally independent from the hardware platform where the software components run or from the communication media among them. When VAN creates a standardised communication platform, the implementation of the standardised OCEAN framework on this platform will provide more strength and more chances of industrial acceptance to both these results.

7.7 PROTEUS (EUREKA/ITEA)

7.7.1 General Information

- Research project supported by ITEA (EUREKA cluster project)
- National funding in France and Germany
- Duration: 29 month, October 2002 – February 2005
- Work Packages:
    - technical work packages
    - 1 management work package
- Consortium:
    - Research Institutions: BIKIT vzw, ifak, Fraunhofer IML, LAB LIFC, LORIA INPL, TUM, Université Paris 6
    - Industrial Partners: AKN Eisenbahn AG, ARC Informatique, CEGELEC GmbH, CEGELEC SA, Pertinence Data Intelligence, Schneider Electric, TIL TECHNOLOGIES, Vartec SA
- Coordination: CEGELEC SA
- Information: http://www.proteus-iteaproject.com
- Achievements: Specification of an integration platform architecture and methodology, Prototype implementations + demonstrators

7.7.2 Technical Achievements

PROTEUS is focusing Maintenance Application Integration (MAI). The basic idea of the PROTEUS platform consists in using existing maintenance applications (tools) in order to provide the integrated maintenance services. The integration is based on co-operative and orchestrated execution of distributed processes, which are running on heterogeneous hardware/software platforms and communicating via Web Services. The architecture of the PROTEUS platform is mainly focused on the infrastructure for integration rather then on the provision of dedicated tools.

It is possible to distinct three tiers, which software applications implement completely or partially. In the PROTEUS platform we have the following situation:

- The Data Tier is represented by the data models hosted by existing applications.
- The Business Logic Tier is partially represented by the business logic, which already exists in the legacy applications. Business logic, which spans multiple applications, is implemented in business logic objects (BLOs), which reside either in Intelligent Core Adapters (ICA) or in Functional Core Applications (FCA). ICAs and FCAs are specified within the PROTEUS project.
- The Presentation Tier is partially represented by user interfaces of the legacy tools. The PROTEUS project specifies a supplementary Web portal as interface for workflows, which span multiple legacy applications and for selected functionalities of these applications.

Several Central Service Applications have been specified within the Platform Integration Core:

- Central Object Relation Data Base (CORD): This application provides linkage between all PROTEUS applications. For example the CORD provides links between a temperature sensor type in the DAS and documentation in the E-Doc server, a spare part in the CMMS and asset information in the ERP.
- Central Access Rights and Authorization Server (CAAS): This application performs all login operations and controls access operation within the PROTEUS platform.
- Central Event Distribution Server (CEDS): The CEDS is defined as a central point for collection and distribution of events.

The heart of Intelligent Core Adapters (ICAs) and Functional Core Applications (FCAs) is a collection of Business Logic Objects (BLOs). They are used to control workflow as well as to transform data into or from a common exchange format used for communication within the PROTEUS platform. The consequent use of BLOs opens the way to real distributed design and execution of maintenance tasks while improving or even replacing centralized maintenance management through distributed components.

7.7.3 Introduction

Maintenance is a very important activity for all industrial enterprises. It is necessary for the improvement of the plant performance and the stabilization of the product quality. The maintenance covers most domains of the enterprise, like

- the plant and the equipment to be maintained,
- the organization of different maintenance strategies (preventive, predictive and corrective maintenance),
- the management of operators, material and spare parts,
- the computer aided diagnosis systems,
- the documentation management

and many further domains. Maintenance is an activity, which needs the integration of several software systems associated to these domains. All these software systems are currently based on different data, communication and workflow models. They are normally complementary, but sometimes redundant, incoherent and mostly heterogeneous.

The PROTEUS objective is the integration of these necessary software systems by using a unique and coherent description of the equipment (through an ontology description) and a generic communication system architecture (based on the “Web Services” technology).

7.7.4 Results interesting for VAN project

Within the PROTEUS project effort was spent to the application of web service technology to maintenance and integration platform (middleware). The working packages were not dedicated to the development of new communication technologies rather than on the exploitation of existing technologies. Consequently there is no direct influence on the communication technology related WPs within the VAN project. Nevertheless experience coming from the adapter concept of PROTEUS could be interesting regarding application of proxy/bridging concepts and the management of entities. Regarding management and engineering the VAN project could also benefit from experience coming from device modeling.

7.8 SIRENA (EUREKA/ITEA)

7.8.1 General Information

- Research Project funded by National authorities within the EUREKA/ITEA programme
- Duration: 2003-2005,
- Work Packages:
    - 6 technical WP
    - 1 Management WP
- Consortium: 15 partners, from France, Germany and Spain
    - 4 Research Institutions: Fraunhofer Institut FIRST / Germany; University Dortmund / Germany, University Paderborn / Germany, University Rostock / Germany
    - 11 Industrial Partners: Capgemini, France; EADS, France; Schneider Electric / France; ROBOTIKER / Spain; ZIV / Spain; ESC / Germany, INVERA / Germany; Materna / Germany, Siemens / Germany; Traveltainer / Germany.
- Coordination: Schneider Electric, Grenoble, France,
- Information: www. SIRENA-ITEA.org

7.8.2 Technical Achievements

Define a service-oriented framework for developing distributed applications in various real-time embedded environments: industrial, automotive, home, telecoms

Build proof-of-concept demonstrators

Expected results: With SIRENA: Sensors and actuators are connected over a common network infrastructure (e.g., Ethernet) and communicate directly using IP-based network protocols. Connections are "plug-and-play", owing to automatic device and service discovery mechanisms. The devices incorporate their own intelligence, making them self-contained and obviating the need of a higher-order control device. What's more, no automation program is needed anymore, as the devices

expose their capabilities in the form of high-level services (e.g., "raise shutter, level=0.75"). The use of common networking and service infrastructure grants interoperability between devices belonging to different domains, thus, paving the way for new, service-oriented applications.

7.8.3 Introduction

The SIRENA project is an ongoing European R&D project aiming to develop a Service Infrastructure for Real-time Embedded Networked Applications. Given the tendencies it has been decided to adopt the Devices Profile for Web Services (DPWS) as the foundation technology for the SIRENA framework.

Device-level SOA using Web Services – the DPWS

Web Services technology constitutes the preferred implementation vehicle for service-oriented architectures. Web Services are totally platform-agnostic and can communicate with and/or be aggregated with other Web Services. Besides the standardization and wide availability of the Internet itself, Web Services are also enabled by the ubiquitous use of XML as a means of standardizing data formats and exchanging data.

The DPWS protocol stack, depicted in fig x, integrates all the relevant core standards. With DPWS, all messaging is based on the use of SOAP and WS-Addressing.

<table>
<tr><td colspan="3">Application Specific Protocol</td></tr>
<tr><td colspan="2">WS-Discovery</td><td>WS-Eventing</td></tr>
<tr><td colspan="2">WS-Security
WS-MetadataExchange</td><td>WS-Policy
WS-Addressing</td></tr>
<tr><td colspan="3">SOAP 1.2
WSDL 1.1, XML Schema</td></tr>
<tr><td colspan="2" rowspan="2">UDP</td><td>HTTP 1.1</td></tr>
<tr><td>TCP</td></tr>
<tr><td colspan="3">IPv4/IPv6</td></tr>
</table>

Fig. 7-1: Devices Profile for Web Services protocol stack.

To the above-mentioned Web Services core protocols, DPWS adds Web Services protocols for discovery and eventing.

- WS-Discovery is a protocol for plug-and-play, ad hoc discovery of network-connected resources. Leveraging the SOAP/UDP binding, it defines a multicast protocol to search for and locate devices. Once discovered, a device exposes the services it provides. As multicast-based discovery is limited to local subnets, the notion of discovery proxy is introduced so as to allow for enterprise-wide scalability
- WS-Eventing defines a publish-subscribe event handling protocol allowing for one Web Service ("event sink") to subscribe with another Web Service ("event source") in receiving

event notification messages. WSEventing is intended to enable implementation of a range of applications, from device-oriented to enterprise-scale publish- subscribe systems, on top of the same substrate.

Migration to device level:

The convergence between computing and networking, fuelled by advances in semiconductor and transmission technologies, are revolutionizing the way communications are organized at the level of embedded devices. Indeed, as the intelligence of computing and communications can be driven down to the lowest device levels, higher-level device communication paradigms supported by open Internet protocol standards are emerging. Homing in on this tendency and leveraging the widespread adoption of service-oriented architectures using Web Services standards, the SIRENA project has implemented a high-level framework for service-oriented communication between devices, as well as between devices and applications. This approach enables novel device networking architectures and holds the promise of allowing seamless integration of device-level functionality into enterprise-level business processes, prolonging the paradigm of holonic manufacturing systems across the entire spectrum of industrial automation networks.

7.8.4 Results interesting for VAN project

Within the VAN project the infrastructure for distributed application processes will be developed. Thus, the service oriented architecture will persistently influence the mechanisms of distributed applications. Because the aim of SIRENA is to bring the DPWS to the field devices, the consequences of service-oriented application architecture should be investigated within the WP 2, WP 7, and WP 8.

Glossary

3GPP	The scope of 3rd Generation Partnership Project
8PSK	8 Phase Shift Keying
A3, A5, A5	Ciphers used in cellular phones
AES	Advanced Encryption Standard (AES)
ALG	Application Level Gateways
AP	Application Process or Access Point
APDU	Application Data Unit
API	Application Programming Interface
APL	Application Layer
APS	Application Support Sublayer
AR	Application Relationship
ARP	Address Resolution Protocol
ARPM	Application Relationship Protocol Machine
ARQ	Automatic Repeat Request
AuC	Authentication Centre
BER	Bit Error Ratio
BLO	Business Logic Objects
BOOTP	Bootstrap Protocol
BS	Base Station
BSS	Base Station System
BTS	Base Station
BWA	Broadband Wireless Access
CA	Certification Authority
CAAS	Central Access Rights and Authorization Server
CBA	Component Based Architecture
CBC	Cipher Block Chaining
CCK	Complimentary Code Keying
CDMA	Code Division Multiple Access
CEDS	Central Event Distribution Server

CI	ControlNet International
CiA	CAN in Automation
CIP	Common Industrial Protocol
CK	Cipher Key
CMU	Co-operative Manufacturing Units
CNC	Computer Numerical Control
CORBA	Common Object Request Broker Architecture
CORD	Central Object Relation Data Base
COTS	Commercial off-the-shelf
CPS	Common Part Sublayer
CRC	Cyclic Redundancy Check
CS	Convergence Sublayer
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CST	Composite State Transfer protocol
CTR	Counter Mode
D8PSK	DECT 8PSK
DCE	Distributed Computing Environment (DCE)
DCF	Distributed Coordination Function
DCOM	Distributed Component Object Model
DCRF	Distributed Control System Real-Time Framework
DCS	Distributed Control System
DECT	Digital Enhanced Cordless Telecommunications
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMPM	Data Link Mapping Protocol Machine
DPRS	DECT Packet Radio Service
DPWS	Devices Profile for Web Service
DQPSK	DECT QPSK
DSL	Digital Subscriber Line
DSP	Dogital Signal Processor
DSSS	Direct Sequence Spread Spectrum
E/E/PE	Electrical/Electronic/Programmable Electronic

EAP	Extensible Authentication Protocol
ECSME	EPA Communication Scheduling Management Entity
EDCF	Enhanced Distributed Coordination Function
EDGE	Enhanced Data rates for GSM Evolution is a digital mobile phone technology
EDS	Electronic Data Sheets
EMI	Electromagnetic Interference
EPSG	Ethernet PowerLink Standardisation Group
ERP	Enterprise Resource Planning or Emitted Radio Power
ES	Engineering System
ETSI	European Telecommunications Standards Institute
EUC	Equipment under Control
FAL	Application Layer
FBAP	Function Block Application Process
FCA	Functional Core Applications
FDA	Field Device Access
FDD	Frequency Division duplex
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FFD	Full Function Device
FHSS	Frequency Hopping Spread Spectrum
FIFO	First In, First Out
FP	Fixed Port
FPGA	Field-Programmable Gate Array
FSPM	Service Protocol Machine
GEA3	GPRS Encryption Algorithm 3
GERAN	GSM/EDGE Radio Access Network
GGSN	Gateway GSN
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GPS	Global Position System
GSM	Global System for Mobile
GSN	GPRS Support Node
HCF	Hybrid Coordination Function

HCI	Human Computer Interaction
HIDS	Host Intrusion Detection Systems
HLR	Home Location Register
HMA	HSE Management Agent
HMAC	Hashed Message Authentication Code
HMI	Human Machine Interface
HSE	High Speed Ethernet
ICA	Intelligent Core Adapters
IDA	Interface for Distributed Automation
IDL	Interface Description
IEA	Industrial Ethernet Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IO	Input/Output
IP	Internet Protocol
IPC	Industrial PC
IRT	Isochronous Real-Time
ISM	Industrial, Scientific and Medical
ISO	International Standards Organisation
IST	Information Society Technologies
IT	Information Technology
IV	Initialization Vector
KASUMI	Block cipher used in UMTS
LAN	Local Area Network
LLC	Logical Link Control
LMPM	Link Layer Mapping Protocol Machine
LOS	Line-Of-Sight
LRE	LAN Redundancy Entity
LVDS	Low Voltage Differential Signals
MAC	Media Access Control
MAC-I	Message Authentication Code for Integrity

MAI	Maintenance Application Integration
MAN	Metropolitan Area Networks
MBWA	Mobile Broadband Wireless Access
MCS	Modulation and Coding Scheme
MD5	Message-Digest Algorithm 5
MEER	Ministry for Energy and Energy Resources
MES	Manufacturing Execution System
MIB	Management Information Base
MIC	Message Integrity Code (Check)
MS	Mobile Station
NIDS	Network-Based Intrusion Detection System
NLOS	Non-Line-Of-Sight
NMA	Network Management Agent
NSR	Non-Safety Relevant
NT	New Technology
NTP	Network Time Protocol
NWK	ZigBee Network Layer
OD	Object description
ODVA	Open DeviceNet Vendor Association
OFDM	Orthogonal Frequency Division Multiplexing
OPC	OLE for Process Control
OSACA	Open System Architecture for Controls within Automation System
OSF	Open Software Foundation
P2M	Point-To-Multipoint
P2P	Point-To-Point, Peer-To-Peer
PA	Product Agent
PAN	Personal Area Network
PAS	Public Available Specification
PBCC	Packet Binary Convolution Coding
PC	Personal Computer
PCD	PROFINET Component Description
PCF	Point Coordination Function
PCP	Peripherals Communication Protocol

PCU	Packet Control Unit
PDU	Protocol Data Unit
PFD	Probability of Failure on Demand
PHY	PHY is physical layer of OSI model
PID	Proportional Integral Derivative
PKI	Public Key Infrastructure
PKM	Privacy Key Management
PLC	Programmable Logic Controller
PMA	Plant Management Agents
PNO	PROFIBUS user organisation
PP	Portable Port
PSK	Pre-Shared Key
PTP	Precision Time Protocol
QoS	Quality of Service
R&D	Research and Development
RA	Residential Agent
RF	Radio Frequency
RFD	Reduced Function Device
RFID	Radio Frequency IDentification
RLC	Radio Link Control
RPC	Remote Procedure Call
RSA	algorithm for public-key encryption
RT	Real-Time
RTI	Real-Time Innovations, Inc.
RTP	Real-time Transport Protocol
RTPS	Real-Time Publish/Subscribe
SA	Security Association
SCADA	Supervisory Control and Data Acquisition
SGSN	Serving GPRS Support Node
SHA-1	Secure Hash Algorithm
SIL	Safety Integrity Level
SIM	Subscriber Identity Module
SMK	System Management Kernel

SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SNTP	Simple NTP
SOA	Service Oriented Architecture, State-of-the-Art
SOAP	Simple Object Access Protocol
SOHO	Small-Office-Home-Office
SPS	Speicherprogrammierbare Steuerung [De], stands for PLC
SQL	Structured Query Language
SR	Safety Relevant
SRD	Short Range Devices
SS	Subscriber Station
TBF	Temporary Block Flow
TC	Traffic Class
TCP	The Transmission Control
TD	TORERO Device
TDD	Time Division Duplex
TDM	Time-Division Multiplexing
TDMA	Time Division Multiple Access
TIDE	TORERO IDE
TKIP	Temporal Key Integrity Protocol
TMSI	Temporary Mobile Subscriber Identity
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UPnP	Application of Plug-and-Play capabilities in the field device level
USIM	UMTS SIM
UTRAN	UMTS Terrestrial Radio Access Network
VAN	Virtual Automation Network
VCR	Virtual Communication Relationships
VFD	Virtual Field Device
VLAN	Virtual LAN

VLR	Visitors Location Register
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Network
WCDMA	Wideband CDMA
WLL	Wireless Local Loop
WS	Web Service
XML	Extensible Markup Language
ZDO	ZigBee Device Object
ZVEI	Zentralverband der Elektrotechnik und Elektronikindustrie

References

[3GPPSpec] *3GPP Specifications*, www.3gpp.org

[AJ04] Andy Jones: Proceedings of the 3rd European Conference on Information Warfare and Security – 2004, Academic Conferences Limited, ISBN 0954709624

[ASI] *AS-Interface - The Automation Solution*. AS-International Association, Germany, 2002

[ASISafe] AS-Interface Safety at work. *Safety in Automation – Introduction and application examples*. AS-International Association, Germany, 2004

[ATV00] Alves M, Tovar E, Vasques F. *Ethernet Goes Real-Time: a Survey on Research and Technological Developments*. Techn. Rep. HURRAY-TR-0001, Polytechnic Institute of Porto, 2000.

[AW03] Agarwal A and Wang KB. *Supporting Quality of Service in IP multicast networks.* Computer Communications, Volume 26, Issue 14:1533-1540, 2003.

[Bal05] Balzer, D.: Unpublished Working Paper, AUCOTEAM GmbH, Berlin, October 2005.

[BLM03] Bonaccorsi A.; Lo Bello L.; Mirabella O.; Neumann P.; Pöschmann A. (2003). *A Distributed Approach to Achieve Predictable Ethernet Access Control in Industrial Environments*. 5th IFAC International Conference on Fieldbus Systems and their Applications (FET 2003) Aveiro: Proceedings 173 - 176.

[BSB00] Baek-Young Choi, Sejun Song, Birch N and Huang J (2000). *Probabilistic approach to switched Ethernet for real-time control applications*. Seventh International Conference on Real-time Computing Systems and Applications 2000: Proceedings 384-388.

[BS96] Bruce Schneier, Applied Cryptography, 2nd edition, Wiley, 1996, ISBN 0471117099.

[BW97] Brasche G, Walke B [1997]. *Concepts, Services, and Protocols of the New GSM Phase 2+ General Packet Radio Service*. IEEE Communications Magazine, pp. 94-104, Aug 1997.

[CCL02] Carpenzano A.; Caponetto R.; Lo Bello L.; Mirabella O. (2002). *Fuzzy Traffic Smoothing: an Approach for Real-Time Communication over Ethernet Networks.* 4th IEEE International Workshop on Factory Communication Systems WFCS'02, Västerås: 241-248.

[CEPNeum] Neumann P.: *Communication In Industrial Automation – What is going on?*, Unpublished paper accepted by Control Engineering Practice, 2005

[CIPSafe] Open DeviceNet Vendor Association, *CIPSafety*, White Paper, 2003.

[CLM03] Caponetto R., Lo Bello L, Mirabella O (2003). *Experimental Assessments of Fuzzy Smoothers for Ethernet Networks*. 15th Euromicro Conference on Real-Time Systems, Porto 2003: Proceedings 57-60.

[DANY05] Demachi Kouji, Akabane Kuniharu, Nakajima Takeshi, Yokoi Toyoaki. *Vnet/IP Real-Time Plant Network System*. Yokogawa Technical Report English Edition, No. 39 (2005).

[DH03] Dolejs O, and Hanazalek Z (2003). *Simulation of Ethernet for real-time applications.* IEEE International Conference of Industrial Technology (ICIT 2003):1018-1021.

[EDGEWP] *EDGE White Paper*, www.ericsson.com

[EMSW02] Eklund C, Marks R, Stanwood K, Wang S [2002]. *IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access*, IEEE Communications Magazine, June 2002.

[EN 954-1] EN 954-1: 1997-03; Safety of machinery – Safety-related parts of control systems – Part 1: Generalprinciples for design. Beuth Verlag Berlin 1997.

[EPS04] Pfeiffer, A: *ETHERNET Powerlink Safety Protocol,* Ethernet Powerlink Standardization Group, http://www.omimo.be/vpr/layout/display/pr.asp?PRID=7999, 2004

[EPS05] *ETHERNET Powerlink -Safety and Security,* Ethernet Powerlink Standardization Group*,* http://www.ethernet-powerlink.org/index.php?id=94

[Eth01] *Ethernet/IP specification (2001), Release 1.0*. June 5, 2001, ControlNet International and open DeviceNet Vendor association.

[FAA01] Frederickson, A., A.: *Relationship of EN 954-1 and IEC 61508 Standards* QA020002.pdf, http://www.safetyusersgroup.com, 2004

[Fur03] Furrer F J (2003). *Industrieautomation mit Ethernet-TCP/IP und Web-Technologie.* 3rd ed. Hüthig; 2003.

[Gor05] Gorka J. (2005). *1394automation. Ergebnisse und nächste Schritte.* Polyscope,Volume 37. Issue 3: 27-29.

[GRD02a] Georges J-P, Rondeau E, and Divoux T. (2002a). *How to be sure that switched Ethernet networks satisfy the real-time requirements of an industrial application?* IEEE Int. Symposium on Industrial Electronics. ISIE 2002, Volume 1, pp. 158-163.

[GRD02b] Georges J-P, Rondeau E, and Divoux T (2002b). *Evaluation of switched Ethernet in an industrial context by using the network calculus*. IEEE 4th Workshop on Factory Communication Systems WFCS´02, Västerås, 2002: 19-26.

[Hei99] Heine G [1999]. *GSM Networks: Protocols, Terminology and Implementation*. Artech House Publishers, 1999.

[HJH02] Hoang H, Jonsson M, Hagstrom U, and Kallerdahl A (2002). *Switched real-time Ethernet and earliest deadline first scheduling-protocols and traffic handling.* 10th International Workshop on Parallel and Distributed Real-Time Systems, Fort Lauderdale, Florida, USA, April 2002.

[HL04] Haertig H and Loeser J (2004). *Using Switched Ethernet for Hard Real-Time Communication.* International Conference on Parallel Computing in Electrical Engineering (PARELEC 2004), Sept. 2004, Dresden, Germany: 349-353.

[HM02] David Hucaby, Steve McQuerry: Cisco Field Manual: Catalyst Switch Configuration, Cisco Press, ISBN: 1587050439

[HVBG] Fachausschuss Elektrotechnik, *Guigeline for the Test and Certification of "Bus Systems for the trasmission of Safety Relevant Messages"*, 5/2002.

[HSE01] *High Speed Ethernet Specification documents FF-801, 803, 586, 588, 589, 593, 941.* Fieldbus Foundation, Austin 2001.

[IBClub] Interbus Club e.V., www.interbusclub.org

[IDA] IDA Group*. IDA - Interface for Distributed Automation*,http://www.modbus-ida.org.

[IDA02] IDA Group. *IDA - Interface for Distributed Automation. Architecture Description and Specification.* Revision 1.1, November 2002.

[IDASafe] IDA Group. *IDA - Interface for Distributed Automation. IDA Safety Data Transmission Protocol, V4.3*, 9/2001.

[IEC61158] IEC 61158 series, Edition 3: *Digital data communication for measurement and control - Fieldbus for use in industrial control systems*.

[IEC61499] IEC61499, Edition 1.0: *Function Blocks*, Geneva 2005

[IEC61508] IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Parts 1-7*.

[IEC61588] IEC 61588: *Precision clock synchronization protocol for networked measurement and control systems.*

[IEC65C341] IEC 65C/341/NP. *Real-Time Ethernet: MODBUS-RTPS.*

[IEC65C352] IEC 65C/352/NP. *Real-Time Ethernet: Vnet/IP.*

[IEC65C353] IEC 65C/353/NP. *Real-Time Ethernet: TCnet (Time-critical Control Network).*

[IEC65C355] IEC 65C/355/NP. *Real-Time Ethernet: ETHERCAT.*

[IEC65C356] IEC 65C/356/NP. *Real-Time Ethernet: POWERLINK.*

[IEC65C357] IEC 65C/357/NP. *Real-Time Ethernet: EPA (Ethernet for Plant Automation)*.

[IEC65C358] IEC 65C/358/NP. *Real-Time Ethernet: SERCOS III.*

[IEC65C359] IEC 65C/359/NP. *Real-Time Ethernet: PROFINET IO. Application Layer Service Definition & Application Layer Protocol Specification.*

[IEC65C360] IEC 65C/360/NP. *Real-Time Ethernet: P-NET on IP.*

[IEC65C361] IEC 65C/361/NP. *Real-Time Ethernet: EtherNet/IP with time synchronization.*

[IEC8802] ISO/IEC 8802-3. *Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and Physical Layer specifications*.

[IEEE802.16] *IEEE Std. 802.16-2001, IEEE Standard for Local and Metropolitan Area Networks, part 16,* "Air Interface for Fixed Broadband Wireless Access Systems," IEEE Press, 2001.

[IEEE1588] 1588 I*EEE Standard for a Precision Clock Synchronisation Protocol for Networked Measurement and Control Systems,* Institute of Electrical and Electronics Engineers, New York, November 2002.

[IEEE1588-2] http://ieee1588.nist.gov/

[ISA02] Berge J: *Fieldbuses for Process Control*. ISA – The instrumentation, Systems, and Automation Society, USA, 2002.

[Jas02] Jasperneite J. *Leistungsbewertung eines lokalen Netzwerkes mit Class-of-Service Unterstützung für die prozessnahe Echtzeitkommunikation*. Aachen: Shaker: 2002. ISBN 3832208321.

[Jen02] Jennings, S.: *Hier ticken alle Uhren gleich*; In: IEE Automatisierung und Datentechnik, Heft 7, Hüthig Verlag GmbH, Heidelberg Germany, 2002.

[JN01a] Jasperneite J, Neumann P (2001). *Switched Ethernet for Factory Communication.* IEEE conference on Emerging Technologies and Factory Automation (ETFA´01). Antibes Juan-les-pins, France : 205-212.

[JN01b] Jasperneite J, Neumann P. *Performance Evaluation of Switched Ethernet in Real-Time Applications.* 4th International Conference on Fieldbus Systems and their Applications, FET2001 Nancy; 2001: 144-151.

[JSW04] Jasperneite J, Shehab K, Weber K (2004). *Enhancements to the Time Synchronization Standard IEEE- 1588 for a System of Cascaded Bridges*. 5th IEEE International Workshop on Factory Communication Systems, WFCS2004, Vienna, Austria; 2004: 239-244.

[KK00] Kweon, S-K and KG Shin (2000). *Achieving real-time communication over Ethernet with adaptive traffic- smoothing.* 6th IEEE conference on Real-Time Technology and Applications Symposium, RTAS, Washington D.C, May 2000: 90-100.

[KSZ99] Kweon, S-K, Shin, KG, and Zin Zheng (1999). *Statistical real-time communication over Ethernet for manufacturing automation systems.* 5th real-time technology ans applications symposium, 1999: 2-4.

[KT98] Micki Krause, Harold F. Tipton : Handbook of Information Security Management, CRC Press LLC), ISBN: 0849399475

[LA05] Lorentz K, Lüder A, *IAONA Handbook, Industrial Ethernet*, Third Edition, July 2005.

[Lar05] L. Larsson, *Fourteen Industrial Ethernet solutions under the spotlight*, The Industrial Ethernet Book, September 2005.

[LE03] Lee, K.; Eidson, J.: Workshop on IEEE-1588, *Standard for a Precision Clock Synchronisation Protocol for Networked Measurement and Control Systems*, National Institute of Standards and Technology; Gaithersburg, Maryland; September 2003.

[LH04] Loeser J, Haertig H. (2004). *Low-latency hard real-time communication over switched Ethernet.* 16th EURIMICRO Conference on Real-time Systems ERTS 2004: 13-22.

[Liu00] Liu W S (2000). *Real-Time Systems*. Prentice Hall; 2000.

[LL02] Lee KC, and Lee S (2002). *Performance Evaluation of Switched Ethernet for Networked Control Systems*. IEEE 28th International Conference on Industrial Electronics, Control, and Instrumentation (IECON 2002), Industrial Electronics Society: 3170-3175.

[LL05] Lüder, A., Lorentz, K. (editors): *IAONA Handbook Industrial Ethernet*. 3rd edition, Magdeburg, 2005.

[LON95] LonWorks *Engineering bulletin EB179/1995*, LonMark Interoperability Association, Echelon Corp., USA 1995.

[Mar04] Marshall PS (2004). *Industrial Ethernet*. ISA Book; 2004. ISBN 1556178697.

[Mei02] Meindl A (2002). *Ethernet Powerlink, Application in Practice*. PRAXIS ProfiLine - Industrial Ethernet. April 2002: 55-57

[Mes03] Messerschmidt, R.: *Real-Time Concepts for Ethernet - Basics and Developments in Ethernet Real-Time.* In: Klostermeyer, A.; Lorentz, K. (Editors) Praxis Profiline: Industrial Ethernet – Erfolgsstory vom Büro bis in die Fabrik (German/English), Würzburg, Vogel-Publishers, April 2003.

[Mes04] Messerschmidt, R.: *IEEE 1588 Clock Synchronisation for Ethernet.* In: Klostermeyer, A.; Lorentz, K. (Editors) Praxis Profiline: Industrial Ethernet – Ein Trend etabliert sich (German/English), Würzburg, Vogel-Publishers, April 2004.

[Neu05] Neumann, P.: *Virtual Automation Networks – An Overview.* Presentation to the VAN Consortium, Frankfurt/Main, June 9th 2005.

[OCE05] http://www.fidia.it/english/research_ocean_fr.htm

[ODVA] Open DeviceNet Vendor Association, http://www.odva.org/.

[OSFC706] OSF C 706. Open Software Foundation (OSF). *C706, CAE Specification DCE11: Remote Procedure*.

[PA05] Pedreiras P, Almeida L (2005). *Approaches to enforce real-time behavior in Ethernet.* In The Industrial Communication Technology Handbook, Zurawski R. (Ed.), CRC Press, Boca Raton, FL, 2005.

[PAB04] http://www.pabadis.org/

[PG02] Peter Gutman. "PKI: It's Not Dead, Just Resting," IEEE Computer, vol. 35, no. 8, pp. 41-49, August, 2002

[PNO] Profibus Nutzerorganisation e.V., http://www.profibus.org.

[PNO03] 4.132 *PROFINET System Description*, November 2003, http://www.profibus.com.

[POW02] *Ethernet Powerlink – Data Transport Services*, Bernecker + Rainer, GmbH., 2002

[PRO03] PROFIBUS Guideline (2003). *PROFINET Architecture Description and Specification, Version V 2.0.* Karlsruhe: PNO; 2003.

[PROT05] http://www.proteus-iteaproject.com

[PW03] Pöschmann A, Werner T (2003). *Studie "Ethernet in der Automation"* (in German), Frankfurt: ZVEI; 2003.

[REM05] http://www.rempli.org/

[RFC1157] RFC 1157, *Simple Network Management Protocol* (SNMP).

[RFC1541] RFC 1541, *Dynamic Host Configuration Protocol*.

[RFC2030] RFC 2030, *Simple Network Time Protocol.*

[RFC768] IETF (1980). RFC 768. *User Datagram Protocol*. IETF, available at http://www.ietf.org.

[RFC791] IETF (1981a). RFC 791. *Internet Protocol*. IETF, available at http://www.ietf.org.

[RSA98] RSA Cryptography Standard, *RSA Public Key Cryptography Standard #1 v. 2.0,* RSA Laboratories, Oct. 1998, . http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/.

[SIR05] http://www.sirena-itea.org/Sirena/Home.htm

[SKS02] Song Y, Koubaa A, and Simonot F (2002). *Switched Ethernet for real-time industrial communication: modelling and message buffering delay evaluation*. 4th IEEE International Workshop on Factory Communication Systems (WFCS 2002): 27-35.

[SS04] Smith D., Simpson K., *Functional Safety - A straightforward guide to applying IEC 61508 and related standards*, Elsevier Butterwort-Heinemann, Great Britain, 2004.

[STE94] Stevens, W.R.: *"TCP/IP Illustrated, Volume 1: The Protocols"*. Addison-Wesley, 1994, Reading, Mass.

[TK04] Thanikesavan S, Killat U (2004). *Global Scheduling of Periodic Tasks in a Decentralised Real-time Control System*. 5th IEEE International Workshop on Factory Communication Systems WFCS 2004, Vienna: 307-310.

[TOR02] http://www.uni-magdeburg.de/iaf/cvs/torero/

[WiFiAlnc] *Wi-Fi Alliance*, http://wi-fi.org

[WiMAXFrm] *WiMax Forum*, www.wimaxforum.org

[WR04] Wang J, and Ravindran B (2004). *Time-utility function-driven switched Ethernet: packet scheduling algorithm, implementation and feasibility analysis.* IEEE Transactions on Parallel and Distributed Systems. Vol. 15, no.2.

[WRA05] Wratil, P: Safety related networks – Ethernet powerlink safety, PRAXIS Profiline, http://www.ethernet-powerlink.org/uploads/media/ArticleSafetyRelatedNetworks.zip, 2005

[XZY02] Xinggang Fan, Zhi Wang and Youxian Sun (2002). *How to guarantee factory communication with switched Ethernet: survey of its emerging technology.* IEEE 28th Annual Conference, Industrial Electronics Society; 2002.

Appendixes

Appendix A - Parameters of the Selected Communication Technologies

Appendix B - Parameters of the Selected Technologies with Real-time Properties

Appendix C - Parameters of the Selected Safety Technologies

Appendix D - Parameters of the Selected Security Technologies & Methods

Appendix A – Parameters of the Selected Communication Technologies

Technology Name	Wired/Wireless	Typical application field	Safety version available	Maturity level	ISO/OSI Layers	max. Brutto Data Rate(s)	Physical/MAC Layer(s)	Media/ Frequency Band available	Network Topology	Access Method (MAC)	Application Model	Technology Developer	Standards
EtherCAT	Wired	RT Industrial Control	No	Emerging	1-7	10 Gbps	802.3xx	UTP	Line, Tree, Star	CSMA/CD, Token	Prod/Cons	EtherCAT Technology Group	IEC/PAS 62407
EtherNet/IP	Wired	Factory Automation	Yes	Mature	1-4,7	100 Mbit	802.3xx	UTP FO	Star	CSMA/CD, Segments	Client/Server	ODVA	IEC 61158 Type 2 (CIP) IEC 61158 PAS 62413 (Sync)
EPA (Ethernet for Plant Automation)	Wired	Factory Automation	No	Emerging	1-4,7	N/A	802.3	UTP, FO,Air	N/A	CSMA/CD, Timeslots	n/a	Zhejiang Supcon	IEC/PAS 62409
EPL	Wired	IO & Drives Control	Yes	Mature	2-7	100 Mbps	802.3	UTP	Line, Tree, Star	Timeslots	Prod/Cons Client/Server	(EPSG	IEEE 802.3, EN50325-4, ISO 15745-4, IEEE 1588
FF HSE	Wired	Process Automation	Yes	Mature	1-4,7	10 Mbps	802.3	UTP, FO, Air	Line,Tree, Star	CSMA/CD	Client/Server Pub/Sub Report Distribution	FF	IEC 61158
JetSync	Wired	Factory Automation	No	Mature	1-4,7		802.3	UTP	Line, Tree, Star	CSMA/CD	Client/Server	Jetter AG	-
Modbus/TCP	Wired	Factory Automation	No	Mature	5-7	10 Gbps	802.3xx	UTP, FO,Air	Line, Tree, Star	CSMA/CD	Client/Server	Modbus IDA	IEC-61158
P-Net on IP	Wired	n/a	No	Emerging	1-4,7		802.3	UTP, FO,Air	Line, Tree, Star	CSMA/CD	Client/Server	Proces-Data	IEC/PAS 62412
PROFINET	Wired	Factory Automation	Yes	Emerging	1-4,7	100 Mbps	802.3xx	UTP, FO,Air	Line, Tree, Star	CSMA/CD	Prod/Cons Client/Server	Profibus International	IEC61158
Sercos III	Wired	Factory Automation	Yes	Emerging	3-7	100 Mbps	802.3	UTP	Double Ring Line	Timeslots	Master/Slave	Interest Group Sercos (IGS)	IEC 61491, EN 61491
TCnet	Wired	N/A	No	Emerging	1-4,7	N/A	802.3	UTP, FO,Air	Line, Tree, Star	CSMA/CD, ?	Pub/Sub	Toshiba	IEC/PAS 62406
VNet/IP	Wired	Process Automation	No	Mature	1-4,7	10 Gbps	802.3xx	UTP, FO,Air	Line, Tree, Star	CSMA/CD, ?	Prod/Cons	Yokogawa	IEC 61158 PAS 62405
Bluetooth	Wireless	Office, Great Data Quantities	No	Mature	1-7	1 Mbps	802.15.1	Air	Star	TDMA	Server/Client	Bluetooth SIG	IEEE 802.15.1
GPRS	Wireless	Mobile data	No	Mature	1-7	171.2 kbps	ETSI/3GPP TSs Rel 4 & later	Air	P2P/P2MP	TDMA FDMA	P2P/P2MP	ETSI	ETSI/3GPP Specifications
WISA	Wireless	Manufactu-ring Auto-mation	No	Emerging	1,2,7	4x1Mbps	IEEE 802.1	Air 2,4G	Star	FDMA TDD TDMA	P2P	ABB	IEEE802.15.1 (Physical Layer)
ZigBee	Wireless	Office, Building Automation	No	Emerging	1-7	250 kbps	802.15.4	Air	P2P, Star, Mesh	CSMA/CA GTS	P2P	ZigBee Alliance	IEEE 802.15.4 (Physical Layer)

Appendix B – Parameters of the Selected Technologies with Real-time Properties

Technology Name	Cycle (Reaction) Time [ms] / Number of Nodes	Min. Cycle Time	Max CycleTime	Jitter	Device Discovery Time / Number of Nodes	Dropout Discovery Time
AS-Interface 2.1	2.55/16	300 us	35 ms	300 us	2.1-604.5 ms	1.35 - 30.15 ms
EtherCAT	0,1/100	230 us at 33% Bus load	276 us at 44% Bus load	~1 us	N/A	1 cycle
EtherNet/IP	N/A	N/A	N/A	< 1us (CIP Motion)	N/A	N/A
EPL	400 µs/8	200 µs	N/A	<1 µs	N/A	N/A
Interbus	1/512	700 us at min. busconfig	8ms at max.busconfig	5 us	N/A	N/A
ModbusPlus	Token rotation time [ms] = Node count + (((Node Count-1)*2)*(Average Message size *0,016))	Token rotation time [ms] = Node count + (((Node Count-1)*2)*(Average Message size *0,016))	Token rotation time [ms] = Node count + (((Node Count-1)*2)*(Average Message size *0,016))	<200 ns	Token reconstition time [ms] = 50 + (4 * lowest remaining address) + (16 * (total dropped nodes - 1)) + (total remaining nodes - 1)	Token reconstition time [ms] = 50 + (4 * lowest remaining address) + (16 * (total dropped nodes - 1)) + (total remaining nodes - 1)
PROFInet IO	1/60	250 us IRT / 1ms RT	512 ms	IRT < 1us	4s/ 1..n devices	Configurable
SERCOS III	31,25 µs/10	N/A	N/A	<1 µs	N/A	N/A
Bluetooth	1.25 ms	1.25 ms	N/A	N/A	ca 1s/?	N/A
GPRS	N/A	N/A	N/A	N/A	N/A	N/A
EDGE	N/A	N/A	N/A	N/A	N/A	N/A
UMTS	10/15	10 ms	N/A	N/A	N/A	N/A
Wi-Fi	0.25/3	N/A	N/A	N/A	1.2 s (passive mode), >0.45 ms (active mode)/?	N/A
ZigBee, IEEE 802.15.4	min 15 ms.	15 ms	252 s	depending on Beacon, max 15 ms	< 30ms/?	N/A

Technology Name	OSI Layers Assuring RT Performance	Clock Synchronization	RT Data Transfer Method	non-RT Data Transfer Method	Frame Type	Frame Size
AS-Interface 2.1	2-7	None	Polling	Polling	None	14bit master telegram/ 7bit slave telegram
EtherCAT	2-7	IEEE 1588	One total frame for all devices - Summen-rahmenprotokoll"	Protocol Tunelling	Ethernet	>= 84 Bytes
EtherNet/IP	>4	IEEE1588 is intended (CIPSync)	Publish/Subscribe UDP Multicast	explicite Messaging TCP	Ethernet	1500 Byte
EPL	2-7	IEEE1588 is intended	Timeslot / Broadcast	acyclic Timeslot	Ethernet	1500 Byte
Interbus	1, 2	Bus Triggered	One total frame for all devices - "Summenrahmenprotokoll"	peripheral communication ptotocol (PCP)	None	max 8192 bit within summation frame
ModbusPlus	1-7	None	Token Passing	N/A	Proprietary	200 Byte
Profinet	1,2	IRT - IEEE1588	Cyclic Unicast or Multicast Providers	TCP, UPD, IP	EtherType (0x8892)	64-1500
SERCOS III	2-7	None	Timeslot	Acyclic Timeslot	Ethernet	1500 Byte
Bluetooth	1-7 Voice Channel, Other-wise not	None	Bluetooth SCO Packets	Bluetooth ACL Packets	Bluetooth Proprietary	126-2871 Bytes
GPRS	2-7	N/K	Frames, TSs	VGCS	GPRS proprietary	1250 bits (4.6 ms)
EDGE	2-7	N/K	Frames, TSs	VGCS	GPRS/EDGE Proprietary	1250 bits (4.6 ms)
UMTS	2-7	None	Timeslots	Timeslots	UMTS Proprietary	<=160 Bytes
Wi-Fi	2-7	Wi-Fi Beacon	Polling	CSMA/CA	Wi-Fi Proprietary	>= 34 Bytes
ZigBee, IEEE 802.15.4	3-7	ZigBee Beacon	Guar. Timeslots	CSMA/CA	ZigBee Proprietary	<135B

Appendix C – Parameters of the Selected Safety Technologies

Technology Name	IEC 61508 SIL	EN 954-1 category	Fault Detection	Fault Detection Time	Fault Tolerance	Fault Recovery	Fault Recovery Time	Databits per safe-Telegram (short/long)	Transfer-Time Point2Point	Transfer-Time Loop	propability of failure on demand (pfd)	max. telegram per second	Mixed systems (safe, nonsafe)	max number of safety devices	"Black Channel"
AS-i Safety at Work	3	4	Yes	40 ms	No	Yes	100 ms	4	N/A	N/A	N/A	N/A	Yes	31	AS-i
INTERBUS-Safety	3	4	Yes	2 ms	No	No	N/A	14	2ms	10ms	1,0E-09	51282	Yes	126	IB
PROFISAFE V2 (on PN)	3	4	Yes	N/A	No	No	N/A	96/984	1ms	20ms	1,0E-09	10000	Yes	63/>>	PN
CIP-Safety	3	4	Yes	N/A	No	N/A	N/A	16/2000	N/A	N/A	N/A	N/A	Yes	>>	E, D, C
EthernetIP-Safety	N/A	N/A	Yes	N/A	No	N/A	N/A	16/2000	N/A	N/A	N/A	N/A	N/A	N/A	EthIP
DeviceNet Safety	3	4	Yes	N/A	No	N/A	N/A	16/2000	N/A	N/A	1,0E-09	N/A	N/A	64	DeviceNet
ControlNet Safety	N/A	N/A	Yes	N/A	No	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ControlNet
IDA-Safety	3	4	Yes	N/A	No	N/A	N/A	64	N/A	N/A	1,0E-09	N/A	Yes	N/A	Eth, NDDS
LON-Safety	3	4	Yes	N/A	No	N/A	N/A	64	N/A	N/A	1,0E-09	N/A	Yes	127/SN	LON
PowerLink Safety	3(4)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	1023	Powerlink

Appendix D – Parameters of the Selected Security Technologies & Methods

Encryption Algorithms	Min. Encryption Key Length [bits]	Max. Encryption Key Length [bits]	Implementation complexity	Resistance to Known Plain Text Attack	Resistance to Chosen Plain Text Attack	Key Type
RSA	1024–2048	>2048	3	Yes	Yes	Assymetric
3DES	168	168	1-2	Yes	Yes	Symmetric
MD5	N/A	N/A	2-3	No	No	N/A
GEA3	64	128	2-3	Yes	Yes	Symmetric
A5/3	64	128	2-3	Yes	Yes	Symmetric
AES	128	256	2-3	Yes	Yes	Symmetric
KASUMI	128	128	2-3	Yes	Yes	Symmetric

Encryption Algorithms

				Implementation attributes							Attack methods						Relevance	
Technology Name	Security TechNology	Application Domain	Technology or product	Digital Signature Support	Authentication Support	Type of Supported Certificate	Support for Encryption Algorithms	Packet Integrity	Encryption support	Shared secret before communication	Man in the Middle	Eavesdropping	Stream Cipher Attack	Replay Attack	Denial-of-service Attack	OSI Layers covering security aspect	Security rating	Implementation complexity
Bluetooth	private key authentication	Office	OEM Serial Port Adapter	No	Yes	None	No	Yes	Yes	No	No	No	No	No	No	1, 2	3	3
Ethernet	CRC	Office	several	No	No	None	none	low	No	No	Yes	Yes	Yes	Yes	Yes	2	1	1
LonWorks	private key authentication	Building Automation	Neuron Chip	No	yes	None	No	?	No	Yes	?	yes	?	No	?	5	2	1
GSM/EDGE	3GPP security algorithm	Mobile data	Several	Yes	Yes	WTLS, WPKI, SWIM?	A5/3 (based on Kasumi)	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	2,3 (LLC)	2-3	2-3
GSM/GPRS	3GPP security algorithm	Mobile data	Several	Yes	Yes	WTLS, WPKI, SWIM?	GEA3 (based on Kasumi)	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	2,3 (LLC)	2-3	2-3
UMTS	UMTS proprietary	Wireles mobile communications	Mobile handsets	Yes	Yes	WTLS, WPKI	AES, KASUMI	CRC 8, 12, 16, 24	Yes	Yes	No	No	Yes	No	No	2, 3	3-4	3
Wi-Fi + WEP	WEP	Wireless office	WEP drivers	No	Yes	None	RC4	CRC-32	Yes	Yes	No	No	Yes	Yes	No	2	3	3
Wi-Fi + WPA2	WPA2	Wireless office	WPA2 drivers	No	Yes	None	AES	CRC-32	Yes	Yes	No	No	Yes	No	No	2	3-4	3
ZigBee	private key authentication	Process & building control	N/A	No	No	None	AES	MIC-128	Yes	Yes	No	No	Yes	No	Yes	2,3,7	3	2

Legend

Security level		Implement		Example
1	insecure	1	low	8-bit CPU
2	home	2	medium	32-bit CPU, or 8-bit + HW support
3	comercial level			
4	government/milit	3	high	HW support

Security Technologies