



**VAN**

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

***Virtual Automation Networks***

Work Package 1

Requirements and Trend Screening

Task 1.3

Trend Screening and Self evaluation

Trend Screening Report on VAN Relevant  
Technologies

<b>Document type</b>	: Report
<b>Document version</b>	: Final
<b>Document Preparation Date</b>	: 10/02/06
<b>Classification</b>	: Public
<b>Contract Start Date</b>	: 01.09.2005
<b>Duration</b>	: 31.08.2009



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

<b>Rev.</b>	<b>Content</b>	<b>Resp. Partner</b>	<b>Date</b>
1.1	Basic chapters structure and outline of Executive summary, Introduction, Chapters 5 and 8	CARTIF, BUT, Phoenix Schneider	21/12/05
1.2	Added Ch. 3, 4, 5, 6	Schneider, Phoenix, Siemens, CVS, Ifak, TSA	13/01/06
1.3	Revisions of Ch. 1, 2 & 4	BUT, Siemens, Phoenix	18/01/06
1.5	Chapter 5 updated	TSA	23/01/06
1.6	Chapter 2 splitted into two chapters	Siemens	24/01/06
1.7	Exec. Summ. and Introduction updated	BUT, Cartif	25/01/06
1.8	Chapter 7 updated Chapter 6 updated	Ifak TSA	25/01/06
1.11	Chapter 7 finished	Ifak	26/01/06
1.12	Chapter 4 finished Chapter 9 outlined -draft- Small changes in Exec. Summary	CVS Cartif	27/01/06
1.13	References sorted alphabetically Chapter 9 small additions	Cartif	27/01/06
1.14	Glossary finished Chapter 9 updated	Cartif	29/01/06
1.15	Small changes on Exec. Summary Chapter 9 finished	Cartif	29/01/06
2.1	Editorial corrections	Cartif, BUT	2/02/06
2.2	Introduction chapter update Chapter 5 updated (references inserted)	Cartif, BUT, Phoenix	3/02/06
2.3	Changes in general section of Ch. 9 Reference to risk analysis inserted in Exec. Summ.	Cartif	3/02/06
2.4	Fine tuning of Chapter 9 from chapter editors and WP 1 Leader	All	7/02/06
2.5	Final draft version	All	9/02/06
Final	Updated cover	Cartif	10/02/06
2.6	Conclusions remarks added according with EC review	Cartif	25/06/06

<b>Final approval</b>	<b>Name</b>	<b>Partner</b>
<b>Review Task Level</b>	Diego Moñux	Cartif
<b>Review WP Level</b>	Frantisek Zezulka	BUT
<b>Review Board Level</b>	Axel Klostermeyer	Siemens
	Michael Grosse	FZK

## Executive summary

This report belongs to the first set of VAN project deliverables. It's aimed to complement and reinforce gathered information about the current status of VAN project related technologies. This report is closely connected with other WP 1 deliverables: those emerging from Task 1.1 "State of the Art", and from Task 1.2, "Requirements and Technological Roadmap"<sup>1</sup>. These referred documents on their first versions should be considered along with this report to obtain an overall view of VAN project starting up conditions.

Another important objective of this document is to provide criteria for continuously tracking industry and technology trends and to check if VAN advances and progression are in accordance with them. Results coming from this deliverable are the basis to the risk analysis process along VAN project. In addition, to clearly identify drivers, pushing or pulling the technological evolution, should be considered as an important goal of this document. To achieve these objectives, four revisions of this document with updated information are planned to be released over the whole project time frame on months 12, 24, 36 & 42.

From the trend point of view, not all technologies and methods can be equally treated, as the representative time frames of each evolution, interdependencies, emerging features and progress indicators are quite different in some cases, closely related in others. Some of the technologies described here will succeed in their evolution and application in industrial environments, some others will be abandoned. The forecasting of the future of ICT's related to VAN is not the aim of this document, but it is difficult to avoid entering evaluation concerning some of them.

The document is structured in 9 chapters. Chapter 1 is the main introduction (BUT), chapters 2 to 7 directly deal with VAN project main technical figures, which correspond with VAN technical work packages: Wireless in industries (Siemens), Real time considerations (CVS), Safety (Phoenix), Security (TSA), Co-operation of private and public networks (Ifak, TSA), and Engineering tools (Schneider). Chapter 9 is a summary of collected conclusions from all the chapters (Cartif). Since wireless technologies are the most dynamical and their trends should be observed closely to market evolution, a specific chapter (3, Siemens) deals with these figures.

The structure of each chapter is first introduced by an overview of each selected technology, a description of its recent evolution including main drivers and market figures, when available. Each description is completed with a maturity analysis and finalised with overall conclusions.

---

<sup>1</sup> Public Deliverable that will be available on Feb. 2006 at VAN project web-site: [www.van-eu.org](http://www.van-eu.org)

# Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>9</b>
<b>2</b>	<b>TRENDS IN WIRELESS TECHNOLOGIES .....</b>	<b>11</b>
2.1	OVERVIEW .....	11
2.2	EVOLUTION.....	11
2.2.1	<i>General</i> .....	11
2.2.2	<i>Comparison of different wireless transmission technologies</i> .....	13
2.3	MATURITY .....	15
2.3.1	<i>General</i> .....	15
2.3.2	<i>Strengths</i> .....	15
2.3.3	<i>Weaknesses</i> .....	16
2.4	CONCLUSIONS.....	17
2.4.1	<i>Wireless in Industrial Environments</i> .....	17
2.4.2	<i>Wireless in Non-Industrial Environments</i> .....	20
<b>3</b>	<b>MARKET APPROACH IN WIRELESS TECHNOLOGIES .....</b>	<b>21</b>
3.1	STATUS QUO.....	21
3.1.1	<i>Key Industries</i> .....	21
3.1.2	<i>Geographic Markets</i> .....	22
3.2	WORLD MARKET FORECAST.....	22
3.2.1	<i>Industrial Wireless Market</i> .....	22
3.2.2	<i>Non-Industrial Wireless Market</i> .....	23
3.3	GEOGRAPHIC MARKET FORECAST.....	24
3.4	KEY INDUSTRIES FORECAST.....	25
3.5	PRODUCT FORECAST.....	25
<b>4</b>	<b>TRENDS IN REAL TIME PROPERTIES OF INDUSTRIAL COMMUNICATION SYSTEMS .....</b>	<b>27</b>
4.1	INTRODUCTION .....	27
4.2	PHYSICAL LAYER (IEEE802.3XX).....	27
4.3	NETWORK LAYER (INTERNET PROTOCOL).....	28
4.4	NETWORK COMPONENTS.....	29
4.5	REAL TIME IN AUTOMATION .....	29
4.5.1	<i>Important Ethernet-based Protocols</i> .....	30
4.5.2	<i>Example for IEEE1588 implementation</i> .....	32
4.5.3	<i>Real Time in Closed Loops</i> .....	34
4.6	REAL TIME IN PUBLIC NETWORKS.....	35
<b>5</b>	<b>TRENDS IN SAFETY OF INDUSTRIAL COMMUNICATION SYSTEMS .....</b>	<b>36</b>
5.1	INTRODUCTION .....	36
5.2	PROFISAFE .....	36
5.2.1	<i>Overview of PROFIsafe</i> .....	36
5.2.2	<i>Evolution of PROFIsafe</i> .....	36
5.2.3	<i>Maturity of PROFIsafe</i> .....	37
5.3	INTERBUS SAFETY .....	37
5.3.1	<i>Overview of Interbus Safety</i> .....	37
5.3.2	<i>Evolution of Interbus Safety</i> .....	37
5.3.3	<i>Maturity of Interbus Safety</i> .....	38
5.4	DEVICENET SAFETY .....	38
5.4.1	<i>Overview of DeviceNet Safety</i> .....	38
5.4.2	<i>Evolution of DeviceNet Safety</i> .....	38
5.4.3	<i>Maturity of DeviceNet Safety</i> .....	38
5.5	AS-INTERFACE SAFETY AT WORK.....	39
5.5.1	<i>Overview of AS-interface Safety at Work</i> .....	39

5.5.2	<i>Evolution of AS-interface Safety at Work</i> .....	39
5.5.3	<i>Maturity of AS-interface Safety at Work</i> .....	39
5.6	ETHERNET POWERLINK SAFETY .....	39
5.6.1	<i>Overview of Ethernet Powerlink Safety</i> .....	39
5.6.2	<i>Evolution of Ethernet Powerlink Safety</i> .....	40
5.6.3	<i>Maturity of Ethernet Powerlink Safety</i> .....	40
5.7	ETHERCAT SAFETY .....	41
5.7.1	<i>Overview of Ethercat Safety</i> .....	41
5.7.2	<i>Evolution of Ethercat Safety</i> .....	41
5.7.3	<i>Maturity of Ethercat Safety</i> .....	41
5.8	SERCOS III SAFETY .....	42
5.8.1	<i>Overview of Sercos III Safety</i> .....	42
5.8.2	<i>Evolution of Sercos III Safety</i> .....	42
5.8.3	<i>Maturity of Sercos III Safety</i> .....	43
<b>6</b>	<b>TRENDS IN SECURITY OF COMMUNICATION SYSTEMS .....</b>	<b>44</b>
6.1	TRENDS IN SECURITY ISSUES – AN OVERVIEW .....	44
6.1.1	<i>Basic security technologies for virtual automation network environments</i> .....	44
6.1.2	<i>More than technology</i> .....	45
6.1.3	<i>The current status</i> .....	45
6.1.4	<i>Trends</i> .....	46
6.2	NEEDS FOR SECURITY .....	48
6.3	LEGAL DRIVERS FOR SECURITY .....	49
6.3.1	<i>Trusted computing platforms</i> .....	49
6.3.2	<i>Cyber crime</i> .....	49
6.3.3	<i>Roaming</i> .....	50
6.3.4	<i>Challenges</i> .....	50
6.4	INTEGRATION OF SECURITY FUNCTIONS INTO THE IP STACK .....	50
6.4.1	<i>Overview</i> .....	50
6.4.2	<i>Evolution</i> .....	51
6.4.3	<i>Maturity</i> .....	51
6.5	ELLIPTIC CURVE CRYPTOGRAPHY .....	52
6.5.1	<i>Overview</i> .....	52
6.5.2	<i>Evolution</i> .....	52
6.5.3	<i>Maturity</i> .....	52
6.6	ID-BASED CRYPTOGRAPHY .....	52
6.6.1	<i>Overview</i> .....	52
6.6.2	<i>Evolution</i> .....	53
6.6.3	<i>Maturity</i> .....	53
6.7	GROUP KEYING .....	53
6.7.1	<i>Overview</i> .....	53
6.8	ADDITIONAL TRENDS .....	54
6.8.1	<i>Trusted and secure automation devices</i> .....	54
6.8.2	<i>Secure reconfiguration of automation devices</i> .....	55
6.8.3	<i>DRM security architectures and protocols</i> .....	55
6.8.4	<i>Protection of the virtual network against attacks</i> .....	55
6.8.5	<i>Heterogeneous network access control security</i> .....	56
6.8.6	<i>Seamless security handover at the network level</i> .....	56
6.8.7	<i>Protection of service networks against attacks</i> .....	56
6.8.8	<i>Application security framework</i> .....	56
6.8.9	<i>Single sign-on based on authentication</i> .....	57
6.8.10	<i>Authorisation privacy</i> .....	57
6.8.11	<i>Lightweight stream ciphers</i> .....	57
6.8.12	<i>Truly practical cryptographic mechanisms in constrained environments</i> .....	57
6.8.13	<i>Delegation of cryptographic operations</i> .....	57
6.8.14	<i>Lightweight key management infrastructures</i> .....	57
6.9	RESEARCH ISSUES SUMMARY .....	57
<b>7</b>	<b>TRENDS IN CO-OPERATION OF PRIVATE AND PUBLIC NETWORKS .....</b>	<b>59</b>
7.1	TRENDS IN GENERAL .....	59
7.2	TRENDS IN AUTOMATION.....	65
<b>8</b>	<b>TRENDS IN ENGINEERING TOOLS FOR VAN GOALS .....</b>	<b>67</b>

8.1	INTRODUCTION .....	67
8.2	OPC.....	67
8.2.1	<i>Overview of OPC</i> .....	67
8.2.2	<i>Evolution of OPC</i> .....	67
8.2.3	<i>Maturity of OPC</i> .....	68
8.2.4	<i>Conclusions about OPC</i> .....	68
8.3	FDT/DTM.....	68
8.3.1	<i>Overview of FDT/DTM</i> .....	68
8.3.2	<i>Evolution of FDT/DTM</i> .....	69
8.3.3	<i>Maturity of FDT/DTM</i> .....	69
8.3.4	<i>Conclusions about FDT/DTM</i> .....	69
8.4	PLUG-AND-PLAY .....	69
8.4.1	<i>Overview of Plug-and-Play</i> .....	69
8.4.2	<i>Evolution of Plug-and-Play</i> .....	70
8.4.3	<i>Maturity of Plug-and-Play</i> .....	70
8.4.4	<i>Conclusions about Plug-and-Play</i> .....	70
8.5	SNMP AND MIB.....	70
8.5.1	<i>Overview of SNMP and MIB</i> .....	70
8.5.2	<i>Evolution of SNMP and MIB</i> .....	71
8.5.3	<i>Maturity of SNMP and MIB</i> .....	71
8.5.4	<i>Conclusions about SNMP and MIB</i> .....	71
8.6	WEB SERVICES .....	71
8.6.1	<i>Overview of Web Services</i> .....	71
8.6.2	<i>Evolution of Web Services</i> .....	72
8.6.3	<i>Maturity of Web Services</i> .....	72
8.6.4	<i>Conclusions about Web Services</i> .....	72
8.7	OVERALL CONCLUSIONS ABOUT ENGINEERING TOOLS .....	73
<b>9</b>	<b>SUMMARY OF CONCLUSIONS .....</b>	<b>74</b>
<b>10</b>	<b>CONCLUDING REMARKS; FURTHER WORK AND LINKS WITH OTHER WORK PACKAGES.....</b>	<b>79</b>
	<b>GLOSSARY .....</b>	<b>81</b>
	<b>REFERENCES .....</b>	<b>86</b>

## List of figures

Fig. 1 Merging of automation and office technology .....	10
Fig. 2 Wireless Automation Value Proposition (cf. [Inf05], p. 5) .....	11
Fig. 3 The wireless landscape (cf. [Boy05], p. 3) .....	12
Fig. 4 The RUNES technology roadmap for industrial control and automation (cf. [Kou et al 05], p. 6). .....	18
Fig. 5 Worldwide Current and Forecasted Commercial and Industrial-Grade Products (cf. [Tay04a], p. 5) .....	23
Fig. 6 Worldwide Current and Forecasted Industrial-Grade Products (cf. [Tay04a], p. 5).....	23
Fig. 7 Worldwide Wireless Infrastructure Product Purchases by Category, 2002-2009,(cf. [Kor05a]) .....	24
Fig. 8 Prediction on Industrial Ethernet growth .....	27
Fig. 9 Ethernet-based Real Time Architectures .....	30
Fig. 10 CIP Sync - IEEE 1588 Implementation for EtherNet/IP .....	33
Fig. 11 Needed loops within a closed loop motion control.....	34
Fig. 12 Boundary conditions for future automation security.....	46
Fig. 13 Large network provider routing entries evolution (Feb. 2005 - Jan. 2006) .....	51
Fig. 14 Architecture approaches .....	54
Fig. 15 Divulgence of VoIP and Broadband (Source: Forrester Research).....	59
Fig. 16 Worldwide distribution of the plesiochronous and synchronous technologies .....	62
Fig. 17. Illustration of the basic trend analysis purpose.....	79
Fig. 18 Interrelations of trend reports along VAN project.....	79

## List of tables

Tab. 1 A comparison of major wireless standards using the ISM band.....	14
Tab. 2 A comparison of major wireless protocols. ....	14
Tab. 3 Worldwide Shipment and Shipment Forecasts of the Wireline and Wireless Ethernet Infrastructure .....	22
Tab. 4. Overview on Ethernet-based real-time protocols.....	32
Tab. 5 Pros and cons for each architecture approach .....	54
Tab. 6 Trend / issues resume .....	78

# 1 Introduction

Present embedded technologies are continuously evolving to fulfill demands of the market. Many demands of, for example low cost, high throughput and high security, are usually in contradiction. It means that each technology is satisfactory in some features, parameters, but it is worse in others. However, possible future progress in research, development and manufacturing can rapidly increase their today's potential. Some improvements of technologies can lead to new fields of application.

One of the fastest evolution occurred in the area of wireless devices. Low cost and simple deployment of devices known as Wi-Fi, ZigBee and Bluetooth leads to significant consumer demand and consequently growth of the market with wireless devices. This process comes together with an intensive standardization procedure which incorporates, among others, quality of services (QoS), which strictly defines throughput and latency of a communication channel. Now, these standards can be adopted to meet industrial requirements for monitoring and control.

Improvements in the Ethernet physical layer, which reaches speeds of 100Gbps, offer less delay and jitter required by real-time processes in automation. In public networks, it can lead to wider spread of video and voice services. Increasing number of interconnected devices leads to wide spreading of the IPv6 protocol that overcomes addressing limitations of the IPv4 protocol.

Significant growth of wireless networks in the last years is significantly affected by low security. Today's trend is, among others, preventing unauthorized access to private resources by authentication and eavesdropping by strong cryptographical methods.

At present, a connection between private and public networks is ensured by gateways. To protect a private network against penetration from outside and vice-versa, gateways are equipped by security features such as firewalls, VPNs and e-mail filters.

In the office world, end-to-end security is ensured by security protocols that can be modified and adopted to fulfill industrial requirements. However, in this area, there are still many open issues in adaptation of these security concepts to embedded devices that have limited resources, i.e. memory and CPU power. Secure and trusted communication among automation devices and between these devices and their operators are goals addressed in the VAN project.

Nowadays, almost each industrial company, involved in automation, has incorporated its own safety concept, which meets international standards, into its fieldbus technology. The trend is incorporation of a safety mechanism into TCP/IP wired and wireless networks, which allows operation of safety-related devices over heterogeneous VAN structure.

In the last years, several data interfaces were developed to exchange and access data pertaining to automation devices and systems. Some interfaces can be used together with web services and thus operators have now powerful tools for remote supervising of devices and systems via public networks.

Previously mentioned aspects allow penetration of office technologies, which are based on the Ethernet, into the automation domain based on fieldbus systems (see Fig. 1). Merging both the domains allows "vertical integration" between office automation and process automation domains, encompassing both wired and wireless technologies, the Internet and telecommunications systems. This trend requires solving safety, security and real-time issues which is the scope of the VAN project.

Merging automation and office technologies allows devices to operate over a heterogeneous network. This network then allows centralized supervision of geographically distributed plants instead of today's local supervision of each plant separately. Such a central supervisory centre can be located anywhere in the VAN network.

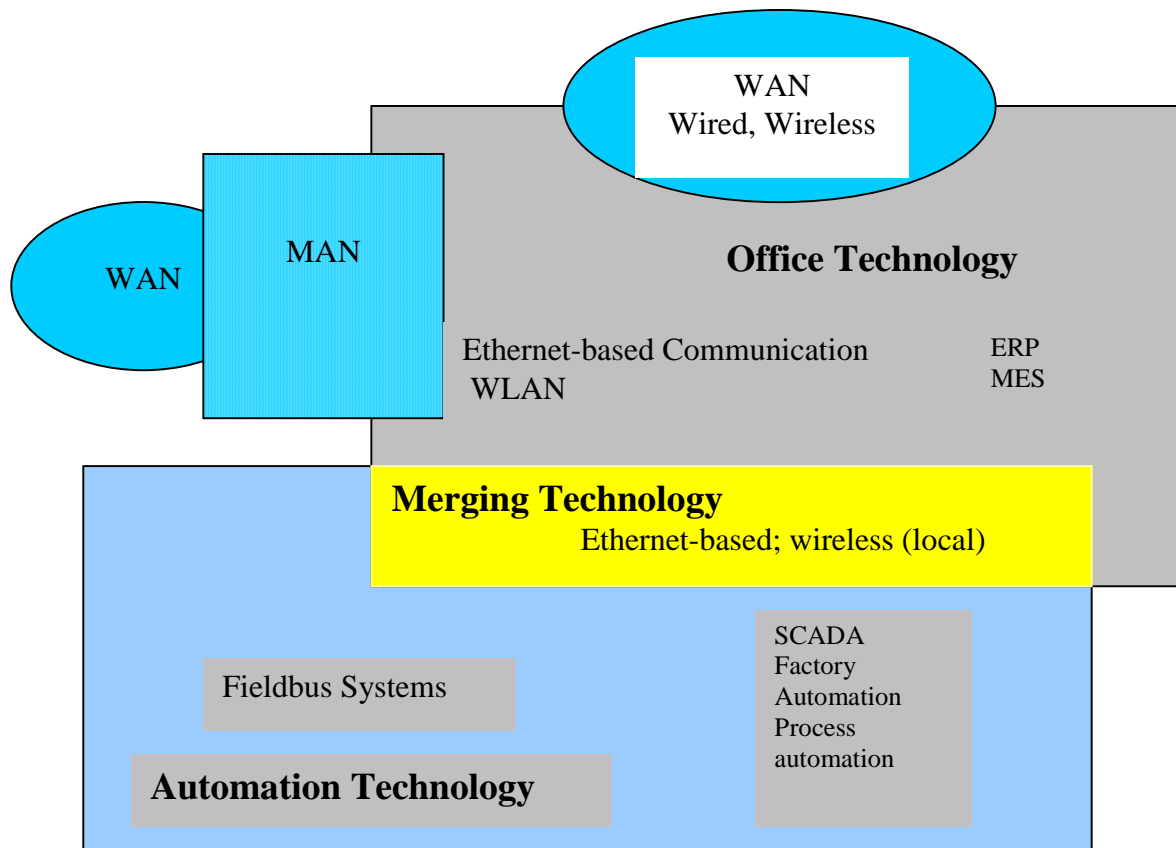


Fig. 1 Merging of automation and office technology

In the VAN architecture, mobile communications technologies like UMTS and wireless local area networks, which directly support QoS over TCP/IP protocol, will no longer be restricted to monitoring and data acquisition, but they will control embedded devices in a closed-loop mode.

To keep the goals of the VAN project up-to-date, these trends in relevant technologies are looked into. Special attention is given to wireless technologies that are not only investigated from technical, but also from market point of view. Consequently, each chapter covers overview, evolution and maturity of relevant technologies and solutions.

## 2 Trends in wireless technologies

The following two chapters address the evolution, maturity and forecasted future development of wireless technologies in the industrial environment. The 'Evolution' chapter is held short since history and status quo of wireless technologies have been described in Task 1.1 'State of the Art' and partly in Task 1.2 'Requirements and Roadmap'. Differences in wireless technologies are outlined. The 'Maturity' chapter lists the current pros and cons. The last chapter 'Conclusions' gives an overview about recent technological trends.

### 2.1 Overview

Among the most significant aspects of the on-going digital revolution is the introduction of a plethora of new wireless technologies that add mobility and flexibility to existing processes and solutions (cf. [Inf05], p. 2). This affords the opportunity for new ways of working and the emergence of totally new business models (cf. Fig. 2).

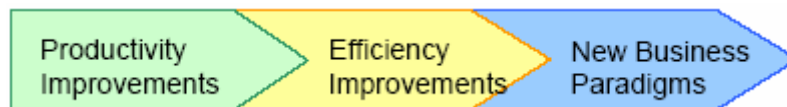


Fig. 2 Wireless Automation Value Proposition (cf. [Inf05], p. 5)

Wireless automation solutions are often adopted initially to solve specific business issues, e. g. (cf. [Inf05], p. 5):

- to remotely monitor the functioning of a machine and either prevent breakdown or enable rapid repair to take place in the event of failure
- to schedule deliveries to meet just-in-time requirements, or
- to measure and monitor flows to ensure smooth functioning
- to track valuable goods and equipment.
- to control cranes/hoists

The U. S. Department of Energy sponsored in 2002 an Industrial Wireless Workshop. Three key industrial wireless markets were identified according to their typical distance requirements (from shortest to longest): factory automation, process automation, and supervisory control and data acquisition (SCADA) or telemetry. The final report describes the status quo in 2002 like "most of the industrial applications currently in use perform monitoring rather than control due to remaining security and performance issues" (cf. [Ene02], p. 5). Regarding the results of a recent VDC survey, security and reliability are still big issues for the expected acceptance of wireless technologies in true control applications (cf. [Tay05a], p. 7).

## 2.2 Evolution

### 2.2.1 General

In the opinion of Merritt (cf. [Mer05]) the biggest issue in wireless appears to be the lack of a universal standard. Three groups are working on it: WINA (Wireless Industrial Networking Alliance), ISA-

SP100<sup>2</sup> (Instrumentation, Systems, and Automation Society) and ZigBee, a consortium of component-level OEMs. "Not having a single backbone slows down adoption," says Gene Chen product manager at Honeywell. "Several cases exist where customers spent resources to deploy wireless networks to support tablet PCs for operators, but found the network wouldn't support wireless sensors. Other customers had the opposite problem when they installed wireless sensors". Gene Chen further points out that Honeywell is an executive sponsor of the three main bodies mentioned above trying to define a wireless industrial standard. Gene Sierra, wireless marketing manager at Emerson Process Management, says that Emerson is working with HART and ISA (cf. [Mer05]).

According to VDC analyst Jake Millete, ZigBee looks promising, but vendors are sticking to their proprietary methods: "Many vendors feel ZigBee is an excellent solution for a variety of applications," notes Millete, "but for industrial applications where a robust network is essential, some develop their own mesh networks. We'll see many more ZigBee-based solutions in the industrial market as the standard matures." (cf. [Mer05]).

"The current landscape of existing wireless networking protocols and standards (cf. Fig. 3) overlay the bus network landscape", says Boyes (cf. [Boy05], pp. 3-4): "Here we have more axes: power consumption, cost and complexity vs. data transmission rate."

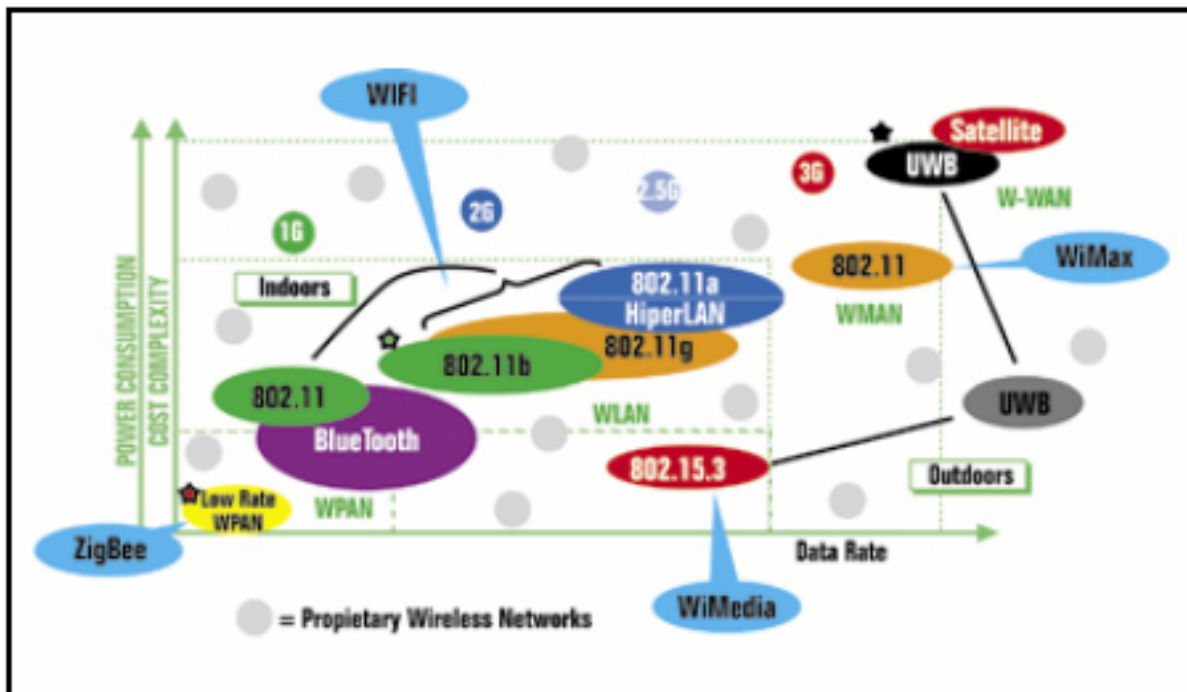


Fig. 3 The wireless landscape (cf. [Boy05], p. 3)

Unlike other industrial standards, the eventual industrial wireless one must achieve total interoperability with the existing IEEE series of wireless standards, including Wi-Fi, WiMax and others. That is going to be necessary because of the growing interpenetration of the plant-floor space and the enterprise, where the IEEE standards are ubiquitous (cf. [Boy05], pp. 3-4). This is one of the reasons why this document considers advances in wireless technologies for industrial as well as non-industrial applications. Another reason is that both commercial and industrial-grade Ethernet infrastructure components are used in industrial facilities. This is the result of a wireless market study conducted by VDC (cf. [Tay04a]).

<sup>2</sup> The task of the ISA-SP100 committee is to "create standards, recommended practices, and/or technical reports to define procedures for implementing wireless systems in the automation and control environment at the field level" (cf. [Ive05]).

## 2.2.2 Comparison of different wireless transmission technologies

The 'landscape' of requirements for wireless industrial networks is very similar in its diversity to the current landscape of different wireless standards and protocols. Koumpis et al (cf. [Kou et al 05]) describes the current situation as follows: "The information being communicated in industrial environments is typically state information and as such in normal operation it takes the form of recurring streams of small packets. At the same time, these packets are associated with harsh environments and critical tasks having strict timing requirements. The latter may include extreme temperatures, high humidity levels, intense vibrations, explosive atmospheres, corrosive chemicals and excessive electromagnetic noise. Thus, in general, the required data throughput of the network is relatively low, but its reliability needs to be very high. In industrial environments, apart from lower installation and maintenance costs, wireless connectivity offers ease of equipment upgrading and practical deployment of mobile robotic systems and micro-electromechanical systems (MEMS)."

According to different industrial requirements the existing wireless transmission technologies are complementary rather than competing to each other. They address different needs and have different strengths. Tab. 1 compares Bluetooth, ZigBee and Wi-Fi.

Andersson (cf. [And02], cited by [Kou et al 05], p. 2) characterizes Bluetooth and ZigBee as follows:

"Bluetooth requires a low-cost transceiver chip in each device to be connected. Each device has a unique 48-bit address and the transceiver transmits and receives in the ISM band. Connections can be point-to-point or multipoint with a range of 20-100m. Data can be exchanged at a rate of 1-3Mbps and a Frequency Hopping Spread Spectrum (FHSS) scheme allows devices to communicate even in areas with a great deal of electromagnetic interference. However, this makes it extremely difficult to create extended networks without large synchronization cost. Built-in encryption and simple verification is also provided by Bluetooth."

"ZigBee moves data only a quarter as fast as Bluetooth but can handle orders of magnitude more devices at once and has been optimized for low power consumption. This low power consumption is achieved by the Direct Sequence Spread Spectrum (DSSS) which allows devices to sleep without the requirement for close synchronization."

ARC analyst Harry Forbes (cf. [For05], p. 7) also addresses low power consumption as an advantage of ZigBee in comparison to Bluetooth and WLAN. This affords the use of battery-powered devices over several years without interruption. However data rate is low as well. Moreover ZigBee allows more nodes in the network than Bluetooth does. From Forbes' point of view one primary target market of ZigBee is building automation not industrial automation. In industrial automation, Bluetooth and WLAN are more common.

Pacelle (cf. [Str05]), Vice President of Marketing for Millennial Net, considers low power consumption as the first important enabling factor for wireless networks: "Low power consumption enables mesh networks to be powered by small batteries that last years at a time. This enables quick, low-cost, pervasive deployment of sensor nodes throughout a target area – one of the important attributes of sensor networks. A low power profile is particularly critical in an industrial environment. In one industrial monitoring application currently in field trial, our customer is using solar energy to trickle charge the mesh node for continuous, maintenance free operation. This would not be possible without a power-efficient network protocol. A second related factor is the scalability of the network. Again, pervasive deployment drives the creation of BIG networks. Network nodes need to be added, removed or replaced as needed to meet the changing control requirements of a space or building. The mesh technology enables this by creating multiple node interconnections throughout the network. This creates redundant network paths and with dynamic routing, the network becomes more robust with each additional node."

Andersson and Forbes are mentioning a further wireless technology namely UWB (Ultra-Wideband). UWB broadcasts simultaneously on a very large frequency range at low power. The idea is that the signal is spread so thinly that interference will be negligible in any given frequency. UWB is expected to be able to deliver high throughput, particularly in areas with physical obstacles (cf. [And02], cited by [Kou et al 05], p. 2). UWB has been approved recently by the US regulatory authority Federal Communications Commission (FCC). UWB enables radio communication with high data rates over

short distances. But the use of this technology in Europe does not have big relevance at the moment, so Forbes. It targets the electronic consumer goods market (cf. [For05], p. 7).

Standard (market name) <sup>2</sup>	802.15.1 (Bluetooth)	802.11b (Wi-Fi)	802.15.4 (ZigBee)
Application focus	Cable replacement	Web, email, video	Control & monitoring
Bandwidth (Kbps)	1000-3000	11000	20-250
Transmission range (m)	20 (Class 2) 100+ (Class 1)	100+	20-70, 100+ (ext amplifier)
Nodes supported	7	32	2 <sup>64</sup>
Battery life (days)	1-7	.5-5	100-1000+
Power consumption (transmitting)	45mA (Class 2) <150mA (Class 1)	300 mA	30 mA
Suitability for low duty-cycle applications	Poor (Slow connection time)	Poor (Slow connection time)	Good
Spread spectrum technology	FHSS	DSSS	DSSS
Memory footprint (KB)	50+	70+	40
Success metrics	Cost, convenience	Speed, flexibility	Power, cost

Tab. 1 A comparison of major wireless standards using the ISM band<sup>3</sup> (cf. [Kou et al 05], p. 2).

Tab. 2 offers another comparison of different wireless protocols including IEEE 802.11b, Bluetooth and ZigBee. According to the table above and the comment of Rammig (cf. [Ram05], p. 5) a range of 70-300m for ZigBee seems to be a bit too optimistic:

Feature	IEEE 802.11b	Bluetooth	ZigBee
Power Profile	Hours	Days	Years
Complexity	Very complex	Complex	Simple
Nodes/Master	32	7	64000
Latency	Enumeration up to 3 sec.	Enumeration up to 10 sec.	Enumeration 30ms
Range	100m	10m	70-300m
Extensibility	Roaming possible	No	Yes
Data Rate	11Mbps	1Mbps	250Kbps
Security	Authentication Service Set ID (SSID)	64 bit, 128 bit	128 bit AES and Application Layer user defined

Tab. 2 A comparison of major wireless protocols (cf. [Hei04], cited by [Ram05], p. 5).

<sup>3</sup> The IEEE 802 standards typically create the specifications at the physical layer and portions of the data link layer. The higher layer protocols are left to the industry and the individual applications. Hence the standard and market names are not always interchangeable.

## 2.3 Maturity

### 2.3.1 General

Although the IEEE 802.11 standards continue to gain in share, proprietary protocols operating the 900 MHz band maintained the largest share of North American shipments in 2004. Proprietary networks are often preferred in industrial applications where there is need for longer transmission distances and bandwidth requirements are not high (cf. [Tay05b]). According to the VDC worldwide wireless survey in 2004 the IEEE 802.11b standard had the largest share of usage in industrial facilities but the IEEE 802.11g standard is expected to be used by about 75% of the respondents in the near future (cf. [Tay04a], p. 11).

The development of the IEEE 802.15.4 and ZigBee standards is helping to expand the use of mesh networking in industrial monitoring and control applications. These standards meet the need for low complexity, low cost, low power consumption and low data rate wireless networks (cf. [Tay05b]). Although ZigBee-ready products were available in 2004, the standard is very new. The ZigBee specification was finalised in December 2004, and the first 'official' ZigBee-compliant products were shipped in April 2005 (cf. [Tay05a], p. 4).

Specific requirements of wireless networks are largely application specific. Material handling equipment and tank level monitoring and control held the largest shares of overall shipments (cf. [Tay05b]).

ARC senior analyst Harry Forbes about the maturity of wireless transmission technologies in industrial applications (cf. [For05], pp. 6-7):

- Forbes points out that the maturity of different wireless technologies for industrial applications is not at the same level: WLANs, for example, belong today to the established technologies with enormous growth rates, whereas the new Personal Area Networks, the different Metropolitan Area Networks and WiMax are still at the beginning of their development. The mentioned technologies differ from each other regarding application area, data rate, power consumption of devices and the used RF-modulation. All technologies have in common that they advance at a great speed.
- He does not see a 'killer application' that could push wireless technologies enormously. In his opinion it does not make sense to talk about one 'must have' requirement because of the diversity of wireless technology. One important application area is definitely to provide plant information. One unbeatable advantage of a wireless infrastructure is that production data is available always and everywhere, so Forbes.

In view of the large quantity of publications 'Wireless' is hype. However, every new technology comes with several advantages and disadvantages. The following two sections give a short overview about the most mentioned pro and con arguments in publications:

### 2.3.2 Strengths

#### *Wireless Networks*

The strengths of wireless networks include (cf. [Tay04a], p. 3):

- Easier maintenance – Wireless networks can allow more efficient maintenance and repair, thereby lowering maintenance costs and downtime;
- Enables mobile applications – For example, portable operator interfaces having wireless monitoring and control capabilities. This allows operators, engineers, maintenance personnel, and others to interface with equipment without having to be in fixed locations;
- Lower cost components – Extensive and growing use of wireless Ethernet or Wi-Fi in high-volume commercial and consumer markets is leading to inexpensive components compared to those of other wireless networks;
- Lowers cost of wireline – Wireless networks negate the cost of the wire previously needed to connect devices and controllers. Wireless solutions allow networks to be established over distances or in applications where the price of cable might have been prohibitive, and

- Offers more flexibility – Wireless solutions offer greater flexibility for ease of change-outs and expansion. This is especially valuable in applications where change-outs and/or expansions are frequent and expensive.

From the users point of view the following reasons motivate to use wireless Ethernet networks in industrial facilities. Rankings are based on user responses in the VDC worldwide wireless survey (cf. [Tay04a], p. 10):

1. Need for Mobile Applications
2. Flexibility/Ease of Expansion/Relocation
3. Provides Long Distance/Remote Coverage
4. Easy/Fast Installations
5. Low Cost Installations
6. Need where Installing Wireline Would Not Be Possible, or Very Costly

### **ZigBee**

In a recent WebForum organized by ARC the suitability of ZigBee for industrial applications was discussed (cf. [ARC05]). The advantages that came up are:

- ZigBee Alliance moves deliberately
- ZigBee is a full device interoperability framework
  - Allows "private" application profiles
- ZigBee development methodology from IEEE 802
- Well planned, controlled access to technology

### **Mesh Networks**

Mesh Networks and their advantage for industrial monitoring and control applications are also discussed very often relating to wireless technologies. Pacelle, VP of Marketing for Millennial Net, gives the following reasons (cf. [Str05]):

"Mesh networks offer a very cost-effective approach to deploying a sensor network. The technology is easy to install and manage. Mesh networks automatically adjust to network topology changes. Nodes can be added, removed, replaced or relocated without the need for traditional network administration. Mesh networks can optimize or increase the visibility into dynamic systems, such as the environmental conditions inside a commercial building or the condition of machinery in a manufacturing plant, without the cost and administration of a wired network."

### **2.3.3 Weaknesses**

In the VDC worldwide wireless survey (cf. [Tay04a], p. 10), high reliability and high security are indicated as the most important motivations for the usage of wireline networks. The advantages of wireline networks are at the same time the biggest hurdles for wireless control applications. In order to gain greater acceptance by users, solutions for interference and security problems need to be addressed by future developments of wireless technologies.

#### **IEEE 802.11 standard**

Suppan (ComConsult Research) (cf. [Sup06], p. 2) discusses some of the shortcomings of the IEEE 802.11 standard that may lead to lower future investments in this technology.

- Weaknesses in the standard, particularly the procedure for media access and the reduction to 3 non-overlapping 2.4GHz channels. The procedure DCF for media access not only uses half of the

available bandwidth, it can also collapse if there are too many stations per cell. The reduction to a maximum of 3 non-overlapping channels means that an area-wide design without interference is practically impossible. Usually a partial disruption in individual cells through intensive use of an area has to be expected.

- The available antennas purpose-built for the 802.11g standard have a big disadvantage: They strongly radiate into the neighbouring channels and destroy the advantages obtained by the OFDM coding.
- The usage of the 2.4 GHz band leads to incalculable interferences with other wireless networks/products. For the future, operation reliability is in question because this license-exempt frequency band is increasingly overcrowded with only three available channels.
- Neither IEEE 801.11b nor 11g are backbone-technologies; they are not more than client technologies. In particular, the maximum transmission power is usually insufficient to cover greater distances in stable conditions.

### **ZigBee**

In the ARC WebForum mentioned above the following weaknesses of ZigBee were identified (cf. [ARC05]):

- Not frequency-agile (no provision for channel-swapping)
- Optimized for low BOM cost devices (and for BAS applications)
  - Does not define "nice-to-haves" of more expensive devices
    - Network Coordinator redundant backup
    - Transport layer
    - Over-the-air software update
- Expects routers to be powered 100% of the time (mains power)
- Optimized for run-time interoperability, not software portability
  - No API defined – can't easily switch development tools

## **2.4 Conclusions**

### **2.4.1 Wireless in Industrial Environments**

Pacelle (VP of Marketing for Millennial Net) (cf. [Str05]) expects growth for wireless networks, no contrary views found in publications: "The trend we are seeing is growth – each network deployed is larger than the last, with networks on the order of hundreds of nodes. There is a definite increase in the number and size of wireless networks being deployed. A few years ago we were mostly selling evaluation kits and now we are deploying high-end, highly scalable networks in several markets."

In his opinion, wireless will have a significant influence on the controls industry over the next years: "Today, industrial plant managers are coming under increasing competitive pressure to improve plant efficiency by even 2-3 percent. Wireless sensor networking is a technology that will play a pivotal role in this effort. Mesh networking has fundamentally changed the economics of deploying monitoring and control networks allowing opportunities for improved operational decision-making, process optimization and predictive maintenance. In building automation, wireless sensor networking is being utilized in applications such as building environmental monitoring, hotel guest room control and energy services which characterize an important trend towards improved control over building services and cost savings to the building owners (cf. [Str05])."

### **Technology Roadmap**

The technology roadmap for industrial control and automation shown in Fig. 4 was developed by the RUNES project. This project funded by the European Commission (contract IST-004536) has a vision to enable the creation of large-scale, widely distributed, heterogeneous networked embedded systems that interoperate and adapt to their environments (cf. <http://www.ist-runes.org/>).

The project part working on "Wireless Industrial Control and Monitoring beyond Cable Replacement" describes the development of wireless technologies as follows:

"The use of wireless systems for industrial applications is in its infancy. The adoption period is expected to be longer than other sectors (building automation and control, medical care, disaster response and automatic meter reading) reviewed in the RUNES technology roadmaps as end-users migrate incrementally from wire to wireless. Companies dealing with automotive, food processing, petrochemical and asset tracking applications were identified as the early adopters. A clear difference in the adoption time scales between wireless in control and monitoring was revealed. While technologies are maturing, wireless will not be used for critical control applications. Monitoring in hazardous and inaccessible areas will be given priority in the short/medium term and in moving towards this some lessons can be learnt from successful automatic meter reading deployments. Many wireless systems on the market today do not meet local/national regulations, because they transmit too much power or operate in frequencies that are not approved for unlicensed use. Therefore, it is important to determine whether or not the radio subsystems can be programmed to meet these regulations. Since 2003 the ATEX directive has become mandatory for all electrical and mechanical equipment used in potentially explosive atmospheres and any new networked embedded components will need to comply with it" (cf. [Kou et al 05], p. 6).

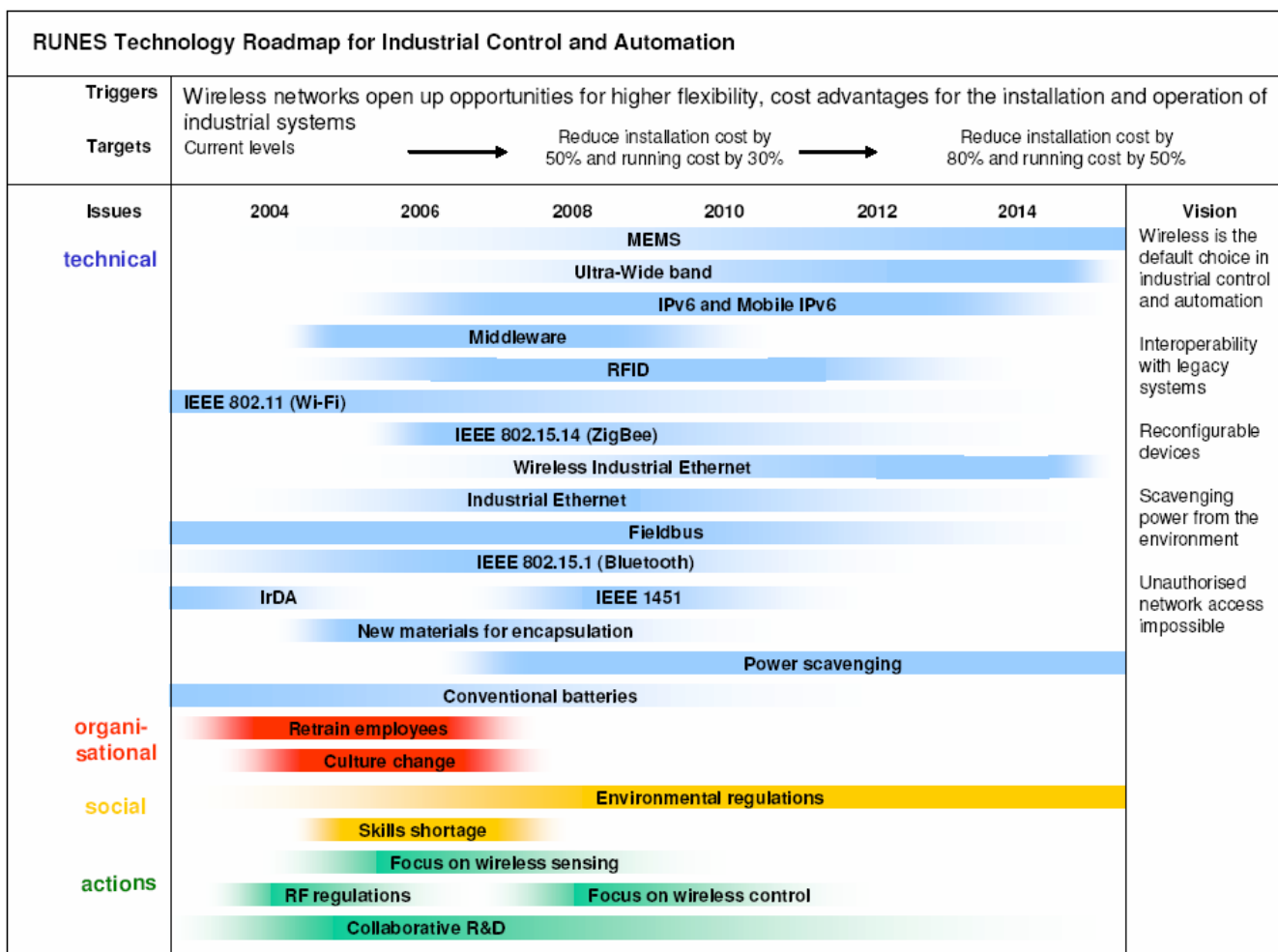


Fig. 4 The RUNES technology roadmap for industrial control and automation in graphical form (cf. [Kou et al 05], p. 6).

### **Protocol Usage**

Among the wireless Ethernet users, HTML (HyperText Markup Language) was by the VDC worldwide market study most identified as a protocol being used. It is also expected to be used by the largest number in 2006, although by few. Significantly more of the user respondents expect to be using the XML (Extensible Markup Language) protocol in 2006 than in 2003 (cf. [Tay04a], p. 11).

In the opinion of IEEE, wireless technologies can bring many benefits to industrial applications, one of them being the ability to reduce machine setup times by avoiding cabling. "The market offers mature wireless solutions, such as the IEEE 802.11 standard, the IEEE 802.15.4 standard, or Bluetooth. So far, however, wireless technologies have not gained widespread acceptance on the factory floor. One reason for this lack of acceptance is the difficulty in achieving the timely and successful transmission of packets over error-prone wireless channels. With the design of suitable protocol mechanisms and transmission schemes, along with the careful combination of these schemes, important steps towards increasing the acceptance of wireless technologies for industrial applications can be made" (cf. [Wil et al 05], pp. 38-39).

"The approach based on 'hardening' the protocol stack can benefit from relaxing user requirements and making applications more tolerant against errors. In fact, a key observation from the field of wireless sensor networks is that the joint design of applications (here: controllers) and the networking stack, along with careful cross-layer design within the networking stack itself, is more likely to give better results than designing each element in isolation" (cf. [Wil et al 05], pp. 38-39).

### **Wireless Sensors**

Merritt (cf. [Mer05]) identifies 'power' as a big issue that has to be solved: "Wireless device-level network and sensors have yet to take off due to limitations of battery technology and lack of standardization," says Jonas Berge, marketing manager at Smar. "Unlike wireless consumer devices such as mobile phones or PDAs, sensors can't have their batteries charged or changed every week. Conserving battery power is therefore very important." Because of the power problem, wireless sensors often transmit less often than wired sensors, and at slower speeds. "As a result, wireless sensors are not suitable for control or functional safety," says Berge.

Merritt (cf. [Mer05]) is going on: "Slow response also happens when too much wireless traffic occurs nearby, so the sensor has to wait for the frequency to clear to transmit. No one wants to base a real-time control decision on inputs from a wireless sensor. For the immediate future, it appears that wireless will be limited to monitoring."

Hesh Kagan, director of new technology marketing at Invensys Process Systems, says motes (wireless nodes) and mesh networks are coming: "At the low end, wireless sensors use mesh networking with auto-adaptive, self-healing capabilities," says Kagan. "Companies such as Millennial Net and Ember are driving standards-based end nodes, radios on a chip, mesh-networking software, gateways and development environments." (cf. [Mer05]).

Kagan sees tremendous opportunities for wireless sensors in process applications. "Most process plants today take measurements at only about 10% of the possible points. But if the attachment and sensor costs were low enough, as mote technology promises, you could measure at many more points, giving you a much richer process model with which to work." (cf. [Mer05])

### **Proposed Research Focus**

Willig et al [Wil et al 05] identifies the following research opportunities in the fields of wireless field bus systems and wireless industrial communications: "One opportunity involves the search for new protocol mechanisms to improve real-time capabilities. A key component in the design and evaluation of such mechanisms is the formulation of appropriate performance measures, benchmark applications, and wireless channel models that have been adapted to industrial environments. Another opportunity involves the assessment of the many emerging wireless technologies (Ultra-wideband, MIMO techniques, smart antennas, wireless ad hoc and sensor networks) from both a technological and a market perspective in terms of their potential use in industrial applications. Yet another research opportunity concerns a trend in field bus systems to carry multimedia and TCP traffic in addition to control traffic. As a consequence, there is a need for wireless-adapted protocol support for these data types, which would not degrade the quality of service rendered to the control

traffic. From a practical perspective, plant engineers need software tools for planning, configuration, and maintenance of wireless industrial networks. One component of such a software suite would need to determine the placement of wireless stations and coupling devices. An optimization goal might be to minimize the installation costs while satisfying the real-time requirements of individual stations." (cf. [Wil et al 05], pp. 38-39).

## 2.4.2 Wireless in Non-Industrial Environments

For the non-industrial wireless market, the forecasts are similar: Wireless belongs to one of the growing technologies in the future, says BCC Research in its recently published worldwide wireless infrastructure study:

"Wireless LANs are seeing growth on two fronts: Increasingly, corporations are installing these devices on their premises to make it simpler for users to access networks and transmit data/voice information. In addition, consumers are moving to digital households where a variety of consumer devices are connected, and they need wireless LANs for these links. As users become more mobile, they need devices to help them access corporate and home networks. The variety of mobile devices has been expanding from notebook computers to personal digital assistants, and now to smart phones. The result is that sales of these products are increasing. Carriers need software to support their wireless services. Increasingly, they are purchasing billing, customer care, security, and network management systems" (cf. [Kor05b], p. 5).

A wide discussion is taking place about the IEEE 802.11n standard. Several manufacturers have built the Enhanced Wireless Consortium (current members are Apple, Atheros, Broadcom, Buffalo, Cisco Systems, Conexant, D-Link, Gateway, Intel Corporation, Lenovo, Linksys, NETGEAR, SANYO, Sony, Symbol Technologies, Toshiba, USRobotics, WildPackets). The objective is to create a pre-standard to IEEE 802.11n for the consumer market (cf. [CoC05]).

ComConsult (cf. [CoC05]) outlines the impact of IEEE 802.11n on the wireless market as follows:

"IEEE 802.11 will significantly change the wireless market and will remain for a couple of years the wireless standard commonly used. All current wireless standards like 802.11 a, b, and g will lose importance in the next years and will disappear from the market with the exception of some special cases. After adoption of 11n, further developments will address the use of the full bandwidth of 600 Mbit/s. However for a period of three to four years I expect the coexistence of new 11n devices and a significant high number of devices with 11b or 11g interfaces, which has to be integrated.

The consumer market will be the pioneer. The reason is a high demand for high bandwidths and range for multimedia applications in households (wireless HDTV is here the driver). If manufacturer in the consumer market like D-Link, Linksys, Netgear come out with 11n products in high units this might be the end for 11b and g. Furthermore the participation of Broadcom and Intel might push the change in the notebook market. Higher prices at the beginning are expected to drop to the current level very fast.

For many companies the adoption of IEEE 802.11n will be inevitably followed by an adoption of the 5 GHz band. It is difficult to predict the future development of IEEE 802.11n because this technology is very new.

Suppan (also ComConsult Research) makes the following prognosis about IEEE 802.11n (cf. [Sup06], p. 3):

"I am convinced that the IEEE 802.11n hype is coming up in 2006. Manufacturers has completed the change to the 5 GHz band, at least there are a sufficient wide range of products (e. g. from Lancom).

According to the current developments, the time-to-market for WiMax-Client-products with the 802.16e standard will be too long. From the technological point of view these products will outmatch present wireless products but they will meet a saturated client market and remain more expensive. In the provider market big geographic differences in the acceptance of WiMax are expected. Especially in countries where large areas with a low population density exist, the costs for WiMax are not beatable."

## 3 Market approach in wireless technologies

This chapter gives an overview about wireless technologies from the business perspective. Main sources for market size and growth forecasts are market studies recently conducted by market research institutes like VDC and ARC. Considering the efforts towards integration of office and industrial networks, results from non-industrial wireless market studies have also been analysed and included.

### 3.1 Status Quo

"Although some users are wary of wireless, it has taken center stage in the industrial networking theater", says Merritt (cf. [Mer05]). Sales are still at entry levels for a new technology (about \$75 million in 2003), but market researchers predict good times ahead.

Due to ARC senior analyst Harry Forbes (cf. [For05], pp. 6-7) "cost savings due to cable replacement are the highest in process automation. In factory automation the applications are at the very beginning. But a wireless infrastructure is much more than a simple networking system without cable. Its primary advantage is not that it replaces cable but that it makes manufacturing processes better, faster and more precise."

#### 3.1.1 Key Industries

As in the worldwide industrial wireless market study, published by VDC, the worldwide largest 2003 consuming markets for the wireless Ethernet products were the ranked below. They accounted for about 66% of total worldwide shipments (cf. [Tay04a], pp. 6-7).

1. Oil & Gas
2. Water/Waste Water Utilities
3. Electric Power
4. Oil Refining & Petrochemical
5. Automotive

The five largest consuming North American industries for the wireless monitoring & control products in the recently published industrial wireless market study, spec. for the North American market, were (cf. [Tay05a], p. 6):

1. Oil & gas
2. Primary metals
3. Automotive
4. Water/Wastewater
5. Chemical/petrochemical

Pacelle (VP of Marketing for Millennial Net) (cf. [Str05]) considers that the main markets are building automation, industrial process control, and medical systems: "These are markets that have a strong inclination for an ever-increasing amount of sensor data. Wireless offers a cost-effective option for augmenting a wired network or creating a mobile sensor network. Wireless is also used in a variety of other markets, including agriculture, security, and precision instrumentation."

There are three primary markets for ZigBee: residential, commercial, and industrial automation, where the technology can be used to replace proprietary single-source solutions. Sensor systems for

controlling utility systems have become ZigBee's main applications. Products for such purposes are expected to dominate maker releases in the next 12 months (cf. [Glo05]).

### 3.1.2 Geographic Markets

Markets in the Americas (North, Central and South America) accounted for about 42% in the worldwide shipments of the **wireline** Ethernet infrastructure products under study for industrial applications in 2003. EMEA (Europe, Middle East and Africa) accounted for almost 40%. The Asia-Pacific region accounted for about 17%, with countries in the rest of the world accounting for the remainder (cf. [Tay04a], p. 6).

In the **wireless** Ethernet infrastructure products, the Americas 2003 market share was much higher at about 66%, with EMEA having about a 22% share, the Asia-Pacific region about 11%, and again with the remainder to countries in the rest of the world (cf. [Tay04a], p. 6).

## 3.2 World Market Forecast

### 3.2.1 Industrial Wireless Market

Worldwide shipments of **wireline** Ethernet infrastructure components and network software for use in industrial facilities totalled \$879.5 million in 2003. Shipments of these are forecasted to grow at a compound annual growth rate (CAGR) of 22.0%, reaching \$1,596.3 million in 2006 (cf. Tab. 3) (cf. [Tay04b]).

Worldwide shipments of **wireless** Ethernet infrastructure components and network software for use in industrial facilities totalled \$75.1 million in 2003. Shipments of these are forecasted to grow at a compound annual growth rate of 34.7%, reaching \$183.4 million in 2006 (cf. Tab. 3) (cf. [Tay04b]).

	Base Year	Forecast			CAGR
	<u>2003</u>	<u>2004</u>	<u>2005</u>	<u>2006</u>	<u>2003-2006</u>
For Wireline Networks	879.5	1070.5	1305.7	1596.3	22.0%
For Wireless Networks	75.1	100.9	136.0	183.4	34.7%

Tab. 3 Worldwide Shipment and Shipment Forecasts, For Use in Industrial Facilities, of the Wireline and Wireless Ethernet Infrastructure Components and Network Software (Dollar in Millions) (cf. [Tay04a])

Both commercial and industrial-grade Ethernet infrastructure components are used in industrial facilities. For all the component types under study<sup>4</sup>, there are expected shifts toward greater use of industrial-grade products as Ethernet becomes more popular in industrial facilities, and as vendors offer more products designed for this market (cf. [Tay04a], p. 5).

Fig. 5 and Fig. 6 show the overall trends expected between commercial and industrial-grade product shipments of access point/networking components for the markets under study:

<sup>4</sup> Range of wireless products under study: Access Point/Networking components, Bridges, hubs, modems, transceivers, Console/Device servers, Distributed/remote I/O, Gateways (protocol converters), Repeaters, Routers, Switches, and network analysis and management software (cf. [Tay04a], p. 2).

### Wireline Networking Components

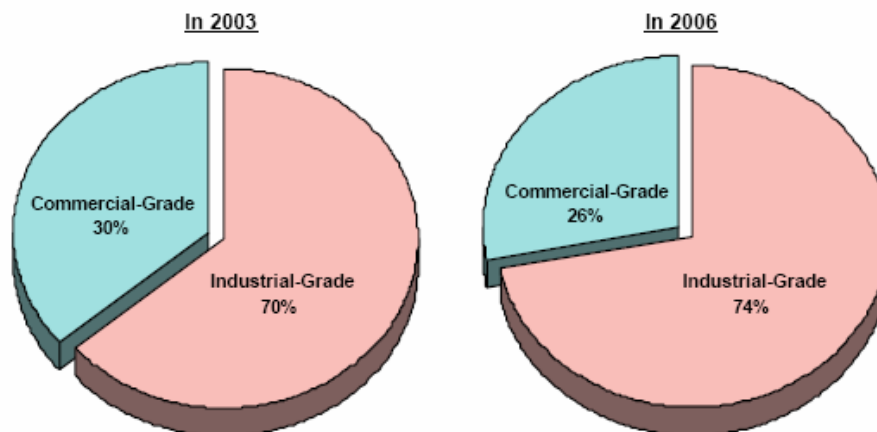


Fig. 5 Worldwide Current and Forecasted Shipment Shares of Wireline Ethernet Networking Component Shipments Segmented Between Commercial and Industrial-Grade Products (cf. [Tay04a], p. 5)

### Wireless Access Point/Networking Components

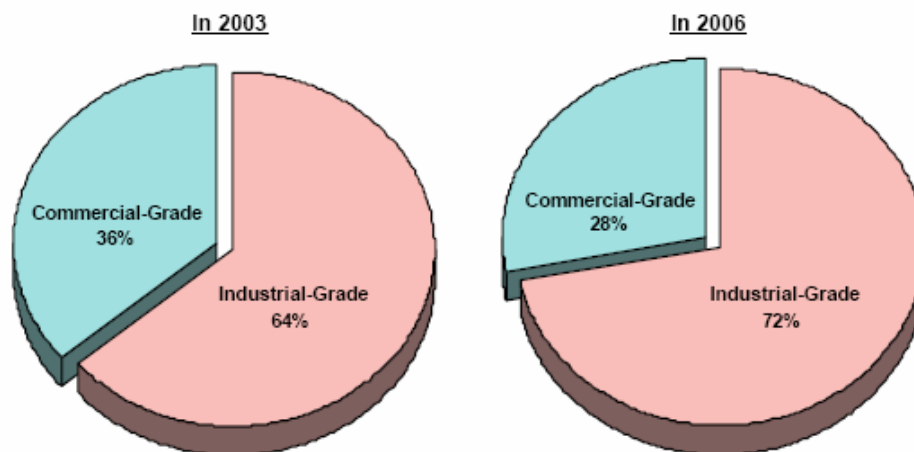


Fig. 6 Worldwide Current and Forecasted Shipment Shares of Wireless Ethernet Infrastructure Access Point/Networking Component Shipments Segmented Between Commercial and Industrial-Grade Products (cf. [Tay04a], p. 5)

Taylor (cf. [Tay04a], pp. 5-6) notes that there are large differences between the market shares in commercial versus industrial-grade shipments for the individual product categories: "For example in 2003, worldwide shipments of wireline Ethernet console servers for industrial use was about 95% of commercial-grade products, versus only about 9% for Ethernet distributed/remote I/O products. Reasons for the considerable differences involve the location of the product types (on the plant floor, in an office, or enclosed in a cabinet, for example) and the number of vendors offering industrial-grade products."

Frost & Sullivan projects that wireless sales will quadruple by 2006. A recent IDG. World Expo report goes even further, predicting that the wireless sensing technologies market (including sensors) will be greater than \$10 billion by 2010 (cf. [Mer05]).

### 3.2.2 Non-Industrial Wireless Market

Korzeniowski from BCC Research (cf. [Kor05a]) forecasts for the non-industrial wireless market:

- Worldwide wireless infrastructure expenditure currently is estimated at \$177.5 billion for 2004. Expected to expand at an AAGR (average annual growth rate) of 2.5%, this market will reach \$201.4 billion by 2009 (cf. Fig. 7).

- The two largest segments in the market are WAN hardware and end-user devices. WAN hardware will see an AAGR of 1.8% as carriers move to 3G technology and start to ship more video transmissions over their networks. End-user devices account for more than half the revenue generated and represent an area of intense innovation.
- The fastest growing segment is WLANs that just now are entering the rapid ramp-up phase, a trend underscored by growing interest in home networking.

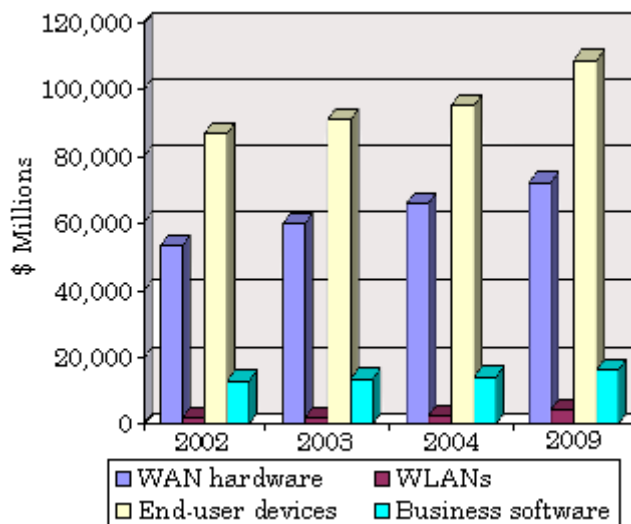


Fig. 7 Worldwide Wireless Infrastructure Product Purchases by Category, 2002-2009, (\$ Millions) (cf. [Kor05a])

Datamonitor (cf. [Dat06]) has recently published a wireless market study addressing trends in the enterprise market. The report highlights are:

“The enterprise WLAN market is now moving away from trial implementation stage and towards campus-wide coverage. To facilitate this move, centralized management of WLAN solutions is set to become increasingly commonplace over the next three years, which will in turn drive the potential of voice over WLAN services.

Enterprise WLAN infrastructure revenues will grow from \$890 million in 2004 to almost \$1.4 billion in 2008. Access points accounted for around 59% of equipment revenues in 2004, although a combination of falling prices and increased spend on wireless switches will dilute the importance of these devices in revenue terms. North America will remain the largest market with regard to WLAN spending, with enterprises in the region investing over \$500 million in related equipment in 2008.

Increasing complexity and scope are driving the need for more centralized management of WLAN solutions. As a result, revenues relating to wireless switches/appliances are set to grow rapidly over the next three years.”

### 3.3 Geographic Market Forecast

The key findings of the VDC worldwide industrial wireless survey concerning the adoption of wireless technologies in different regions are (cf. [Tay04a], p. 6):

“The highest regional market growth rate for the **wireline** Ethernet infrastructure products is expected for the Asia-Pacific region. This will be due to the regions overall high growth rate for manufacturing (specifically in China and India), the increasing level of automation, the specification of Ethernet in new plants, and the retrofitting of old plants.

The highest regional market growth rate for the **wireless** Ethernet infrastructure products is forecasted for the EMEA region. Although Europe has adapted wireless industrial facility networking more slowly than North America, the regions’ wireline Ethernet markets for industrial applications are

similarly sized, suggesting the EMEA region's implementation of wireless Ethernet will catch up, although not during the forecast period."

VDC forecasts shipments of RF/microwave wireless products for industrial monitoring and control applications to markets in North America to increase from \$154.1 million in 2004, at a compound annual rate (CAGR) of 39.6%, reaching \$419.3 million in 2007 (cf. [Tay05a], p. 2).

In the opinion of VDC, factors contributing to this robust growth rate include:

- General growth in the awareness of the benefits provided by the use of wireless technology
- Lower installation and maintenance costs versus wired networks
- Increased use of Ethernet and distributed networking in industrial automation; and
- New wireless standards, such as ZigBee, able to meet industrial users' specific needs.

### 3.4 Key Industries Forecast

The forecasted fastest growing worldwide industry market segments, in ranked order are (cf. [Tay04a], pp. 6-7):

1. Semiconductor and Pharmaceutical
2. Pulp & Paper
3. Mining

The industries in North America forecasted to have the largest growth in total dollar volume, in order, are (cf. [Tay05a], p. 6):

1. Oil & gas
2. Water/Wastewater
3. Chemical/petrochemical
4. Electric Power
5. Automotive

### 3.5 Product Forecast

ARC analyst Harry Forbes (cf. [For05], p. 7) expects that the product range for wireless devices for use in industry will expand in the next years. First devices are available. Suppliers for the automation industry, small and big ones, do tremendous research & development work in the field of wireless.

"Many big vendors are jumping on the wireless wagon. The HART Communication Foundation is adding wireless capability to its HART devices, and all the major control vendors are keeping an eye on what wireless is going to mean to process control and automation", says Merritt (cf. [Mer05]). Venture Development reports that mesh networks will grow from a miniscule \$6 million in 2004 to \$25 million in 2007, a growth rate of 60%.

VDC forecasts the development of different product categories will be the following [Tay05a], pp. 2-3):

**“Network Products:** The market segment for network products was the largest in 2004 and is expected to remain the largest in 2007. Wireless modems account for the largest share of shipments of these. However, higher market growth rates are forecasted for wireless I/O devices, repeaters, and network access points. Connection of devices (actuators, sensors, etc.) through I/O devices with the multiplexing of signals over networks typically provides cost effective solutions. Wireless access points allow tapping into wired LANs increasingly being utilized in industrial automation, to give good coverage for mobile and other applications. Repeaters also provide the capability for broader and better coverage.

**On-Site Operator Interface Terminals:** This was the third largest product market segment in 2004, but is forecast to become the second largest in 2007. The largest application for these is expected to

be in mobile controller maintenance usage. These enable personnel to monitor and interact with equipment without having to be in a fixed location. This makes more efficient use of the time of personnel, leads to quicker fixes or adjustments, and thus higher productivity, and profitability, and can reduce the number of needed employees. The most popular form factors for these terminals are handheld and notebook computers.

**Off-Site Portable Operator Interface Terminals:** This small market segment is forecast to reach only \$10 million in 2007. The primary products used are notebook computers, handheld computers, and PDAs. This segment is small because most off-site monitoring and control is dominated by use of the Internet, as it is cheaper medium relative to using wireless WANs, and for most applications there will be no need for wireless data connectivity with mobile terminals.

**Remote Controls:** This market segment is expected to experience the slowest growth rate among all the products under study. The market segment is expected to go from being the 2<sup>nd</sup> largest under study in 2004 to the 3<sup>rd</sup> largest in 2007. The use of wireless remote controls in crane and hoist controls and other material handling applications have been around for decades and there have not been many revolutionary product designs, nor are many anticipated in the future.

**Sensors/Transducers:** This market segment is totalled about \$11 million in 2004. It is expected to exceed \$32 million in 2007. For most applications there is a need for wireless transmission of sensor data, this can be most cost effectively provided via the use of wireless I/O devices and modems rather than sensors with self-contained wireless transmitters or transceivers. However, there are applications where such integration can be desirable, most typically when there is only one sensor at a given location.

**Mesh Networking Products:** Mesh networking is a topology that allows devices to communicate with many redundant data transfers between other devices. The shipment of these mesh networking products for industrial monitoring & control applications to North American markets amounted to \$6 million in 2004. However, these are forecasted to have the highest market growth rates of all the networking products studies. It should also be noted that significant wireless (RF/microwave) mesh networking markets are expected in building and home automation, military, and security markets, which are not covered in this study."

## 4 Trends in real time properties of industrial communication systems

### 4.1 Introduction

This chapter describes the recent trends concerning real time technologies with the final focus on industrial environment applications. For a long time, real time technologies have been a critical driver in automation and - even if real time is not equal to high speed - the top development of real time communication technologies is always a trend setter concerning high speed transmission. This is because usually the limit of what is possible concerning reliable high speed transmission is under consideration of the real time communication research and development community, and influences automation networks of the next future.

The document comprises different aspects concerning the latest and future development of the industrial real time field. Since the general trend in automation is to take over and adapt IT technologies only Ethernet-based fieldbuses are worth to be further considered. This is underlined by the ARC study "Industrial Ethernet Devices Market Outlook Study" showing the prediction of growth of Industrial Ethernet Devices [ARC01].

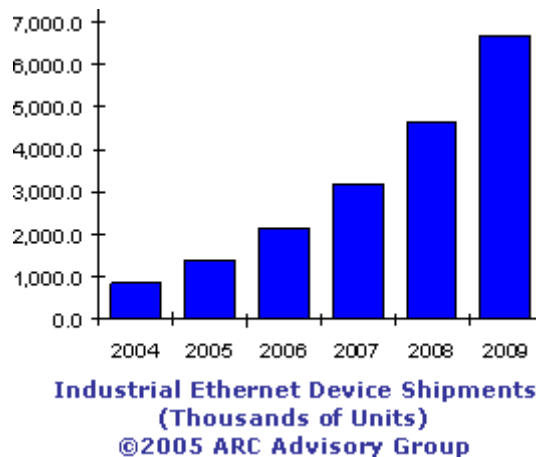


Fig. 8 Prediction on Industrial Ethernet growth

Also in [CoC04] it is shown that fieldbuses lose strong market shares compared to Industrial Ethernet.

There is a general approach that about 20% to 30% of all fieldbus applications are really real-time applications. But real-time control devices are often also used for no-real-time applications so the market share is hard to separate.

The next subchapters describe the trends of the involved layers and fields that are relevant for the further development of Industrial Ethernet real-time communication.

### 4.2 Physical Layer (IEEE802.3xx)

By using Ethernet (as the established future basic physical layer) automation is faced and benefits from the "automatical" further development of this standardised IT technology. So automation is faced now with the faster physical layer versions 1Gigabit, 10Gigabit Ethernet and soon 100Gigabit Ethernet. This enables a faster data exchange on the physical media that is firstly used where high

bandwidth is needed as in backbones. For sure these technologies will one day become "the standard" and also reach the lower automation levels. A meaning is only given if also the following upper data transmitting and processing layers fits according to this speed. Thus, the physical layer will not be the bottleneck of next future automation real-time networks. The migration should be already considered in related product designs.

### 4.3 Network Layer (Internet Protocol)

The recent and wide spread Internet Protocol is IPv4. A new version IPv6 is specified and already implemented in some products. Especially in Asia it is an already spreading network technology. A main intention of the development was a running out of addresses in IPv4. The address range is hiked from 32 bits in IPv4 to 128 bits in IPv6. Besides the enhanced address space or the implemented IPsec the Internet Protocol next generation (IPnG, IP version 6) [RFC1883] offers special features that are also related to real time. IPv6 was designed to correct lacks in communication with IPv4 detected as result of experiences during a long period of time (routers were overloaded i.e. because of fragmentation, etc.).

Below there is an extraction on what might be supporting real-time applications:

- The strong hierarchical address organisation can be seen as a facilitator for plant management and control applications
- IPv6 provides inbuilt quality of service or content prioritisation features
- Improved support of Extensions and Options
- IPv6 auto-configuration can help to ease device replacement
- The simplified packet header eases processing of IP packets, important for routers – optimised routing
- In opposite to v4 headers, have a fixed size, this could improve transmission jitter
- Most fields in the header are adjusted to the 64bit limit, to accelerate memory access in routers
- Ipv4 checksum fields have been abandoned in IPv6 due to the prevalence of error checking at other levels of the protocol stack, this relieves especially routers.

For QoS (Quality of Service) purposes IPv6 introduces the parameter Traffic Class. It enables to classify the data transfer and packets, i.e. it is possible to distinguish e.g. real-time traffic from Web traffic on protocol level. A further new parameter Flow Label can also be used for QoS and real-time applications. This value identifies a continuous data flow that means a sequence of packets from sender to receiver combined with special conditions for the transfer via the router (i.e. real-time services for audio/video). Routers keep track of flows and can process packets belonging to the same flow more efficiently because they do not have to reprocess each packet's header [IPv6Wiki]. The use of the Flow Label field is experimental and still under discussion at the IETF at the time of this writing. Refer to Chapter 6 for more information.

Disadvantages or reasons for a hesitated use of IPv6 are:

- IPsec originally developed for IPv6 is already a wide spread technology in IPv4 networks
- Heavy computational load for IPv6 security mechanisms especially concerning embedded devices
- Some consider the protocol as over-featured
- Many running systems can not be changed in short time or will ever be modified at all

Still there is the question about when and how fast Industry Nations are faced with the real transition to IPv6 and how this will influence Ethernet-based real-time systems in industry. There are no really practical investigations available in public literature; contributions seem to be more assumptions than proved facts of test environments. The migration is not considered as coming very soon, and a

transition strategy is still missing [Geo05]. As a major drive force for IPv6 mobile users and applications are seen. IPv6 seems to have especially important features for the real-time interconnecting of (sub)networks.

## 4.4 Network components

In [Fur03] the future trends of switching are listed as following:

Standardisation, acceptance and implementation of end-to-end QoS abilities

Extension from QoS abilities to Guarantee of Service GoS

Extension of switch-ability to multiple protocol handling as Multiprotocol Label Switching MPLS

Enhancement of switch technologies (fast, non-blocking switch matrices, photonic switches-no optical-electrical conversion for switching of optical signals)

## 4.5 Real Time in Automation

In the recent and coming years the degree of automation is growing rapidly in all industry fields – just being a step ahead or at least keeping pace with this assures companies to produce efficiently and to remain competitive with their products in the markets.

This means that more automation devices are to be found in ever faster industrial processes. For an automatic decision making, this means that more and more data have to be processed faster and therefore to be exchanged faster between the single components. This means again that the processing and exchanging (communication) of larger data amounts needs to be sped up – the time constraints are getting harder. This influences all in any way involved automation systems belonging to a production process that goes from the product development to the last sensor/actuator.

Another (and not mainly economical driven) important aspect is that some processes have strict constraints to be able to be controlled at all, e.g. the reaction in a nuclear power plant or a highly unstable or reactive chemical process. To control this, the reaction time for balancing or controlling measures are given by the physical or chemical process itself and have to be strictly followed to avoid fatal damages. Also here development shows that for the control more and more “side data” are drawn for better detailed and by this, safer control.

Beside this the whole life cycle process of a product, including production, is getting more complex so that several companies contribute to and process a product. Thus many data, including production data, have to be exchanged fast between company's networks (also over public) networks. By this data exchange of hard scheduled (e.g. production) processes expands steadily from single factory networks. For car manufacturing examples exist, where in one production line (trolley conveyor) for car assembly several companies take over parts of the assembly. This is a static example, but cooperation of companies do - and will - in a higher degree refer to flexible, temporal (and exchangeable) cooperation, thus also the demands for needed or advantageous network connections, including more and more real-time features, must be flexible too.

With reference to the fact that production management software is growing very rapidly it is stated in [ARC03] that the market demand for enterprise integration and real-time information from plant equipment regarding material location and tracking remain strong. In a further study from ARC Advisory Group Inc., Dedham, Mass. titled “Total Automation Business for the Process Industries Worldwide Outlook,” an annual growth for the global process automation market of 5.1 percent is projected over the next five years [ARC02]. This study also predicts broader application of Real-time Performance Management (RPM), for example, in which real-time data is collected from multiple plant sources and then organized for display to appropriate individuals to support smarter decision-making.

ARC's research also indicates that the proliferation of commercial-off-the-shelf (COTS) technology and other baseline technologies such as Microsoft operating systems has been both a blessing and a curse to manufacturing end users. “When process automation equipment employs COTS, it helps the users, because it does offer cost advantages and it raises their capability”. But because life cycles of COTS technology are significantly shorter than those of traditional process automation equipment, it

can drive a requirement for more frequent equipment upgrades, while also complicating migration issues.

The ARC study further says that much of the growth in the process automation market today is coming from services. Because users have drastically pared down their internal engineering staffs, they are looking outside for automation engineering support, and many are forming collaborative partnerships for these services with their process automation suppliers. Other high growth areas include safety systems, as well as systems designed to support regulatory compliance. On an industry basis, the fastest growth currently is coming in pharmaceuticals, food and beverage, and water and wastewater.

### 4.5.1 Important Ethernet-based Protocols

The following shows the existing parallelisms and differences that can be found at the growing real-time Industrial Ethernet technology market.

In principle three generic architecture variants for real time capable Ethernet based communication protocols can be distinguished.

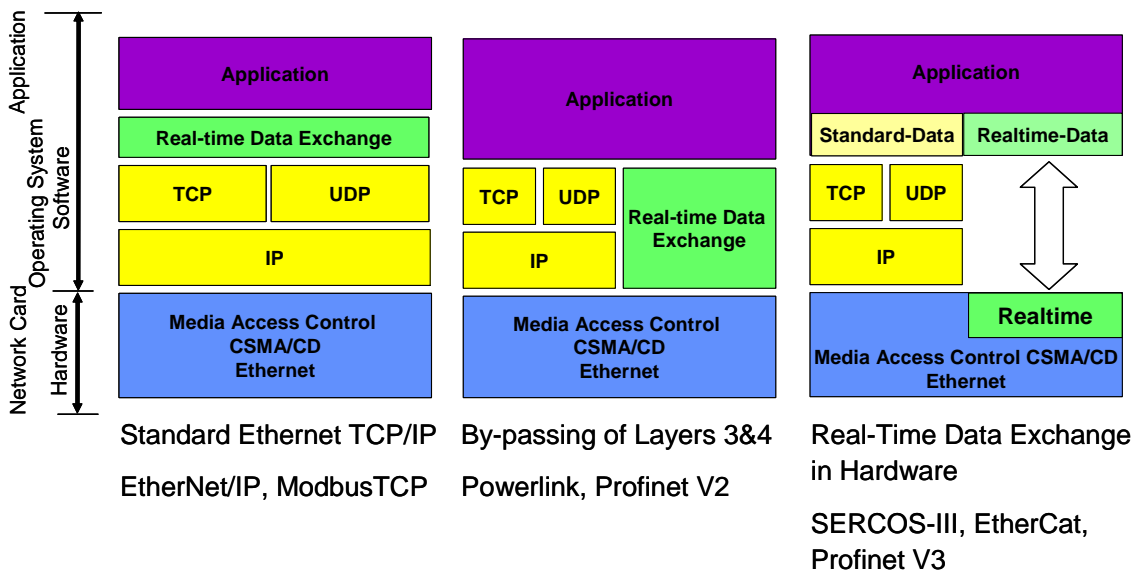


Fig. 9 Ethernet-based Real Time Architectures

In the architecture presented on the left side both the exchange of non timecritical 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 table below gives an overview of the important real-time relevant Ethernet-based protocols. Powerlink, Sercos-III, EtherCat and PROFINet IRT are deterministic protocols targeting on applications with high real-time demands. EtherNet/IP did originally not target such applications, but with the CIP Sync resp. CIP Motion extension that is still under development also motion control is targeted by EtherNet/IP. CIP Sync bases on the IEEE1588 - a precise clock synchronisation protocol, that enables to use standard Ethernet hardware implementing IEEE 802.3 and TCP/IP to provide the high performance, deterministic control required for closed loop drive operation.

By this IEEE1588 allows to establish control systems for isochronous real-time applications without an isochronous communication. This is especially interesting concerning the requirement on compatibility between industrial and office Ethernet and is in opposite to the trend to use special hardware solutions for isochronous Ethernet control systems.

The extension with the IEEE1588 clock synchronisation standard is announced by all the listed protocols and is thus a general trend, even if the use differs a little, because some protocols will use it mainly for synchronising different subnets.

Despite EtherNet/IP, all listed protocols are layer 2 protocols or set up directly on layer 2. EtherNet/IP is the only protocol setting up on layer 4 using the full Ethernet IP protocol suite also for real-time traffic.

All the protocols have means for the transmission of acyclic (non-real-time) data.

Sercos-III and PROFINET IRT are the youngest protocols with first products shown at fairs in 2005.

The use of already existing device profiles shows that an easy interchanging with data of classic fieldbuses is strived.

All protocol specifications are in the hand of organisations with different companies as members.

	<b>Powerlink</b>	<b>Sercos-III</b>	<b>EtherNet/IP</b>	<b>EtherCat</b>	<b>PROFINet IRT</b>
<b>Technology</b>	Time-slot, strong deterministic	Time-slot, strong deterministic	not deterministic, Clock synchronisation with CIPsync extension	deterministic but not isochron	Isochron, strong deterministic,
<b>Real-time Data Transmission</b>	Ethernet Frames as Broadcast	Ethernet Frame	Publish/Subscribe (implicit Messages via UDP), Standard IP Frames	Ethernet-Frames, alternatively UDP/IP possible	Ethernet Frames
<b>Acyclic Traffic</b>	acyclic Time-slot	IP-Channel (acyclic Time-slot)	explicit messages via TCP	protocol tunnelling (diagnostic and parameter data)	IP-Channel
<b>TCP/IP Stack</b>	parallel to real-time stack for acyclic data	parallel to real-time stack	completely, no separate real-time stack	UDP/IP is possible	parallel to real-time stack for acyclic data
<b>Ethernet Transmission Rate</b>	100MBit/s	100MBit/s	100MBit/s / 10MBit/s	100MBit/s	100MBit/s
<b>Technology Availability</b>	Standard Ethernet Chips, no special ASICS	scheduled: Sercos-Core (SercosIII-IP) for FPGA Integration	sample code	ASIC	ASIC
<b>Products since</b>	2001	~2005	2000	2003	~2005
<b>Hardware solution</b>	Implementation at separate communication processor recommended	yes	no	completely	yes
<b>Placement in OSI Model</b>	Layer 2 protocol	above Layer 2	above Layer 4	Layer 2	Layer 2
<b>Device profiles</b>	CANopen	Sercos	Devicenet (CAN), Controlnet	CANopen, Sercos	Profibus
<b>Homepage</b>	<a href="http://www.ethernet-powerlink.org">www.ethernet-powerlink.org</a>	<a href="http://www.sercos.de">www.sercos.de</a>	<a href="http://www.odva.org">www.odva.org</a> oder <a href="http://www.ethernetip.de">www.ethernetip.de</a>	<a href="http://www.ethercat.org">www.ethercat.org</a>	<a href="http://www.profibus.com">www.profibus.com</a>

Tab. 4. Overview on Ethernet-based real-time protocols

#### 4.5.2 Example for IEEE1588 implementation

Since the use of the open standard IEEE1588 is a general trend an example extracted from the IAONA Handbook Industrial Ethernet [LA05] will be described in the following. The EtherNet/IP related CIP Sync is used as example since its high performance real-time capability completely relies on IEEE1588 mechanism and the robustness of the solution still has to be proved in praxis.

Traditional closed loop control of distributed drives uses event-based synchronization, which requires absolute hard delivery of time-critical cyclic data across the network. Jitter of  $<1\mu\text{s}$  for cyclic data is necessary for precise speed and/or position control. The Ethernet IEEE 802.3 CSMA/CD data link layer is not capable of delivering data with  $<1\mu\text{s}$  jitter. One way of resolving this issue is by using a time scheduled algorithm to replace the CSMA/CD network data link layer as applied by Powerlink, Sercos-III, EtherCat and PROFINet IRT.

EtherNet/IP's implementation for motion applications uses a different approach called "Time Synchronized Distributed Control". Time Synchronized Distributed Control uses time stamped packets to relax the strict requirement of <math><1\mu\text{s}</math> jitter for cyclic data delivery. With this approach, the CSMA/CD data link layer does not have to be replaced with a proprietary driver or ASIC, allowing full IEEE 802.3 compliance, while providing a robust solution with the performance necessary for closed loop operation of high performance digital drives.

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

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. The time services provide a distributed time reference for the packet time stamping used in the Time Synchronized Distributed Control scheme. CIP Sync is fully compliant with the IEEE-1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. 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. With time synchronization, it is possible to synchronize operations across distributed nodes. The CIP Sync 1588 implementation is shown in Fig. 10.

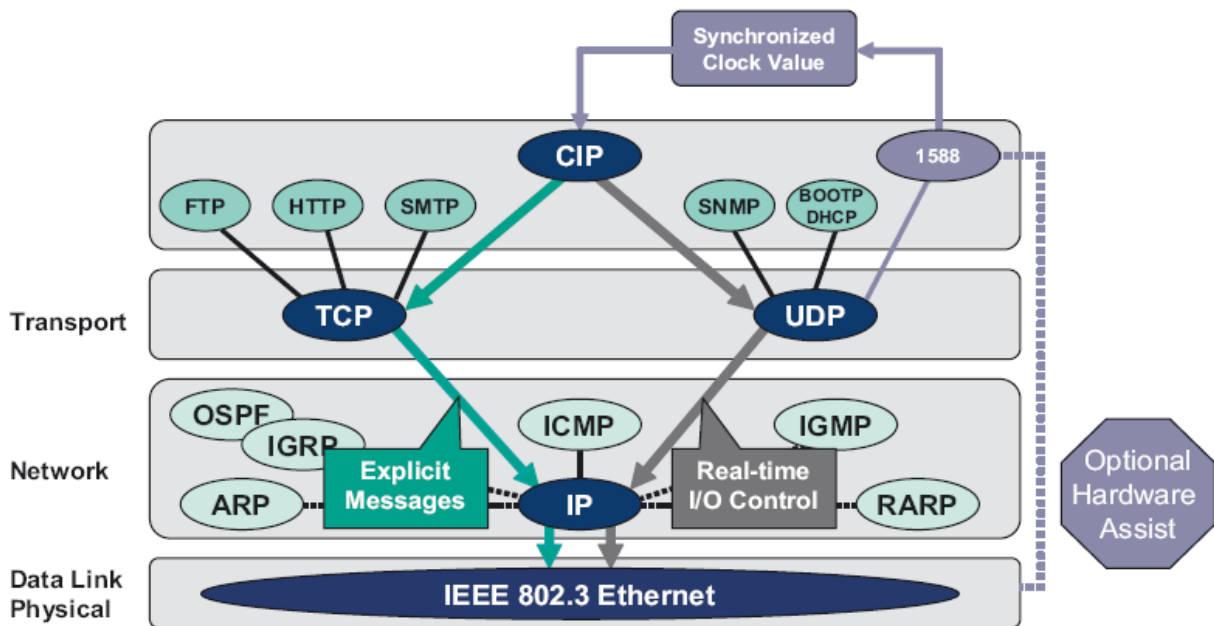


Fig. 10 CIP Sync - IEEE 1588 Implementation for EtherNet/IP

When a cyclic data motion packet is constructed, a time stamp is included as part of the packet. A single cycle timing model for cyclic data transfer delivers a fresh command value from the motion planner to each drive based on the actual position values sampled at the beginning of the cycle. Typically the motion planner will reside in the motion controller, with the data delivered to the distributed drives via EtherNet/IP. If a motion packet is late for the next cycle, the time stamp of the packet can be used to compensate for the delay. This time based compensation technique eliminates the need for absolute, hard data delivery, allowing the IEEE 802.3 CSMA/CD data link layer to be used.

The CIP Motion profile is currently under development by the ODVA Distributed Motion JSIG. Like CIP, the CIP Motion extensions will be fully open, with compliance and interoperability assured by comprehensive conformance testing.

### 4.5.3 Real Time in Closed Loops

The most sophisticated control in industrial automation are closed loop controls. They enforce precise and stable behaviour of the basic automation tasks on the lowest control level. The days of analog implementation of control loops are over, and industrial busses have penetrated this field.

Contrary to the tolerant approach to communication within supervisory level, the latencies and jitters of control information have to be kept as short as possible in control loops.

Some applications are very tardy and the time constants of the controlled system may reach hours or days. For instance some slow chemical and biochemical processes possess very long time constants, thus, the communication latency does not have to be paid attention. Opposed to this, drive control requires isochronous real time communication as the latency of even about 1 ms would cause significant control inaccuracies.

As the drive control is the most time critical task in industrial automation, the basic control approach will be introduced and two actual, however contradicting, trends in this field will be presented.

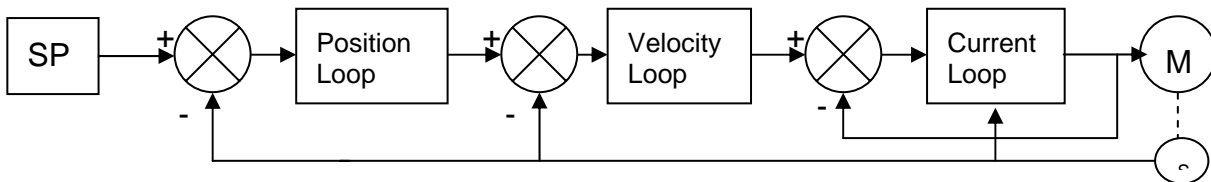


Fig. 11 Needed loops within a closed loop motion control

The three closed loops shown in Fig. 11 are nested. These are current loop, velocity loop and position loop. The sample rate of the current loop is at least 10 KHz, while the sample rate of each adjacent loop is ten times smaller.

Implementation of these loops depends on particular situation. Generally speaking, the basic commands come from the Numeric Control (NC) block, where the whole axis rotation is generated. Commands generated in NC are passed to a drive. Drive takes care about transforming the command of NC into electrical current fed into the motor using thick wires. The following trends appear in this field:

- **Intelligent drives.** The drive is commanded by a NC via a communication interface. Usually it is a classic industrial fieldbus or in the latest and future time an Ethernet-based fieldbus. The command represents required position (rotation), which means that all three control loops are implemented in the drive. The implementation of the loops is very straightforward and the responses are very fast. If only one motor is driven, this solution is very effective

Many vendors are competing in giving more and more intelligence to the drives (soft-start algorithms, parking functions, diagnostics, etc.). Moreover, the spatial integration is still higher. While formerly the drives were of dimension of 10 cm x 10 cm x 15 cm, now they are becoming implemented directly in the motors and the dimensions are negligible.

- **No drives at all.** This trend tends to implement all loops in NC and makes the drive very primitive. This would mean that all calculations of the three controllers would be performed in the NC. The drive would become a mere interface converter changing the received control packets into electrical current, and, of course, providing data acquisition to NC (current and velocity). This control approach is very efficient either for intelligent control algorithms, where the control loops interact in a more complicated manner, or when more axes are to be synchronised.

This trend is not feasible with the current communication technologies, thus, 10Gbps Ethernet is being looked forward to.

## 4.6 Real Time in Public Networks

The development trends of the EthernetIP Suite which are independent from automation (e.g. IPv6) are already considered above. This subchapter describes further trends from the non automation application point of view.

Real-time is also getting an important topic in public networks (IT world). It is already applied for multimedia applications as VoIP, Video streaming and IPTV and are faced to a growing importance and spreading. So further worldwide (standardisation) development efforts and outcomes can be expected. Especially for IPTV under the headline "efficient Ethernet converged networks" measures (from the provider side) and technologies are covered to enable real time voice, data and video traffic over existing Ethernet networks [Luc06]. There are also IEC activities concerning an Internet Model for Control of Converged Networks [IEC06].

A new standard that define how communications technologies can work together to deliver new services in order to enrich communications for end-users is the IMS — Internet Protocol Multimedia Subsystem. IMS defines a layered and generic architecture which offers to operators the opportunity to build an open IP based service infrastructure that will enable an easy deployment of a variety of multimedia communication services mixing telecom and data services. It is an international standard, first specified by the Third Generation Partnership Project (3GPP/3GPP2). For users, IMS-based services enable person-to-person and person-to-content communications in a variety of modes – including voice, text, pictures and video, or any combination of these – in a personalized and controlled way. For operators, IMS takes the concept of layered architecture one step further by defining a horizontal architecture, where service enablers and common functions can be reused for multiple applications. The horizontal architecture in IMS also specifies interoperability and roaming, and provides bearer control, charging and security. What is more, it is well integrated with existing voice and data networks, while adopting many of the key benefits of the IT domain [IMS01].

# 5 Trends in safety of industrial communication systems

## 5.1 Introduction

Safety technology is now available for most of the fieldbuses. These solutions use the same wire for non safe and safe data. The motivation for this approach is clearly to save costs. Although solutions exist where a pure safety bus is used, these solutions are not wanted by the end-user. He then has to use two different bus systems – one for the non safe, the other on for safe data. Following this major requirement – one single busline, nowadays all large fieldbus organisations have specified and developed their safety bus.

Ethernet is moving with a breath-taking speed from the office world into the plant factories. The advantages are the vertical integration of automation processes in the overlaying MES and ERP systems. The vision was to have one single Ethernet for vertical and horizontal communication. This vision did not come true. Each fieldbus organization developed its specific Industrial Ethernet protocol, and even new players came into the field, such as Ethernet Powerlink and Ethercat. And all these protocols are quite incompatible.

The success of all the Ethernet protocols depends very much on how quickly all the “good features” of the fieldbuses will integrate. One critical “good feature” is the safety functionality. Therefore, all corresponding Industrial Ethernet Protocols are heading towards safety functionality.

This chapter gives an overview of the safety capabilities of the major fieldbuses, their Ethernet “successors” and the new players in the field of industrial communication networks.

## 5.2 PROFIsafe

### 5.2.1 Overview of PROFIsafe

PROFIsafe safety measures are performed 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.

### 5.2.2 Evolution of PROFIsafe

The first PROFIsafe products were available by the end of 1999, and were used mainly in the process industry. The first products designed for machinery industry were available in the middle of 2002.

The PROFIsafe specifications have been adapted during 2005 in order to allow the use of PROFINET mediums, so first products are also available since the end of 2005 for PROFINET including radio communication. Meanwhile, PROFIsafe has proven to be a reliable and cost efficient solution for medium and higher safety applications, with a lot of advantages compared to traditional solutions. Altogether, until the end of 2005 more than 16.000 applications have been built in all over the world. Most of the applications are realized in the machinery industry from press controllers to transfer lines and in the process industry for offshore platform or chemical industry. In addition some applications

are also concerning people transportation (ropeways and train applications). More than 137.000 safe nodes have been performed up to today.

### 5.2.3 Maturity of PROFIsafe

The bus communication and the data protocol have been evaluated as safe by BGIA and by TÜV. The system can be used up to control system category 4 according to EN 954-1 or up to SIL 3 according to IEC 61508 and may be used for stop category 0 and 1 according to EN 60204-1. In the US, the safety system has been given NRTL listing.

The product portfolio comprises failsafe PLCs with diverse CPU sizes and performances associated to IP20 or IP65/67 input/outputs modules. In addition, dedicated field devices like light barriers, laser scanners or drives with new safety functions are available (safe stop, safe reduced speed, safe reduced torque). Regarding process industry, devices for gas analysis like devices for PROFIBUS PA will be available by the beginning of 2006.

Next steps will be the development of sector specific interfaces, to allow the users to fulfil complete and adequate safety functions.

## 5.3 Interbus Safety

### 5.3.1 Overview of Interbus Safety

Interbus Safety is a special "safety-related expansion" for Interbus, which is widely used in machine and industrial applications. The topology of Interbus is an active ring. This means that all devices are actively integrated into a closed transmission path. Interbus works using the master-slave principle. It has a fixed telegram length and is therefore deterministic. All bus devices include repeater functionality.

Interbus Safety uses the Safe Control concept, which is independent of both the bus system and the host system. The basis for this is the Safe Control unit. It must be installed directly after the Interbus master and therefore receives all the IO information of the connected devices. A safety protocol is used between the Safe Control unit and the connected safety IO devices that guarantees the required safety of the data transfer and can only be interpreted by connected safety devices.

The Interbus Safety protocol extends the standard Interbus system to include a safe transmission channel, which transmits application data up to category 4 of EN 954-1 or SIL 3 of IEC61508

### 5.3.2 Evolution of Interbus Safety

Interbus is one of the largest and most successful fieldbus technologies in service today. With an installed base of over 7.5 million nodes, the technology has been enhanced through three generations, beginning in 1987, of products with a fourth-generation on the way in 2006. INTERBUS is a leading fieldbus technology in automotive applications such as robotics, body shop, and paint. Products are available from 270 suppliers and encompass 1,700 offerings that have been deployed in over 650,000 applications. This popularity is remarkable given that Interbus is not the preferred network of any major automation supplier, but instead is supported mainly by a larger number of mid-sized automation suppliers led by Phoenix Contact, which initially developed Interbus.

Interbus Safety is the latest enhancement of Interbus technology. The development started few years ago, the first certification from the corresponding institutes was granted in the beginning of 2005. Now Interbus Safety is well used in automation industries, especially in car manufacturing plants.

The Interbus Club decided to adapt to Profinet as Industrial Ethernet protocol. Thus, Interbus Safety will not be adapted for Ethernet.

### 5.3.3 Maturity of Interbus Safety

The Interbus Safety system has been evaluated as safe by BGIA and by TÜV. The INTERBUS Safety system meets safety functions up to Cat. 4 according to EN 954 and SIL 3 according to IEC 61508. The product portfolio comprises failsafe PLC, the Safe Control associated to IP20 or IP65/67 input/outputs modules.

## 5.4 DeviceNet Safety

### 5.4.1 Overview of DeviceNet Safety

DeviceNet Safety is a initiative to facilitate DeviceNet with safety features. The basic DeviceNet protocol is maintained, but additional safety features are defined for the safety devices. A DeviceNet network can include both normal DeviceNet devices and DeviceNet Safety devices. The topology and the communication media are not affected by DeviceNet Safety. A DeviceNet Safety network can consist of up to 64 nodes. Latency times of 20ms, from input capture to output actuation, are possible.

DeviceNet Safety boast of suitability to category 4 of EN 954-1 or SIL3 of IEC61508 with 1% safety budget consumption. To achieve such high level of safety, redundancy must be applied for input capture, control program execution and for output actuation. Therefore, starting from CAN controller, all hardware (including the controller CPU) must be replicated either by using two (or more) devices or by using two-channel devices. The cable and the transceiver are not replicated. Due to single channel transmission, a basic DeviceNet Safety network does not support systems where the continuous state is the safe state (in other words, where a steady safe state cannot be identified). It is possible to replicate such DeviceNet Safety networks to introduce replicated communication media and therefore increase reliability performance and tolerance of a single fault to a level, which might enable the usage of DeviceNet Safety in safety-related systems with no steady state.

Besides redundancy, to achieve the required reliability, DeviceNet Safety applies an additional safety protocol layer on top of normal DeviceNet. The safety protocol consumes two bytes of the maximum eight DeviceNet data bytes. The two trailing bytes are used for a sequence count (2 bits) and for redundancy check (CRC-S1, 12 bits). The remaining bits are reserved for future purposes.

### 5.4.2 Evolution of DeviceNet Safety

DeviceNet safety achieved TÜV approval in 2003 for its system specification. Products have been submitted for TÜV approval in 2004 and have arrived on the market in 2005. DeviceNet safety meets the requirement of IEC61508.

### 5.4.3 Maturity of DeviceNet Safety

DeviceNet safety products are nowadays available. This includes, for example, PLCs with a two-processor safety architecture and integrated safety functions rated up to a Safety Integrity Level (SIL) 3 functionality; a DeviceNet Safety Scanner which allows to send and receive safety and standard

control information over a single DeviceNet network and is TÜV certified for up to SIL 3 Category 4 applications and servo drives with torque off capability that disables the drive output, certified by TÜV to meet the requirements of EN-954-1 Category 3 and IEC-61508 SIL 3.

## **5.5 AS-Interface Safety at Work**

### **5.5.1 Overview of AS-interface Safety at Work**

AS-interface (AS-I) is applicable in systems, which connect simple on/off information and (small) power between switches, PLC and output units. An AS-interface Safety at Work system is composed of a standard AS-I network along with a safety monitor and safety-related slaves (max. 31). Safety-related slaves are connected to safety devices or switches and safety outputs. The safety monitor controls the communication between modules all the time and if it detects failure, it starts a fault-handling procedure and de-energizes its two output relays. Safety PLC is not required in the system. The network is controlled by a master unit, which sends a request to a slave unit, which answers immediately. If the answer is not correct, it may answer again and the master sends a request to the next slave.

A mixed operation of both safe and nonsafe AS-Interface slaves is possible without problems.

### **5.5.2 Evolution of AS-interface Safety at Work**

The safety concept was added to the AS-Interface system in 1999, and the first products were available by the end of 2000. Meanwhile, AS-I Safety at Work has proven to be a reliable and very cost efficient solution for small and medium safety applications, with a lot of advantages compared to the conventional hard wiring. Altogether, until the end of 2005 more than 30.000 safety monitors have been built in all over Europe, North America, Japan and China. Counting in average, 4 safety slaves for each safety monitor, more than 120.000 safe nodes have been performed up to today.

### **5.5.3 Maturity of AS-interface Safety at Work**

The bus communication and the data protocol have been evaluated as safe by BGIA and the technology has been certified by TÜV Nord. The system can be used up to control system category 4 according to EN 954-1 or up to SIL 3 according to IEC 61508 and may be used for stop category 0 and 1 according to EN 60204-1.

In the US, the safety system has been given NRTL listing. In France, a positive statement from the INRS insurance agency has been made.

The product portfolio comprises up to now, safe field and switch cabinet modules from various manufacturers. Also available are integrated slaves, including intelligent safety sensors and safety command devices with AS-Interface chip.

The next step of development will involve the development of safe outputs for AS-I Safety at Work slaves. Applications can then be extended to integrated safety actor functionality, for e.g. pneumatics and drives.

## **5.6 Ethernet Powerlink Safety**

### **5.6.1 Overview of Ethernet Powerlink Safety**

Ethernet Powerlink (EPL) is based on the standard IEEE 802.3 layers according to ISO/OSI model and modifies the OSI stack by adding a middleware between layer 2 and 3 for the TCP/IP stack and between the layer 2 and 7 for the real-time transmissions.

The current physical layer is 100Base-X Fast Ethernet (100 Mbit/s). It agrees with standard Ethernet technology and infrastructure and does not compromise standard Ethernet frames in order to achieve its results [Sc05].

EPL offers the possibility to perform both the publisher/subscriber and master/slave communication method [Ce04] and to develop subnets with their own collision-free domains.

Powerlink is the first real-time deterministic Ethernet: the problem with standard Ethernet protocols for real-time control applications, such as motion control, is that they lack determinism, that is they are unpredictable in terms of when precisely data will arrive from one device to another, and when exactly a device will be able to send or receive data. EPL resolves this lack of determinism by managing the nodes' access to the network within allocated time slots, with implemented cycle times as low as 200 microseconds and less than 1µs cyclic jitter for precise control [FeSa04]. Data exchange with each node takes place under the control of a manager node; this prevents collisions and ensures that deterministic data is exchanged on schedule.

This alone has safety implications. But to meet the international safety standard for control networks (IEC 61508), the Ethernet Powerlink Standardization Group (EPSG) has developed the next generation safety protocol for real-time industrial Ethernet: Ethernet Powerlink Safety (EPLsafety) [Wr05].

EPL safety is a protocol extension particularly suitable for safety-related applications, which introduces further mechanisms of protection, such as the use of a continuous check of the transmitted data through a cyclic redundancy check (CRC) and of the senders through a look-up table inside each device, a clear distinction between safety-relevant and non safety-relevant data via an embedded data frame inside standard communication messages and, consequently, the use of flexible safety-related telegram formats for different dates purposes [Wr05].

In this way EPL safety presents measures to avoid common communication errors and to guarantee a good tolerance to failures due to errors when applied within safety applications; it is IEC 61508 compliant and fulfils the requirements of SIL 3 and, within specific architectures, also SIL 4 [Sc05].

### **5.6.2 Evolution of Ethernet Powerlink Safety**

In November 2001 Ethernet Powerlink was introduced by B&R; in April 2002 the technology was opened to other parties, in February 2003 the implementation services started and in November 2003 Ethernet Powerlink specifications were released [Sc04].

The EPSG (Ethernet Powerlink Standardization Group) was founded in June 2003, it originated from a group of leading automation companies. Each EPSG member has always had the opportunity to decide about the future of Ethernet Powerlink.

In fact, many EPSG members have contributed to the rapid development of the design and test tools for Ethernet Powerlink applications.

In 24 March 2004 the EPSG announced that Ethernet Powerlink is a winner in "ELEKTRONIK Magazine's 2003 Product of the Year Awards competition" (the Product of the Year Awards were established to honour the most innovative and useful products introduced to the electronics market) and it is confirmed as an approved technology deployed in more than 80,000 nodes [EPSG04].

EPL Safety, instead, has been introduced by EPSG in September 2004 as an open and independent technology, compliant with international standards.

Its objective was to increase the advantages of Ethernet for high performance real-time networking systems based on the Ethernet Powerlink Real-Time protocol introduced by B&R [Wr05].

### **5.6.3 Maturity of Ethernet Powerlink Safety**

Ethernet PowerLink safety is mature for safety-critical applications according to IEC 61508 SIL 3 and EN 954-1 category 4. The maturity of the protocol has already been tested and approved. EPL safety

is suitable for all safety categories in applications required for power plant construction or railway technology without any limitations.

Several device manufacturers are already working intensively on safety systems based on EPL safety. The first prototypes have been implemented in the middle of 2005.

The EPSG is working on the further development of the specifications to add even more capabilities in areas like safety, security, system redundancy or precision clock synchronisation in heterogeneous Ethernet/Internet topologies.

In the future it could also be based on faster Ethernet variants such as Gbit Ethernet, if necessary [Sc05].

## **5.7 Ethercat Safety**

### **5.7.1 Overview of Ethercat Safety**

EtherCAT is the Ethernet based fieldbus system which creates new performance standards. In the standard Ethernet individual frames are used for each device and the shortest frame length is 84 bytes. EtherCAT medium access control is based on the Master/Slave principle. Each EtherCAT slave device reads and writes data when the frame passes through the node. The full-duplex features of 100BaseTX are used.

Safety-related communication and control communication are performed on the same network. No additional hardware separated from the automation network is needed. The safety protocol is based on the application layer of EtherCAT, without influencing the lower layers. EtherCAT fulfils all requirements for Safety Integrated Level (SIL) 4 of IEC 61508 standard. Protocol uses variable data length and that's why this protocol is suitable for safety drive technology. Like other EtherCAT data, the safety data can be routed without requiring safety routers or gateways.

### **5.7.2 Evolution of Ethercat Safety**

The EtherCAT Technology Group (ETG) was established during the SPS/IPC/DRIVES fair on November 26<sup>th</sup> 2004 in Nuremberg, heralding the opening of EtherCAT. The ETG aims to prepare EtherCAT optimally for as wide a range of applications as possible. Within four months, there were more than 60 members - among them several well-known international companies - joined the group. EtherCAT was developed by Beckhoff and presented for the first time at the 2003 Hanover Fair.

Nowadays the EtherCAT Technology Group (ETG) already has more than 230 members. The EtherCAT specification has been published by IEC. EtherCAT has been approved as an ISO standard and is being standardized by the IEC as a communication system for both CANopen and IEC-61491 drive profiles. Safety implemented in EtherCAT technology is called Safety over EtherCAT. Safety over EtherCAT enables safety-related communication and control communication on the same network. The protocol developed according to IEC61508 can be transferred via EtherCAT or even across gateways. In addition to EtherCAT, fieldbus systems such as PROFIBUS, CANopen, SERCOS or Ethernet can be used as the transport layer. In conjunction with the TwinSAFE product family, safety technology can be implemented without sophisticated safety control [EtherCAT].

### **5.7.3 Maturity of Ethercat Safety**

More than 40 manufacturers produce products based on the EtherCAT. All the parts of the EtherCAT automation network system are available. Different manufactures produce master devices based on PC control as well as embedded controllers and small controllers. It is possible to buy servo drives, frequency converters and whole sets of sensors. The product range is completed by I/O devices, safety devices, valve manifolds, digital servo valves, gateways, infrastructure components, communication modules and communication chips.

## 5.8 Sercos III Safety

### 5.8.1 Overview of Sercos III Safety

SERCOS safety is a protocol extension, which is compliant with the established transmission mechanisms of the SERCOS interface. The extension is available both for SERCOS II and SERCOS III communication protocol and also for other transmission physics; it achieves its best performance when used in combination with SERCOS III [IGS03].

SERCOS safety concept takes advantages of SERCOS III characteristics (profiles, message structures, synchronisation, topology) to realise safety functions.

Therefore it combines the proven real time mechanisms of the actual SERCOS III interface with the benefits of Ethernet physics.

As in SERCOS III, any standard IP telegram (e.g. TCP/IP and UDP/IP) can be transmitted via a configurable IP parallel channel, in a non real time slot, independently of the real time processing. This mechanism ensures collision-free data transmission between slaves.

The hardware-based synchronisation, which has 31.25  $\mu$ s cycle time for up to 8 drives with 8 byte cyclic data and only a few nanoseconds of jitter, guarantees besides determinism; data rate is 100 Mbit/s. [IGSRT].

SERCOS safety uses the same topology of the existing SERCOS interface: full-duplex connections between nodes create a double ring that guarantees reliable and redundant data transmission. With SERCOS III, in case of a break at any point in the ring, the communication continues: the machines or system continue to run fault free, and integrated diagnostics report the fault.

Hot plugging allows connection and removal of nodes during ongoing operation, however, this feature would be advantageous in some motion control applications.

Due to the routing capability of the protocol, a safety network may even be extended over several subordinate SERCOS networks [SE05].

The safe data container, which is embedded in the SERCOS III data telegram, may transfer up to 64bit of safe user data.

Safe data can be exchanged between slaves directly using the peer-to-peer cross-communication capabilities of SERCOS III, without collection and redistribution of data by a central master (safety control) [TE03].

### 5.8.2 Evolution of Sercos III Safety

SERCOS III (SErial Real-Time COmmunication System) has been developed by The Interests Group SERCOS (IGS), that is a group composed by more than 60 member companies, located in North America, Europe and Japan, who submit their products to a standardised certification process.

SERCOS III is the next logical step in the evolutionary history of the SERCOS interface; it has been presented in April 2003 [IGSRT].

From then on the SERCOS organisations have intensively worked.

The basic concept has been defined and approved by the SERCOS member organisations; detailed specifications have been developed by a technical working group, which includes various member companies. Since SERCOS-III is based on proven and tested profiles, work on the specifications have mainly been concentrated on the hardware and additional features.

In November 2004 first hardware platforms and prototype implementations have been presented, including control systems, servo drives and I/O devices. At the same time, the SERCOS III specification was released and officially submitted to IEC for standardisation.

First products have been offered in 2005.

The SERCOS III interface, that was originally intended to be a drive interface, following this evolution, has become a universal motion control interface in various industries, especially for multi-axis applications.

In the last months of 2005 in Nuremberg the SERCOS trade organisations introduced a safety concept that allows a safe data transfer based on the SERCOS interface [SE05].

### **5.8.3 Maturity of Sercos III Safety**

SERCOS III safety seems to be suitable for transfer of safety-relevant data implementing the necessary safety functions for critical real time motion application, such as electronic line shafts in printing machines, packaging machines or multi-axes machine tools. It could be used within safety applications up to SIL3 according to IEC61508.

SERCOS III safety is currently being investigated by international technical service providers which are evaluating and testing the safety characteristics and quality of it.

The specification should be approved in the first months of 2006, so the first SERCOS III safety products will be available in 2006 [SE05]. SERCOS III safety has to be considered an emerging maturity level protocol extension.

## 6 Trends in security of communication systems

This chapter aims at providing a rationale for recognising security and privacy in the context of Virtual Automation Networks both based on fixed line and mobile/wireless communication infrastructures. It proposes major trends in security issues as well as an up-to-date guide to the issues related to virtual automation network privacy and security and the research and standardisation activities needed to address these issues.

### 6.1 Trends in security issues – an overview

A state of the art review was elaborated taking into account ongoing research activities as well as developments in standards bodies and user forums. From this review, a list of existing and emerging security and privacy-enhancing technologies was obtained. The gaps between the needs and the state of the art resulted in preliminary recommendations for further research. To further refine and balance the priority of the research issues, non-technical aspects (socio-cultural, economic, legal) as well as a European perspective, were also taken into account. [Cordis]

An up-to-date and prioritised list of issues has been identified. The main future topics in the area of virtual automation network privacy and security are:

#### **Trusted platforms and application/software management for virtual automation network security and privacy**

- Trusted and secure devices.
- Secure reconfiguration of devices.
- Automation specific security architecture and protocols.

#### **Virtual automation network network/transport security**

- Protection of the virtual network against attacks.
- Heterogeneous network access control security.
- Seamless security handover at network level.
- Security architectures for virtual networks.

#### **Automation application security**

- Automation application security framework.

#### **Identity management**

- Single sign-on based on authentication.
- Authorisation 'privacy'.

#### **6.1.1 Basic security technologies for virtual automation network environments**

- Lightweight stream ciphers.
- Truly practical cryptographic mechanisms in constrained environments.
- Delegation of cryptographic operations.
- Lightweight key management infrastructures.
- Group keying.

## 6.1.2 More than technology

Privacy and security of virtual automation network information systems have been approached in the past mainly from the perspective of technological dependability (availability, security, confidentiality, etc). Recent developments in information and communication technologies, users' expectations and business models make it imperative to take a broader perspective on security, embracing the technical, socio-economic, policy and business aspects.

### Analysis of the research topics

To establish a coherent future for virtual automation network's trust and security in the developing telecommunication world there is a great need to consider security as a fundamental pillar from the beginning of the design. Traditional approaches are not sufficiently holistic to cover all the upcoming interacting technologies. Networks of services can only be built on a trustworthy foundation of solid security for interaction.

The increasing heterogeneity of technologies such as UMTS, WLAN and Bluetooth in the new mobile environment is one of the most visible trends [Kni03]. To provide secure access to all these networks flexible authentication and authorisation procedures have to be in place. Different types of credentials and contexts provided at different layers and secure sessions need to be handed over when dynamically changing network connections. Single sign-on (SSO), which is currently driven by non-European IT companies, can provide a unique opportunity for virtual automation network operators which can integrate SSO into their systems and provide a harmonic usage environment for the user.

Virtual automation networks offer numerous interfaces to users and service providers. Some communication partners might change frequently. To provide services without intensive consideration of the security issues would pose a high risk not only to the infrastructure, but also to the services themselves. The list of threats range from Denial of Service attacks, injection of malicious code, viruses, worms, hijacking of sessions and servers, to theft of confidential information. To protect the virtual automation networks suitable network Intrusion Detection Systems, proxies, firewalls and other technologies have to be investigated. If these concerns are not addressed the whole deployment of new VAN services is at risk.

Numerous security enhancing tools have already been investigated (e.g. signature schemes, authentication protocol etc), but many of these are impractical in constrained environments. The current practical requirements of security tools need to be investigated and their efficiency (round trip time, usage of memory etc) and performance need to be tested. Other required functionalities have not been investigated at all from a lightweight perspective e.g. stream ciphers, key management infrastructures and group keying. Virtual automation network profiling of security and privacy functionality (e.g. outsourcing expensive operations to servers) could build a cornerstone of the new security approach for the virtual automation network environment.

Finally, to achieve the goal of security in future automation, communication networks will require further research and technology development. The virtual automation network roadmap has identified the areas where research, standardisation and development will be most needed and beneficial in the coming years

## 6.1.3 The current status

The fundamental requirement, or rather assumption, that is identified here is the need to establish foundations for security provision at the outset of the design and development of the next generation of VAN communications technology.

The goal is secure, trusted communication between automation devices and between these devices and operators.

The scope of this next generation is yet undefined, but it will paradoxically reach out in one direction towards greater integration with the fixed networks and their established procedures and in the almost opposite direction towards ad hoc networking with its opportunities (or threats) for free-for-all quasi anarchy. The roles of network operator and service provider will become increasingly fuzzy as responsibilities move from well-established commercial entities to less well-defined niche operations or even individuals.

There are no real surprises in the identified requirements: the headline topics are the same as ever. What is new is a change of emphasis and a change in the complexities and difficulties of providing security. The history of IT and communications security runs along the dissemination of technology and the provision of ease access. In the past, the problem was the distribution of rotors to Enigma machines and the strength of entry locks on the door of the computer room. Among the new and conflicting challenges are the concepts of secure ad hoc networking and the need for maintenance of control over sensitive information in a partly high volatile environment.

Ad hoc networking is not the only wireless automation development that raises the security stakes for automation networks. Packet-switched data, seamless roaming with heterogeneous access networks, reconfigurable terminals and software-defined radio all add to the complexities of delivering an uninterrupted, secure, high-quality service. There are implications for all the usual security primitives such as authentication, confidentiality, integrity, availability etc. The problem as ever is to devise protocols to do the job and then to deliver the right keys to the right places at the right time.

A parallel need that emerges deals with some persistent control over owned information. This may be enterprise data that must be protected in some specifiable way, or it may be system information concerning identity or location relating to automation devices. In both cases the user is looking for rights over its use, propagation and disclosure.

The automation terminal or device must be able to protect its information and control the processes that can access and use it. It may be assumed that the powerful, static server can fairly easily look after itself using established technologies and procedures, but the designer of a trusted automation device must be very conscious of the practical concerns of costs and power consumption, portability and usability in addition to basic technical feasibility.

These confidentiality issues point leads to a need for common approaches to the provision and use of trusted execution and storage environments. Cryptography traditionally protects our information during transmission, but what ensures that it is handled according to rules or expectations at the end points, particularly in the highly dynamic picture that is starting to appear? There is a need for trusted platforms, secure modules and system software with known credentials that will handle information in prescribed ways and will ensure the validity of software that may need to be imported.

These and more aspects (see Fig. 12) form the boundary conditions of the playground for future automation security research and development.

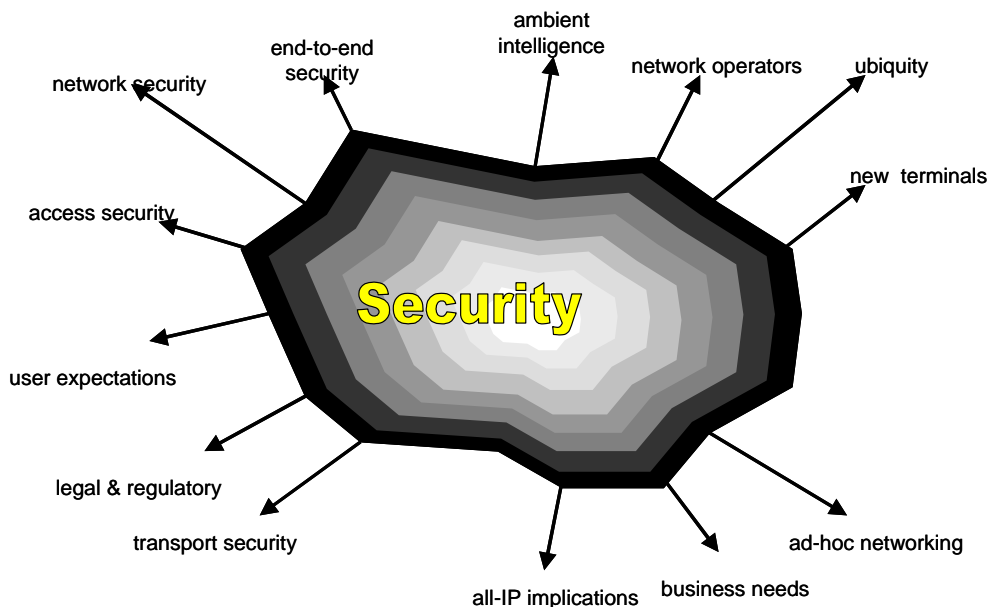


Fig. 12 Boundary conditions for future automation security

#### 6.1.4 Trends

The explosive growth in wireless networks and services over the last few years, can be characterised by a notorious lack of effective security. For instance, deployments of the IEEE 802.11b based WLAN

standard, one of the most prominent WLAN technologies available today, often feature very little security control and potentially present a 'backdoor' gateway to gain unauthorised access between devices and data, systems and networks. Also, the Wireless Application Protocol (WAP) showed serious security gaps after its introduction and Bluetooth, again, has been widely deployed without adequate security measures. Vulnerabilities in these technologies leave them open to eavesdropping, session hijacking, data alteration and manipulation, and an overall lack of privacy.

Security measures are gradually being added, but these additions do not offer a sufficient level security. Current solutions lack the flexibility and interoperability that is needed for securing reliable data communications.

Limitations and inherent vulnerabilities of wireless security are:

- Access points are easily accessed by users outside the physical location;
- Eavesdropping is relatively easy, difficult to detect, and can be done from afar;
- Many wireless/mobile technologies do not have built-in authentication measures;
- Encryption of data and key management procedures have been found to be flawed many times.

Despite the existence of security solutions, often they are not used to their full extent: security may be switched off or a sub-optimal level of security is used. Why is this? The reasons for omitting or neglecting security vary. Most enterprises still do not apply security measures because they inconveniences to both workers and managers, and are widely seen as acting as a brake on progress and as being counter-productive. Moreover, most information technology security breaches and incidents take advantage of known, patchable flaws that exist because of poor enterprise security practices, bad corporate culture and a lack of investment in system protection. Other reasons for poor security are:

- Rapid development of technology to meet high user expectations;
- Implementing good security is seen as too much work in a compressed time line;
- Building secure software is a complicated endeavour, particularly because software technology is constantly evolving and many companies have yet to focus on software as a critical piece in the security puzzle;
- Many industries just did not emphasise security in the past;
- Despite affected sales, many industries have deferred the decision for security until a proper solution is found;
- Most consumers are not concerned about security today;
- Careless software installation and maintenance (e.g. security patches are not installed, WLAN encryption protocols are not turned on, etc.);
- Managing passwords is seen as burdensome; consequently, many passwords are shared and rarely refreshed;
- Laws in certain countries restrict the length of the encryption keys used for export, import or use;
- Limited processing power and storage capabilities of the device;
- People are not aware of the potential threats and their consequences when security is not in place and need to be educated about the risks;

Current solutions lack the flexibility that is needed for securing data communications and are therefore switched off [AB02].

From these examples it is obvious that often a combination of technical, human, social, economic and legal factors lie behind incorrect use of security.

Fortunately a long-term cultural shift seems to be under way. Digital security has been growing in importance in recent years, as more and more aspects of business have come to depend on fixed and mobile terminals. New technologies, facilities and capabilities will generate new requirements for security of service information, protection of services and other digital assets, safety and integrity of management and control of underlying systems and infrastructure. New trends include general ubiquity, new context-aware applications and services, new network and terminal technologies, flexible spectrum management and dynamic reconfiguration of terminals and networks in response to capacity optimisation.

In short, computing is in the midst of a transition from an optional tool to a ubiquitous utility. People expect utilities to be reliable and secure. And these trends from the office domain project to the automation domain in several areas.

## 6.2 Needs for security

Security is a basic feature of any public communication infrastructure whether fixed or mobile; it must provide user confidence and economic opportunity and must protect the values of society. Security of information and communications plays a fundamental role in ensuring that European Economy realizes benefits from these services.

Already most communication of sensitive *data* on the fixed networks is subject to some protection. but, because of the dynamic topology and connectivity, security is fundamental to the successful operation of all aspects of wireless systems and must be given consideration in all new research and development undertakings in this field. It must be an essential part of the architecture in terms of placement of functionality, protocols and mechanisms – *what* goes on *where* and *how*.

The following standard security issues need to be addressed in many new contexts:

- *Privacy*: keeping information confidential; preventing disclosure to unauthorised users;
- *Access control*: permitting only authorised users to access specified information and services;
- *Integrity*: providing assurance that information has not been tampered with during handling;
- *Authentication*: providing proof of the *credentials*<sup>5</sup> of the originator of information or a participant in a service;
- *Non-repudiation*: preventing a participant in a service or transaction from denying having taken some specific action.

The VAN process of identifying requirements was mainly an analysis of extensive sources and externally available material (e.g. from the IRG, ISTAG, WWRF, etc.). The project constructed a number of application scenarios, based on diverse realistic assumptions about future technologies, applications and business situations using available input material to describe actors, technologies, and communication models of the scenarios. Requirements for privacy, security, and data protection were described from each actor's point of view. Requirements were then grouped, structured and prioritised. Of particular interest was the work of related roadmap projects, including AMSD ([www.amsd.org](http://www.amsd.org)), RAPID ([www.ra-pid.org](http://www.ra-pid.org)), RESET ([www.ercim.org/reset](http://www.ercim.org/reset)), and STORK ([www.stork.eu.org](http://www.stork.eu.org)). In the next step, the research challenges were extracted from the requirements, and a first tentative recommendation of priorities was given.

An outline of requirements for security is given below.

---

<sup>5</sup> *Identity* may not be the only attribute to be authenticated; other attributes such as location, functionality, or capability may be more significant in certain circumstances [Za02].

## 6.3 Legal drivers for security

Effective regulation plays an important part both in the initial and ongoing shaping of liberalized telecommunications markets. The specific processes and structures for implementing interconnection, access, pricing and other regulations will shape the market, and thereby shape the extent and significance of universal service problems.

Law/self regulation challenges are:

- Appropriate for all types of Information Society services and applications;
- Protect key interests such as consumer rights and privacy;
- Involve all actors;
- Promote self-regulation and co-regulation;
- Simple, flexible and technology-neutral.

Policy measures can be more effective if they are part of a pan-European approach, respect the effective functioning of the internal market, build on increased co-operation between member states and internationally, and support innovation and the ability of European enterprises to compete at global level. [RAPID]

A very important subject with any new technology is deciding how current laws deal with new issues that might be raised by a new generation of products. In the following sections we shall address several drivers for privacy and security.

Issues that cannot be tackled technically or are hampered by social or economical forces may perhaps only be solved via legislation. For instance, governments usually push the introduction of smartcards for identification of citizens since there is little economical or social support for it; even though it is technically possible. [Cyb01]

### 6.3.1 Trusted computing platforms

A truly secure computing platform might reduce the threat private data exposure to unscrupulous data processors. A secure computing platform could make enforcement of the legal use of data possible. For instance, a data controller might require data processors to use a secure computing platform to access personal data.

The EU directive on a Community framework for electronic signatures has some requirements on the 'secure signature-creation device', a device that creates an electronic signature in a secure way. The private key has to be under exclusive control of the owner of an electronic signature. The secure signature-creation device is often a smart card, but it could be a mobile device as well if it complies with the requirements of the EU directive.

### 6.3.2 Cyber crime

An issue of growing concern is the challenge posed by the emergence of cyber-crime, such as electronic money laundering, illegal money gambling, malicious hacking, or copyright infringement. International cooperation is already well advanced in a number of key areas, such as the fight against organised trans-national crime on new communication networks. Faced with new forms of high technology and computer crime on global networks (reported criminal hacking cases are doubling every year), governments have responded vigorously [6].

In Europe (Europol), as well as in the wider international environment (P8), specialised task forces have been set up, and trans-border operational cooperation reinforced in such key areas as the real-time "trap and trace" of online criminals and "search and seize" of digital evidence. Efforts are similarly being made to harmonise the criminalisation of computer offences and avoid digital havens. A high-level Group, set up following the Dublin Council, is finalising an Action Plan to fight cyber crime. These efforts are crucial to reinforce trust and confidence in trans-national electronic commerce.

### 6.3.3 Roaming

With wireless networks it is not always easy to determine where we are connected. While moving around our own property it might be possible to inadvertently connect to the access point of the neighbour's wireless network because its signal is more powerful. It might be possible to unintentionally damage or overload the network by using bandwidth or other resources. Who is going to pay the bill if this neighbour gets billed for exceeding his bandwidth usage from his ISP? What does the law say about this?

To address this issue, the FBI stated in a memo to its agencies: "Identifying the presence of a wireless network may not be a criminal violation, however, there may be criminal violations if the network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, theft of trade secrets, and other federal violations."

### 6.3.4 Challenges

A sound and flexible regulatory framework, which generates confidence for both business and consumers and ensures full and unlimited access to a single market, is an essential key to Europe's success. Such a regulatory framework will be a major competitive advantage in itself. Steps must also be taken to improve the business environment: to exchange best practices, facilitate access to venture capital and stimulate training. Ultimately, global solutions must be found. The Community should be in the lead in exploring and offering solutions at an international level.

Europe, the US and the Asian Pacific area share a strong interest in the development of the global telecoms system. Market opening is crucial. The aim of regulators must be to open markets and ensure pro-competitive market structures for the choice and benefit of the users and as a base for the development of our countries. All regions must have the opportunity to contribute their best technology. The result should be systems reflecting best global practice and experience.

A substantial body of legislation relevant to network and information security is already in place, notably as part of the EU's legal framework for telecommunications, electronic commerce and electronic signatures. However, the rise of new services that fully exploit the inherent characteristics of e.g. mobility automation devices (e.g. location and context awareness), impose new legal requirements on providers of such telecommunications services to take appropriate technical and organisational measures to safeguard the security of their services. As well as further research on the development of technologies and organisational measures in order to provide an appropriate level of security, a corresponding and appropriate legal framework must be defined as well.

Large-scale introduction of wireless networks (e.g. wireless local loop, wireless local area networks, third generation mobile) will bring the challenge of effectively encrypting data transmitted over radio signals. It will therefore be increasingly problematic to require by law weak encryption of those signals.

There is a scope for the government to further review developments in convergence between telecommunication and broadcasting. In particular, as regards merging legal frameworks to ensure that carriage regulation comes within the scope of a single regulatory framework.

## 6.4 Integration of security functions into the IP stack

### 6.4.1 Overview

With the introduction of the next generation internet protocol other extensions than just the address space were implemented and provide several security related functionalities such as the integration of IPSec.

IPv6 offers some features like anycast (increases availability by adding stand by routines on the network level), IPSec (encryption in every end device without additional software), strongly hierarchical address distribution (easier routing and access control configuration), the abolition of NAT (with its overrated security "function", now more precise filtering rules), local address prefixes (stronger than RFC 1918, site local and link local) and device classes (identification and addressing of all routing instances in a network) which definitely have a strong impact on the design of a secure network.

IPv6 is a definite path that most networks will follow within the next years. The US American government plans to be using this next generation internet protocol throughout all institutions by 2008.

### 6.4.2 Evolution

The graph shows the number of entries in the routing table of a large network provider from 10-Feb-2003 2010 to 19-Jan-2006 showing a steady growth but without the explosive trends of the IPv4 world. One has to keep in mind that this moderate increase is mainly due to improvements in the effectiveness of routing entries in the specification of IPv6.

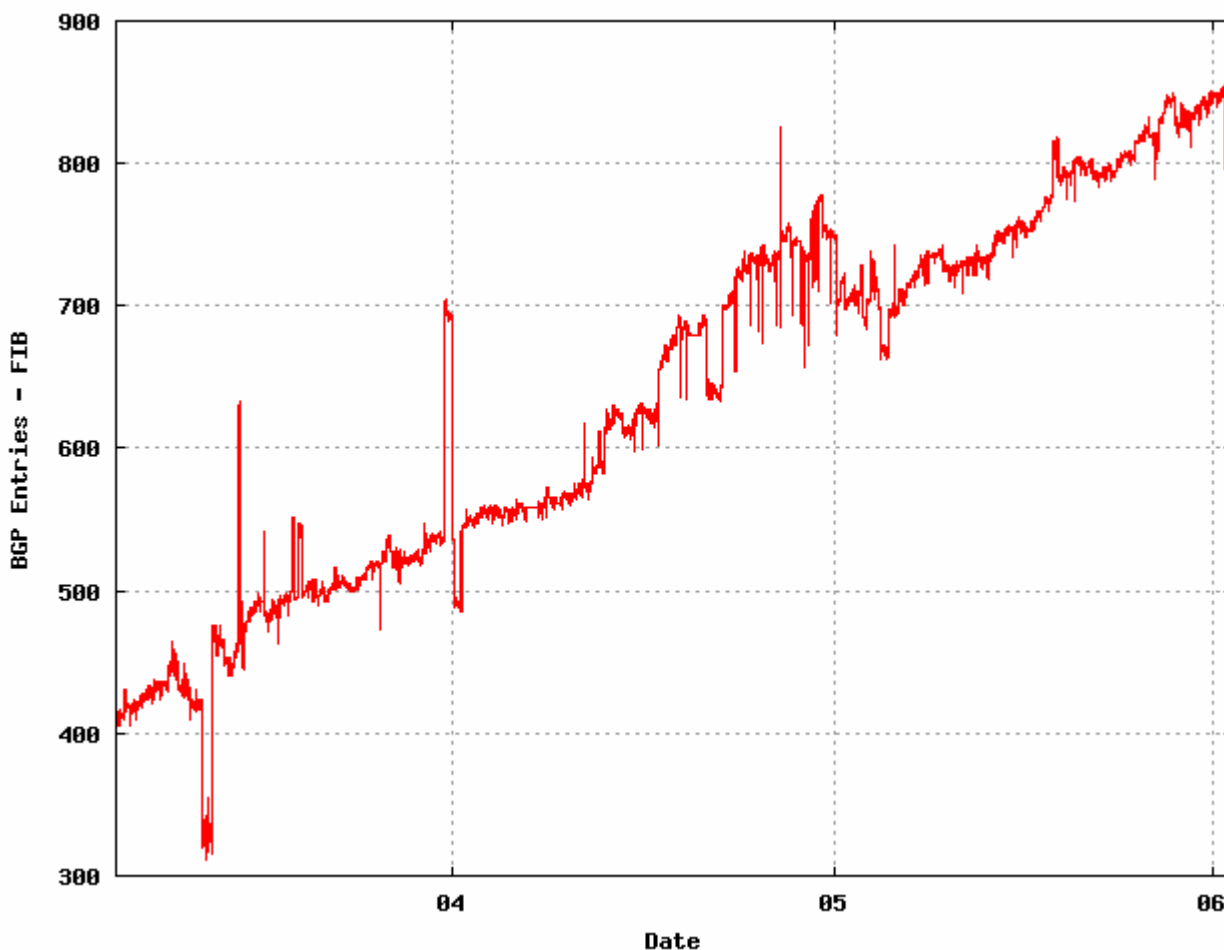


Fig. 13 Large network provider routing entries evolution (Feb. 2005 - Jan. 2006)

### 6.4.3 Maturity

IPv6 is an existing and usable standard. Most parts of it are fixed and the areas still being worked at can be clearly identified and isolated.

Implementations exist for all major operating systems including embedded OS like VxWorks and QNX. On 20 July 2004 ICANN announced that the root DNS servers for the Internet had been modified to support both IPv6 and IPv4.

## 6.5 Elliptic curve cryptography

### 6.5.1 Overview

ECC is a public key crypto process based on the mathematical construction of elliptic curves. It's an attractive alternative to the currently best known asymmetric algorithm RSA. The underlying mathematical problem is –similar to the DSA approach – the calculation of a discrete logarithm in a finite set, here in a set of points in an elliptic curve.

The difference to other asymmetric methods is in the drastically higher complexity of the underlying math. While with RSA (and DSA) elementary knowledge of modular arithmetics is sufficient, the implementation of elliptic curve crypto requires clearly more know-how especially in the choice of adequate system parameters.

The crucial advantage is that known fast algorithms to solve the discrete logarithm problem in finite bodies, which DSA is based on, cannot be applied here. As there are only general operations for the DL problem in the point cloud of elliptic curves available drastically shorter keys and parameters are sufficient without reducing security. This is especially suitable for limited resources as in embedded devices.

### 6.5.2 Evolution

ECC is the first variant of the asymmetric encryption method RSA algorithm. Like the RSA algorithm, the ECC technology is based on a mathematical problem: the calculation of discrete logarithms (DL) in suitable amounts.

Since its proposal by Victor Miller and Neal Koblitz in the mid 1980s, Elliptic Curve Cryptography has evolved into a mature public-key cryptosystem. Extensive research has been done on the underlying math, its security strength, and efficient implementations.

Since then ECC has been introduced into the following standards:

- ISO/IEC 14888-3: "Digital Signature with Appendix Part 3: Certificate-based Mechanisms"
- ISO/IEC 9796-4: "Digital Signature with Message Recovery, Discrete Logarithm based Mechanisms"
- ISO/IEC 15946: "Cryptographic Techniques Based on Elliptic Curves", I-III,

### 6.5.3 Maturity

The description of the level of maturity and standardisation is easiest illustrated by the acceptance by users usually highly concerned with security: There is a vision that elliptic curve based cryptography is going to replace cryptography based on integer factorisation (e.g., RSA) and finite-field cryptography (e.g., DSA). At the RSA Conference 2005 the National Security Agency (NSA) announced Suite B which exclusively uses ECC for digital signature generation and key exchange. The suite is intended to protect both classified and unclassified national security systems and information

## 6.6 ID-based cryptography

### 6.6.1 Overview

Identity-based systems allow any party to generate a public key from a known identity value such as the VAN ID. A trusted third party, called the Private Key Generator (PKG), which might be the VAN CA, generates the corresponding private keys. To operate, the PKG first publishes a "master" public key, and retains the corresponding master private key. Given the master public key, any party can compute a public key corresponding to the identity I by combining the master public key with the identity value. To obtain a corresponding private key, the party authorised to use the identity I contacts the PKG, which uses the master private key to generate the private key for identity I.

## 6.6.2 Evolution

The first identity-based cryptosystem was a signature scheme developed by Adi Shamir in 1984, which allowed users to verify digital signatures using only public information such as the user's identity. Modern schemes include Boneh/Franklin's pairing-based encryption scheme, and Cocks's encryption scheme based on quadratic residues.

Today most systems available are using a users ID such as the email address as the basis to create the public key of the user.

## 6.6.3 Maturity

The use of ID based systems is not yet as wide spread as other flavours of public key encryption but has gained a substantial importance in some specific fields.

Unfortunately, all identity-based cryptographic schemes have inherent weaknesses, a "key escrow" property because the PKG issues private keys for user using its master secret key. As a result, the PKG is able to decrypt or sign any message. In terms of encryption, this property might be useful in some situations where user's privacy can possibly be limited. For example, due to the involvement in the crime, the user's message should be opened by a court order. However, in terms of signature, this key escrow property is not desirable at all since the "non-repudiation" property is one of the essential requirements of digital signature schemes.

As long as IBE does not overcome this issue with a widely adopted scheme it can not be considered as mature enough to be used in VAN.

## 6.7 Group keying

### 6.7.1 Overview

Many scenarios involving multi-party automation communications assume the existence of efficient cryptographic protocols for dynamic group keying. While 'theoretical' protocols already exist in the cryptographic literature, work is needed to ensure these are sufficiently lightweight and reliable in the automation setting.

The main purpose of group keying is to ensure that encrypted communication is not only possible in a point-to-point scenario where the two partners actually exchange and verify their keys and make sure that no other instance with access to the communication line can actually listen to or actually participate in this communication. This is not suitable for multicast environments or other groups with one-to-many or many-to-many communication schemes.

In order to solve this problem different architectures have been approached:

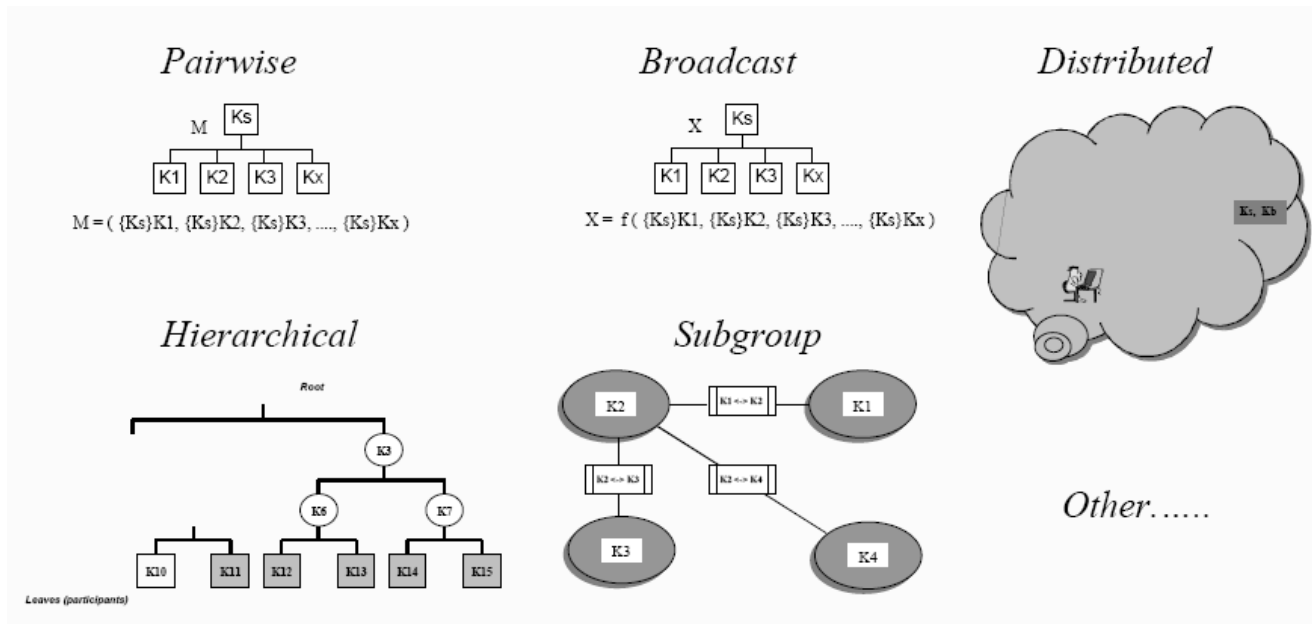


Fig. 14 Architecture approaches

The pros and cons of these have been assembled here:

Architecture	Advantages	Disadvantages
<b>Pairwise</b>	<ul style="list-style-type: none"> <li>Simple and straight forward approach.</li> </ul>	<ul style="list-style-type: none"> <li>Not scalable to large groups.</li> <li>Not efficient for providing perfect forwards/backwards secrecy.</li> </ul>
<b>Hierarchical</b>	<ul style="list-style-type: none"> <li>Scales logarithmically because of hierarchical design.</li> </ul>	<ul style="list-style-type: none"> <li>Changes in group membership require group key to change.</li> <li>Addressing required for key material.</li> </ul>
<b>Broadcast</b>	<ul style="list-style-type: none"> <li>Anonymity for rekey.</li> <li>Common rekey package.</li> </ul>	<ul style="list-style-type: none"> <li>Processing may approach pairwise techniques.</li> </ul>
<b>Distributed</b>	<ul style="list-style-type: none"> <li>Robust -&gt; any active participant can distribute key material.</li> </ul>	<ul style="list-style-type: none"> <li>Trust is distributed.</li> <li>Membership lists or CRLs must be synchronized.</li> </ul>
<b>Subgroup</b>	<ul style="list-style-type: none"> <li>Membership changes only affect subgroup level</li> </ul>	<ul style="list-style-type: none"> <li>Architecture is not inherently robust</li> </ul>

Tab. 5 Pros and cons for each architecture approach

## 6.8 Additional Trends

### 6.8.1 Trusted and secure automation devices

End-to-end security protocols can only be meaningful between properly secured end-points. Automation devices with a secure default configuration need to be provided. Trusted paths from the automation device to the user need to be foreseen (“what you see is what is happening”). A good balance should be found between allowing potentially dangerous tools (such as code) and enforcing the appropriate usage of them (i.e., in security applications).

Furthermore, substantial research and development efforts concerning trusted execution environments (operating system and hardware platform) for automation devices still are of paramount importance. There seems to be a fundamental conflict between, on the one hand the desire for user-friendliness, functionality, openness and freedom, including the user's right (in a non-organisational context) to disable/enable and configure the security features of this platform, and on the other hand the level of security that such a platform can offer. If users have options to choose, it will always be possible to lure them into choosing the least secure configuration, and whatever security the platform could offer will be circumvented. This might not be a problem for the few experienced users, but it is a real threat for all the inexperienced end-users.

Thus, a secure and trusted device is a core ingredient for secure automation solutions. We need more research into and development of devices that provide just enough user-friendly functionality and still remain authentic and trustworthy.

### **6.8.2 Secure reconfiguration of automation devices**

Security issues concerning the reconfiguration of automation equipment heavily depend on the kind of data to be transferred to the automation device (such as pure application software, software updating the equipment's operating system, software and parameter data modifying the radio properties of a mobile device, data used to reconfigure FPGAs) and on the entities involved in the reconfiguration process (such as software providers, network operators, device manufacturers, the device, its user). The conceivable reconfiguration scenarios can be rather complicated, and for such scenarios, it will probably not be possible to provide a reliable security architecture. Current reconfiguration scenarios that serve the needs of the different entities involved and that simultaneously allow for trustworthy security solutions cannot be seen as providing a complete picture, and must therefore be addressed by future research.

With respect to a given, concrete reconfiguration scenario, security issues concerning authorisation (who is permitted to initiate and execute the download), data origin and integrity, privacy (not everybody should know which software is on a certain automation device), and conformance with regulatory requirements have to be investigated. In addition, protection mechanisms have to be in place to meet the requirements of network operators. The main issues are the split of authority for reconfiguration in decentralised scenarios, and approaches to dealing with failures. Furthermore, some reconfiguration scenarios may require investigation of digital rights management, confidentiality and non-repudiation issues.

### **6.8.3 DRM security architectures and protocols**

Today's DRM standards and proprietary DRM solutions still have many shortcomings and security weaknesses. Many of them are based on obfuscation and security by obscurity. A good DRM system should be secure even if all technical details are published. This requires underlying security technology components like tamper-resistant memory, tamper-resistant execution environments, tamper-resistant network interfaces, secure clocks, device specific keys and certificates. Using such secure components and secure environments, secure DRM architectures can be developed by specifying suitable data formats, and authentication and data exchange protocols. Such secure DRM architectures have yet to be developed to maturity, and to be tested and scrutinised.

### **6.8.4 Protection of the virtual network against attacks**

Automation networks are opening up more and more, leading to an increased vulnerability to both internal and external attacks (and failures). There is a need to research mechanisms that reduce the risk of attacks against the core network.

Of particular importance is protection against Denial-of-Service attacks, which becomes increasingly important as IP becomes ever more pervasive. Trust assumptions valid today that allow hop-by-hop security solutions in the network may be no longer valid, and may necessitate alternative solutions for core network security in the future. The partial sharing of network resources (e.g. radio access networks) among operators raises many security issues. A means to counter Denial-of-Service attacks in the network is the use of intrusion detection tools. Such tools need to be tailored to the

requirements of the automation telecommunications environment to be effective. The range of Internet solutions for IDS is quite broad, but investigation of adaptation and enhancements of existing solutions and standards is required for the special case of an automation infrastructure.

Other forms of attacks against networks, e.g. eavesdropping, impersonation or viruses also require research.

Protection could for instance be improved by conducting systematic threat analysis and by designing a catalogue of countermeasures against e.g. Denial of Service and Distributed Denial of Service attacks. Those could include cryptographic measures (cookies, client puzzles, etc.) as well as networking measures (intrusion detection systems, active networking technology). Research in network protection is of utmost importance.

### **6.8.5 Heterogeneous network access control security**

The increasing heterogeneity of the networking environment is one of the long-term trends, which requires new security approaches [Mel02]. The main challenges include:

- The investigation and development of unified, secure and convenient authentication mechanisms that can be used in different access networks and for different services (single sign-on). Authentication and key agreement is the central component of secure access procedures. Currently, there are no protocols available that are light-weight, can be carried over arbitrary access networks and are flexible enough to be re-used in many different contexts in future systems. The development of new authentication protocols may be required here.
- In addition to the key agreement, the efficient negotiation of security contexts is not available in some settings. The secure negotiation of configuration information is also an open issue.
- Access procedures need to be hardened against Denial-of-Service attacks.
- Today's access procedures do not provide non-repudiation.
- Architectures for the flexible use of different types of access credentials need much further research and standardisation.
- Efficient key distribution for multicast remains a research topic.

### **6.8.6 Seamless security handover at the network level**

Seamless handover means that a user can switch between points of attachment to networks with performance guarantee and without experiencing degradation in the quality of the service. Currently this is only possible between networks of the same or similar type. Security is an issue here, as re-authentication often causes prohibitive delays, so efficient security context transfer schemes are needed. Security solutions still need to be developed for seamless handover between different network types.

### **6.8.7 Protection of service networks against attacks**

Service networks offer numerous internal and external interfaces. Some of the communication partners might change frequently, for instance external service providers or end-users.

### **6.8.8 Application security framework**

Given the growing heterogeneity of the user's communication environment, there is a need to develop and validate a coherent framework for security and trust for automation applications. The traditional approach to security is to adopt a layered architecture to solve specific aspects of an overall problem. However, what is needed is a holistic, comprehensive approach to security for automation systems, as the security of a system is only as strong as the weakest element. Key elements of the framework are a suitable architecture for automation applications and a methodology guiding the use of the framework. Security architectures need to ensure that the user can access a multitude of applications with only one or a small number of access credentials, using unified, easy to use procedures [Pampas03].

### **6.8.9 Single sign-on based on authentication**

Single sign-on is currently driven by the (non-European) IT giants. There is, however, a chance, that automation suppliers, could play an important role in single sign-on solutions. Investigations should include not only technical aspects but also end user experience.

### **6.8.10 Authorisation privacy**

Authorisation plays a particular role on privacy, since too often a lot of private information is distributed to enable access control. In particular, the client-server model, on which most Internet applications are developed, can be considered as privacy-intrusive: generally, the server grants or denies access to a client according to the identity claimed by the client.

In many cases, the user should be allowed to access services by providing, instead of his identity, a proof that he is authorised, e.g. an attribute certificate proving his organisation membership, or that he is certified to perform a certain task. Different certification authorities could issue such attributed certificates, which is a way to implement multiple identities. Zero-knowledge can be used to guarantee that the certificate belongs to the user. Of course, the management of multiple identities raises problems of ease-of-use, as well as unlinkability [SANS01].

Another related approach is to use cryptographic functions to prove certain attributes of a certificate without disclosing other attributes.

More research is needed to develop similar solutions and experiments on large-scale operations should also be supported.

### **6.8.11 Lightweight stream ciphers**

Research is needed to develop lightweight stream ciphers with a well-understood level of security for application in constrained environments. Current efforts such as NESSIE have not resulted in such primitives.

### **6.8.12 Truly practical cryptographic mechanisms in constrained environments**

Making truly practical in constrained environments the cryptographic mechanisms associated with payment, digital rights management, privacy and anonymity protection are a challenge to cryptography from automation applications. These mechanisms include special signature schemes and key exchange and authentication protocols.

### **6.8.13 Delegation of cryptographic operations**

Further research is needed to develop mechanisms that support delegation of cryptographic operations from constrained automation devices to more powerful and more trusted devices.

### **6.8.14 Lightweight key management infrastructures**

There is a need to develop and standardise lightweight key management infrastructures supporting the deployment of public key technology in automation networks, and to ensure the interoperability of infrastructures from different telecommunication/wireless standards..

## **6.9 Research issues summary**

Taking into account all relevant criteria for automation security and privacy we can summarise the results as follows.

To establish a coherent future for automation trust and security in the developing automation world, it is of paramount importance to consider security as a fundamental pillar from the beginning of the design. Traditional approaches are not holistic enough to cover all the approaching technology interactions. Networks of services can only be built on a trustworthy foundation of solid interworking security.

The increasing heterogeneity of radio technologies like UMTS, WLAN and Bluetooth in the new mobile environment is one of the most visible trends [ITU02]. Flexible authentication and authorisation procedures have to be in place to provide access to all these networks. Different types of credentials and context provided at different layers and secure sessions need to be handed over when dynamically changing network connections. Single sign-on (SSO), which is currently driven by non-European IT companies, can provide a unique opportunity for mobile network operators who can integrate SSO into their systems and provide a comfortable usage environment to the user.

Future automation networks offer numerous interfaces toward users and service providers. Some communication partners might change frequently. To provide services without intensive security consideration would pose a high risk to the infrastructure, but also to the services provided. The list of threats range from Denial of Service attacks, injection of malicious code, viruses, worms, hijacking of sessions and servers, to the stealing of confidential information. To protect the service networks and core networks, intrusion detection systems, proxies, firewalls and other technologies that are suited to the mobile environment have to be investigated. If these concerns are not addressed the whole deployment of new services is at risk [Pampas02].

Numerous security and privacy enhancing tools have already been investigated (e.g. signature schemes, DRM, authentication protocol etc), but many of these fail in constrained environments. The current practical requirements of security and privacy tools need to be investigated and their efficiency (round trip time, usage of memory, etc.) and performance to be tested. Other required functionalities have not been investigated from a lightweight perspective at all, e.g. stream ciphers, key management infrastructures and conference and group keying. Automation profiling of security and privacy functions (e.g. outsourcing expensive operations to servers) could build a cornerstone of the new security approach for the automation environment.

## 7 Trends in co-operation of private and public networks

### 7.1 Trends in General

On the one hand a permanent growth of private networks in firms, authorities, and private homes can be observed. On the other hand a fast further development of internet technology can be registered.

Internet technology offers powerful and simple to handle network services such as e-mail and WEB browsing. Therefore the connection of private networks among each other and with the internet by using public networks is also an increasing trend.

Moreover, the new technical innovations spawn, for instance mobile phones, multimedia devices, or electrical appliances with integrated internet interface, over the next few years. With the rising number of network participants, the network traffic increases continuously. The kind of data is also changing more and more from textual data to multimedia data such as videos and voice. This fact leads to relevant increased network traffic.

According to the increasing claim to the public networks, the underlying techniques develop further.

The steady changeover from remote data transmission to broadband networks allows new pretentious network services such as e-commerce and multimedia services. This enables above all the higher data throughput of the broadband networks. Fig. 15 shows the rising divulgence of broadband networks in percent for the next 15 years.

Simultaneously the growing use of the Voice and other multimedia services (triple play over IP) increases the overall volume of transmitted data, requiring backbone providers to increase throughput and hence the availability rises and market prices for broadband access decrease.

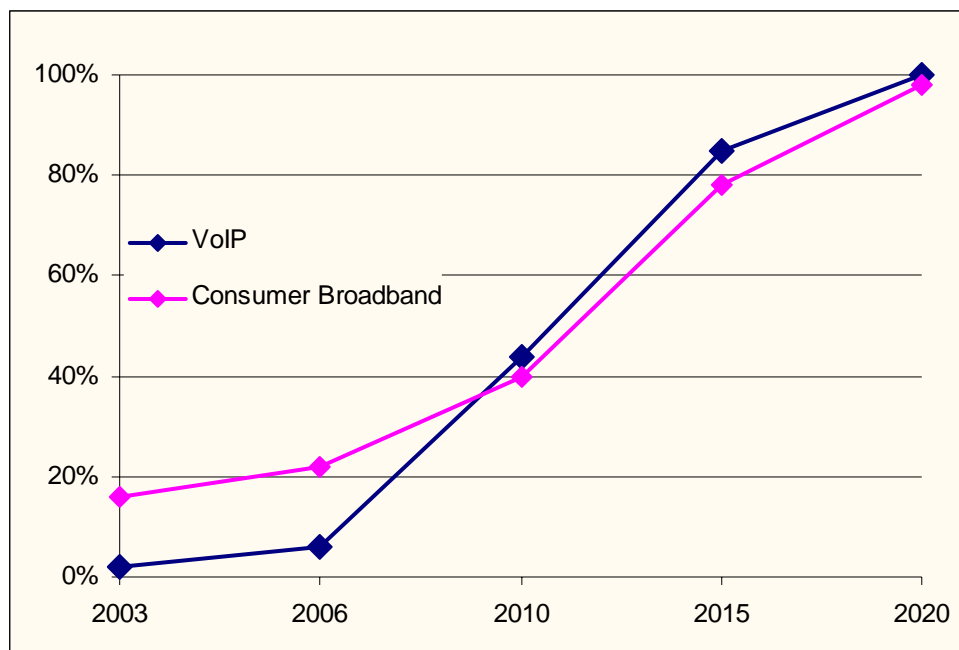


Fig. 15 Divulgence of VoIP and Broadband (Source: Forrester Research)

Because of the large amount of internet users and the common and cheap possibility to access the global network, new requirements regarding security aspects can be expected. Negative aspects of the world wide connectivity, such as worms and viruses, spam, denial of service or hack attacks, must be considered and special measures i.e. access right management or data encryption must be taken.

The development of the gateways which implement the connection from the private to the public network is a further important item. The currently simple data router is being replaced more and more by gateways which contain security features such as Firewalls, VPNs, e-mail filter, access control etc. This enables the use of the public network for confidential data.

Besides the security aspects, the new gateways are equipped with diverse user-friendly network tools and features to manage the gateway. Moreover other features for multimedia, VoIP and data storage are being included in the future.

Public networks are often used by office domains, where IP-based communication i.e. for internet has a large stake in the whole traffic. Because of the trend that communication in automation will be more and more based on Ethernet together with the internet protocol suite or special automation protocols, the data exchange between plants and via public networks must be considered.

One question of a future marketplace is how fast providers can deliver the unique packaging of applications and network services to meet the needs of a great number of consumers and businesses. Therefore, service providers have to adapt their offered services and service level agreements rapidly regarding these requirements. In this case cost efficiency and greater scalability are important terms.

Future high-performance infrastructures will also be based on optical networking. They are characterised by efficient switching and routing and the support of flexibility to handle any network protocol. Next-generation wireless networks will provide seamless roaming and transparent access to the internet no matter where users live or travel. Therefore the wireless radio transmission is a further aspect of public networking with growing impact.

### **Usage of IPv6 versus IPv4**

The internet protocol version 6 [RFC1883] (often called IPng - next generation) implicates a long-dated increase of growth [Sor04]. IPv6 offers many qualities to support the mobility, the security, and above all the growing of the world wide networking. The migration from IPv4 to IPv6 began slowly in 2005. IPv6 offers four times as many internet addresses as IPv4. Therefore not only computers but also mobile phones, cars, refrigerators and subsystems can be uniquely addressed.

However, in the western world IPv6 is presently not absolutely necessary and therefore out of scope because there is no lack in available IPv4 addresses. The Americans have reserved about 70% of the available IPv4 addresses. The remainder is reserved by the Europeans. In these regions more than 50% of the assigned addresses are still free. Also improved technical aspects of IPv6 do not lead to switch the technology immediately because sufficient and approved workarounds like NAT (Network Address Translation) are available. Only a small part of the IPv4 address range is available for internet newcomers such as South America or Asia. That is why i.e. the market of China is able to push the divulgation of this technology into the next future [Hill05].

### **More Autonomous Systems for IPv6 registered**

The classic definition of an Autonomous System is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS, and using an exterior gateway protocol to route packets to other ASes.

Since this classic definition was developed, it has become common for a single AS to use several interior gateway protocols and sometimes several sets of metrics within an AS. The use of the term Autonomous System here stresses the fact that, even when multiple IGPs and metrics are used, the administration of an AS appears to other ASes to have a single coherent interior routing plan and presents a consistent picture of which networks are reachable through it.

The number of AS for IPv6 has been growing constantly over the last decade but there was no corresponding increase. Just in the last few years the acceptance of Version 6 became a driving force for network operators to actively claim a share of the address space and accordingly set up and register Autonomous Systems.

### **Move from dedicated leased lines to virtual private networks**

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The main purpose of a VPN is to give the company the same capabilities as private leased lines at much lower cost by using the shared public infrastructure. Phone companies have provided private shared resources for voice messages for over a decade. A virtual private network makes it possible to have the same protected sharing of public resources for data. Companies today are looking at using a private virtual network for both extranets and wide-area intranets.

Falling internet access costs, the wide availability of broadband connections, the move from classical Voice lines to Voice over IP and the availability of suitable encryption solutions have been the cause for many companies to switch from exclusive, expensive leased lines to packet switched networks with encrypted tunnels.

### **Reduction of complexity in routing by using MPLS**

Multi-Protocol Label Switching (MPLS) was developed as a packet-based technology and is rapidly becoming the key for use in core networks, including converged data and voice networks. MPLS does not replace IP routing, but works alongside existing and future routing technologies to provide very high-speed data forwarding between Label-Switched Routers (LSRs) together with reservation of bandwidth for traffic flows with different Quality of Service (QoS) requirements.

MPLS was originally proposed by a group of engineers from Cisco Systems, Inc.; it was called "Tag Switching" when it was a Cisco proprietary proposal, and was renamed "Label Switching" when it was handed over to the IETF for open standardisation.

Today MPLS functions can be provided by a lot of brands of networking devices and are most commonly used by infrastructure service providers reducing the overall complexity of routing tables. This is achieved by a tunnelling scheme (labelling) which covers the complexity of attached networks. Attaching a customer's network for the service provider means accepting any traffic delivered at one perimeter router to be transported to the according end point without further routing decisions other than those implied by the own network structure. At the end point the covering label is removed and the customer takes care of the packet.

Even though the initial intention of routing any protocol via MPLS today there is a vast majority of purely IP transferring links in operation.

### **Increasing use of synchronous data transfer technologies in time critical applications**

The network provider constitutes more and more the trend-setting technique SDH. The Fig. 16 shows the trend from the year 1988 until the year 2000. This trend will continue during the next few years.

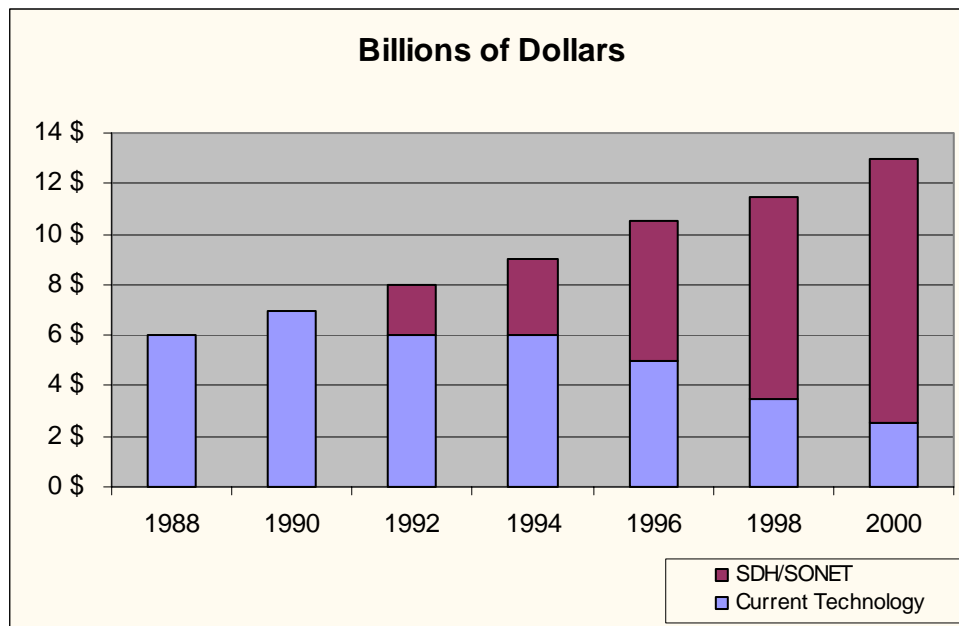


Fig. 16 Worldwide distribution of the plesiochronous and synchronous technologies (Source: Dataquest, 1997)

Unlike the previous techniques such as PDH, SDH offers the following qualities:

- high transfer rates up to 10 GBit/s (The chips coming on the market can handle up to 622Mbit/s speeds. [Ele04])
- simple add & drop functionality
- high availability and effective use of the network capacity
- several automatic security mechanisms and resiliency
- future-proof platform for new services such as Video-on-Demand or Digital Video Broadcasting over ATM

In [Ele04] two important trends concerning Sonet/SDH are shown.

The first trend centres on the interrelated goals of building new and more network resiliency, more bandwidth on demand and more revenue-generating services into Sonet/SDH equipment. The new technology is flexible enough to dynamically change the level of protection and priority for a customer service, allowing on-demand resiliency and quality of service.

The second trend focuses on Sonet/SDH equipment and chip integration that is driving reduction in Sonet/SDH equipment and chip costs. The chips are becoming highly integrated with Ethernet, framing, and network processor traffic management-functions typically executed on separate chips.

### Decrease in use of ATM

ATM was intended to provide a single unified networking standard that could support both synchronous channel networking and packet-based networking simultaneously while providing multiple levels of quality of service for packet traffic. [Wiki05]

ATM has been accepted by most analysts as the technology of choice for future high-performance networks. A recent Gartner Group report in 1996 stated that Gigabit Ethernet should not be considered as a replacement for enterprises looking to implement ATM because it was believed that ATM will remain a superior technical solution for LAN and WAN backbones. Moreover of the requirements on wide bandwidth came from multimedia applications since ATM was designed with multimedia transmissions on mind so even 25 Mbps ATM LAN connections would match 100 Mbps Fast Ethernet connections for performance. IBM in their document [IBM1] claims that *"It's not all about raw speed. Control, flexibility, adaptability, cost, and manageability are all significant aspects."* Quality of Service is an important issue for many applications. The network delay, jitter, and packet loss ratio,

are very important when dealing with real-time applications. Fast Ethernet has no notion of QoS and therefore compares to an Unspecified Bit Rate (UBR) in ATM, ATM's lowest QoS. ATM has three higher service levels defined in its architecture. [IBM1]

Numerous telecommunication companies have implemented wide-area ATM networks, and many ADSL implementations use ATM. However, ATM has failed to gain wide use as a LAN technology, and its great complexity has held back its full deployment as the single integrating network technology in the way that its inventors originally intended.

In recent years frame switching for Ethernet has emerged as a solution to congestion problems of Ethernet based networks. The switches extend the multiport bridging concept and implement routing protocols like spanning tree or source routing. Initially, the LAN switches were expensive and their use was justifiable for interconnection of network segments and connection of high-performance workstations and servers. Recently the cost of 100/1000 Mbps switches has dropped and they have become an affordable method for congestion reduction. On the other hand, the ATM is increasingly challenged by speed and traffic shaping requirements of converged networks. In particular, the complexity of SAR imposes a performance bottleneck, as the fastest ATM SARs (Segmentation and Reassembly chips) known run at 2.5 Gbit/s and have limited traffic shaping capabilities. [Wiki05]

As the cost of 100/1000 Mbps Ethernet switched port came near to the cost of a HUB port, each workstation can be attached to its own port on the switch to maximise the bandwidth capability of each device. The unshared ports can be operated in full-duplex mode, which effectively doubles the available bandwidth and the fully switched network connection is collision free.

One of the possible motivations for deployment of ATM was, at least from the telecom point of view, that it is easier to manage traffic when it is cleanly separated into unique connections. It is very hard to count IP packets and decide who should pay for them. But it is easy to keep track of who opens a connection and how long that connection stays open for. In short, ATM would allow Internet providers to charge by usage, instead of a flat rate. [Wired96] However this payment model is obsolete today.

Also the need for ATM cells to reduce jitter has disappeared as transport speeds increased as described above. Improvements in voice over IP have made the integration of speech and data possible at the IP layer, which again removed the reason for broad deployment of ATM. Most telecommunication companies are now planning to integrate their voice network activities into their IP networks, rather than vice versa. [Wiki05]

### **Security functionalities built in (packet filters, access lists, application layer gateway)**

The recent trend is to embed security functionalities into networking devices to provide at least a basic level of security even if the user does not care about the security at all. Because the security rules sometimes have to limit the functionality of the device, the device producers have to carefully look for a compromise between out-of-the-box security and functionality.

Typical security functions of a networked device are:

- packet filters
  - stateless – security algorithm does not keep information on previous interactions between communicating parties,
  - security algorithm does not keep information on previous interactions between communicating parties.
  - stateful - security algorithm keeps information on previous interactions between communicating parties and controls correct state flow of connection oriented transmissions.

A stateless filtering algorithm evaluates rules defining allowed inbound and outbound connections, the rules define certain kinds of traffic as allowed and the other as disallowed (e.g. specific protocol, specific protocol option, etc.). The typical stateless filtering of Ethernet traffic evaluates the following communication attributes:

- EtherType value

- Specific IPv4 or IPv6 addresses or address prefixes and IP protocol options
- Specific domain names contained within DNS queries and resolution responses
- Specific TCP options
- Specific ICMP (Type, Code) pairs

Stateful filtering algorithms enhance the stateless algorithms by the monitoring of network packets during communication and comparing the packets against a list of possible (correct) states. Packets that violate the standardised state flow are dropped. The advantage of stateful filtering is that a complete table with rules is queried once per connection, while with the stateless filtering a query for each packet has to be performed [NVIDIA05]. The trend is clearly towards the stateful packet inspection as it enhances security and reduces communication latencies due to lower utilisation of a CPU. The only disadvantage of stateful filtering is the need to keep track of pending connections, which might be a challenge for devices that have to handle enormous amounts of simultaneous connections only.

Access control based on access list has been integrated into various network devices to prevent access of unauthorized users or devices to the network. Originally a broad range of proprietary solutions have been developed in the recent years. The following solutions have been developed in the past:

- MAC address filtering – device has for communication port a list of allowed MAC addresses.
- Extended MAC protection – algorithms preventing DHCP snooping, IP Source guarding, Dynamic ARP Inspection, CAM Table Overflow Attacks [Svet05, Demu05].
- Password based authentication [Svet05]
  - PAP (Password Authentication Protocol) – unencrypted password is being transmitted between devices, authentication is done only at the beginning of communication relation;
  - CHAP - Challenge Authentication Protocol – hashed password instead of open password is being transmitted during the authentication process, authentication can be performed both at the beginning and during the communication relation;
  - Extensible Authentication Protocol and IEEE 802.1x - an encrypted tunnel is created for communication between the untrusted client (Supplicant) and the trusted device. The IEEE 802.1x is called EAP over LAN (EAPOL). Authentication server (e.g. RADIUS server) is used for the user authentication itself. Various modifications and extensions of the EAP are being developed (EAP-MD5, EAP-OTP, EAP-TLS, EAP-PEAP etc.). These variants differ in the level of security.

In general the MAC address based access control is not very secure as the MAC address of many devices can be modified by the user. The MAC address of trusted devices can be eavesdropped easily at both wired and wireless LANs. The MAC address based access control is suitable for prevention of unintentional access to the (wireless) network; however it cannot stop a malevolent user.

Password based authentication has developed from the most simple authentication schemes to very smart and trustworthy authentication schemes. Authentication based on IEEE 802.1x schemes is recommended for enterprise networks as it allows easy, flexible and consistent management of large amounts users and devices.

Sometimes the protection on the network level is not sufficient. If there are attack scenarios within the given communication protocol or there are known weaknesses of the server application dealing with the request the communication protocol has to be decoded as well.

So the next step is to provide a dedicated service that handles exactly one protocol on layer 7 of the OSI reference model hence being able to decode and analyse the communication request in greater detail. Application layer gateways provide protection servers and applications, because:

- The server cannot be changed, as it is a third party development

- Time and/or costs do not allow for changes in the implementation of the service
- The protocol has inherent weaknesses
- The target device does not have enough resources for additional security checks
- Extended access control should be applied

Sometimes ALGs (application layer gateway) [ALFWIKI] are just used in order to apply a second border protection technology (often of an especially hardened operating system) to avoid technological monoculture which is often one weak spot of security concepts.

Application level gateways (sometimes called application level firewalls) encapsulate an application which is to be protected and verify every communication before it is passed through to the target. This separates the application server from the possible source of danger (intended attacks as well as random events) by one level and can serve further valid requests while the ALG takes care of possible fraud requests.

According to the specific usage scenario authentication can be implemented in and delegated to the ALG in order to further reduce resource consumption in the server/device and to implement single sign on and group authentication at the perimeter.

## 7.2 Trends in Automation

Because of the existence of more and more world wide distributed factories and plants, it is necessary to coordinate and synchronise the related automation parts, i.e. to guarantee material flow and to provide overall diagnosis to ERP systems. Private automation networks are often locally restricted to the special plant(s) of one factory. To enable the coordination and diagnosis between locally separated plants, public networks are used. For diagnosis purposes this is state-of-the-art. However, process data with real time aspects are currently not transferred via public networks. For management and maintenance purposes as well as the total integrated engineering of distributed automation, enhancements of available tools are necessary.

The communication via private automation networks within a plant is free of charge. Manufacturer or plant carriers only have to consider costs for the network infrastructure and their maintenance. However, using public networks is also associated with costs for the transfer of data that must be taken into account as a new parameter. New and flexible cost models and service level agreements can be expected on the part of the service providers.

Public networks can be accessed by everyone in principle. Therefore, safe security mechanisms are necessary and must be applied to protect the sensitive manufacturer's data. In the future security will become more important. Automation devices with implemented security mechanisms or special security devices that are switched on will be available.

Industrial Ethernet and the IP protocol suite are becoming more and more important in automation domains. However present fieldbus systems with their large amount of installed nodes will also stay significant over the next few years.

Network transitions like gateway and router are used to connect different network types. Because of the available heterogeneous network structure and increased communication between such networks, more transition types are necessary and will also be used. They will become more and more equipped with special security functionalities.

To distinguish i.e. process relevant real-time traffic from non real-time traffic like web, mail and ftp, this data must be associated with special quality of service (QoS) parameters. This must be supported by the network and the infrastructure. Therefore the QoS will have more relevance in the future.

New multimedia features supported by the IP suite such as video and voice and corresponding devices offer new possibilities for the automation. The usage and integration into Ethernet based automation solutions can also be expected in the future.

Successful protocols of the IP suite that are often used in an office environment will also be reused in automation solutions. They are used i.e. to get access to automation devices or for web based diagnosis. To fulfil real-time requirements from an automation point of view, special Ethernet compatible solutions based on layer two were developed that are not available in office domains.

## 8 Trends in engineering tools for VAN goals

### 8.1 Introduction

The VAN project targets on integration of different communication technologies in order to get a consistent view of automation systems based on heterogeneous networks. State of the art for the technologies used in engineering of embedded automation systems has not been in the focus of a dedicated task in workpackage 1, but a short introduction into the engineering technologies, as well as requirements and a roadmap for these technologies, have been provided in task 1.2. The following chapter will add an analysis of the trend for engineering technologies relevant for VAN.

However, these technologies have also been in the scope of task 1.2, and therefore a short description of the technologies can also be found in deliverable D01.2-1-V1, the analysis for each technology in the following chapter also starts with a basic overview of the technology in order to make a self-contained description which is comprehensible on its own.

Since the examined technologies are not controlled by the parties participating in the VAN project and the primary business of the VAN partners is focused on components and solutions but not on the engineering technologies, there are no marketing activities dedicated to quantitative figures for market penetration of these technologies. Therefore, the analysis of trends follows a qualitative approach and uses availability of components and implementations as well as acknowledged compliance tests and certification procedures as indicators for the trends of the engineering technologies.

The trend for each technology will be described in two sections on evolution and maturity. The evolution section gives a summary on the origin and the history of specifications, responsible standardisation bodies or consortia, and available implementations and applications using the technology. In the maturity section information on deployment and acceptance of the technology is given as far as it is publicly available from the concerned bodies and consortia. Also, other qualitative indicators for the maturity of the technology are presented in this section.

The description of each technology is concluded by a summary of the trends of the technology and the prospective impact on the VAN project.

The technologies described in the following focus on engineering task related to management of automation systems and data exchange across heterogeneous communication networks, while functional aspects like application development and device description are not considered. The selection is based upon the results of task 8.1, where an analysis of existing engineering tools was performed and requirements of engineering for automation systems have been identified.

### 8.2 OPC

#### 8.2.1 Overview of OPC

OPC (OLE for Process Control) [OPC] defines software interfaces, which provide a common way for applications to access data from any data source like a device or database. Adding the OPC specification to Microsoft's OLE technology in Windows has made development of applications independent from development of the software for devices. While the manufacturers provide OPC servers access to information of the devices, it is possible to develop independently various OPC client applications, which need access to the data of the devices, like HMIs and SCADA systems.

#### 8.2.2 Evolution of OPC

The first specification OPC-DA (Data Access) was released by the OPC foundation in 1996 as a result from the collaboration of a number of leading worldwide automation suppliers working in

cooperation with Microsoft. Initial concerns about possible performance losses have been proven to be negligible in practice.

Beside new releases of the OPC-DA specification the OPC foundation extended its standardisation efforts and also launched specifications for communication of other types of data like Alarm & Events, Batch, Data Exchange, Historical Data Access and Security.

Moreover, a XML-DA specification was released in order to overcome the limitation to the OLE technology and the usage of DCOM for access in a distributed environment. The XML-DA specification standardised mechanisms for data exchange based on XML frameworks and Web services. For definition of more complicated data types such as binary structures and XML documents the Complex Data specification was added as a companion specification to OPC-DA and XML-DA specifications.

Currently, the OPC Foundation is working on the creation of the OPC-UA (Unified Architecture), a completely new system design. The goal of OPC-UA is to modernise and enhance all the functionality of the existing OPC-defined interfaces. In future end-user should be able to choose the COM or Web services flavour depending on his tradeoffs between speed and other attributes, such as cross-platform or internet friendliness. The OPC-UA specification is even written to be as platform independent as possible, to simplify the migration of the OPC specification to other platforms when and if this becomes desirable [Lut04].

### **8.2.3 Maturity of OPC**

Nowadays OPC applications for online data exchange based on DCOM are state-of-the-art for software running under Windows operating systems. There are thousands of OPC servers and clients and for the creation of new OPC components several software development toolkits are available.

The adherence to the OPC standards can be verified by self-certification using the compliance test tools provided by the OPC foundation. There are also regular OPC interoperability workshops where vendors can test their products with other vendors' products to validate interoperability.

Applications using XML-DA are also available. Several toolkits support development of XML-DA compliant software on different platforms. Compliance test for XML-DA exist and are passed by some applications. But the majority of products have not completed their compliance tests.

Since the OPC-UA specification is not released there are no certified products available. But it is to be expected that compliance tests will be available after the release of the specifications and that they will be applied to new or extended applications, which implement the OPC-UA specification.

### **8.2.4 Conclusions about OPC**

OPC is a well established technology used in many engineering tools and supported by many components. The upcoming OPC-UA approach allows the combination of OPC with Web services. This facilitates the integration of IT technologies into industrial communication technologies for embedded, networked, distributed automation systems – one of the main goals of the VAN project.

## **8.3 FDT/DTM**

### **8.3.1 Overview of FDT/DTM**

FDT (Field Device Tool) [FDT] is a technology, which allows the integration of software for devices of different vendors in one engineering tool. This technology is established as an open standard and therefore it is vendor independent. The key feature is its independence from the communication protocol and the software environment of either the device or the host system. FDT allows any device to be configured and accessed from any host through any protocol. DTM (Device Type Manager) is a piece of software that the device manufactures add to their individual field devices. FDT compliant software tools use DTMs to communicate with the devices across different fieldbuses.

### 8.3.2 Evolution of FDT/DTM

A working group for definition of the interfaces of FDT was established by ZVEI (German association for electrical and electronics industry) [ZVEI] in 1998. In the last years the specification was controlled by FDT Joint Interest Group, which has been reorganised into a formal organisation, called FDT Group. The latest version 1.2.1 of the FDT interface specification has been released in March 2005.

The FDT specification is organised in such a way that protocol specific extensions and communication schemas are located in separate annexes. This approach allows extending the specification to additional fieldbuses without the need to release a new version of the specification. Currently, annexes have been released for Profibus, HART, and Foundation Fieldbus. Extension of the specification by annexes for Interbus, AS-I, Modbus, Profinet I/O are under development. Additionally, a base specification for CIP-based protocols is prepared, which will be used to extent the FDT specification for DeviceNet in a first step [FDTPress].

Several FDT compliant frame applications exist and meanwhile there are DTMs for lots of devices from different vendors. Since the latest version of the FDT interface specification was released only a few months ago, there are still frame applications and DTMs in accordance with the previous 1.2 specification. Due to backward compatibility it is possible to use DTMs and frame applications of version 1.2 and version 1.2.1 together.

### 8.3.3 Maturity of FDT/DTM

FDT tools are in use at thousands of locations worldwide and DTMs are available for hundreds of devices.

For the implementation of the conformity test, a test tool was developed for DTMs. A corresponding test tool for frame applications is not yet available but should have been developed in the course of 2005. The certification process has been defined and test laboratories have been accredited to conduct the tests and issue the test reports. First components were certified by the FDT Group in October 2005.

### 8.3.4 Conclusions about FDT/DTM

FDT/DTM is adopted by more and more vendors and tools and components are already widely used. The remarkable list of newly supported fieldbus protocols foreshadows a strong growth of devices and components for a variety of communication networks. The FDT/DTM technology bears good prospects for the VAN project, since it supports integration of engineering applications for different devices from different vendors and it allows to access components from an engineering station across hierarchical, heterogeneous networks.

## 8.4 Plug-and-Play

### 8.4.1 Overview of Plug-and-Play

Plug-and-Play technology provides a combination of hardware and software support that enables applications and the system to recognise and adapt to changes in hardware configuration.

UPnP (Universal Plug-and-Play) [UPNP] extends Plug-and-Play to include the entire network, enabling discovery and control of network connected devices and services, such as printers, Internet gateways, and consumer electronics equipment, which is attached to the network. The goals of UPnP are to allow devices to connect easily and to simplify the implementation of networks in the home and corporate environments.

The UPnP architecture offers pervasive network connectivity of PCs, intelligent appliances, and wireless devices. The UPnP architecture is a distributed, open networking architecture that leverages TCP/IP and the World Wide Web to enable seamless networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between.

The UPnP architecture supports zero-configuration, invisible networking, and automatic discovery, whereby a device can dynamically join a network, obtain an IP address, announce its name, convey

its capabilities upon request, and learn about the presence and capabilities of other devices. DHCP and DNS servers are optional and are only used if they are available on the network. A device can leave a network smoothly and automatically without leaving any unwanted state information behind.

Moreover the UPnP technology can run on any medium including phone lines, power lines, Firewire, Ethernet, infrared (IrDA), radio links (Wi-Fi, Bluetooth), etc. Any operating system and any programming language can be used to build UPnP products.

#### **8.4.2 Evolution of Plug-and-Play**

The standardisation of UPnP technology is dealt with from the UPnP Forum, which was created in 1999. It defines UPnP Device and Service Descriptions (called Device Control Protocols or DCPs) according to a common device architecture contributed by Microsoft. The standardisation process started from the basic devices like printer or scanner. Today standards cover a wide area of devices like internet gateways, media servers, etc. and there are also general purpose standards e.g. for security and quality of service, which can be applied to any type of device.

#### **8.4.3 Maturity of Plug-and-Play**

Nowadays the UPnP Forum is an association of more than 700 vendors who are industry leaders in consumer electronics, computing, home automation and security, home appliances, computer networking, mobile devices, etc.

The latest versions of the Windows operating systems and many devices already include UPnP support. Moreover, on the market there are many software tools that help to develop the UPnP functionalities for new devices.

The device certification process is administrated from the UIC (UPnP Implementers Corporation) [UIC] which is a non-profit corporation. UIC provides a certification test tool, which can be used to verify that the device implements standards, which are written and approved by the UPnP Forum.

#### **8.4.4 Conclusions about Plug-and-Play**

Plug-and-Play technologies can noticeably disburden the engineering tasks during configuration and commissioning and therefore should be considered in the VAN project. Similar to Web service technologies UPnP allows not only to discover devices but also to discover their capabilities (services). Since UPnP is prevalent in the consumer electronics market the penetration in the automation area has to be observed.

### **8.5 SNMP and MIB**

#### **8.5.1 Overview of SNMP and MIB**

SNMP (Simple Network Management Protocol) [SNMP] is a network management standard widely used in TCP/IP networks. SNMP provides a method of managing network hosts such as workstation or server computers, routers, bridges, and hubs from a centrally-located computer running network management software.

SNMP can be used to configure remote devices, monitor network performance, detect network faults or inappropriate access, or trigger alarms on network devices when certain events occur.

The management data of SNMP-enabled devices such as routers, switches, and access points are stored in a so called MIB (Management Information Base) [MIB]. A MIB is a database which comprises a collection of objects that represent information about IP and IPX components on the network, such as the list of network interfaces, the routing table, the ARP (Address Resolution Protocol) table, the list of open TCP connections, or ICMP (Internet Control Message Protocol) [ICMP] statistics.

## 8.5.2 Evolution of SNMP and MIB

Starting from the first version in 1988 in order to provide network-device-monitoring capability for TCP/IP-based networks, SNMP was approved as an Internet standard in 1990 by the IAB (Internet Architecture Board) [IAB] and is in wide use since that time.

The first version of SNMP was soon revised by SNMPv2 and in 2004 by SNMPv3, which improved the performance, security, confidentiality, manager-to-manager communication, and data exchange of larger amounts in a single request.

## 8.5.3 Maturity of SNMP and MIB

Nowadays SNMP is considered one of the most widely used standards to manage IP networks. The IETF (Internet Engineering Task Force) [IETF] recognises SNMP version 3 as the current standard version of SNMP and considers earlier versions as "Obsolete" or "Historical". In practice, SNMP implementations often support multiple versions: typically SNMPv1, SNMPv2c, and SNMPv3.

Recently, IPX (Internetwork Packet Exchange) has added support for SNMP.

On the market many software tools of different vendors are present and can be used to manage SNMP and MIB functionalities. Many standard MIBs (defined in RFCs) and vendor specific MIBs are available, which can be integrated into any SNMP management tool. However, some vendor specific MIBs include information redundant to existing standard MIBs and other vendor's MIBs. Even MIB implementations from the same vendor are often completely different and contain redundant information.

## 8.5.4 Conclusions about SNMP and MIB

SNMP is supported by almost all industrial network components and thus allows standardised access to these devices for engineering tasks during configuration and commissioning but also during production and maintenance in the runtime phase. Although there are some deficiencies caused by inconsistent structure of the used MIBs, SNMP is to be considered for employment in the engineering tools for VAN just because of the widespread usage.

## 8.6 Web Services

### 8.6.1 Overview of Web Services

Web services are used for application to application communication across networks like the Internet in a manner similar to inter-process communication on a single computer. The software applications can be written in different programming languages and they can run on various platforms. The communication is based on exchange of messages.

In the office domain Web services are used to provide functionality across the Internet. In order to call a Web service a message describing the function and parameters is conveyed from the requester to the provider of the Web service using HTTP methods [HTTP]. The XML formatted message may conform to a messaging standard such as SOAP (Simple Object Access Protocol) [SOAP]. Moreover, the actual command and parameters have to be in conformance with the interface of the Web service. The Web service description, including the interface and protocols, can be described by WSDL (Web Services Description Language) [WSDL]. If the requester does not already know what provider it wishes to engage, then it can use UDDI (Universal Description, Discovery, and Integration) [UDDI] to discover an appropriate Web service in a universal business registry (catalog), where potential providers have previously published descriptions of their Web services.

To enable interoperability between devices and Web services the DPWS (Devices Profile for Web Services) [DPWS] was specified. DPWS is based on a set of Web services specifications and prescribes how to use them in concert to enable secure Web services messaging, discovery, description, and eventing on resource-constrained devices. Sharing a common protocol framework allows devices to contribute to Web services scenarios that are traditionally beyond the reach of individual devices. Moreover, this commonality allows vendors of devices and software to leverage

development tooling when writing applications for devices, and it allows IT departments to leverage service management infrastructure down to the factory floor. DPWS applies SOAP for message exchange and WSDL for the description of services but instead of using UDDI for announcement and discovery of services, the WS-Discovery [WS-Discovery] specification is used.

### 8.6.2 Evolution of Web Services

Many standards are used to enable Web services. Open standards for Web services are developed and maintained mainly by the W3C [W3C] and OASIS [OASIS], which do control the basic standards like SOAP, WSDL, and UDDI. Beside the standards controlled by the official bodies, many specifications are defined and published by varying coalitions of companies, which want to push their technologies. These specifications are handed over to some official standardisation bodies only after publication, if at all. This attitude results in a sheer enormity of specifications and standards on Web services and in some areas even lead to multiple, competing standards.

The first version of DPWS was published in May 2004 and the latest version was released as a public specification in May 2005. This is the third joint publication of the profile. Beside the basic standards, DPWS also uses WS-Eventing [WS-Eventing] and WS-Discovery [WS-Discovery] specifications, which have been published by different coalitions around Microsoft in January 2004 and October 2004, respectively.

DPWS provides similar functionality like UPnP for dynamic discovery of devices and services as the UPnP. Since the launch of UPnP predated the widespread adoption of Web Services, the current version of UPnP is not fully compatible with Web Service technology. In contrast, DPWS uses SOAP for all messages, whether related to discovery, control, or event notification. This facilitates deployment of other Web services standards, like e.g. mechanisms to secure the communication between services as provided in the WS-Security [WS-Security] specification. Also Microsoft promotes DPWS as an alternative to UPnP for network connected devices.

### 8.6.3 Maturity of Web Services

Although standards for Web services are still enhanced and the scope is continuously extended there are already many Web services established for business applications in the Internet and Intranet domain. Also, many commercial and some open source platforms and development tools for deployment of Web services in the office domain are available since several years.

For devices in the industrial automation domain, Web services are not yet widely used. In the context of the SIRENA project [SIRENA] a DPWS implementation was performed, which implements all the DPWS protocols except WS-Security. Also a DPWS Toolkit has been developed, which has been ported to several target software platforms and runs on various hardware platforms. Moreover, DPWS will be natively integrated into the next-generation Windows platform (Windows Vista) and Microsoft will also provide the WSDAPI (Web Services for Devices API) in the Windows SDK for Windows Vista [JMS05].

Workshops on Web services [WSPW] are organised by Microsoft in order to learn about and give feedback on Web services specifications developed by Microsoft in coalition with some partners. In feedback workshops the authors of a specification discuss the content of the specification and solicit feedback from attendees. In interoperability workshops companies with implementations of a particular Web services specification come together to test the interoperability of their implementations with others. Feedback and interoperability workshops have been held in 2004 for the specifications WS-Discovery and WS-Eventing used for DPWS. It is also planned to re-offer interoperability workshops for both specifications.

### 8.6.4 Conclusions about Web Services

Web services are widely used and further penetrating IT applications. Adopting this technology also for communication networks and devices of automation systems results in consistent approaches in the two areas of IT technology and embedded automation systems. Thus, it provides a natural approach for integration of these two areas, as it is targeted by the VAN project. Moreover, the recent

advances for DPWS in concert with the upcoming enhancements for OPC-UA will push Web services in the industrial automation and communication environment.

## 8.7 Overall Conclusions about Engineering Tools

Engineering of communication networks and embedded devices in a VAN system can build upon the basis of existing engineering technologies. Beside the well settled technologies like OPC and SNMP there are also emerging technologies like DPWS and substantial advances for technologies like FDT/DTM and OPC-UA.

Especially for FDT/DTM and the technologies related to Web services the future development has to be observed in order to correlate these trends with the ongoing analysis and development of engineering tools in the VAN project. Although it is not clear, whether all of these technologies will prevail in the automation area their current state is sufficiently advanced for adoption in the engineering tools of VAN systems.

## 9 Summary of Conclusions

To summarise conclusions for all the technologies included in this deliverable is not an easy task. Each chapter can be considered independent from the others, but simultaneously, several cross dependencies exist, and several approaches can be taken.

The manufacturing concept has moved from products to services, integrating in the product life cycle whole value-chain [MaSRA05]. All steps should be observed, from the initial design to the final delivery to customers, post-sales services or even the obsolete equipment recycling. It is not only a matter of cost savings, efficiency or productiveness improvement, but also of survival in the emerging globalised world. The necessity of this acts as strong driver pulling technology to provide supporting systems to deal with this complexity.

Industry sector is conservative regarding new technologies adoption, and it is necessary to reach an acceptable level of maturity, reliability "industry-grade", performance, stability, technology life cycle matching, maintenance efforts and other aspects, prior to these new technologies to be adopted. This is especially true for safety processes where specific and restricted regulations must be observed.

In IST world, it is common that technologies originally devised for targeting SOHO's or entertainment market, would further be adopted, after a specialization period, by the industry world. Examples of this are PCs, general purpose operating systems, SMS, WWW, and many others. Some of the emerging ones are VoIP, VOD or wireless HDTV, that have been identified as drivers, pulling technology evolution to reach and feed massive markets.

Globally observed trends in industries are shortening the time frame for new technologies adoption and the growth in adoption of COTS systems, bearing the risk of immature adoption. However, there are still some mismatches, due to different life cycles and migration issues, to be solved.

### **Wireless**

Wireless communication technologies have evolved in a fast and dynamical way during last years and have always generated big expectations in industry.

One of the main drivers for industry is the plant productivity and efficiency improvement (near to 2-3%) expected to be reached with wireless devices, among others, like cost savings in wires and installation.

Global trends observed in wireless communication are:

- Continuous growth experienced during last years. Although the market share is still significantly under wired networks, the expected CAGR is 55% higher in wireless than in wired. Growth affects both the number of wireless networks, and the number of nodes in network.
- The simultaneous presence of several standardised radio technologies; Wi-Fi, WiMax, Bluetooth, ZigBee, and so forth, including sophisticated modulation schemas and shared media access management strategies.
- Radio frequency spectrum is limited and subjected to several regulations from governments and organisations (i.e ITU). Moreover, there is a growing social perception identifying radiated electromagnetic fields with environmental pollution, thus, it is expected that more regulations will come regarding to it. The use of unlicensed ISM "free" frequency bands has been massively adopted. These limitations act as drivers, pushing technology to improve data rates, BER, spectrum efficiency, radiated power and others. I.e. antenna technologies are in a continuous growth.

## **Real time**

For a long time, real time technologies have been a critical issue in automation and - even if real time is not equal to high speed - the top development of real time communication technologies is always a trend setter concerning high speed transmission.

Real time matters are going beyond the strict plant-floor control issues and reaching higher importance on the overall decision-making process in industries. Wider application of Real-time Performance Management (RPM) is observed.

A high growth is observed on the market penetration of Industrial Ethernets. On the contrary, a decrease of classical fieldbuses implementation is clearly stated.

New specific features of IPv6 protocol are expected to provide improvement of real time capability especially over small network limits, but a migration strategy to IPv6 in automation cannot be found yet.

Progressive implementation of QoS, MPLS and other advanced abilities in switching network infrastructures are arising.

Trend of IEEE1588 standard adoption (particularly the Precise Time Protocol) by some existent and recent Industrial Ethernet technologies enables a new dimension of highly precise control of applications with high synchronisation requirements.

Faster Ethernet physical layer adoption (10Gigabit) will allow e.g. new motion control techniques ("no drives at all"), expected to improve control efficiency.

Increasing importance and spreading of multimedia applications like VoIP, Video streaming or IPTV. IMS standard adoption is highly expected.

## **Safety**

There are well-established safety technologies within fieldbuses, and a good level of efficiency and resource optimisation has been achieved by sharing safety and non-safety traffic in the same bus/wire.

Safety technologies are observed to follow the general trend in automation that comprises to take over and adapt IT technologies. Under this approach, there is an observed trend to implement safety features on the top layers of other growing protocols (i.e. Industrial Ethernet) or even emerging ones (i.e. those derived from wireless networks fast evolution).

There is no compatibility between safety specific protocols of different fieldbuses, but several efforts have been made to standardise, regulate and certify safety characteristics.

## **Security**

Security is currently one of the most wide-spread issues on ISTs, embracing societal, political, economic and technological aspects. Awareness of security is growing, and policies and regulations are moving to tackle security from a holistic approach. Nevertheless, it is commonly stated that there are strong mismatches between IST fast evolution and pervasive services deploying, and the required security measures, user awareness and education, and overall approaches to be adopted. Cyber crime, cyber terrorism, hijacking, spam, virus, trojans, worms, piracy and others, take part in a relatively new vocabulary where the main actor is the abuse, or a bad use, of a technology. If a technology is restricted, risks derived from bad use are also restricted, while becoming measurable and manageable as well. However, if the technology is widely and easily available (i.e. through ISTs,

COTS based systems, etc.) risks can become unpredictable, mainly if there is not a clear policy and regulation, not only targeting users, but also technology providers. Under this frame, it is obvious that VAN project deals directly with these issues, and should closely track and match security issues.

### ***Co-operation of private and public networks***

Permanent growth of private networks in firms, authorities, and private homes can be observed. In parallel a fast further development of Internet technology and wireless networks can be registered.

The connection of private networks with each other and with the Internet by using public networks is also an increasing trend. Many companies are switching from exclusive, expensive leased lines to packet switched networks with encrypted tunnels.

The kind of data is also changing more and more from textual data to multimedia data such as videos and voice. This fact leads to relevantly increased network traffic.

Because of the trend that communication in automation will be more and more based on Ethernet, together with the Internet protocol suite or special automation protocols, the data exchange between plants and via public networks must be considered.

The migration from IPv4 to IPv6 began slowly in 2005; nevertheless, IPv6 is considered as "a must" within five years in public networks. In addition, only a small part of the IPv4 address range is available for Internet newcomers such as South America or Asia. That is why i.e. the market of China is able to push the divulgation of this technology into the next future [Hill05].

Multi-Protocol Label Switching (MPLS) was developed as a packet-based technology and is rapidly becoming the key for use in core networks, including converged data and voice networks.

### ***Engineering tools***

Engineering tools for automation systems are, either adopted from existing COTS and applications already used in the IST world, or newly developed for technologies devoted to automation systems. Engineering tools for the former group cover technologies like SNMP, PnP, Web services and their specialization towards DPWS. The latter group clearly comprises FDT/DTM and all engineering tools used for management and configuration of fieldbuses and programming of PLCs. In any case, engineering tools must be able to support and manage the technologies to be employed in the VAN project.

Different engineering tools are used for a variety of tasks during the individual phases of the life cycle of an automation system. Although each individual engineering tool facilitates important cost savings and methods for efficiency improvements, there is often no or only little interaction or automatic data exchange between the different engineering tools. Especially for engineering tools from different vendors, this interoperability can be improved by common standards, like FDT/DTM, OPC, etc.

Obviously, further development and future trends have to be observed for new technologies like FDT/DTM and the DPWS. But also recent and upcoming advancements for established technologies like OPC, SNMP and PnP have to be tracked within the VAN project.

The next table resumes an overview of the main trends and/or issues related.

<b>Trend/issue</b>	
<b>General</b>	<ul style="list-style-type: none"> <li>• Continuous growth of automation levels in industries</li> <li>• Manufacturing concept is moved from products to services</li> <li>• Distributed &amp; flexible manufacturing. JIT systems</li> <li>• Holistic approach of whole value chain and logistics in manufacturing</li> <li>• Time to market and life cycle shortening</li> <li>• New emerging processes in nano-scale and bio-materials</li> <li>• Environmental regulations increasing</li> </ul>
<b>Wireless</b>	<ul style="list-style-type: none"> <li>• Continuous, spectacular growth and technology advances</li> <li>• Several simultaneous technologies exist</li> <li>• Wireless device-level network and sensors have yet to take off due to limitations of battery technology and lack of standardization</li> <li>• Radiated power &amp; spectrum limitations and regulations is increasing</li> <li>• Security concerns are increasing but not solved</li> <li>• Trend to development of new protocols for real time properties improvement</li> <li>• Trend to development of software tools for monitoring, configuring and managing wireless embedded systems</li> </ul>
<b>Real Time</b>	<ul style="list-style-type: none"> <li>• Critical issue in automation. Broader application of Real- time Performance Management (RPM)</li> <li>• High growth of Industrial Ethernets</li> <li>• Migration from IPv4 to IPv6 protocol is clear, but the strategy in automation networks is still under discussion</li> <li>• Trend of IEEE1588 standard adoption (PTP) by several Industrial Ethernet technologies</li> <li>• Growing importance and spreading of multimedia applications like VoIP, Video streaming or IPTV. IMS standard adoption is highly expected</li> </ul>
<b>Safety</b>	<ul style="list-style-type: none"> <li>• Solved and well-established in proprietary fieldbuses</li> <li>• Trend is to share safety data with standard traffic</li> <li>• Trend of one single busline</li> <li>• Under strict regulations and certifications protocols.</li> <li>• Including safety in different layers of existent protocols</li> <li>• Trend to adapt safety principles into Industrial Ethernets</li> </ul>
<b>Security</b>	<ul style="list-style-type: none"> <li>• Pervasive issue, concerning societal, political, economical and technological aspects</li> <li>• Society has not a clear perception of security related risks. Nevertheless, there is a continuous growth of awareness of security issues (virus, worms, attacks...)</li> <li>• Holistic security concept adoption is growing</li> <li>• Several existent technologies and standards</li> <li>• Recent regulations and policies reinforce the security adoption</li> <li>• Advances in embedded computing (processing capacities) and algorithms will make it feasible to include security in all devices</li> </ul>

<p><b>Cooperation of Private and Public Networks</b></p>	<ul style="list-style-type: none"> <li>• Continuous growth of private networks</li> <li>• To connect private networks through public ones and/or Internet</li> <li>• Network traffic increasing, from textual to multimedia data</li> <li>• Emerging new services based on public networks infrastructure</li> <li>• QoS technologies and end-to-end concept adoption is increasing</li> <li>• Increasing features and lowering prices in network infrastructure equipments</li> <li>• IPv6 protocol adoption is a must within 5 years in public networks. High growth is expected from South America and Asia.</li> <li>• Strongly conditioned by security issues</li> </ul>
<p><b>Engineering</b></p>	<ul style="list-style-type: none"> <li>• Further developments have to be observed for new and emerging technologies like FDT/DTM and DPWS, as well as for established technologies with strong evolution like OPC-UA and UPnP</li> <li>• All the technologies like OPC, FDT/DTM, PnP, SNMP and Web services are sufficiently advanced for adoption in the engineering tools of VAN systems</li> <li>• Especially for new technologies like DPWS, it is not clear whether they will prevail in the automation area or not</li> </ul>

Tab. 6 Trend / issues resume

## 10 Concluding Remarks; further work and links with other work packages

This report comes as the result of a study on the recent evolution of VAN related technologies. Technology trends have been selected, categorised and evaluated extensively, taking into account several factors, such as relevance, recent past related to industry, current penetration and market nature. Trends related to wireless technologies have been specifically treated due to their observed fast evolution.

The report is revolving in order to ensure a continuous tracking of advances in current technologies and possible new emerging ones, along the time frame of the VAN project.

The main objectives intended to be reached through the process defined in this deliverable are:

- To track technologies evolution, performing a continuous surveillance process
- To avoid redundant efforts, considering new results coming from other RTD projects
- To warn with enough anticipation about the possible changes due to external agents

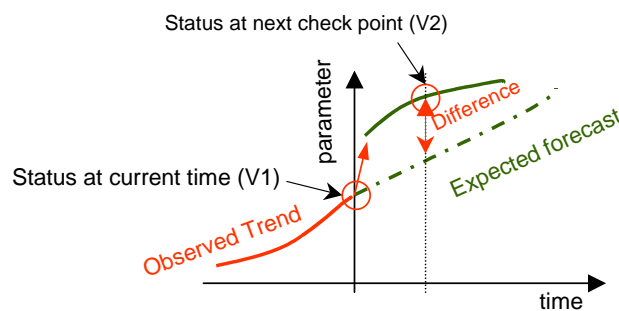


Fig. 17. Illustration of the basic trend analysis purpose

This report will be updated four times. The results, (jointly performed with those derived from Task 1.1 "State of the art" and Task 1.2 "Requirements") are intended to provide updated information to the in-progress technical WPs (WP3 to WP8). As currently these WPs have completed their initial analysis phase, the next versions of this report should be considered as one of the common matching points to horizontally update and provide new inputs to VAN project.

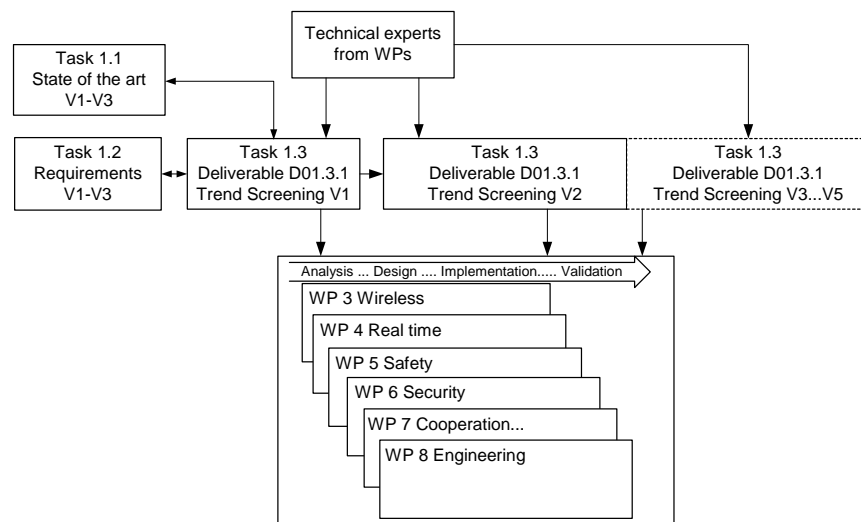


Fig. 18 Interrelations of trend reports along VAN project



## Glossary

3GPP/3GPP2	Third Generation Partnership Project
AAGR	Average Annual Growth Rate
AES	Advanced Encryption Standard
ALGs	Application Layer Gateway
AMSD	<a href="http://www.am-sd.org">www.am-sd.org</a>
API	Application Programming Interface
ARC	ARC Advisory Group: <a href="http://www.arcweb.com/">http://www.arcweb.com/</a>
ARP	Address Resolution Protocol
AS	Autonomous System
AS-I	AS-Interface
ASIC	Application-Specific Integrated Circuit
ATEX	ATmosphere EXplosible, Directive 94/9/EC
ATM	Asynchronous Transfer Mode
B&R	Bernecker and Rainer
BAS	Building Automation Systems
BCC	Business Communications Company
BER	Bit Error Rate
BGIA	Berufsgenossenschaftliches Institut für Arbeitsschutz [DE]
BOM	Bill Of Materials
BOOTP	Bootstrap Protocol
CA	Certification Authority
CAGR	Compound Annual Growth Rate
CAM	Content-Addressable Memory
CAN	Controller Area Network
CHAP	Challenge-Handshake Authentication Protocol
CIP	Common Industrial Protocol
COM	Component Object Model
COTS	Commercial-off-the-shelf
CPU	Central Processing Unit
CRC-S1	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DCF	Distributed Co-ordination Function
DCOM	Distributed Component Object Model

---

DCP	Device Control Protocol
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DL	Discrete Logarithms
PDWS	Devices Profile for Web Services
DNS	Domain Name Server
DRM	Digital rights management
DSA	Digital Signature Algorithm
DSSS	Direct Sequence Spread Spectrum
DTM	Device Type Manager
DVB	Digital Video Broadcast
EAP	Extensible Authentication Protocol
EAP-MD5	EAP-Message Digest 5
EAPOL	EAP- Over LAN
EAP-OTP	EAP- One Time Pad
EAP-PEAP	Protected Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security
ECC	Elliptic Curve Cryptography
EMEA	Europe, Middle East and Africa
EPL	Ethernet Powerlink
EPSSG	Ethernet Powerlink Standardisation Group
ERP	Enterprise Resource Planning or Emitted Radio Power
ETG	EtherCAT Technology Group
EU	European Union
FCC	Federal Communications Commission
FDT	Field Device Tool
FHSS	Frequency Hopping Spread Spectrum
FPGA	Field-Programmable Gate Array
HART	Highway Addressable Remote Transducer
HDTV	High Definition TV
HMI	Human Machine Interface
HTML	Hyper Text Markup Language
I/O	Input/Output
IBE	Identity-Based Encryption
ICANN	Internet Corporation for Assigned Names and Numbers.
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
ID	Identity
IDG	International Data Group

---

IDS	Intrusion Detection System
IEC	International Engineering Consortium
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Internal Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IGS	Interest Group Sercos
IMS	Internet Protocol Multimedia Subsystem
INRS	Institut National de Recherche et de Sécurité
IP	Internet Protocol
IPng	Internet Protocol Next Generation
IPSec	IP Security
IPTV	Internet Protocol TeleVision
IPX	Internetwork Packet Exchange
IrDA	Infrared Data Association
IRT	Isochronous Real-Time
ISA	Instrumentation, Systems, and Automation Society
ISM-band	Industrial, Scientific, and Medical band
ISO	International Standards Organisation
ISP	Internet Services Provider
IST	Information Society Technologies
ISTAG	Information Society Technologies Advisory Group
IT	Information Technologies
JIT	Just In Time
JSIG	Java Special Interest Group
LAN	Local Area Network
LSR	Label-Switched Routers
MAC	Media Access Control
MAN	Metropolitan Area Networks
MEMS	Micro-electromechanical Systems
MES	Manufacturing Execution System
MIMO	Multiple Input Multiple Output radio systems
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NC	Numeric Control
NRTL	Nationally Recognized Testing Laboratory
NSA	National Security Agency
ODVA	Open DeviceNet Vendor Association

OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OPC-DA	OPC Data Access
OPC-UA	OPC-Unified Architecture
OS	Operating systems
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PC	Personal Computer
PDA	Personal Digital Assistant
PDH	Plesiochronous Digital Hierarchy
PKG	Private Key Generator
PLC	Programmable Logic Computer
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAPID	<a href="http://www.ra-pid.org">www.ra-pid.org</a>
RARP	Reverse Address Resolution Protocol
RESET	<a href="http://www.ercim.org/reset">www.ercim.org/reset</a>
RF	Radio Frequency
RFC	Request for Comments document
RPM	Real-time Performance Management
RSA	Algorithm for public-key encryption by Ron Rivest, Adi Shamir and Len Adleman
RUNES	Reconfigurable Ubiquitous Networked Embedded Systems
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SDK	Software Development Kit
SERCOS	SErial Real-Time COmmunication System
SIL	Safety Integrated Level
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOHO	Small Office Home Office
Sonet/SDH	Synchronous optical network/SDH
SPS	Speicherprogrammierbare Steuerung [De], stands for PLC
SSID	Service Set Identifier
SSO	Single Sign On
STORK	<a href="http://www.stork.eu.org">www.stork.eu.org</a>
TCP	Transmission Control Protocol

---

TwinSAFE	Safety Bus Terminals Technology from Beckhoff
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UPnP	Universal Plug-and-Play
UWB	Ultra Wide Band
VDC	Venture Development Corporation
VOD	Video On Demand
VoIP	Voice Over IP
VP	Vice President
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Privacy
Wi-Fi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WINA	Wireless Industrial Networking Alliance
WLAN	Wireless Local Area Network
WSDAPI	Web Services for Devices API
WWRF	Wireless World Research Forum
XML	Extensible Markup Language

## References

### Wireless

- [And02] M. Andersson, Bluetooth for Industry, In: The Industrial Ethernet Book, Sept. 2002, pp. 10-12, cited by [Kou et al 05].
- [ARC05] ARC Advisory Group, WebForum: ZigBee: Suited for Industrial Applications, Nov. 2005.
- [Boy05] W. Boyes, Users Want an Industrial Wireless Standard, <http://www.controlglobal.com/articles/2005/480.html>, Sept. 2005.
- [CoC05] ComConsult: Technologie-Warnung: Wireless LANs im Visier des Enhanced Wireless Consortiums, Email, Oct. 2005.
- [Dat06] Datamonitor, Embedding WLANs in the Enterprise, <http://www.datamonitor.com/~ee24e06338584e7a80000ffc12b7b8cc~/industries/research/?pid=DMTC1168&type=Report>, Jan. 2006.
- [Ene02] U. S. Department of Energy – Office of Energy Efficiency and Renewable Energy, Industrial Wireless Technology for the 21st Century – Based on the views of the Industrial Wireless Community, [http://www.eere.energy.gov/industry/sensors\\_automation/pdfs/wireless\\_technology.pdf](http://www.eere.energy.gov/industry/sensors_automation/pdfs/wireless_technology.pdf), Dec. 2002.
- [For05] H. Forbes, Wireless – Mehr als nur ein Modetrend? Computer&AUTOMATION, Sonderausgabe 3, 2005, pp. 6-7.
- [Glo05] Global Sources, ZigBee to Thrive on Industrial Automation, <http://www.globalsources.com/gsol/I/Mobile-wireless/a/9000000067662.htm>, Oct. 2005.
- [Hei04] B. Heile, Emerging Standards – Where does ZigBee fit, ZigBee Alliance, Oct. 2004, cited by [Ram05].
- [Inf05] Informa Telecoms & Media, Wireless Automation – the Quiet Revolution. <http://shop.informatm.com/content/marlincontent/ITMG/ibctelecoms/publishing/WA%20white%20paper%20-%20Quiet%20Revolution.pdf>, Sept. 2005.
- [Ive05] W. Iversen, ISA Forms Wireless Standards Committee, <http://www.automationworld.com/articles/Departments/1196.html>, Feb. 2005.
- [Kor05a] P. Korzeniowski, G-246R Worldwide Wireless Infrastructure Expenditures - Overview, <http://www.bccresearch.com/comm/G246R.html>, March 2005.
- [Kor05b] P. Korzeniowski, G-246R Worldwide Wireless Infrastructure Expenditures - Sample, <http://www.bccresearch.com/comm/sampleG246R.pdf>, March 2005.
- [Kou et al 05] K. Koumpis / L. Hanna / M. Andersson / M. Johansson, Wireless Industrial Control and Monitoring beyond Cable Replacement, <http://www.ist-runes.org/docs/publications/PROFIBUS05.pdf>, June 2005.
- [Mer05] R. Merritt, New trends and old friends in network choices, <http://www.controlglobal.com/articles/2005/542.html>, Oct. 2005.
- [Ram05] R. Rammig, ZigBee – A Standard for Automation and Home Networking, Feb. 2005.
- [Str05] Strata Resource, Wireless Mesh Network – An interview with Mark Pacelle, VP of Marketing for Millennial Net, <http://www.automatedbuildings.com/news/apr05/interviews/capuano.htm>, Apr. 2005.

- [Sup06] Dr. J. Suppan, WiMax kontra IEEE 802.11n: Hat WiMax wirklich eine Perspektive? In: Der Netzwerk Insider, Jan. 2006, pp. 2-3.
- [Tay04a] J. K. Taylor, A White Paper On: Worldwide Industrial Markets for Wireline and Wireless Ethernet Infrastructure Components and Network Software, <http://www.vdc-corp.com/industrial/white/04/04industrialeternet.pdf>, May 2004.
- [Tay04b] J. K. Taylor, Worldwide Industrial Markets For Wireline And Wireless Ethernet Infrastructure Components and Network Software – Overview, <http://www.vdc-corp.com/industrial/reports/03/br03-31.html>, May 2004.
- [Tay05a] J. K. Taylor, A White Paper On: The North American Market for RF/Microwave Wireless Monitoring and Control Products in Discrete and Process Manufacturing, 2nd Edition, [http://www.vdc-corp.com/industrial/white/05/05wireless\\_monitoring.pdf](http://www.vdc-corp.com/industrial/white/05/05wireless_monitoring.pdf), July 2005.
- [Tay05b] J. K. Taylor, The North American Market for RF/Microwave Wireless Monitoring and Control Products in Discrete and Process Manufacturing – Overview, 2nd Edition, <http://www.vdc-corp.com/industrial/reports/04/br04-27.html>, July 2005.
- [Wil et al 05] A. Willig / K. Matheus / A. Wolisz, Wireless Technology in Industrial Networks. In: Proceedings of the IEEE, Vol. 93 (2005), No. 6 (June), pp. 1130-1151, [http://www.tkn.tu-berlin.de/publications/papers/wireless\\_fieldbus.pdf](http://www.tkn.tu-berlin.de/publications/papers/wireless_fieldbus.pdf).

#### Real time

- [ARC01] ARC Advisory Group Inc.: ARC News, Dedham, Massachusetts; April 28, 2005.
- [ARC02] ARC Advisory Group Inc., Report: Total Automation Business for the Process Industries Worldwide Outlook, [www.arcweb.com](http://www.arcweb.com), Dedham, Massachusetts; March , 2005.
- [ARC03] ARC Advisory Group Inc., Report: Total Automation Business to Discrete Industries to Exceed \$38 Billion, [www.arcweb.com](http://www.arcweb.com), Dedham, Massachusetts; Dec 21, 2005.
- [CoC04] ComConsult Technologie Information GmbH: Technologie-Report: Ethernet in Industrie-Umgebungen, Aachen, 2004.
- [Fur03] Furrer, Frank, J.: Industrieautomation mit Ethernet-TCP/IP und Web-Technologie; 3rd edition, Hüthig Verlag, Heidelberg Germany, 2003.
- [Geo05] George, Bill: Industrial Ethernet and IPv6 address a range of possibilities In: The Industrial Ethernet Book, July 2005, Issue 27, GGH Marketing Communications, UK, 2005.
- [IEC06] Internet Model for Control of Converged Networks at [http://www.iec.org/online/tutorials/internet\\_control/topic01.html](http://www.iec.org/online/tutorials/internet_control/topic01.html)
- [IMS01] IMS-IP Multimedia Subsystem, White Paper, October 2004.
- [IPv6Wiki] <http://de.wikipedia.org/wiki/IPv6>
- [LA05] Lorentz K, Lüder A, IAONA Handbook, Industrial Ethernet, Third Edition, July 2005.
- [Luc06] Converged Ethernet Transport Solutions, January 2006, [download at [www.lucent.com](http://www.lucent.com)].
- [RFC1883] IETF (1998). RFC 1883, Internet Protocol, Version 6 (IPv6) Specification, IETF, available at <http://www.ietf.org>.

## Safety

- [AISSafe] AS-Interface Safety at work. Safety in Automation – Introduction and application examples. AS-International Association, Germany, 2004
- [ASI] AS-Interface - The Automation Solution. AS-International Association, Germany, 2002
- [Beck] Beckhoff: Principle of operation, <http://www.beckhoff.com/english>
- [Ce04] G. Cena, A. Valenzano, S. Pitturi, Reti real-time per applicazioni industriali e autoveicolistiche, [www.ieiit.cnr.it/](http://www.ieiit.cnr.it/), 2004.
- [CIPSafe] Open DeviceNet Vendor Association, CIPSafety, White Paper, 2003
- [EPG04] ETHERNET POWERLINK Standardization Group, Award for ETHERNET Powerlink, Press Release Winterthur, 24-03-2004, Available on: [www.ethernet-powerlink.org/index.php?id=35&no\\_cache=1&file=55&uid=307](http://www.ethernet-powerlink.org/index.php?id=35&no_cache=1&file=55&uid=307).
- [EtherCAT] EtherCAT Technology Group, <http://www.ethercat.org>
- [FeSa04] M. Felser, T. Sauter, Standardization of Industrial Ethernet, 2004. Available on: <http://www.ict.tuwien.ac.at/wfcs2004/papers.html>.
- [IBClub] Interbus Club e.V., [www.interbusclub.org](http://www.interbusclub.org)
- [IEC61508] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems - Parts 1-7
- [IGS03] Interests Group SERCOS interface, SERCOS-III - (Third Generation SERCOS interface), Version 1.3.3, November 2003. Available on: [www.sercos.com/pressroom/pdf/SERCOS-III.pdf](http://www.sercos.com/pressroom/pdf/SERCOS-III.pdf) .
- [IGSRT] Interest Group SERCOS INTERFACE, The 31.25 story: Hardened real-time, 2005. Available on [www.sercos.com/downloads/pdf/sercos3brochure.pdf](http://www.sercos.com/downloads/pdf/sercos3brochure.pdf) .
- [ODVA] Open DeviceNet Vendor Association, <http://www.odva.org/>
- [PNO] Profibus Nutzerorganisation e.V., [www.profibus.org](http://www.profibus.org)
- [Sc05] H. Scheitlin, Ethernet Powerlink- Basics, 2005. Available on: <http://www.ethernet-powerlink.org/index.php?id=90>.
- [SE05] SERCOS N.A., SERCOS Safety -- The Safety Protocol for SERCOS interface, news letter issue #16, 2005 Available on: <http://www.sercos.com/pressroom/issue16>.
- [Te03] P. E. Teague, Milestones in motion control, 2003. Available on: [www.eedesign.com.tw/article/ Forum/NS\\_forum-E\\_010710\\_01.htm](http://www.eedesign.com.tw/article/Forum/NS_forum-E_010710_01.htm).
- [Wr05] P. Wratil, Safety-related networks - Ethernet powerlink safety , November 2005. Available on: <http://www.ethernet-powerlink.org/index.php?id=35>.

## Security

- [AB02] Privacy & American Business (2002) Privacy On and Off the Internet: What Consumers Want, Privacy & American Business, Hackensack, NJ.
- [Cordis] See the EU Information Technologies Programme, <http://www.cordis.lu/esprit/>.
- [Cyb01] CyberVote, D4 Volume 2, Report on electronic democracy projects, legal issues of Internet voting and users (i.e. voters and authorities representatives) requirements analysis, <http://www.eucybevot.org/KUL-WP2-D4V2-v1.0.pdf>.
- [ITU02] ITU 2002, Internet for a Mobile Generation Report. Statistical Annex ITU, Geneva, <http://www.itu.int/osg/spu/publications/mobileinternet/>.

- [Kni03] A general comparison between 3G and WiFi is described in W. Lehr and L.W. McKnight, "Wireless Internet Access: 3G vs. WiFi", Telecommunications Policy 27, 351-370, 2003.
- [Mel02] William H. Melody, "Trends in European Telecommunication: 2002 Status Report of Denmark's Progress in Telecom Reform and Information Infrastructure Development", October 2002, LIRNE.NET, [http://www.lirne.net/resources/denmark\\_2002.pdf](http://www.lirne.net/resources/denmark_2002.pdf).
- [Pampas2] PAMPAS. Pioneering Advanced Mobile Privacy And Security, deliverable D02, Preliminary Roadmap, December 2002. Available at <http://www.pampas.eu.org/>.
- [PAMPAS3] Pioneering Advanced Mobile Privacy And Security, deliverable D03, Refined Roadmap, February 2003. Available at <http://www.pampas.eu.org/>.
- [RAPID] Roadmap for European Legal Research in Privacy and Identity Management, <http://www.law.kuleuven.ac.be/icri/publications/421rapid.pdf>.
- [SANS01] E. Piepers, "Cost-effective Information Security", SANS Institute Information Security Reading Room, June 6, 2001, <http://rr.sans.org/audit/cost-effective.php>.
- [Za02] S. Zakiuddin, S. Creese, B. Roscoe, and M. Goldsmith, "Authentication in Pervasive Computing", PAMPAS Workshop #1, Leuven, 16/17 September, 2002, Position Paper, [http://PAMPAS.eu.org/Position\\_Papers/QinetiQ.pdf](http://PAMPAS.eu.org/Position_Papers/QinetiQ.pdf).

#### Co-operation of Private and Public Networks

- [RFC1883] IETF (1998). RFC 1883, Internet Protocol, Version 6 (IPv6) Specification, IETF, available at <http://www.ietf.org>.
- [ALFWIKI] Application Layer Firewall; [http://en.wikipedia.org/wiki/Application\\_layer\\_firewall](http://en.wikipedia.org/wiki/Application_layer_firewall)
- [Demu05] Demuth, T., Leitner, A.: Traffic Trics – ARP spoofing and poisoning, WWW.LINUX-MAZGAZINE.COM, Issue 56, [http://www.linux-magazine.com/issue/56/ARP\\_Spoofing.pdf](http://www.linux-magazine.com/issue/56/ARP_Spoofing.pdf), July 2005.
- [Ele04] Electronicstalk, Sonet evolves resiliency, services and integration, News Release from: Agere Systems, Edited by the Electronicstalk Editorial Team on 18 October 2004.
- [Hill05] Jürgen Hill: "IPv6: Der fast vergessene Jubilar,,", 13.12.2005, [http://www.computerwoche.de/produkte\\_technik/netzwerke/569863/](http://www.computerwoche.de/produkte_technik/netzwerke/569863/).
- [IBM1] <http://www.networking.ibm.com/nhd/webnav.nsf/pages/atm:atm25fe.html>
- [NVIDIA05] ForceWare Networking and Firewall Administrator's Guide, 7th edition, NVIDIA Corporation, April 2005
- [Sor04] Soreon Research, Soreon Top Technologie Trends 2005, November 2004.
- [Svet05] Technologies for improvement of network security (In Czech) [http://www.svetsiti.cz/view\\_list.asp?rubrika=Tutorialy&temaID=289](http://www.svetsiti.cz/view_list.asp?rubrika=Tutorialy&temaID=289)
- [Wiki05] [http://en.wikipedia.org/wiki/Asynchronous\\_Transfer\\_Mode#Successes\\_and\\_Failures\\_of\\_ATM\\_Technology](http://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode#Successes_and_Failures_of_ATM_Technology)
- [Wired96] Steinberg, S.: Netheads vs Bellheads, Wired Magazine, October 1996, [http://www.wired.com/wired/archive/4.10/atm.html?topic=&topic\\_set=](http://www.wired.com/wired/archive/4.10/atm.html?topic=&topic_set=)

#### Engineering tools

- [OPC] OPC Foundation, <http://www.opcfoundation.org>

- [DPWS] Device Profile for Web Services, May 2005,  
<http://specs.xmlsoap.org/ws/2005/05/devprof/devicesprofile.pdf>
- [FDT] FDT Group, <http://www.fdtgroup.org>
- [FDTPress] Press Conference of the FDT group at the SPS/IPC/DRIVES, 2005,  
[http://www.fdtgroup.org/\\_PDF/pr\\_11-23-2005/SPS\\_2005\\_FDT\\_Press\\_Conference.pdf](http://www.fdtgroup.org/_PDF/pr_11-23-2005/SPS_2005_FDT_Press_Conference.pdf)
- [HTTP] RFC 2616, Hypertext Transfer Protocol (HTTP/1.1), <http://www.ietf.org/rfc/rfc2616.txt>
- [IAB] Internet Architecture Board, <http://www.iab.org>
- [ICMP] RFC 792, Internet Control Message Protocol (ICMP), <http://www.ietf.org/rfc/rfc0792.txt>
- [IETF] Internet Engineering Task Force, <http://www.ietf.org>
- [JMS05] F. Jammes, A. Mensch, H. Smit. Service-Oriented Device Communications Using the Devices Profile for Web Services. In 3rd International Workshop on Middleware for pervasive and ad-hoc Computing, 1-8, Grenoble, November 2005
- [Lut04] J. Luth. Unified architecture – The future of OPC. In ControlGlobal.com, 2004,  
<http://www.controlglobal.com/articles/2004/229.html>
- [MIB] RFC 1066, Management Information Base for Network Management of TCP/IP-based internets (MIB), <http://www.ietf.org/rfc/rfc1066.txt>
- [OASIS] Organization for the Advancement of Structured Information Standards (OASIS),  
<http://www.oasis-open.org>
- [SIRENA] SIRENA Project, <http://www.sirena-itea.org>
- [SNMP] RFC 1157, Simple Network Management Protocol (SNMP),  
<http://www.ietf.org/rfc/rfc1157.txt>
- [SOAP] W3C Recommendation, Simple Object Access Protocol (SOAP), Version 1.2,  
<http://www.w3.org/TR/soap12>
- [UDDI] OASIS Standard, Universal Description, Discovery and Integration (UDDI), Version 3.0.2, [http://uddi.org/pubs/uddi\\_v3.htm](http://uddi.org/pubs/uddi_v3.htm)
- [UIC] UPnP Implementers Corporation, <http://www.upnp-ic.org>
- [UPNP] UPnP Forum, <http://www.upnp.org>
- [W3C] World Wide Web Consortium (W3C), <http://www.w3.org>
- [WS-Discovery] Web Services Dynamic Discovery, April 2005,  
<http://specs.xmlsoap.org/ws/2005/04/discovery/ws-discovery.pdf>
- [WSDL] W3C Note, Web Service Description Language (WSDL), Version 1.1,  
<http://www.w3.org/TR/wsdl>
- [WS-Eventing] Web Services Eventing, August 2004,
- [WSPW] Web Services Protocol Workshops, MSDN Microsoft,  
<http://msdn.microsoft.com/webservices/community/workshops/default.aspx>
- [WS-Security] OASIS Standard, Web Services Security: SOAP Message Security, Version 1.0,  
<http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf>
- [ZVEI] Zentralverband der Elektrotechnik und Elektronikindustrie (German association for electrical and electronics industry), <http://www.zvei.de/>  
<http://msdn.microsoft.com/library/en-us/dnglobspec/html/ws-eventing.asp>

General

- [Pin04] J. Pinto, "Intelligent Sensor Networks" , Article in "Automation World" First published 05.04, p. 62. Available at:  
"http://www.automationworld.com/articles/Departments/681.html?ppr\_key=05.2004&sky\_key=05.2004&term=05.2004"
- [ARCDH04] "IT in Manufacturing: Issues Remain" Dick Hill; Vice President ARC Advisory Group  
<http://www.arcweb.com/NewsMag/auto/it-ins49-030404.asp>
- [MaSRA05] *ManuFuture* Technology Platform Strategic Research Agenda (SRA) Author: Manufuture High Level Group and Support Group Collaborator: Emerging Production Paradigms Laboratory (EPP Lab of ITIA-CNR, Italy) pp. 8, 34. Executive Summary is available at: <http://www.manufuture.org/SRA/2005-12-06%20Manufuture%20SRA%20-%20SUMMARY1.pdf>