



VAN

FP6/2004/IST/NMP/2 - 016969 VAN

Virtual Automation Networks

Work Package 1

Requirements and Trend Screening

Task 1.3

Trend Screening and Self-evaluation

D01.3-1-V4

Trend Screening Report on VAN Relevant
Technologies

Version 4

Document type	: Report
Document version	: Final version 1.1
Document Preparation Date	: 04.09.2008
Classification	: Public
Contract Start Date	: 01.09.2005
Duration	: 31.08.2009



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

Rev.	Content	Resp. Partner	Date
0.0	Draft Version	CARTIF	22-05-08
0.2	Corrected draft	CARTIF	13-06-08
0.4	Chapter 2: Wireless	SIEMENS	03-07-08
0.4	Chapter 4: Real Time	CVS	03-07-08
0.4	Chapter 7: Public Networks	IFAK	03-07-08
0.5	Chapter 9: Summary of Conclusions	CARTIF	11-07-08
0.5	Executive Summary	CARTIF	11-07-08
0.6	Chapter 5: Safety	Phoenix Contact	01-08-08
0.6	Executive Summary	CARTIF	01-08-08
0.6	Chapter 9: Summary of Conclusions	CARTIF	01-08-08
0.7	Chapter 2: Wireless	SIEMENS	21-08-08
0.7	Chapter 1: Introduction	BUT	21-08-08
0.7	Chapter 9: Summary of Conclusions	CARTIF	21-08-08
0.8	Chapter 8: Engineering tools	SCHNEIDER	22-08-08
0.9	Chapter 2 added	BUT	28-08-08
0.9	Chapter 1 finalized	BUT	28-08-08
0.9	Revisions made	BUT	28-08-08
1.0	Document consolidation	CARTIF	01-09-08
1.1	Board revision	SIEMENS	04-09-08

Final approval	Name	Partner
Review Task Level	Anibal Reñones	CARTIF
Review WP Level	Frantisek Zezulka	BUT
Review Board Level	Axel Klostermeyer	SIEMENS

Executive summary

This report is the fourth version for the trends on technologies related with VAN used. Therefore it is intended to give an overview of the current position of VAN used and non-used technologies regarding the different technological aspects, which are covered in the technical work packages of the project.

The structure of the document is similar to the one used in previous versions of deliverable D01.3, and may explain the new items markets are pointing to currently. Due to this, the information held previously may complete the one included in this report, and therefore all the previous versions may be taken as references for this one.

It should be taken into account that not all the technological fields that VAN is researching on are having the same growing rates. This fact may lead to a better understanding of the trends, having in mind that some of them are in a peak of growth, while some other ones are at different stages of their life, and therefore figures and expectances for them stand for being different.

The report starts with an introduction in Chapter 1 to 3 with a special focus on trends in technology areas which are used for the VAN platform in chapter 2, and considerations about the (wireless) market approach in industry in chapter 3.. Chapters from 4 to 8 report the current state and market trends on any of the technological fields technical work packages deal with: Wireless (SIEMENS), Real-Time (CVS), Safety (PHOENIX), Security (TSA) and Cooperation of Private and Public Networks (IFAK). Chapter 9 stands for Engineering Tools Trends (SCHNEIDER), and finally a summary of collected conclusions is given at chapter 10.

Chapter 1 gives results of screening of VAN relevant contributions from IFAC and IEEE international conferences and magazines in order to compare recent trends in control and communication theories and the VAN goals.

Chapter 2 concentrates on technologies which the VAN platforms relies on. It is necessary to make sure that the core technologies will not outdate prior to VAN technology coming to market.

Chapters 3 and 4 stand for trends on wireless technologies and wireless market approach, where sensor networks (SANETs) are expected to lead the growth. Concerns about integration of SANETs within automation motivate technology leaders to adapt automation standards for wireless communications.

Chapter 5 describes the trends in real-time, centered on the different merging proprietary Ethernet-based solutions supporting real-time and real-time features regarding QoS, protection against interferences and other possible failures.

Chapter 6 describes the current trends in safety of industrial networks, fieldbus and industrial Ethernet basically. Also issues to be resolved by safety technologies are addressed, as well as protocols already standardized within the 61784-3.

Chapter 7 shows the current trend in security technologies and hot threats. The focus is set on two vulnerabilities affecting technologies addressed by VAN, that is, openSSL and DNS poisoning.

Chapter 8 gives an overview of market trends regarding public networks infrastructure on backbone and end-user approach, both regarding wire and wireless technologies, and its importance to automation adoption of Ethernet and IP technologies.

Chapter 9 reviews the trends in key technologies for the engineering concept like OPC-UA, FDT/TDM and web services.

Chapter 10 summarizes the conclusions of previous chapters.

Contents

EXECUTIVE SUMMARY	3
CONTENTS	4
LIST OF FIGURES	6
LIST OF TABLES	7
1 INTRODUCTION	8
1.1 TECHNOLOGY TRENDS	8
1.2 MARKET TRENDS	9
1.3 TRENDS IN AUTOMATION COMMUNICATION SYSTEMS	10
2 TRENDS IN TECHNOLOGIES CONSIDERED FOR THE VAN PLATFORM	11
2.1 OPENVPN	11
2.2 OPC UA	12
2.3 COEXISTENCE OF WIRELESS TECHNOLOGIES	12
2.4 WEB SERVICES	12
2.5 IPV4 / IPV6	12
3 MARKET APPROACH IN INDUSTRY COMMUNICATION	13
3.1 GENERAL TRENDS IN INDUSTRIAL COMMUNICATION SYSTEMS	13
3.2 WIRELESS TRENDS IN INDUSTRY	14
3.3 MARKET TRENDS IN WIMAX	17
4 TRENDS IN WIRELESS TECHNOLOGIES	19
4.1 IEEE 802.11N	19
4.1.1 Status of approval	19
4.1.2 Product requirements and user plans	19
4.2 BLUETOOTH	20
4.2.1 Compatibility with UWB and Wi-Fi	20
4.2.2 Ultra Low Power Bluetooth	20
4.3 WIRELESS PERSONAL AREA NETWORK	20
4.4 OTHER WIRELESS NETWORKS	21
4.4.1 WirelessHART	21
4.4.2 ISA100.11a	22
4.4.3 Mesh Networking: IEEE 802.11s	23
4.4.4 ZigBee: IEEE 802.15.4	23
4.5 REAL-TIME COMMUNICATION IN IEEE 802.11 NETWORKS	24
4.6 ENERGY-EFFICIENCY	24
5 REAL TIME	25
5.1 INTRODUCTION	25
5.2 MARKET ANALYSIS FOR INDUSTRIAL REAL TIME COMMUNICATION	25
5.2.1 HSCI	25
5.2.2 RAPIenet	25
5.2.3 AFDX	27
5.2.4 TTEthernet	27
5.2.5 CC-Link IE (Industrial Ethernet)	27
5.3 CONCLUSION	28
6 SAFETY	29
6.1 STATUS OF STANDARDISATION OF SAFETY NETWORKS	29

6.2	UNRESOLVED ISSUES FOR SAFETY TECHNOLOGIES.....	30
7	SECURITY.....	31
7.1	CURRENT STATUS OF SECURITY THREATS	31
7.1.1	<i>Vulnerabilities</i>	31
7.1.2	<i>Spam and Phishing</i>	31
7.1.3	<i>Malware</i>	32
7.1.4	<i>Other threats</i>	32
7.2	IMPORTANT VULNERABILITIES FOR THE TECHNICAL BASIS OF VAN	32
7.2.1	<i>Cryptographic weaknesses in openssl based systems</i>	32
7.2.2	<i>DNS poisoning attacks</i>	32
7.3	NEW TRENDS IN SECURITY TECHNOLOGIES	33
7.3.1	<i>VPN</i>	33
7.3.2	<i>WEB 2.0</i>	33
7.3.3	<i>Enterprise Master Data Management</i>	34
7.4	APPLICABLE SECURITY STANDARDS AND THEIR ORIGINS	34
8	COOPERATION OF PRIVATE AND PUBLIC NETWORKS.....	36
8.1	TRENDS IN GENERAL.....	36
8.1.1	<i>Metro Ethernet equipment sales up 27% in 2007, more carriers using and testing</i>	36
8.1.2	<i>Carriers report 90-100% increase in Ethernet traffic</i>	37
8.1.3	<i>Service provider router and switch sales hit all-time high in 2007, led by Cisco, Juniper</i>	38
8.1.4	<i>WiMAX equipment market up 46% in 2007, forecast to hit \$7.7B in 2011</i>	39
8.1.5	<i>Mobile backhaul equipment market set to skyrocket due to exploding mobile data/video use</i>	40
8.2	TRENDS IN AUTOMATION.....	41
9	ENGINEERING TOOLS.....	42
9.1	INTRODUCTION	42
9.2	OPC.....	42
9.3	FDT/DTM	42
9.4	PLUG-AND-PLAY	43
9.5	SNMP AND MIB.....	43
9.6	WEB SERVICES	43
9.7	CONCLUSIONS ABOUT ENGINEERING TOOLS.....	43
10	SUMMARY OF CONCLUSIONS	45
	Wireless.....	45
	Market Approach in Wireless Technologies	45
	Real-Time.....	45
	Safety	46
	Security	46
	Cooperation of Private and Public Networks	46
	Engineering Tools	46
	GLOSSARY	48
	REFERENCES	53

List of figures

Fig 3-1 IMS Study of Installed Network Nodes	13
Fig 3-2 Forecast of Market for Ethernet-based nodes	14
Fig 3-3 Industrial Wireless Market Growth in Millions of Dollars (cf. [WINA07], p. 18).....	15
Fig 3-4 Use of CIT Equipment for Field Operations (in %)	16
Fig 3-5 User Plans for Wireless LAN (in %)	16
Fig 3-6 Benefit of Back-end Applications from Mobile Computing in Field Operations (in %).....	17
Fig 3-7 Worldwide WiMAX Equipment Manufacturer Revenue Forecast	18
Fig 4-1 Timeline of Wireless HART approval (cf. [HART07b]).....	22
Fig 4-2 Number of Installed HART Devices (acc. to [HART07b])	22
Fig 5-1: Forwarding and Receiving Ethernet Frames with RAPIEnet	26
Fig 5-2: Link status monitoring	26
Fig 5-3: CC-Link IE Specification	28
Fig 6-1 Safety Gateway between PROFIsafe-DP and ASI-Safe	30
Fig 8-1 Worldwide Metro Ethernet Manufacturer Revenue by Technology	37
Fig 8-2 Traffic Growth by Protocol	38
Fig 8-3 Worldwide Service Provider Router and Switch Manufacturer Revenue Forecast	39
Fig 8-4 Worldwide WiMAX Equipment Manufacturer Revenue Forecast	40
Fig 8-5 Worldwide Mobile Backhaul Equipment Revenue	41

List of tables

Tab 4-1 Methods for Supplying Additional Power (cf. [Gar08], p. 2)	20
Tab 4-2 ISA100 Usage Classes (cf. [ISA08b]).....	23
Tab 6-1 Examples of Fieldbus and Industrial Ethernet Safety Protocols.....	29

1 Introduction

Due to the review recommendations, a comprehensive screening of VAN relevant contributions in proceedings of 17th IFAC World Congress, IEEE conferences, scientific magazines, and other relevant conferences and symposia as well as reputable scientific and technology magazines have been done in order to specify trends in the control and communication theory and practice towards VAN goals and VAN methods and development procedures. After this screening the following trends have been recognized:

1.1 Technology Trends

Since first years of the 21st century one of the hot topics in the control engineering community seems to be a discussion about a lack of control theory for purposes of modern digital automation of machines, production lines and technological processes. The modern automation is characterized by digital distributed controllers, hierarchical organization of a computer control, non-synchronous sampling period in distributed control systems and overloading of embedded microcontrollers, sophisticated control algorithms and ubiquitous high-speed communication.

This situation is mirrored by many contributions from technical and scientific conferences, and in technical and scientific magazines. The result of such investigations is that the control theory has too few relevant methods for such purposes. For such systems the term of Networked Control System (NCS) has been newly established. The specification of the NCS is in relevant references available [Zam08], [Lit08].

One of the first steps in response to the abovementioned situation represents the special issue [Hir08] of the reputable German scientific magazine *Automatisierungstechnik* 1/2008. The issue is dedicated exclusively to the NCS. A reason for it is that the German scientific – technical society – the Deutsche Forschungsgemeinschaft announces a project and provides financial support to an interdisciplinary 6-years program Nr.1305 titled *Control Theory for Networked Control Systems*. The aim of the program is investigation and evolvement of modelling, analysis and design of recent and future phenomena in NCS. The theory should come out from existing control theory and extend it towards solution of phenomena brought in by NCS. The solution incorporates optimal design of control and communication systems or extension of control theory towards control theory of nonlinear NCS. Furthermore stability of NCS with time varying delay, failure compensation or performance index changes by aimed change of the control structure and others. Authors of the program believe that the potential theory that has to be developed will integrate existing theory of digital communication and digital control theories. It is well known that the classical control theory systems originally derived from frequency methods for electronic particles, and physical systems are insufficient for the NCS. It is assumed that NCS will unify the modern communication and control theories of digital systems, due to the integration of communication systems into the control systems [Hir08], [Hal05].

Further trend stems from the area of computer systems for purposes of automatic control [Hal05]. One of the very important research directions within the area of dependability is reconfiguration of control systems. This issue is highly related to the research carried out in the area of fault detection and fault diagnosis. The results of a diagnosis should directly influence remedial measures to be taken, resulting in adaptation of control laws or complete reconfiguration of control strategies.

The trend to work out a theory of Networked Control Systems as well as strengthen of tendency towards reconfigurable control systems respect the recent control architecture, characterized by ubiquitous communication among distributed instrumentation, control and supervisory systems and try to solve theoretical problems of such architecture. It corresponds well with VAN goals. VAN aims is to make the communication open, transparent, real-time, safe and secure with particular attention to wireless technologies with development of appropriate engineering tools. Hence, VAN goals are in the

practical level, and the above specified trends in the control theory confirm correctness of VAN goals and VAN methods.

Trends related to the VAN are indicated in the area of embedded systems and stem from manufacturing area in order to fulfil following requirements (well corresponding with requirements of the VAN requirement database, specified in T1.2): dependability, real-time communication, flexibility/reconfigurability/agility, modularity, openness, location transparency (name based routing), autonomous behaviour, security.

Advances in microelectronics and in SW and communication systems now allow embedded systems to be composed of a set of processing elements and the trend is toward significant enhanced functionality, complexity, and scalability since those systems are increasingly being connected by wired and wireless networks to create large-scale distributed real-time embedded systems (DRES) [Per06]. This tendency influences firstly the manufacturing area. DRES enables to re-examine every aspect of traditional manufacturing needs and their traditional solutions. The IFAC Technical Committee 5.1 concentrates its attention on Manufacturing Plant Control. The main technical event of the committee is INCOM symposium series [Per06]. The contributions from INCOM 2006 confirms that the TC 5.1 indicates a clear trend towards distributed automation architectures, on which automation devices with local processing capabilities are interconnected through industrial communication protocols. This distributed manufacturing automation architecture strongly relies on an underlying architecture composed by the DRES. From the VAN activities so far, it can be traced that VAN trends in manufacturing correspond to trends indicated by the IFAC TC 5.1.

A trend in the area of embedded systems is the idea of intelligent maintenance systems or intelligent prognostics systems. Such systems use information provided by sensors and apply algorithms for health estimation and failure prediction. Embedded computing elements (such as embedded sensors and actuators) will play a fundamental role in the development of such intelligent maintenance systems. Therefore, a trend from manufacturing branch that can be indicated is the penetration of system on chip (SoC), reconfigurable hardware and other new technologies. These will be used as realization platforms for the development of embedded systems for intelligent prognostics [Per06]. The System on Chips are very promising because several integrated processors even of different types (microcontrollers, DSP, RISC, NISC, and multi-core processors [Bar2007]), together with memories and other components enable development of highly flexible embedded components for manufacturing purposes [Per06].

Because embedded systems lie in focus of VAN, the abovementioned trends in manufacturing correspond well with VAN architecture in automation devices and the manufacturing area seems to be one of the main application areas of the VAN outputs.

1.2 Market Trends

The respected organization in the field of market research (ARC advisory group) predicts continuous growth of the market with wireless devices and industrial Ethernet. Potential customers are mainly interested in stability, security, availability, and real-time aspects of wireless solutions.

The nowadays trend in wireless technologies is coexistence of different wireless networks with focus on reliability and interoperability. The also important is effective power management of wireless devices, which opens way to use of renewable energy sources in new areas.

With respect to real-time capabilities, it is expected that only a couple Ethernet protocols will dominate the market, however there are also protocols which offers hard real-time capabilities. These protocols - HSCI, RAPIenet, and AFDX can be considered as alternatives that may solve specific customer requirements.

Although safety layer for fieldbus systems can be considered mature, in industrial Ethernet there are still some unresolved issues caused by different definition of the black channel. The key role in the safety area plays standardization.

The engineering tools relevant to VAN are still evolving. Updated OPC specification offers new version of software development kit with sample implementations for developers. The new compliance certification program for OPC is established. Tools, which are based on FDT technology,

have now more coverage in fieldbus systems. The high future potential will offer utilization of Web services for find, share, and control devices on a network. On the other hand the broader use of Web services and IP based solutions results in stronger demand for trustworthy security solutions at all levels of the communication hierarchy. Defense in depth and distributed security with intrusion detection are the trends in the field of security solutions.

1.3 Trends in Automation Communication Systems

The Trends in Automation are already described in [D01.3-1-V1]. 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 keep significant market share over the next few years. Especially the number of available Industrial Ethernet technologies (e.g. EtherCat, PROFINET, SERCOS III, etc) is growing. Furthermore these proven technologies are supported by further developments and increased functionality and enhanced real-time support. However, in the near future the broad spectrum of such technologies will be confined. The best technologies will become more prevalent and will get broader acceptances and market penetration.

2 Trends in Technologies Considered for the VAN Platform

The main objective when defining the VAN platform in [D02.2-1] has been to keep the platform as open as possible, diminishing the susceptibility of the VAN technology to outdate. However, implementation phase requires sticking to specific technologies to be able to demonstrate the VAN functionality. Nevertheless, it is to say that the chosen technologies may be changed upon need.

In this chapter, we recognize the following focus points to be investigated from the trend perspective as points can be subject to significant evolution:

- OpenVPN
- OPC
- Coexistence of wireless technologies
- Web Services
- IPv4/IPv6

Subsequent chapters will deal with these focus points.

2.1 OpenVPN

As has already been mentioned, the VAN platform is not bound to single specific implementation of the core technologies. Thus, if the OpenVPN implementation appeared to be at the end of the lifecycle, it would be replaced by another one. However, such a risk is not expected for the following reasons introduced at [OpenVPN]. Firstly, the OpenVPN community has reached 2.5 million users. Secondly, the OpenVPN was announced winner for "Best SSL VPN" in the 2007 Best of Open Software Awards by InfoWorld [InfoWorld].

Hence, the core question of the trend evaluation is the use of virtual private networks (VPN). By definition, virtual private networks are used to interconnect enterprise networks over public networks with the same level of service and security as if these networks were a single enterprise network. Based on the research information sources, we assume that the solution based on web services and VPNs is correct.

The milestone report [Nof] introduced at the 17th IFAC World Congress focuses on trends in e-Manufacturing, e-Logistics, and e-Service Systems. It shows a far more advanced role of communication in manufacturing and process industry than a mere control communication based on fieldbuses. Communication over public networks comes to focus, providing new perspectives to industries.

VPNs are an established solution providing the required level of service, especially from the security point of view. An alternative to VPN, providing application level security and being well established, is IPSec. IPSec, though a very ambitious project, is nowadays less established. Apart from the former approach, it relies on network level security. Network level security expects that all network hops on the path accommodate IPSec to provide the security measures. For this reason and also because of inclusion of significant additional processing overhead, VPN approach has remained the core technology.

From the trend point of view, both approaches are persistently evolving. OpenVPN will be exhibited at Interop, in Las Vegas in 2009. IPSec is expected to obtain intrinsic support in IPv6.

2.2 OPC UA

OPC UA (OLE for Process Control - Unified Architecture) was released in 2006. The main difference from the former version is that the technology no longer uses Microsoft Distributed Communication Object Model (DCOM) transport layer but makes use of Web Services. It is to say that the VAN project is in accordance with this trend as we make use of Web Services from the very beginning.

OPC UA is also referred to further in this document. Actual reference to applications of OPC in embedded devices proving its practical use can be found in [Damm07], [Nie07], and [Hop07].

2.3 Coexistence of Wireless Technologies

According to Rauchhaupt [Rau08] the key topics in the wireless area 2008 are the coexistence of different wireless technologies at one location, sensor networks, and wireless PROFIBUS and PROFINET. Rauchhaupt is head of VDI/VDE expert committee "Wireless communication in industrial automation" and head of "Wireless industrial communication" at IFAK Magdeburg. VDI/VDE is planning to publish a directive this year that will address above-mentioned topics.

2.4 Web Services

The ongoing progress in development has been assured by the World Wide Web Consortium (W3C), who develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential. W3C is a forum for information, commerce, communication, and collective understanding.

The milestone report [NOF] also states that web services, among others, are a means to improve enterprise integration in future.

2.5 IPv4 / IPv6

It is still difficult to get bound to a certain IP version. IPv6 promises increased quality of service intrinsically by flow identification number and support to IPSec, however the migration from IPv4 is far slower than expected.

From the investigations, we observe no significant risk in case of migration to IPv6. The ASE definition denote the IP address as a string, thus, allowing IPv6 address if necessary. According to [Chao], the backward compatibility and smooth transition has been assured by *IPv4-mapped address* and *IPv4 compatible address*. The temporal effect caused by a different mechanism of IP-lookup can be studied also in [Chao].

3 Market Approach in Industry Communication

3.1 General trends in industrial communication systems

The studies mentioned in [D01.3-1-V1] and [V2] were replaced by new ones and reevaluated. In general the growth of the use of Ethernet goes, on but with a steadier rate as predicted in 2005. A new study of installed field devices shows that a steady raise of Ethernet based technologies leads to a continuous worldwide stable growth of industrial networks (see Fig 3-1 IMS Study of Installed Network Nodes). An IMS Study [IMS] from 2007 prognoses a mean growth of 13 percent per year within the next 5 years. A higher growth of 20.3 percent is expected for Ethernet based protocols. An above-average growth in field of Ethernet technology is expected in the Asia pacific region with about 26.3 percent. Some years ago, the expectation of growing was even higher but technological borders slow it down. Meanwhile, technologies like EtherNet/IP, IEC 61158-10 or EtherCAT are well founded to build up efficient automation systems with the required performance. Nevertheless, classic fieldbus technology is also still growing, because Ethernet does not fulfill all customer requirements at the moment.

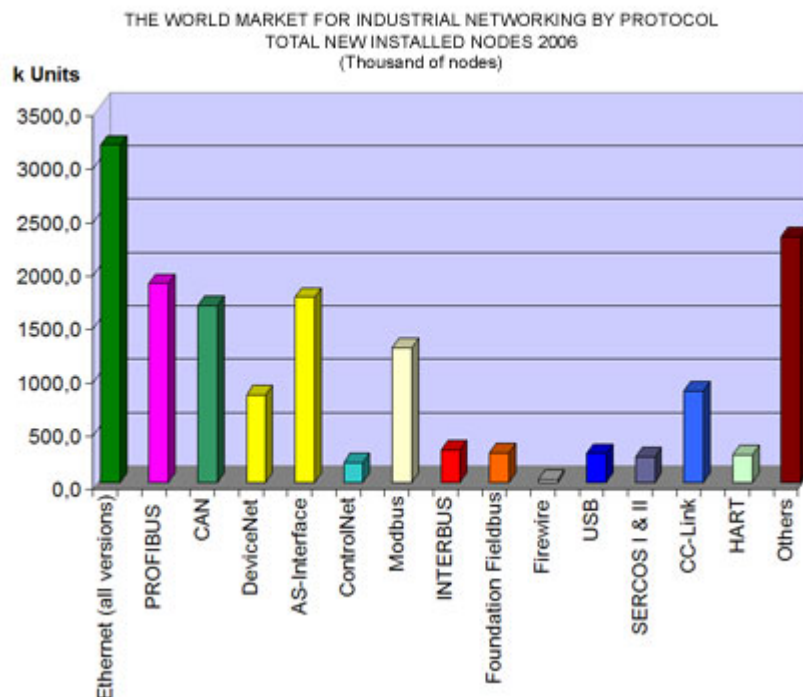


Fig 3-1 IMS Study of Installed Network Nodes

An additional aspect that should be mentioned in this context, is a comment from Senior Market Analyst John Morse that underlines the study: "Industrial Ethernet appears to be following the same path trodden by fieldbus protocols; with a growing number of variations on the theme. Many of the variants will find their niche in the market however, it will come as no surprise that the research found that PROFINET is forecast ultimately to dominate the EMEA region and Ethernet/IP will enjoy the lion's share in the Americas". This is due to the relative strength of Siemens and Rockwell Automation

in EMEA and the Americas respectively. Morse continued, "However, the report predicts that the mix of technologies will be more even in Asia."

A further report coming from the ARC group [ARC] showing a 5 year forecast that says that the worldwide market for Ethernet-based devices and I/O is expected to grow at a compounded annual growth rate (CAGR) of 27.5 percent. The market size totaled over 1 million nodes in 2007 and is forecast to increase to over 3 million nodes by 2012 (Fig 3-2 Forecast of Market for Ethernet-based nodes).

**The Worldwide Market for Ethernet-Based Device Networks
(Thousands of Nodes)**

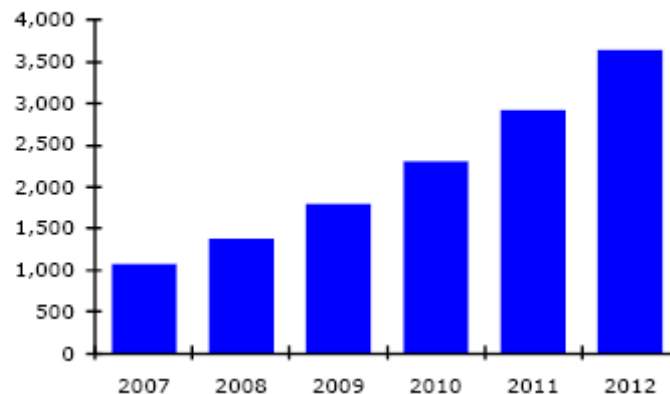


Fig 3-2 Forecast of Market for Ethernet-based nodes

The report claims that the advent of automation-applicable standards, intelligent implementation strategies, and overall improvements in product reliability have made Ethernet a lead option in even the most demanding motion control applications. Of even greater import as far as growth potential is the market emphasis on Ethernet's commonality rather than its openness. The principal author of ARC's "Ethernet-based Device Networks Worldwide Outlook" ARC Vice President Chantal Polsonetti says, the "Standardization of layers 1 and 2 of the Ethernet stack in IEEE 802.3 makes Commercial Off the Shelf (COTS) physical layer products widely available and familiar to potential OEMs and end users, but, as always seems to be the case in the industrial automation segment, each major supplier wants to support their own higher-level protocols. For the customer, this translates to common physical layer components throughout the enterprise but multiple competing protocols at the automation layer".

3.2 Wireless trends in industry

According to Caro and Reizner (cf. [ISA08a], p. 6), an open consensus industry standard is important to the end-user, because without them the price for wireless will not be acceptable to the masses. Van Dierdonck (cf. [Die08]) states more reasons for the need of standardization: "compliance with global regulations, interoperability across brands, second sourcing availability, and the opportunity to tap into a large body of knowledge".

According to ARC, the Industrial Wireless Market is continuing to grow rapidly over the next 5 years (Fig 3-3).

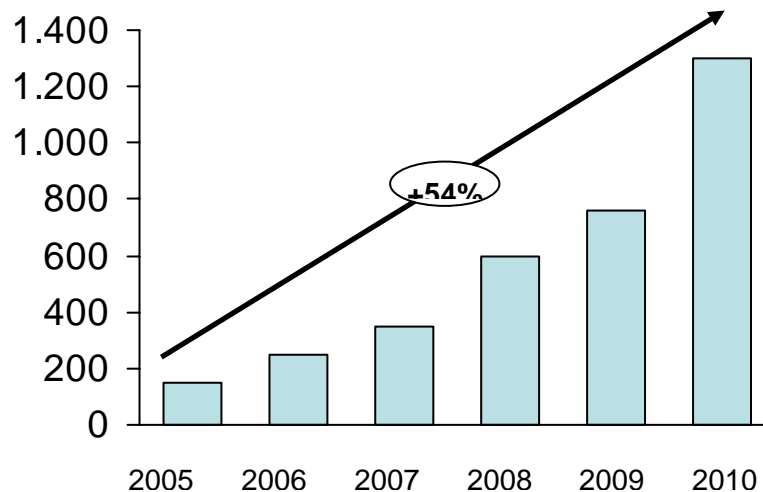


Fig 3-3 Industrial Wireless Market Growth in Millions of Dollars (cf. [WINA07], p. 18)

The market for wireless devices and equipment in process manufacturing will grow to over \$1.1B in 2012, a growth rate of 32% per year, according to a new ARC Advisory Group study "Wireless in Process Manufacturing Worldwide Outlook." Wireless process sensing is expected to be the fastest growing market segment. The driving force is its dramatically lower installation cost. Wireless LAN use will also grow rapidly, spurred by the introduction of new access points that can safely be installed in the hazardous environments. The longer range and clearer signals of future 11n will also make them attractive to process industry customers (cf. [Con08]).

According to Forbes, senior analyst at ARC, the early adopters of wireless applications in process manufacturing will be (cf. [WINA07], p.19):

- Sensing
- Equipment Condition Monitoring
- Mobile Operator Support
- Location Tracking

A survey conducted by ARC shows the current and planned use of wireless in industrial applications (cf. [WINA07], pp. 6-8):

- What kinds of CIT equipment do your firm use (or plan to use) in support for field operations?

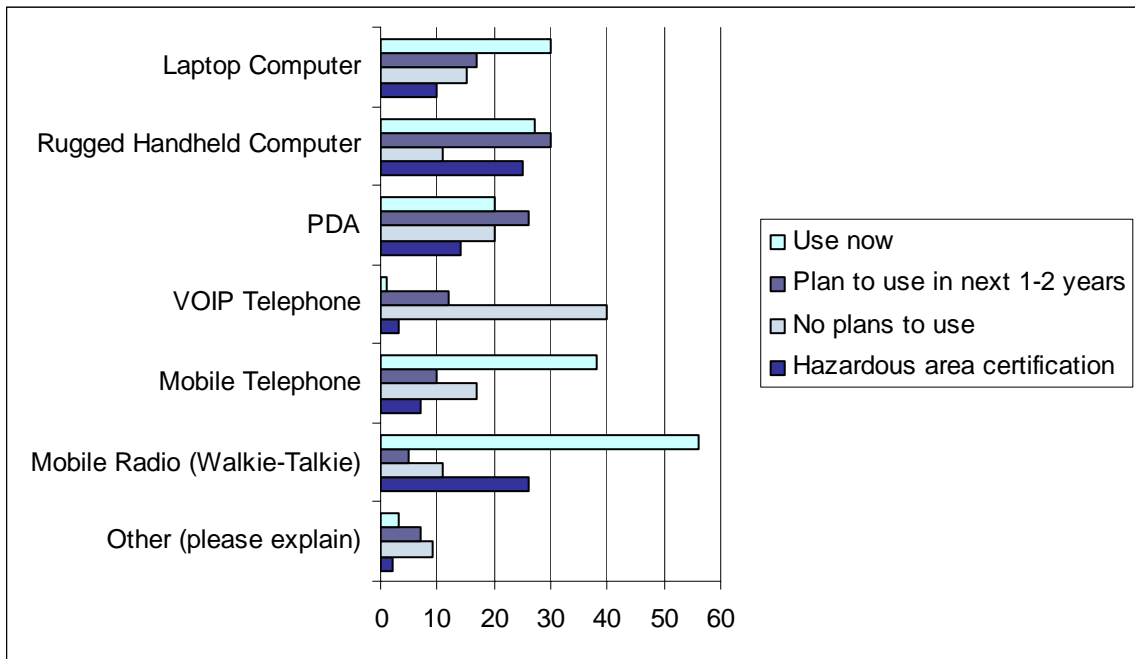


Fig 3-4 Use of CIT Equipment for Field Operations (in %)

- What is your company's plan for providing Wireless LAN coverage in these areas of your plants?

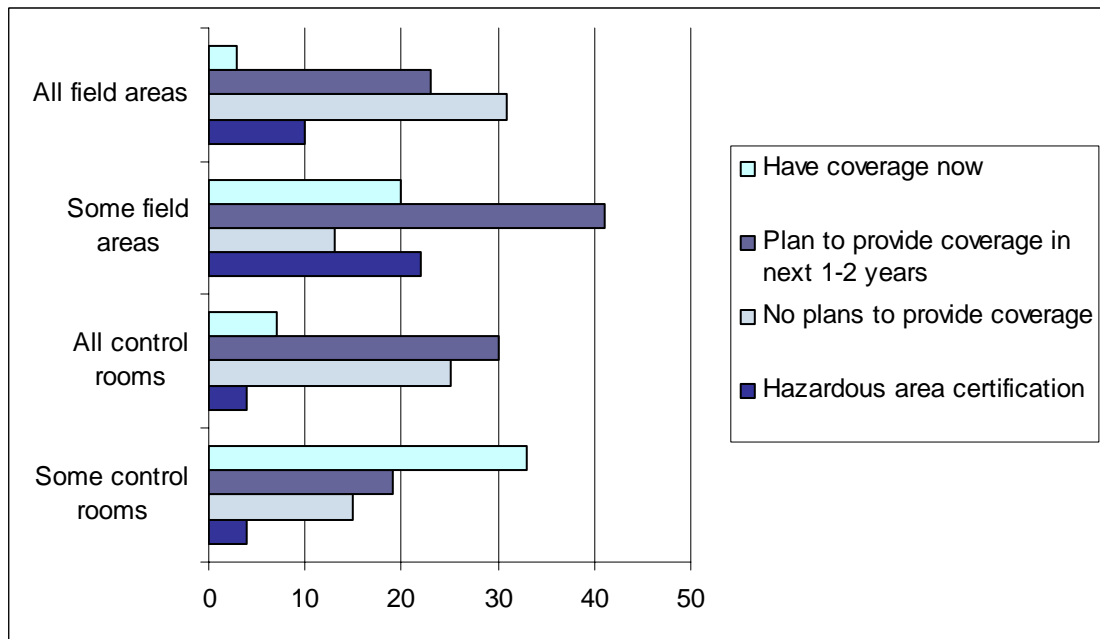


Fig 3-5 User Plans for Wireless LAN (in %)

- How much do you believe these 'back-end' applications can benefit from mobile computing, mobile communication, and IT in field operations?

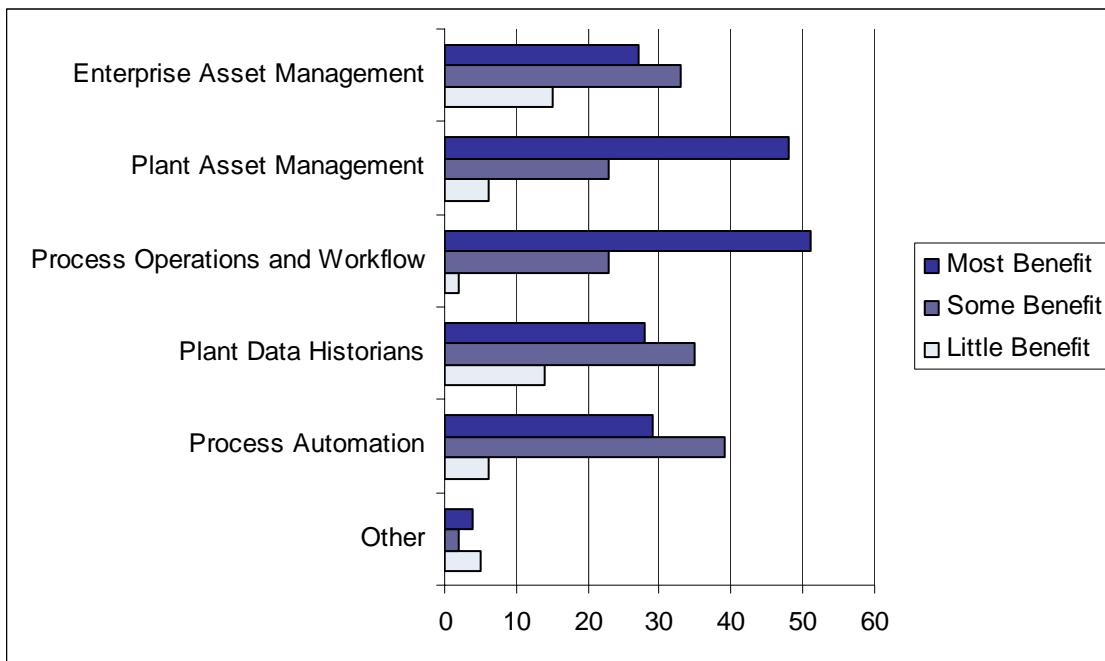


Fig 3-6 Benefit of Back-end Applications from Mobile Computing in Field Operations (in %)

On behalf of VDMA, in January/February 2008 the technical college of Suedwestfalen (FH Suedwestfalen) in Germany conducted a survey among potential users of industrial communication products (engineering companies, engineering consultants). The results show a trend towards wireless (87% of respondents see advantages) but 70% are still concerned about the use of wireless in industrial applications. The main concerns are: stability (76%), IT-security (45%), availability of industrial products (42%), and real-time capability (28%) (cf. [Gri08], pp. 70-73).

Only 25% of respondents indicated to connect automation components via wireless today. However 49% of respondents plan to use wireless technologies in the future. WLAN is remaining the dominating wireless technology: 23% today vs. 41% in future but also the proportion of Bluetooth users will double from 8% to 16% (cf. [Gri08], pp. 70-73).

Despite the lack of a final standard and the higher costs of the associated infrastructure Gartner predicts that 11n APs will surpass a/b/g-only AP shipments by year-end 2009 (cf. [Gar08], p. 3).

3.3 Market trends in WiMAX

LONDON, UK, February 28, 2008—The WiMAX market sequentially grew 11% for the quarter and 46% for the year, with worldwide sales of fixed and mobile WiMAX equipment hitting just under \$800 million in 2007, says Infonetics Research in its latest WiMAX and Mesh Network Equipment and Devices report.

WiMAX has been deployed in more than 80 countries worldwide, and commercial networks will continue to grow in number and size in 2008, the report shows. Infonetics forecasts the WiMAX market to grow to \$7.7 billion in 2011.

“Several recent developments are giving a boost to the WiMAX market,” said Richard Webb, wireless analyst for Infonetics Research. “Among the most significant developments: Cisco’s acquisition of mobile WiMAX vendor Navini Networks, the market entrance of specialist ASN gateway vendor WiChorus, the launch of WiMAX phones and Ultra Mobile PCs, and the new Open WiMAX initiative, which promotes disruptive, all-IP open WiMAX architecture, and should lead to best-of-breed solutions with inter-vendor interoperability.”

Other highlights:

- Mobile WiMAX equipment grew in high double-digit percents every quarter of 2007

- Worldwide sales of ASN gateways, which aggregate traffic from mobile WiMAX base stations, grew nearly 10-fold from 2006 to 2007
- The number of worldwide WiMAX subscribers (fixed and mobile) topped 2.2 million in 2007, led by the Asia Pacific region; the majority are fixed WiMAX subscribers
- Alvarion maintains its lead in worldwide fixed WiMAX equipment revenue share in 2007, followed by Airspan
- Motorola is the leader in worldwide mobile WiMAX equipment revenue share in 2007, followed by Samsung

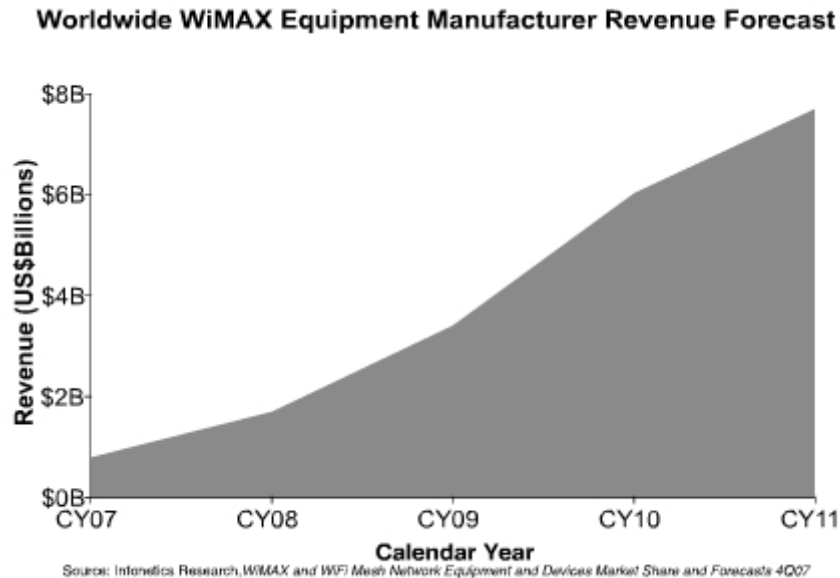


Fig 3-7 Worldwide WiMAX Equipment Manufacturer Revenue Forecast

4 Trends in Wireless Technologies

This chapter summarizes trends in different technologies considered for the VAN project. Advances in development of the considered technologies are focused.

4.1 IEEE 802.11n

4.1.1 Status of approval

As of October 2007, Draft 3.0 has been released, providing revisions for areas such as security establishment, Clear Channel Assessment (CCA) as well as MAC layer management of channel switching and PHY features (LDPC, STBC, etc.) (cf. [Pau08], p. 52). Draft 3.0 offers the potential of throughputs beyond 200 Mbps, based on physical layer (PHY) data rates up to 600 Mbps (cf. [Pau08], p. 28). The standard is expected to be finalized in June 2009 (as of May 2008).

One drawback of the IEEE 802.11n PHY compared to the IEEE 802.11a/b/g standards is that the potential for interference with other radio-based systems operating in the ISM band (2.4 GHz) is substantially higher than with the 11a/g solutions (cf. [Pau08], p. 52).

Although the two standards WiMAX and 11n describe the use of separate frequency bands (resulting in minimal signal interference), co-existence is still a concern due to the similarity of many aspects of the respective usage models (cf. [Pau08], p. 53). Regarding co-existence with Bluetooth, the shared use of the ISM band clearly creates interoperability issues. The frequency hopping used by Bluetooth does not provide significant protection from interference with 11n products. Thus Paul and Ogunfunmi conclude that interoperability of IEEE 802.11n and Bluetooth still remains an area of ongoing research (cf. [Pau08], p. 52-53).

4.1.2 Product requirements and user plans

Although the standard is still in draft it is not expected that the official standard will differ in any meaningful way from the current version of specification, and, if it does, backwards compatibility is all but assured (cf. [Far08], p. 1).

Because of the late approval of 11n (originally approval was planned for 2005) the Wi-Fi Alliance 2007 started a certification program for products based on 11n Draft 2.0. Until now 330 products (as of June 2008) have certified [Wif02]. Pre-N chip sets are also available in the market (cf. [Hof08], p. 12).

According to a survey of 195 IT executives in U.S. and Canada (cf. [Cox07]) 44% already have decided to implement 11n wireless LANs. But there are still concerns about moving to IEEE 802.11n: cost (69%), compatibility (60%), security (47%) and technical complexity (33%).

11n requires a complete redesign of WLAN-components (cf. [Hof08], p. 11-12). APs have to support gigabit and need higher processing power. For the power supply of devices with higher power consumption IEEE is working on the standard 802.3at "Power over Ethernet Plus" (PoE Plus). The PoE standard allowed for 14 W of power is not enough for 11n APs, thus the 3rd Draft of the PoE specification calls for 24 W of power over Ethernet cable (cf. [Schwa08]).

According to Brad Booth, chairman of the Ethernet Alliance, the roadmap beyond PoE Plus is uncertain, but the task force is looking at higher power output over Ethernet, although the current tactic of bundling cables together might not be viable due to the heat generated beyond 24 W at this time (cf. [Schwa08]). Final ratification of the standard is planned for August 2009.

Gartner also discusses the higher power requirement of 11n APs. Since the 11n APs require 20% to 50% more wattage than the a/b/g APs, Gartner proposes several methods for supplying additional power (cf. [Gar08], p. 2):

Method	Available Power	Effect
Power injectors/direct alternating current power to AP	Limited only to the maximum available according to code	Higher initial purchase costs, one more device to manage
Two PoE ports per AP	25.5 watts	Double the cost for PoE ports
Gigabit Ethernet or 802.3 AT switches	30 watts or more	GigE port typically costs two to three times that of 10/100
Proprietary power diverting within the PoE switch	24 watts or more, depending on the solution	Reduced power available for other PoE ports; may require double the port count
Reduce special streams/radio power	12.95 watts	Less than 300/600mbps; reduced coverage footprint

Tab 4-1 Methods for Supplying Additional Power (cf. [Gar08], p. 2)

4.2 Bluetooth

4.2.1 Compatibility with UWB and Wi-Fi

The Bluetooth SIG is developing an innovative method of radio substitution. The new technology will enable Bluetooth connections to hop on neighbouring Wi-Fi networks, when necessary, for high data throughput applications. This architecture is called 'Alternate MAC/PHY'. The core specification is expected to be published to members in mid 2009 (cf. [Bluetooth08b]).

Within the scope of a two-phased roadmap for higher speeds, the Bluetooth SIG is already working with the WiMedia Alliance (since 2006) to use the ultra-wideband (UWB) technology as the high-speed channel for Bluetooth technology. The prototyping phase is expected in 2008 with availability in the first half of 2009 (cf. [Bluetooth08a]).

4.2.2 Ultra Low Power Bluetooth

Since 2007, the Bluetooth SIG began its working on an Ultra Low Power Bluetooth (ULP Bluetooth) specification (originally called Wibree Technology) (cf. [Bluetooth08a]). The announcement of the first version of specification is expected end of 2008 with chip shipments following closely behind. Consumers should be able to purchase the first ULP Bluetooth enabled products in 2009 (cf. [Bluetooth08c]).

But according to Forbes, senior analyst at ARC, "the new technology is not suited for most existing wireless sensing applications, and is certainly unsuited for industrial applications: Manufacturers should expect no impact from Bluetooth ULP on their wireless sensing plans for the foreseeable future." (cf. [For07], p. 78).

4.3 Wireless Personal Area Network

A standard for millimeter-wave-based communications is being developed within Task Group IEEE 802.15.3c. It will specify alternative physical layer (PHY) for the existing 802.15.3 Wireless Personal Area Network (WPAN). This millimetre-wave WPAN will operate in the 57-64 GHz unlicensed band and will allow high coexistence (close physical spacing) with all other microwave systems in the 802.15 family of WPANs. In addition, the millimeter-wave WPAN will support high data rate at least 1 Gbps applications. Final approval of the standard is planned for September 2009 (cf. [IEEE08b]).

Currently the common conclusion of the most publications concerning the coexistence of WPAN and WLAN is that data loss for packets transmitted through WPAN is possible because of WLAN

interference (cf. [Bin08], p. 107). Wireless Personal Area Networks (WPAN) and WLAN use the same ISM 2.4 GHz band. The increase of transmitting power up to 10dBm is in Europe allowed for sensor networks but this can only reduce but not avoid the interference. An automatic frequency adoption (available for WirelessHART and ZigBee 2007) supports the stability of the network (cf. [Bin08], p. 114).

Ecma International (TC48) is also developing a standard for a 60 GHz PHY and MAC for short range unlicensed communications. The standard will provide high rate wireless personal area network (including point-to-point) transport for both bulk data transfer and multimedia streaming. Approval is estimated for December 2008 (cf. [ECMA08a], [ECMA08b]). Ecma is a non-profit industry association of technology developers, vendors and users developing standards for Information and Communication Technology.

In July 2008, the WiMedia Alliance (non-profit industry association that promotes ultra-wideband worldwide) and Ecma International closed an agreement to jointly develop standards in the future. The structure of this relationship between an internationally recognized standards development organization and an industry special interest group is unique (cf. [WiM08]).

4.4 Other Wireless Networks

According to Milosiu (cf. [Mil08], p. 54) Bluetooth and ZigBee are in an inferior position to proprietary solutions regarding energy consumption if packets are below 250 Bit. For packets over 400 Bit standard solutions could be more efficient.

At Fraunhofer Institute for Integrated Circuits (IIS) a wireless transceiver for 868 MHz in CMOS-technology was developed with a current consumption of about 10 μ A. Standard solutions need more than 1mA.

4.4.1 WirelessHART

In September 2007, the WirelessHART standard as part of the HART 7.0 specification was released (cf. [HART07b]). According to the HART Communication Foundation, the WirelessHART standard provides a robust wireless protocol for the full range of process measurement, control, and asset management applications (cf. [HART07a], pp. 1-2).

Key capabilities include:

- **Reliability:** Coexistence with other wireless networks is assured thanks to technologies like mesh networking, channel hopping, and time-synchronized messaging.
- **Security** and privacy for network communications through encryption, verification, authentication, key management, and other open industry-standard best practices.
- **Effective power management** through Smart Data Publishing and other techniques that make batteries, solar and other low-power options practical for wireless devices.

Each WirelessHART network includes three main elements:

- **Wireless field devices** connected to process or plant equipment.
- **Gateways** that enable communication between these devices and host applications connected to a high-speed backbone or other existing plant communications network.
- A **Network Manager** responsible for configuring the network, scheduling communications between devices, managing message routes, and monitoring network health. The Network Manager can be integrated into the gateway, host application, or process automation controller.



Fig 4-1 Timeline of Wireless HART approval (cf. [HART07b])

Fig 4-2 shows the development of installed HART Devices.

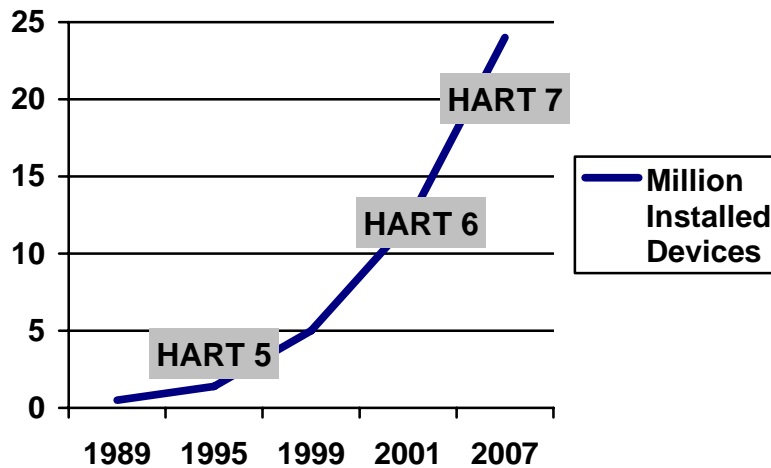


Fig 4-2 Number of Installed HART Devices (acc. to [HART07b])


4.4.2 ISA100.11a

The ISA100 standards committee on wireless systems for automation is developing a new wireless standard (ISA100.11a) that is designed to provide a wireless industrial process automation network to address control, alerting, and monitoring applications plant-wide (cf. [ISA08c]). The approval is expected for October 2008 (Release 1) (cf. [ISA08b]).

Focus:

- Battery powered field devices with the ability to scale to large installations (cf. [ISA08c]).
- According to the ISA100 Usage Classes (Tab 4-2), the first Release will cover class 1 to class 5 applications. Class 0 (critical safety applications) and extremely time sensitive applications will be served in later releases
- Class 1 (non-critical) to class 5 applications such as monitoring. Critical and extremely time sensitive applications will be served in later releases (cf. [ISA08b]).
- Release 1 focuses on process industrial applications; the architecture of ISA100.11a will support factory automation (cf. [ISA08b]).

- Release 1 will only include 2.4 GHz radios (cf. [ISA08b]).

Category	Class	Application	Description	Importance of message timeliness increases 
Safety	0	Emergency action	(always critical)	
Control	1	Closed loop regulatory control	(often critical)	
	2	Closed loop supervisory control	(usually non-critical)	
	3	Open loop control	(human in the loop)	
Monitoring	4	Alerting	Short-term operational consequence (e.g., event-based maintenance)	
	5	Logging and downloading/uploading	No immediate operational consequence (e.g., history collection, sequence-of-events, preventive maintenance)	

Tab 4-2 ISA100 Usage Classes (cf. [ISA08b]).

In May 2008, the ISA100 committee has created a new subcommittee to address options for convergence of the ISA100.11a and WirelessHART standards (cf. [ISA08d]). The goal is to merge the best of both standards into a single converged subsequent release of the ISA standard and thus having one single industry standard for process applications.

4.4.3 Mesh Networking: IEEE 802.11s

The IEEE 802.11s standard is being developed to allow interoperability between heterogeneous mesh network devices. The initial sponsor ballot is planned for July 2009, and final approval is expected for May 2010 (cf. [IEEE08a]). According to Borowka (cf. [Bor08], p. 23) pre-s implementations (similar to 11n) are possible because of the long-lasting approval phase.

4.4.4 ZigBee: IEEE 802.15.4

2008 the ZigBee Alliance announced a new initiative to further enhance ZigBee's connectivity to the Internet and other networks by developing ways to more fully exploit ZigBee's IP capabilities. This new initiative will make it easier for developers and system integrators to deploy ZigBee and to add additional features and functions, including IPv6 support (cf. [Zig08a]).

2007 the ZigBee Alliance added new features to the ZigBee specification. The expanded set of features known as ZigBee PRO maximizes all the capabilities of ZigBee and facilitates ease-of-use and advanced support for larger networks (cf. [Zig07]).

June 2008, the ZigBee Alliance announced the availability of the ZigBee Smart Energy public application profile. The standard supports utilities and technology suppliers by developing products that improve energy management and efficiency (cf. [Zig08b]).

According to Dierdonck, "nowadays, it is widely accepted that IEEE 802.15.4 offers the best solution for wireless sensor applications." Nevertheless suitability for industrial applications is being watched critically: The ZigBee Alliance does not explicitly rule out industrial applications. However, a number of large industrial automation companies have identified the need for extra features that are not on ZigBee's top priority list. The two most important "industrial" features are deterministic latency and deterministic reliability (cf. [Die08]). Latency is an issue because ZigBee does not support "Guaranteed Time Slots". Reliability is not assured because of the interference with Wi-Fi devices. This can lead to packet losses.

4.5 Real-Time Communication in IEEE 802.11 Networks

According to a recent technical insight from Frost & Sullivan "Industrial Wireless Systems for Monitoring & Control" the reliability of wireless systems has increased considerably, driving them to new applications (cf. [Bus08]). However real-time communication in wireless networks is still an ongoing research topic. Since the wireless communication medium is an open communication environment the network load cannot be predicted at system setup time. A real-time communication protocol must be able to guarantee the timing constraints of the RT traffic in a communication environment shared with timing unconstrained traffic (cf. [Mor07], p. 107). Moraes et al propose a VTP-CSMA (Virtual Token Passing) architecture that enhances the real-time properties of IEEE 802.11 networks by circulating a virtual token among real-time devices. This virtual token is complemented by an underlying traffic separation mechanism that prioritizes real-time traffic over non-real-time traffic.

4.6 Energy-efficiency

Energy-efficiency is a topic discussed more intensively in recent research publications to wireless technologies. However they do not yet address industrial applications, some approaches should be presented. The goal is to find mechanism to avoid energy wastage because of the under-utilization of WLANs without compromising WLAN design requirements regarding coverage, client QoS, responsiveness and redundancy. Energy wastage occurs because the existing standard IEEE 802.11 requires that an AP is always active on its assigned channel. Jardosh et al (cf. [Jar07], p. 85) argue that current and future large-scale WLANs must integrate energy efficiency as a design constraint. They propose an algorithm, called Green-clustering which strategically powers on and off WLAN equipment. In a centrally controlled WLAN, the two main consumers of energy are: thin APs and the switches there are connected to. However, the powering on and off of APs and switches in a WLAN is a harder problem to solve because of the spatially dispersed nature of WLANs and the varying wireless channel propagation characteristics.

The Green-clustering algorithm has the following features:

- The central controller in a WLAN makes smart decisions to power on and off portions of a WLAN.
- The building of clusters is based on the distance between APs. The basic premise is that if APs in a cluster are close enough, a single AP from each cluster ('cluster-lead AP') is sufficient to provide basic coverage to users in the vicinity of any AP.
- The WLAN controller monitors the number of users requesting WLAN access in the vicinity of each cluster. Based on this information, the controller decides to power on and off the other APs or 'surrogate APs' within each cluster.
- In addition to controlling APs, centralized controllers can choose to power on and off power-hungry WLAN switches. This is possible only if APs are connected to dedicated switches and AP-switch groups can be powered off simultaneously. But not all WLAN deployments can allow such groupings.
- Further research: accurate user load estimation techniques

A second approach for QoS-enabled power saving APs is to use the IEEE 802.11e unscheduled automatic power save delivery mechanism (cf. [Kho08], p. 2331).

5 Real Time

5.1 Introduction

This chapter continues with the market analysis and trends in context with real time application started with the first version of this task. Previous versions were revised and if it was necessary latest news and updates in context with VAN are added.

5.2 Market Analysis for Industrial Real Time Communication

Like introduced before, finally it is predicted that only a couple of Ethernet protocols will dominate the market, but how analyst John Morse says, many variants will find their niche in the market. Most of these variants are used to fulfil applications with hard time requirements. During the last year new Ethernet based technologies were introduced that have to be monitored. The following sub chapters give a short overview about these technologies.

5.2.1 HSCI

HSCI (Heidenhain Serial Controller Interface) [HSCI] is a new hardware concept for serial interfaces by the company Heidenhain. The master (MC) (central computer) and the control unit (CC) are connected via a real-time Ethernet cable (100BaseT). The protocol is a Heidenhain specific one and is called HSCI. For the connection of the CC and the (measurement-) devices a new measurement devices interface (EnDat 2.2) is used, which works pure digital. This concept is a wholly digital concept from the MC to the devices with following advantages:

- Simple wiring (simple shielded wires with few strands)
- Extensive diagnostic-tools
- Highly interference-resistant (digital data transmission reduces electromagnetic influences)
- Max. 2 CC-unit
- Max. 14 control loops, extern In/Output-modules and one control panel can be installed
- IEC 61505 (SIL2)
- Jitter a few nanoseconds
- Collision-free data transmission
- Electronic identification plate

5.2.2 RAPIEnet

This protocol is an real-time automation protocols for industrial Ethernet (RAPIEnet) by the Hanyang university of the Republic of Korea is applicable for industrial automation environments in which time-deterministic real-time communications are a fundamental requirement (IEC 65C). The aim is to maximize the use of full-duplex Ethernet bandwidth through the use of an internal Ethernet hardware switch.

- Provides a collision-free transmission between two nodes
- Link failure detection using media sensing technologies

A RAPIEnet device is a dual-port switching device that receives and transmits standard ISO/IEC 8802-3 Ethernet frames.

Operating principles

- Frame forwarding and receiving control
- Link status monitoring
- Error detection

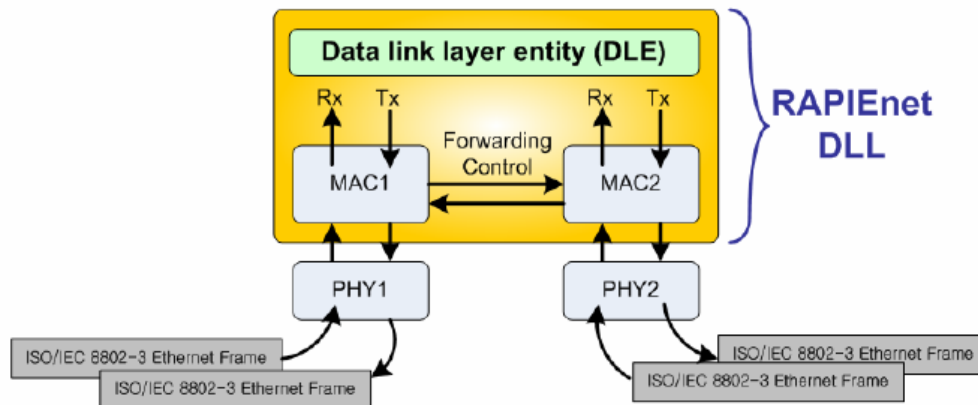


Fig 5-1: Forwarding and Receiving Ethernet Frames with RAPIEnet

- Transmission of frames at any time without collision
- Transmits frames without restriction of medium access (as soon as a frame appears in the transmit queue)
- Forward control for concurrent frames ("round robin" method is used)

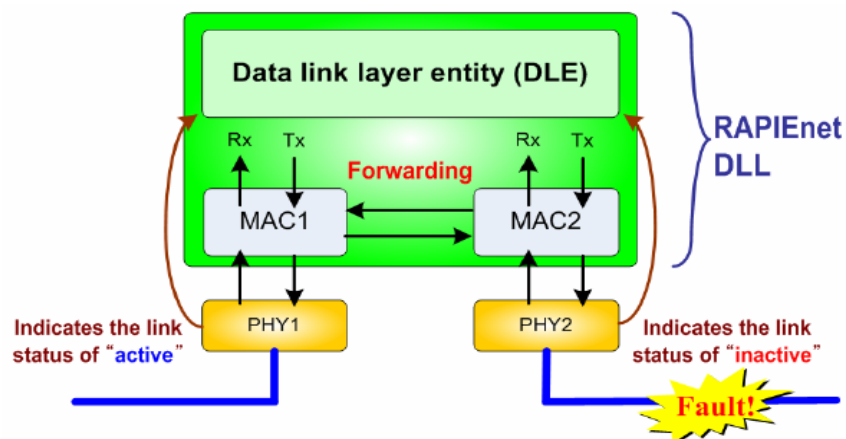


Fig 5-2: Link status monitoring

- Provides efficient mechanism for dynamic network topology management
- Links between nodes can be detected automatically by the devices
- Status information is distributed and shared with all devices (link active or link inactive)
- Error detection
- RAPIEnet devices examines frame check sequence (FCS)
- Invalid frames would not be forwarded to the next device

5.2.3 AFDX

Avionics Full-Duplex Switched Ethernet (AFDX) is based on IEEE 802.3 Ethernet technologies and utilizes commercial off-the-shelf (COTS) components [AFDX].

6 primary aspects argues for this technology:

- Full duplex
- Redundancy
- Deterministic
- High speed performance
- Switched network
- Profiled network

AFDX adopted concepts from telecom standards, asynchronous transfer mode (ATM) to fix the shortcomings of IEEE 802.3 Ethernet.

- Highly reliable full-duplex deterministic network
- Guaranteed bandwidth and QoS
- Possibilities of transmission collisions eliminated
- Buffer transmission and reception packets (to guarantee packet delivery)

5.2.4 TTEthernet

TTEthernet is based on the principle of timing the protocols. A time-critical and a non-time-critical dataflow can be implemented in one network. It is compatible with the existing standards like Profinet, IEEE 1588, ARINC 664 (AFDX) and can be implemented in existing automation environments easily [TTE].

5.2.5 CC-Link IE (Industrial Ethernet)

The CC-Link IE enables seamless data communication from the plant level enterprise network to the production floor network.

Features:

- Redundant media (uninterrupted service through cable)
- Multi-mode fiber optics (high immunity against EMF)
- Automatic ID of segment failures
- No impact of intermittent services
- Real-time communication with guaranteed QoS
- Daisy Chain topology
- Off-the-shelf components can be used (cables and network analyzers)

Basic communication function	Network common memory for real-time communication. And transient (non real-time) communication.
Transmission speed/ data link control	1Gbps/based on Ethernet standard
Network topology/reliability	Dual loop, fiber optic cable
Media	IEEE 802.3z multimode fiber optic cable (GI)
Connector	IEC 61754-20, LC connector
Collision avoidance	Token passing
Size of network common memory	Up to 256K bytes
# Stations per network	Up to 120 stations
Distance between 2 stations	Up to 550 meters cable length
# Interconnected networks	Up to 239 networks (w/120 stations ea.)

Fig 5-3: CC-Link IE Specification

5.3 Conclusion

All mentioned technologies try to solve specific customer requirements – they have not the demand to offer their solutions for the mass market. Some of these technologies are based on well-established standards that serve for higher compatibility. Other vendors provide their own, mainly proprietary solution where specific hardware is necessary. A comparison of all different solutions shows that no uniform standard for Industrial Ethernet will be available in the future. Customers and vendors have to appear a higher variety of industrial communication systems. The current advantages of classic fieldbus solutions, especially in field of real time communication is shrinking. Industrial Ethernet will also cover this area with a wide range of new provided solutions. T

6 Safety

6.1 Status of standardisation of safety networks

Safety Layer definitions for fieldbus systems are now state-of-the-art. The same happens for each industrial Ethernet protocol. The fieldbus organisations are trying to use the same safety protocol. Tab 6-1 shows some examples:

Fieldbus organisation	Fieldbus version	Ethernet version
INTERBUS-Club	INTERBUS-Safety	-
PNO	PROFIsafe V1	PROFIsafe V2
ODVA	CIP-Safety V1	CIP-Safety V2
Safety Network International	SafetyBUS-P	SafetyNET-P
Sercos International	-	CIP-Safety V2

Tab 6-1 Examples of Fieldbus and Industrial Ethernet Safety Protocols

The insight of the specification work is, that there is no chance to enlarge the functionality in a compatible way. The reason therefore is, that the underlying industrial Ethernet black channel is completely different from the fieldbus black channel before. Either the bit transfer rate or the bit error rate or the bus access method (master-slave or producer-consumer) or the failure models and failure possibilities of infrastructure components of the black channel are different or completely new.

Some of the "Second Versions" of Safety Layers additional including the V1 software stack. Typically this complicates the development, certification process and handling for the customer.

4 Safety Layers are standardized in the 61784-3:

- INTERBUS-Safety
- PROFIsafe V2
- CIP-Safety V1
- FF-Safety

From the certification point of view all standardized Safety Protocols are able to use for applications up to SIL3 (61508), CAT4 (954) or PLe (13849).

From the technical point of view some specifications include special conditions or restrictions for use (e.g. special installation guidelines) and implementation guidelines for the development of safety device.

The slogan "simplicity in safety" is more relevant and important then ever.

6.2 Unresolved issues for safety technologies

Regarding the analysed unresolved issues for safety technologies in [D01[1].2-1] in the meantime some earlier issues solved but new issues occurred.

1. Safety communication over different networks: It is not possible for a Safe PLC designed for a certain fieldbus or industrial Ethernet protocol to access a safety device in a different type of network. This issue is still unresolved.
2. Exchange of Safe Variables: In homogeneous systems it is possible to transfer PLC variables from one Safe PLC to another Safe PLC. Therefore the system or Safe PLC vendors developed specific and proprietary solution e.g. special function blocks.
3. Safety Gateways (or Proxy): Gateway and Proxy solutions are very common for non-safe communication protocols. Even for their safety pendants there are some special solutions yet. A safety gateway between PROFIsafe-DP and ASI-Safe is available (see Fig 6-1). The integration of INTERBUS-Safety into PROFIsafe-ProfiNet networks and the coupling of CIP-Safety on Sercos III and CIP-Safety on Ethernet IP are planned.

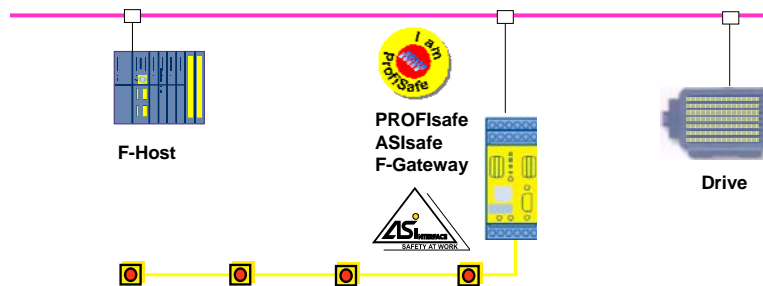


Fig 6-1 Safety Gateway between PROFIsafe-DP and ASI-Safe

4. Common Safety Calculation Guidelines: The “rules” for the calculation of safety relevant parameters (like PFD, PFH, SFF,...) in a plant are given by the standards. But the use of them for the final user is very complicate. Special tools should support this calculation. These tools need common data base of safety relevant parameters of every device integrated in the safety function (safety loop). A new founded working group initiated by TÜV Rheinland and supported by the University of Kassel and some industry partners specify a common data base and develop a safety calculation tool.
5. Calculation of safety response time: The calculation of the safety response time in safety loops based on non synchronized networks is not friendly to use for the user and has a lot of hazards for failures. The user has to handle a lot of watchdog times, cycle times, or program running times of Safe PLC under various conditions. But the delay of a safety demand is the same failure as a wrong transmitted data. Only the strictly synchronized INTERBUS-Safety supports the user with a one parameter setting method for a guaranteed safety response time from Terminal Point of Safe Input Signal to Terminal Point of Safe Output Signal.
6. Integration of “partner” devices: every fieldbus organisation typically is driven by one special company (ODVA – Rockwell Automation; PNO - Siemens; Sercos - Bosch; INTERBUS - Phoenix Contact ;...). These companies control the specification, decisions about future developments, conformance tests and so on. In some cases the leading company uses its role to implement special features into their PLC e.g. for better or “totally integration” of their own devices regarding performance, parameterization, diagnostics, tool-integration and so one. The motivation behind is logical and market oriented. This trend is only acceptable as long as the user accepts this various integration strategies and the safety issues are not toughed.

7 Security

This chapter comprises new security trends and threats. Overview of the most actual threats is based on the very complex report published by IBM [IBMGTS08]. Security technology trends present contemporary used technologies and visions for next years.

7.1 Current status of security threats

According to IBM Internet Security Systems X-Force observations [IBMGTS08], many new and surprising trends surfaced during the first half of 2008. The implications of these trends provide a useful backdrop in preparing to enhance information security for the remainder of 2008 and beyond.

7.1.1 Vulnerabilities

The overall number of vulnerabilities continued to rise as did the overall percentage of high risk vulnerabilities.

- Web-based vulnerabilities and threats continue to increase:
 - Over the past few years, the focus of endpoint exploitation has dramatically shifted from the operating system to the Web browser and multimedia applications.
 - Vulnerabilities affecting Web server applications are climbing and so are the attacks, both evidenced by newcomers to the most vulnerable vendor list and this year's automated SQL injection attacks.
 - Although standard Web browsers are becoming more secure, attackers continue to rely on automated toolkits, obfuscation, and the prevalence of unpatched browsers and plug-ins to successfully gain hold of new endpoint victims.
 - Although the most exploited Web browser vulnerabilities are one to two years old, the availability of public proof-of-concept and exploit code is speeding the integration of more contemporary exploits into toolkits.
 - In the first half of 2008, 94 percent of public exploits affecting Web browser related vulnerabilities were released on the same day as the disclosure.
 - Plug-ins were especially targeted, representing 78 percent of the public exploits affecting Web browsers.
- Although independent researchers disclose more vulnerabilities overall, research organizations still discover the most critical vulnerabilities.
- Independent researchers are almost twice as likely to have exploit code published on the same day as their vulnerability disclosure in comparison to research organizations.
- Although virtual machine breakout vulnerabilities tend to get a lot of attention from the press, they are rare and predominantly target x86 platforms and Type II (virtualization solutions that require a host operating system).

7.1.2 Spam and Phishing

- "Complex" spam (spam that uses images, PDFs, or complex text/HTML) is on the decline and a simpler type of spam is taking its place.
- This simpler spam relies on Web links and short text messages inside spam e-mails, which may be more difficult for some antispam technologies to detect.

- The Web links used in this new type of spam use familiar blog or other "personal" domain names that are more likely to trick users into clicking the Web link in the spam message.
- The lifespan of the URLs associated with URL spam continues to shrink, which is another way to avoid antispam technologies.
- Financial institutions continue to be the main phishing target.

7.1.3 Malware

- For the first half of 2008, a password stealer family that targets online games is in first place on the top ten malware list, and, in the password stealer category, game related malware takes 50 percent of the top ten spots overall.
- One of the most common actions which malware takes after installation is an attempt to evade detection, either by the user or by the security software on the system.

7.1.4 Other threats

- Cisco has already had to patch its VOIP protocol to close a security loophole. Vulnerabilities surely exist in video formats, as well. The ever-growing popularity of videos and video sites such as YouTube ensures that hackers will not neglect this format for long [BC08].
- In February, a major electronics retailer warned customers that a popular model of digital picture frame, which connects to a computer over a USB port to display images, had become infected with the Moxmex Trojan Horse. The popularity of digital photography and music downloads is leading users to connect a wide variety of devices to their computers. Unfortunately, not all these devices are safe. [BC08]
- Major botnets (networks of infected computers) are now for rent to spammers and criminals. The Storm botnet, comprising over 85,000 machines infected by a Trojan, sent about 20% of the world's spam in 2007. Researchers have recently discovered new, even more insidious botnets, such as MayDay. [BC08]

7.2 Important vulnerabilities for the technical basis of VAN

7.2.1 Cryptographic weaknesses in openssl based systems

The widely used package OpenSSL has been reported to be accidentally modified opening a weakness in 2006 causing keys created in a specific environment to be critically attackable. The flaw causes the amount of creatable keys to be limited to 2^{15} making an attack trivial. Besides systems that create TLS keys using OpenSSL such as web servers offering HTTPS connections also VPN solutions such as OpenVPN that run on Debian based operating systems.

This weakness became widely known in the first half of 2008 and caused an extensive patch wave throughout the entire IT sector.

VAN does not dictate the use of a specific OS and hence it cannot be ruled out that also Debian installations are used but then the newest patches must be applied and special regard has to be given to the version of the OpenSSL library to be installed.

7.2.2 DNS poisoning attacks

DNS cache poisoning as an attack method is known since more than 10 years and has been made difficult by makers of DNS resolver software so that it became uncommon due to the huge effort at the beginning of the new century. One of the most effective counteractions was the introduction of a 16 bit transaction number which is based on a random number generator. To forge or guess exactly this number would require statistically 32 768 tries and hence this effort made this method very unattractive.

Unfortunately this attack is still possible but only more difficult with the negative side effect that DNS makers and service providers are less pressed to implement more secure alternatives such as DNSSEC.

An additional attack scenario uses the explicitly allowed feature of the protocol to send additional name records (of type RR) within the answer, which would then be stored in the DNS cache of the system having placed the initial request. To make this way of attack more difficult most implementations of DNS resolvers accept only those records that are related to the original request, so called in-bailiwick records.

More recent investigations show that an attack combining the upper two scenarios becomes more likely again due to the fact that the required effort sinks drastically. The statistical background for this is known as the birthday paradox and the attack hence is a birthday attack. It is based on the fact that a collision of two random numbers is more likely than to exactly guess a number.

The first precondition is a huge number of requests that are to be generated. Usually a prepared website with thousands of one pixel images, each one referring to a slightly different domain name, can be used for that but in the context of VAN simple requests for a huge number of non existing objects via web services might be used instead. With every answer a placement of the additional target record is tried. Non matching transaction numbers will be ignored but if a match is hit this false record is stored in the cache. The answer is considered a related or in-bailiwick record as the name requested is only slightly different from the targets name (usually in the same VAN domain).

A similar and related attack tries to place not an RR record of one resource but a complete A record of an authoritative name server for a whole domain into the cache allowing the wrong system to answer with false IP addresses for a whole domain. DNS cache poisoning becomes more relevant with the increase in phishing attempts but may be used to take over VAN domains as well. The use of additional cryptographic measures is highly recommended.

Another way to improve the security against this type of attack is to implement source port randomization which increases the room of data to be guessed by a port number (between 1024 and 65535) to a mere billion of combinations. Mathematically the number of tests against a transaction number system using a birthday attack is 320 while with the use of additional source port randomization requires about 56 thousand tests. As VAN does not provide an implementation of a specific name server the choice of an appropriate product can be a good recommendation.

7.3 New trends in security technologies

7.3.1 VPN

This year, the trends that are expected to have the greatest impact on businesses' VPN and remote access decisions include [WCVPN08]:

- Designation of data breach prevention as a top IT priority.
- Blurring of the distinction between personal and business applications and devices.
- Progressive enforcement of industry regulations (PCI DSS, FFIEC, etc.).
- Expansion of Windows Vista into the corporate mainstream.
- Increased use of outsourcing for information security services.
- Proliferation of two-factor authentication.

7.3.2 WEB 2.0

Web 2.0 and social networking meet the enterprise. Thanks to an advancing technology-native workforce, ubiquitous broadband, and abundant collaboration and Social Computing tools, information workers can provision their own software tools, information sources and social networks via the Web to support their jobs. But technology populism comes with new risks, including compromised security and privacy and poor control of intellectual property [Cam08].

7.3.3 Enterprise Master Data Management

Master data management's goal is to deliver trusted data throughout the enterprise. But in an effort to open up access to data while enforcing policies and regulations, this strategy must focus on mitigating the organizational, process and business case challenges that an enterprise wide, multi-data-domain, master-data-management business capability introduces before considering comprehensive technology architectures. Enterprise master data management is a multiyear, multiphase, maturing business capability that will allow the delivery of trusted and quality customer product and other critical data [Cam08].

7.4 Applicable security standards and their origins

Whilst safety has been well covered with standards and regulations quite well the application of security measures has suffered from the virtually low importance in automation scenarios. Therefore an overview has been collected to depict the sources of standards commonly referred to.

ITU-T	ITU Telecommunication Standardization Sector
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ATIS	Alliance for Telecommunications Industry Solutions
ETSI	European Telecommunications Standards Institute
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	Internet Engineering Task Force
OASIS	Organization for the Advancement of Structured Information Standards

The organisations above partly apply different procedures for the acceptance of a proposal as a standard. Nevertheless it was possible to collect the most recent topics from these organisations showing what are upcoming standards apart from the issues risen by external triggers like newly found exploits.

The ITU-T has focussed on the following list of questions and topics

- Communications systems security project
- Security architecture and framework
- Cyber security
- Security management
- Telebiometrics
- Secure communication services
- ASN.1 (Fast Infoset security)
- Countering SPAM by technical means

ISO/IEC JTC 1 SC 27 Projects (Current ISO/IEC JTC 1 SC 37 (Biometrics) Projects are not considered as relevant for VAN) on Security include

- "Information Security Management Systems"
- "Cryptography and Security Mechanisms"
- "Evaluation Criteria of Information Security"
- "Information Security Management Systems"

- "Identity Management and Privacy Technologies"

Actual IEEE Information Assurance Committee Projects are

- Standard for Authenticated Encryption with Length Expansion for Storage Devices
- Standard Protocol for Authentication in Host Attachments of Transient Storage Devices
- Standard for Information System Security Assurance Architecture (ISSAA)
- Standard for Information Technology: Hardcopy System and Device Security
- Standard Architecture for Encrypted Shared Storage Media
- Standard for Baseline Operating System Security

In other organisations the subgroups organize individual roadmaps in order to more flexibly adapt to practical demands. An RFC can be prepared and published separately regardless of a roadmap proposing security solutions for specific environments.

8 Cooperation of Private and Public Networks

8.1 Trends in general

This chapter with all its subchapters are based on a very comprehensive market research report [InfoRes] published by Infonetics Research within their press releases.

8.1.1 Metro Ethernet equipment sales up 27% in 2007, more carriers using and testing

CAMPBELL, California, May 6, 2008—Worldwide metro Ethernet equipment sales hit \$13 billion in 2007, up 27% from the previous year, and are projected by analyst firm Infonetics Research to continue growing in the double-digit percents over the next 4 years.

According to Infonetics' latest Metro Ethernet Equipment report, each year more Ethernet equipment is being deployed where previously SONET/SDH or ATM equipment was used.

"By 2011–2012, the majority of access and aggregation equipment being deployed by carriers around the world will be IP, Ethernet, and WDM, not SONET/SDH. In 2007 and especially in 2008, we're seeing more carriers using Ethernet, and more carriers conducting interoperability tests of all sorts of Ethernet products for residential broadband, business connections, and mobile backhaul," said Michael Howard, principal analyst for optical and metro Ethernet and co-founder of Infonetics Research.

According to the report, the hottest selling technologies in the metro Ethernet market are routers and carrier Ethernet switches (CES), Ethernet over DSL, and Ethernet over optical. The fastest growing metro Ethernet technology over the next 5 years is Ethernet microwave, most of which will be used to support the move to IP and Ethernet in mobile backhaul, where microwave is used for 55%-60% of the mobile backhaul connections in the world.

Other highlights:

- Sales of copper and fiber Ethernet access devices (EADs) will nearly quadruple from 2007 to 2011
- ADVA Optical captures the #1 spot for worldwide EAD revenue market share in 2007, followed by RAD Data and ADTRAN
- Worldwide metro Ethernet equipment ports hit 40.5 million in 2007, and will grow quickly through 2011, dominated by VDSL Ethernet 10/100M ports and EPON ports
- The EMEA and Asia Pacific regions are more readily adopting Ethernet than North America and CALA, even though North America is the home of Ethernet; the Asian service providers embrace the simpler, less expensive technology

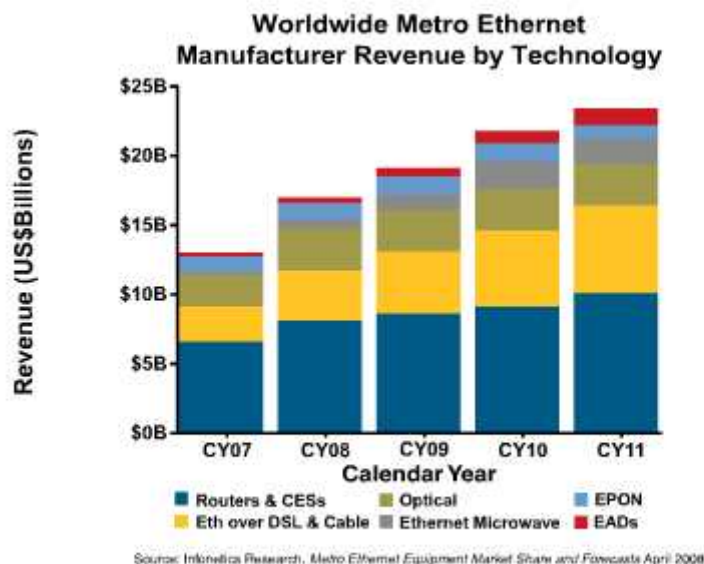


Fig 8-1 Worldwide Metro Ethernet Manufacturer Revenue by Technology

8.1.2 Carriers report 90-100% increase in Ethernet traffic

CAMPBELL, CALIFORNIA, January 7, 2008—In a recent study by Infonetics Research to determine the data network evolution plans and router and switch requirements of service providers in North America, Europe, and Asia Pacific, the increasing importance of Ethernet features prominently.

As carriers transform their networks in an effort to simplify network layers, use fewer technologies, build a more cost efficient infrastructure, and move to all-packet, a new optical transport layer will emerge, according to the study. This new layer will be a fused Ethernet-WDM packet transport with circuit-like capabilities via Ethernet transport tunnels, also known as COE, or connection oriented Ethernet.

The service layer above the Ethernet-WDM transport will be simplified to IP/MPLS/Ethernet, and carriers will gradually reduce their dependence on SONET and SDH in transport and on ATM in service layers, while increasing their use of Ethernet in the service and transport layers. This means a growing IP router and carrier Ethernet switch market, the study says.

“COE Ethernet transport tunnel technologies like T-MPLS and PBT are seeing strong adoption given their early stage of development, and will be an essential ingredient of the service and optical transport layers, as they allow the displacement of SONET/SDH and enable carrier Ethernet switches to displace some routers,” said Michael Howard, principal analyst at Infonetics Research. “As a result, router and carrier Ethernet switch sales should continue strong as Ethernet and IP/MPLS traffic continues to grow, and at even faster rates than seen in a similar study we conducted last year.”

Other highlights from the study:

- Further penetration of broadband, increases in bandwidth usage, and the move to IPTV and triple and quadruple play service offerings will drive Ethernet and IP/MPLS traffic growth over the next 3 to 5 years
- Top applications driving data traffic include broadband, metro Ethernet services, VoIP, and IPTV
- Service providers report 90-100% increases in Ethernet traffic in 2006 and in 2007, and 70%-80% for IP/MPLS traffic
- 72% of the study’s respondents will participate in interprovider QoS in 2008; IP VPNs and VoIP are the most common services that make use of interprovider QoS

- Reliability continues to be the #1 criteria respondents use in selecting an IP router and switch manufacturer
- Cisco, Juniper, and Alcatel-Lucent sweep the field when respondents name the manufacturers of the edge routers they have currently installed

Infonetics' study, *Service Provider Plans for IP/MPLS*, examines market and technology trends, drivers, barriers, implementation plans, expenditures, vendor ratings, and technology preferences of carriers buying IP routers and multiservice switches. Infonetics' analysts interviewed respondents at 29 carriers in North America, Europe, and Asia Pacific, of which:

- 34% are incumbents and 66% are competitive operators
- Average annual revenue is \$14–\$15 billion in 2006–7
- 100% have IP/MPLS networks, 90% have metro Ethernet, 86% broadband access, 76% ATM, and 66% frame relay, and 55% mobile backhaul networks

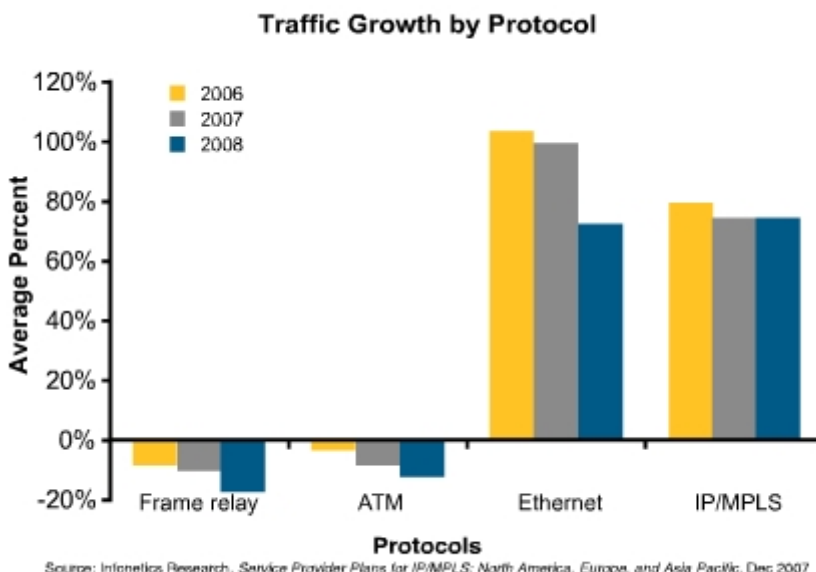


Fig 8-2 Traffic Growth by Protocol

8.1.3 Service provider router and switch sales hit all-time high in 2007, led by Cisco, Juniper

CAMPBELL, California, February 26, 2008—Worldwide sales of service provider routers and switches totaled \$11.2 billion in 2007, up 16% from 2006, an all-time high for routers and switches, which have been steadily climbing since the nadir in 2003, says Infonetics Research in its quarterly report, *Service Provider Routers and Switches*.

“The common drivers pushing the carrier router and switch market upward are 1) the ongoing migration to next generation networks based on IP, MPLS, and Ethernet, and 2) growth in consumer broadband, corporate, IP video, and mobile data traffic,” said Michael Howard, principal analyst and co-founder of Infonetics. “Of course, the traffic jams are being caused by user applications, like music and video downloading, YouTube clips (even corporations are using YouTube for marketing videos), online news, and social networks like MySpace. As an example, I recently watched video feeds of the Amgen Tour of California bicycle race for a few hours at a time, something not possible a year ago.”

Other highlights:

- Cisco’s router and switch sales are up 20% year-over-year, Juniper’s are up 25%
- Content providers are offering new on-demand and broadband video services that eat up more bandwidth into the home

- Residential and commercial developers are trying to outdo the competition with better and more high tech offerings
- Municipalities around the world, most notably in Amsterdam, Stockholm, and Dubai, are upgrading their networks to Ethernet FTTH to keep and attract new jobs in an age where access to digital information is paramount

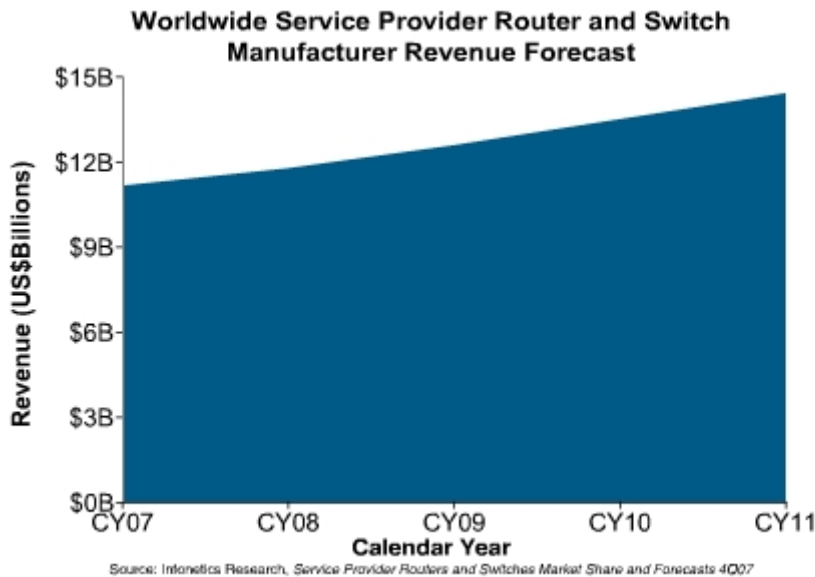


Fig 8-3 Worldwide Service Provider Router and Switch Manufacturer Revenue Forecast

8.1.4 WiMAX equipment market up 46% in 2007, forecast to hit \$7.7B in 2011

LONDON, UK, February 28, 2008—The WiMAX market sequentially grew 11% for the quarter and 46% for the year, with worldwide sales of fixed and mobile WiMAX equipment hitting just under \$800 million in 2007, says Infonetics Research in its latest WiMAX and Mesh Network Equipment and Devices report.

WiMAX has been deployed in more than 80 countries worldwide, and commercial networks will continue to grow in number and size in 2008, the report shows. Infonetics forecasts the WiMAX market to grow to \$7.7 billion in 2011.

“Several recent developments are giving a boost to the WiMAX market,” said Richard Webb, wireless analyst for Infonetics Research. “Among the most significant developments: Cisco’s acquisition of mobile WiMAX vendor Navini Networks, the market entrance of specialist ASN gateway vendor WiChorus, the launch of WiMAX phones and Ultra Mobile PCs, and the new Open WiMAX initiative, which promotes disruptive, all-IP open WiMAX architecture, and should lead to best-of-breed solutions with inter-vendor interoperability.”

Other highlights:

- Mobile WiMAX equipment grew in high double-digit percents every quarter of 2007
- Worldwide sales of ASN gateways, which aggregate traffic from mobile WiMAX base stations, grew nearly 10-fold from 2006 to 2007
- The number of worldwide WiMAX subscribers (fixed and mobile) topped 2.2 million in 2007, led by the Asia Pacific region; the majority are fixed WiMAX subscribers
- Alvarion maintains its lead in worldwide fixed WiMAX equipment revenue share in 2007, followed by Airspan

- Motorola is the leader in worldwide mobile WiMAX equipment revenue share in 2007, followed by Samsung

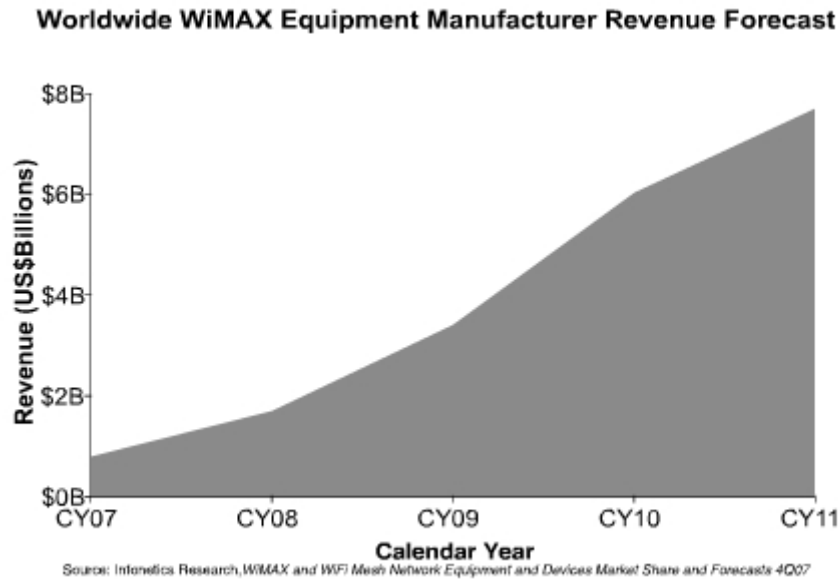


Fig 8-4 Worldwide WiMAX Equipment Manufacturer Revenue Forecast

8.1.5 Mobile backhaul equipment market set to skyrocket due to exploding mobile data/video use

CAMPBELL, California, May 12, 2008—Mobile operators and backhaul transport providers spent \$3.7 billion worldwide on mobile backhaul equipment in 2007, and are expected to increase their spending in the high double-digit percents from 2009 to at least 2011, according to Infonetics Research's latest Mobile Backhaul Equipment, Installed Base, and Services report.

"All market indicators support continued growth of the mobile backhaul market. Manufacturers and service providers have had residential broadband and corporate services as the main thrust of their businesses for a long time, and now mobile backhaul makes up a third area that nearly all of them are focusing on. We expect to see the Ethernet mobile backhaul revolution really kick off in 2009," said Michael Howard, principal analyst of Infonetics Research and lead analyst on the report.

Other highlights:

- There are 3 major factors forcing a migration to packet backhaul:
 - Increasing numbers of mobile subscribers, reaching 4.4 billion worldwide in 2011
 - An explosion in mobile data and video use, particularly on iPhones and their clones, requiring providers to significantly increase bandwidth offerings
 - Rapidly Heavy competition, forcing operators to upgrade their network capacity to improve and add new subscriber services; these upgrades will include IP/Ethernet BTS/NodeBs, WiMAX, and LTE
- New cell site backhaul connections, which drive equipment spending, will roughly quadruple worldwide from 2007 to 2011
- The IP/Ethernet portion of worldwide mobile backhaul equipment revenue is set to skyrocket, racking up a triple-digit 5-year compound annual growth rate from 2007 to 2011
- By 2011, service providers using PDH, ATM over PDH, or SONET/SDH for their mobile backhaul connections will be paying roughly 3 to 40 times as much in service charges per connection as those using Ethernet, DSL, coax cable, or PON

- Most operators are looking at a hybrid approach to mobile backhaul, keeping 2G and 3G voice on current TDM technology, and using packet technology for the growing data service EV-DO, EDGE, and HSDPA traffic
- The T-Mobile, Swisscom Mobile, and Telecom Italia contracts for IP, Ethernet, and pseudowire cell site backhaul are the first of many to come over the next 18 months

Infonetics' report focuses on the network between the BTS/NodeBs at a cell site to the BSC/RNC, whether over air, copper, or fiber. The issues surrounding cell site backhaul include voice and data traffic, the expanding data bandwidth required by EDGE, EV-DO, HSDPA, the monthly recurring charges for backhaul transport services, and the transmission technology alternatives. The report tracks mobile backhaul equipment, connections, and service charges for PDH, ATM over PDH, Ethernet copper and fiber, SONET/SDH, DSL, PON, coax cable, microwave, WiMAX, and satellite. The report also includes top player analysis, fundamental drivers of the market, changes affecting market growth, and more.

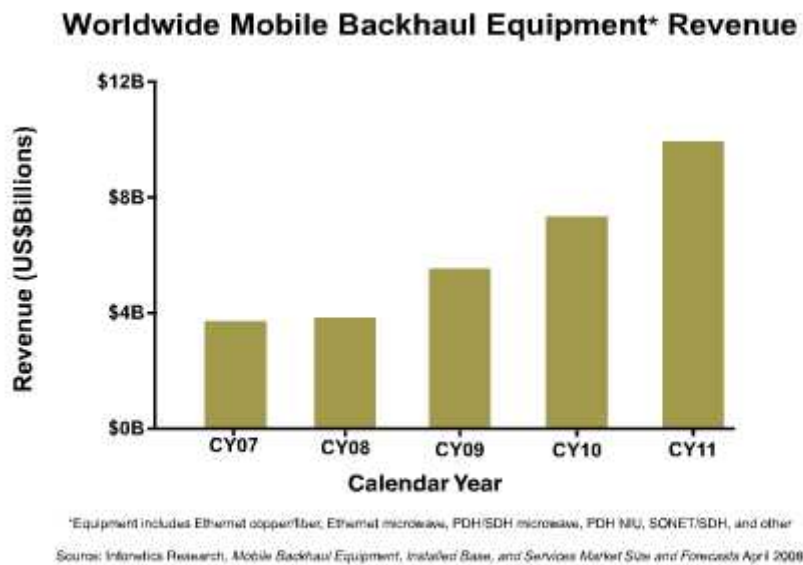


Fig 8-5 Worldwide Mobile Backhaul Equipment Revenue

8.2 Trends in Automation

The Trends in Automation are already described in [D01.3-1-V1].

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. Especially the number of available Industrial Ethernet technologies (e.g. EtherCat, PROFINET, Sercos,...) is growing. Furthermore these technologies are signed by further developments and increased functionality and realtime support. However in the next future the broad spectrum of such technologies will be confined. The best technologies will become more important and get more acceptances and propagation.

9 Engineering Tools

9.1 Introduction

The following chapter compiles the results from the analysis of the technologies relevant for engineering of a VAN system during the recent year. Besides the technologies, which have been initially identified in the first version of this deliverable, no additional engineering technologies have emerged for management of automation systems and communication across heterogeneous communication networks. Therefore, the structure of this chapter will be continuously cried on.

The last subchapter "Conclusions about Engineering Tools" gives a summary of trends for each of the considered technologies.

9.2 OPC

The specification and the code base deliveries for OPC-UA are further evolving. For all but two of the eleven parts of the OPC-UA specifications a first version was released. For part 7 "Profiles" a release candidate is published and part 9 "Alarm" is available as draft. For most of the released specifications updates are already available as release candidates. Additionally, SDKs, wrappers and sample implementations have been released in the code base and updated versions are available as draft or release candidates for some components.

Besides the existing self-certification program with the compliance testing and interoperability testing a new compliance certification program is established. Both client and server products can be submitted for tests by an independent certification test lab. The test lab itself was audited by the OPC Compliance Committee. The compliance certification program does not only aim to improve the quality of existing OPC products, it also certifies interoperability of products developed on the OPC-UA specifications

9.3 FDT/DTM

The coverage of fieldbus types, which are supported by FDT, has further increased since the last update of this deliverable. In the meantime additional annexes with the communication schemas for Modbus and Profinet I/O have been released.

Besides the continuation of the interoperability workshops the FDT test system is extended by a permanent test and certification laboratory. This allows setup of test sessions according to the requests from any company appropriately for the development progress for their components. Additionally the opportunity of remote tests via internet offers comfortable access for developers all over the world.

The successful application of the dtmINSPECTOR for verification of almost 100 DTM for more than 1000 device types has increased the demand for an equivalent tool, which can be used to check also for FTD frame applications, whether they are conformant to the FDT specifications. The development of the equivalent frameINSPECTOR tool has started beginning of 2008 and should be released in the next months.

The discussion around the development of a unified FDI solution, which combines the FDT approach with EDDL technology, is in progress. A comparison of the two technologies, which was commissioned from the International Instrument Users Association WIB [WIB] as a neutral and competent party, concluded as the result of an objective assessment that FDT as well as EDDL are

complementary technologies and control systems as well as device vendors should support both technologies.

9.4 Plug-and-Play

As concluded in the last version of this deliverable the relevance of UPnP is not apparent for VAN systems and therefore the investigation and trend screening of this technology is dropped.

9.5 SNMP and MIB

The protocol of SNMP remained stable during the last period. There have been few updates of MIB definitions but with no relevance for the VAN project.

9.6 Web Services

The "Web Services Discovery and Web Services Devices Profile (WS-DD) Technical Committee" [WSDD] was recently founded by OASIS to define a lightweight subset of the Web services protocol suite that will make it easy to find, share, and control devices on a network. Besides the DPWS [DPWS] specification also the WS-Discovery [WS-Discovery] and SOAP-over-UDP [SOAP-UPD] specifications have been contributed as a basis for the standardization process of this committee.

Driven by integration of DPWS in the Windows Vista operating system the application of DPWS in home automation and industrial automation domains continues to grow and several devices exist, which support the DPWS. Moreover, the source code is not only freely available from [SODA] but not it is also provided for further development and improvements as open source [SOA4D]. Further drive for this technology comes from EU research project SOCRADES [SOCRADES], which also focuses on development of automation devices with DPWS support.

9.7 Conclusions about Engineering Tools

As in the last years there have been no unexpected changes for the considered technologies since the last update of this deliverable.

Specifications and the code base of OPC-UA are available in a first official release and they are further developed. Launching the new compliance certification program will increase acceptance and confidence in the new architecture for this technology.

Continuously extending the coverage of existing fieldbus types by new annexes proves the approach of the FDT Group to split the central specification of the FDT technology and the annexes for the individual communication schemas. The continuation of interoperability workshops, the establishment of a permanent certification laboratory and the start of the implementation of a frameINSPECTOR improve the degree of reliance to certified devices and tools. The development of a unified FDI solution will not converge until the end of the VAN project. Anyway, the assessment of the FDT/DTM and the EDDL technology has already shown that FDI needs to provide a solution which is compatible with FDT/DTM and EDDL.

SNMP and MIB have shown no relevant changes but should be further monitored, since they are integral part of the architecture for VAN devices.

The availability of the DPWS implementation as open source and the standardization of DPWS by OASIS will further promote this technology. Since the standardization committee also considers other specifications it may happen that some modifications on the DPWS part will evolve and need

adaptations on existing implementations. Especially, for the industrial automation domain the EU research project SOCRADES will give fresh impetus to this technology.

10 Summary of Conclusions

The following paragraphs are a summary of conclusions of previous chapters about trends in VAN related technologies.

From the general point of view, automation is dominated by trends of communication penetrating industrial automation. Network Control Systems (NCS) have been defined as a new notion in automation, fostering research and development of new theoretical and technological tools to support dependability (availability and timeliness) of the NCSs. These trends are well in accordance with the VAN main goals.

Furthermore, trends in embedded system electronics support further penetration of Ethernet technology and adjacent TCP/IP socket communication to process level of industrial automation. With the growing hardware and computational resources, the VAN extensions (VAN stack, and software necessary for Web Services and VPN tunnel communication) are more likely to be a part of embedded control and communication devices.

The core technologies chosen for the VAN implementation have been investigated from the trend point of view. We came to the conclusion that the VAN platform has been designed with respect to general automation trends and no significant risk potentials have been found.

Wireless

Regarding current wireless trends, it is seen that industry is moving forward researching at different wireless technologies coexistence, sensor networks and wireless PROFIBUS and PROFINET. Regarding 802.11n, it is currently seen that efforts are needed to make it support greater rates and processing power. Regarding power consumptions research is being made for allowing 24W power through Ethernet cables. As far as Bluetooth is concerns, trends are to make it faster by means of ultra-wideband technologies, while its Ultra Low Power specification seems to will not have any impact on industrial applications.

Regarding the field of Wireless Sensor Networks, three technologies seem to show industry interesting features. WirelessHART standard is a current solution robust enough for a wide range of industrial applications, to be converged with ISA100.11a in order to achieve a single standard merging the best of them for process applications. On the other hand ZigBee is moving towards being IP compliant and energy efficient while still not achieving features such as deterministic latency and reliability, which are important at industry level. Other technologies such as 802.15.3c are seeking for higher transmission bands such as 57-60 GHz for WPAN applications, achieving no interference with other wireless technologies and high binary throughput.

Finally it is of importance the research for energy efficient mechanisms for 802.11 technologies (WLAN), such as the Green-clustering algorithm.

Market Approach in Wireless Technologies

According ARC Advisory Group, the expected market-growing figure is a 54% each year, being wireless process sensing the one of greater growth, followed by WLAN applications and the expectancy for 802.11n features.

On the other hand, surveys on users of industrial communications show that there is a great expectative on wireless communications, though there is still some skepticism regarding features such as stability, IT-security, availability of industrial products and real-time capabilities. The surveys also show that the most used technologies are WLAN and Bluetooth. Finally market trends for WiMAX are shown, lightning out the revenue shares rise of this technology worldwide and equipment manufacturing.

Real-Time

Trends in real-time solutions for industry lead to a convergence to Ethernet based technologies. Market figures show expected growths around 13% for Ethernet based protocols, as well as a clear dominion of PROFINET in European, American and Asian markets due to the importance of two of its members, SIEMENS and Rockwell Automations. Market analysts see Ethernet success in the fact that it sets a common physical layer throughout the enterprise while multiple competing protocols at the automation layer. This takes to several own-proprietary protocols, which as shown, most give a solution for deterministic timing, collision and interference avoidance and guaranteed bandwidth and QoS. However there are still many industrial applications that ought to be addressed by means of fieldbuses.

Safety

Regarding safety, fieldbus organizations intend to converge towards the same protocol, as it happens with industrial Ethernet protocols. However there are no chances to make fieldbus and Ethernet black channels to converge, as currently they differ in many points. Within the 61784-3 four safety protocols have been standardized, which are certified for applications but find differences and special conditions and restrictions at use and implementation of safety devices. On the other hand there are still many issues to be resolved regarding safety technologies, such as safety communication over different networks or integration of solutions from more than one fieldbus organization.

Security

There is a tremendous amount of security related trends and especially exploit messages are available on a daily basis due to the wide distribution of incident report services. Many of these vulnerabilities can be considered of less importance for the technical basis of VAN. Nevertheless openSSL and DNS poisoning can be considered of vital importance for the project. The cryptographic weakness in openssl based systems, like openVPN solution has become widely known this year and has caused a patch wave in the entire IT sector. The DNS cache poisoning attack method is known since more than 10 years. In the beginning, the DNS resolver software makers made difficult to exploit such vulnerability. The proliferation of service providers is making easier to exploit such vulnerability due to the fact that they are less pressed to implement more secure alternatives such as DNSSEC. As VAN does not provide an implementation of a specific name server the choice of an appropriate product can be a good recommendation.

Cooperation of Private and Public Networks

The private and public networks trends are towards the convergence over packet oriented technologies. IP/MPLS/Ethernet is leading the change over technologies such as SONET/SDH, as well as the sales of blackhoul devices such as IP routers and carrier Ethernet switches are growing in the terms of 2-digit percentages rates. There is also a growth in forecast for Ethernet-based and optical-based communications fusion, both in backbone networks and end-user ones. On the other hand mobile communications are experiencing a fast growth, and it is expected that it will keep on holding these trends for the next four to five years. New services provided by the operators include multimedia, which may include not only voice but video and data. Also wireless technologies for the end-user, concretely WiMax, are experiencing a fast growth, being the Asian Pacific Region the one that best represent this trend.

Regarding automation, the future pass through IP and Ethernet technologies, however fieldbuses may be widely used due to they are currently massed used. Ethernet technologies evolution points to a future where the best Ethernet-based solutions may rule the automation networks.

Engineering Tools

There have been no unexpected changes for the considered technologies since the last update of this deliverable. Specifications and the code base of OPC-UA are available in a first official release and they are further developed. The approach of the FDT Group to split the central specification of the FDT technology and the annexes for the individual communication schemas is increasing the coverage of existing fieldbus types by new annexes, as was expected. The degree of reliance to certified devices and tools is being improved by the continuation of interoperability workshops, the establishment of a permanent certification laboratory and the start of the implementation of a frameINSPECTOR.

SNMP and MIB have shown no relevant changes but should be further monitored, since they are integral part of the architecture for VAN devices.

The availability of the DPWS implementation as open source and the standardization of DPWS by OASIS will further promote this technology.

Glossary

3GPP/3GPP2	Third Generation Partnership Project
AAGR	Average Annual Growth Rate
ABS	Anti-lock Braking System
AES	Advanced Encryption Standard
ALGs	Application Layer Gateway
AMSD	www.am-sd.org
API	Application Programming Interface
ARC	ARC Advisory Group: http://www.arcweb.com/
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
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
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
IGP	Internal Gateway 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
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
MIB	Management Information Base
MIMO	Multiple Input Multiple Output radio systems
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NC	Numeric Control
NISC	Network Instruction Set Computer
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
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	www.ra-pid.org
RESET	www.ercim.org/reset
RF	Radio Frequency
RFC	Request for Comments document
RISC	Reduced Instruction Set Computer
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	www.stork.eu.org
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

- [AFDX] http://en.wikipedia.org/wiki/Avionics_Full-Duplex_Switched_Ethernet, 06/2008
- [ARC] <http://www.arcweb.com>, 06/2008
- [Bar07] R. Barth S. Richter, *Multi core in der automation*. In Computer and Automation, 11/2007. pp. 72-76
- [BC08] Blue Coat Systems, Solution Brief: Security Trends 2008, Top 10 Security Trends for 2008, <http://www.bluecoat.com/doc/7524>, 1th of August 2008.
- [Bin08] M. Binhack, Neue Untersuchungen zur Koexistenz von WPAN und WLAN, *VDI-Berichte Nr. 2010*, 2008, S. 107-115.
- [Bluetooth08a] Bluetooth SIG, 2008 Marks Ten Years of Bluetooth Wireless Technology, http://www.bluetooth.com/Bluetooth/Press/SIG/2008_MARKS_TEN_YEARS_OF_emBLUETOOTHem_WIRELESS_TECHNOLOGY.htm, 7th of January 2008.
- [Bluetooth08b] Bluetooth SIG, Bluetooth Technology to Harness the Speed of 802.11, http://www.bluetooth.com/Bluetooth/Press/SIG/BLUETOOTH_TECHNOLOGY_TO_HARNESS_THE_SPEED_OF_80211.htm, 11th of February 2008.
- [Bluetooth08c] Bluetooth SIG, The Bluetooth SIG Goes Ultra Low Power at ISPO Winter Show 2008, http://www.bluetooth.com/Bluetooth/Press/SIG/THE_BLUETOOTH_SIG_GOES_ULTRA_LOW_POWERAT_ISPO_WINTER_SHOW_2008.htm, 23rd of January 2008.
- [Bor08] P. Borowka, Vermaschte Wireless Netze: Funktionsweise, Technologien, Standardisierung unter IEEE 802.11s, *ComConsult Research: Der Netzwerk Insider*, February 2008, S. 18-29.
- [Chao] H. J. CHAO and B. LIU, *High Performance Switches and Routers*. Willey-IEEE Press, 2007, iISBN: 0470053674.
- [Cam08] Cameron, B., Cullen, A., Worthington, B., *The Emerging Technology Trends That CIOs Should Care About*, Forrester ,August 13, 2008
- [CCL] http://www.meau.com/eprise/main/sites/CC-Link/What_is_CC-Link_IE/default
- [Con08] ControlGlobal.com, Wireless for Process Manufacturing to Reach \$1.1B in 2012, <http://www.controlglobal.com/industrynews/2008/127.html>, 14th of April 2008.
- [Cox07] J. Cox, 802.11n Wireless LANs Intrigue Yet Confuse IT Execs, Survey Shows; Wireless LANs to Replace Wired Connections for Client Access, *Network World Fusion*, 1st of August 2007.
- [D02.2-1] U. KÄMMERER, E. FLASCHKA, and A. PÖSCHMANN, "D02.2-1 - topology architecture for the van virtual automation domain," VAN Consortium, Deliverable, 2006.
- [Damm07] M. Damm *Grundlagen der OPC Unified Architecture*. In SPS Magazin 11/2007 pp. 52 - 54

- [Die08] N. Van Dierdonck, Making Sense of Low-Power Wireless Network Standards, <http://www.industrialcontroldesignline.com/206102321;jsessionid=4C3MWWVL F10FIQSNDLRSKHSCJUNN2JVN?printableArticle=true>, 30th of January 2008.
- [DPWS] Device Profile for Web Services, May 2005, <http://specs.xmlsoap.org/ws/2005/05/devprof/devicesprofile.pdf>
- [ECMA08a] Ecma International, Ecma TC48 Draft Standard for High Rate 60 GHz WPANs – Revision 1 – Whitepaper, <http://www.ecma-international.org/activities/Communications/tc48-2008-024-Rev1.doc>, March 2008.
- [ECMA08b] Ecma International, Ecma TC48 Draft Standard For High Rate 60 GHz WPANs – Revision 2, <http://www.ecma-international.org/activities/Communications/tc48-2008-033-Rev2.ppt>, April 2008.
- [Far08] Farpoint Group, 802.11n Access Points and Power over Ethernet: Key Considerations, <http://www.zdnet.de/itmanager/whitepapers/0,39026294,88025101p-39002315q,00.htm>, February 2008.
- [For07] H. Forbes, Lower-power Bluetooth, *AutomationWorld*, <http://www.automationworld.com/columns-3575>, October 2007.
- [Gri08] M. Griesenbruch, Marktstudie Industrielle Kommunikation – Feldbus / Ethernet / Wireless, 2008.
- [Hal05] Halang W.A., Sanz R., Babuska R., Roth H.: Information and Communication technology embraces Control, Proc. of 16th World Congress The International Federation of Automatic Control, Prague 5-9th July, 2005.
- [HART07a] HART Communication Foundation, Why WirelessHART? – The right standard at the right time, http://www.hartcomm2.org/hart_protocol/applications/white_papers/why_wireless_hart.pdf, October 2007.
- [HART07b] HART Communication Foundation, Wireless HART – Simple. Reliable. Secure, http://www.hartcomm2.org/hart_protocol/wireless_hart/wireless_hart_brochure.pdf, 2007.
- [Hir08] Hirche S., Lunze J.: Digital vernetzte Regelungssysteme, Automatisierung 1/2008, pp. 1 – 3.
- [Hof08] S. Hoff, Die nächste Enterprise-WLAN-Generation mit IEEE 802.11n, *ComConsult Research: Der Netzwerk Insider*, March 2008.
- [Hop07] S. Hoppe *OPC UA integriert in eine SPS*. In *SPS Magazin* 11/2007 p. 57-58
- [HSCI] http://www.pdb.heidenhain.de/ansicht/Heidenhain/media/img/571_666-12.pdf
- [IBMGTS08] IBM Global Technology Services, IBM Internet Security Systems X-Force® 2008 Mid-Year Trend Statistics, <http://www-935.ibm.com/services/us/iss/xforce/midyearreport/xforce-midyear-report-2008.pdf>, July 2008.
- [IEC65C488NP.pdf] http://www.canieti.com.mx/assets/files/859/IEC_65C_488_NP.pdf
- [IEEE08a] IEEE 802.11, Official IEEE 802.11 Working Group Project Timelines as of 20th May 2008, http://www.ieee802.org/11/Reports/802.11_Timelines.htm, May 2008.
- [IEEE08b] IEEE 802.15, TG3c Project Plan, <https://mentor.ieee.org/802.15/file/08/15-08-0076-02-003c-tg3c-project-plan.ppt>, May 2008.
- [IMS] www.imsresearch.com, 06/2008
- [InfoWorld] InfoWorld Homepage. 2008. [Online]. Available: www.infoworld.com/bossies

- [ISA08a] D. Caro / J. Reizner, Driving an Open, Consensus Industry Standard, http://www.isa.org/source/2008_02_ISASeminar_EndUserVoice_Caro_Reizner.pdf, February 2008.
- [ISA08b] ISA, ISA100.11a – Release 1 – An Update on the First Wireless Standard Emerging from the Industry for the Industry, http://www.isa.org/source/2008_02_ISASeminar_ISA100.11aStatus_Sexton_Kinney.pdf, February 2008.
- [ISA08c] ISA, ISA100.11a Working Group Completes First Letter Ballot on Draft Standard, ISA100 Wireless e-News, http://www.isa.org/template.cfm?template=/Content/ContentGroups/Standards7/ISA100_e-News/6-25-08.htm#study-group, June 2008
- [ISA08d] ISA, ISA100 Standards Committee Forms WirelessHART Convergence Subcommittee, http://www.isa.org/Template.cfm?Section=Press_Releases5&template=/Content/Management/ContentDisplay.cfm&ContentID=69372, May 2008.
- [Jar07] A. P. Jardosh / G. Iannaccone / K. Papagiannaki / B. Vinnakota, Towards an Energy-Star WLAN Infrastructure, *Eighth IEEE Workshop on Mobile Computing Systems and Applications*, 2007, pp. 85-90.
- [Kho08] A. M. Kholaf / T. D. Todd / P. Koutsakis / M. N. Smadi, QoS-Enabled Power Saving Access Points for IEEE 802.11e Networks, pp. 2331-2336.
- [Lit08] Litz L., Gabriel T., Gross M., Gabel O.: Networked Control Systems (NCS) – State of the Art and Future, *Automatisierung 1/2008*, pp. 4 – 19.
- [Mil08] H. Milosiu, Stromsparende, Integrierte Lösungen für Drahtlose Punkt-zu-Punkt-Sensordatenübertragung für Langjährigen Betrieb, *VDI-Berichte Nr. 2010*, 2008, S. 53-60.
- [Nie07] S. Niermann *OPC UA in einem embedded HMI*. In *SPS Magazin 11/2007* pp. 54 - 56
- [Nof] S. Y. NOF, F. G. FILIP, A. MOLINA, L. MONOSTORI, and C. E. PEREIRA, "Advances in e-manufacturing, e-logistics, and e-service systems," in *Plenary Papers, Milestone Reports, and Survey Papers of the 17th IFAC World Congress*, 2008.
- [OpenVPN] OpenVPN Homepage. 2008. [Online]. Available: www.openvpn.net
- [Pau08] Th. Paul / T. Ogunfunmi, Wireless LAN Comes of Age: Understanding the IEEE 802.11n Amendment, *IEEE Circuits and Systems Magazine*, 1st Quarter 2008, pp. 28-54.
- [Per06] Pereira C.E., Carro L.: Distributed Real-Time Embedded Systems: Recent Advances, Future Trends and their Impact on Manufacturing Plant Control, Proc. of INCOM: 12th IFAC/IFIP/IFORS/IEEE/IMS Symposium Information. Control Problems in Manufacturing Plant Control, May 17-19 2006, Saint-Etienne, France.
- [Rau08] L. Rauchhaupt, Wireless Automation: In Zukunft nur noch drahtlos? *IT&Production*, http://www.sps-magazin.de/artikel/artikel.asp?key=DwEWmZ_EdJ7PvzjDmcYd_&sw=wireless+automation, January/February 2008.
- [Schwa08] E. Schwartz, IEEE Task Force Approves Power Boost Over Ethernet, http://www.infoworld.com/article/08/04/03/IEEE-task-force-approves-power-boost-over-Ethernet_1.html, 3rd of April 2008.
- [SOA4D] Service-Oriented Architecture for Devices, SOA4D Forge; <https://forge.soa4d.org/>

- [SOAP-UPD] SOAP-over-UDP, September 2004,
<http://specs.xmlsoap.org/ws/2004/09/soap-over-udp/soap-over-udp.pdf>
- [SOCRADES] Homepage of the SOCRADES research project;
<http://www.socrades.eu/>
- [SODA] Software download section of the SODA consortium
<http://www.soda-itea.org/Downloads/SoftwareComponents/default.html>
- [TSR1] Trend Screening Report on VAN Relevant Technologies Version 1 (D-1.3-1-1).
- [TSR2] Trend Screening Report on VAN Relevant Technologies Version 2 (D-1.3-1-2).
- [TSR3] Trend Screening Report on VAN Relevant Technologies Version 3 (D-1.3-1-3).
- [TTE] <http://www.elektroniknet.de/home/news/n/d/zeitgesteuertes-ethernet-fuer-industrie-auto-und-a/>
- [WCVPN08] WebCast, Top Trends of 2008 Impacting VPN and Remote Access, TechRepublic,
<http://webcasts.techrepublic.com.com/thankyou.aspx?&docid=335216&view=335216>, January 2008.
- [WIB] International Instrument Users' Association; <http://www.wib.nl>
- [WINA07] Wireless Industrial Networking Alliance, Is Wireless Ready for Prime Time?
http://www.isa.org/source/2008_02_ISASeminar_ISA100.11aStatus_Sexton_Kinney.pdf, December 2007.
- [WSDD] OASIS Web Services Discovery and Web Services Devices Profile (WS-DD) Technical Committee; <http://www.oasis-open.org/committees/ws-dd/charter.php>
- [WS-Discovery] Web Services Dynamic Discovery, April 2005,
<http://specs.xmlsoap.org/ws/2005/04/discovery/ws-discovery.pdf>
- [Zam08] Zampieri S.: Trends in Networked Control Systems, Proc. of the 17th World Congress The International Federation of Automatic Control, Seloul, Korea, July 6-11, 2008.
- [Zig07] ZigBee Alliance, ZigBee Unveils Comprehensive New Features – More Interoperable Choices Creates ZigBee Networks with Numerous Strengths,
http://zigbee.org/imwp/idms/popups/pop_download.asp?contentID=11925, October 2007.
- [Zig08a] ZigBee Alliance, ZigBee Alliance Continues Expanding the Internet of Things – Alliance Forming new Group Chartered to Expand Existing ZigBee IP Capabilities,
http://zigbee.org/imwp/idms/popups/pop_download.asp?contentID=12725, February 2008.
- [Zig08b] ZigBee Alliance, ZigBee Smart Energy: The Standard for Energy Efficiency Available Now – Public Availability Will Accelerate Development of New Energy Management Products,
http://zigbee.org/imwp/idms/popups/pop_download.asp?contentID=13532, 06/2008.