



VAN

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

Virtual Automation Networks

Work Package 1

Requirements and Trend Screening

Task 1.3

Trend Screening and Self evaluation

D01.3-1-V2

Trend Screening Report on VAN Relevant
Technologies

Document type	: Report
Document version	: 1.2
Document Preparation Date	: 29.08.2006
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	Basic template	CARTIF	06-07-10
0.1	Editors comments included	CARTIF	06-07-11
0.2	Introduction included	BUT	06-07-19
0.3	Wireless contents included	SIEMENS	06-07-21
0.3	Engineering Tools contents included	SCHNEIDER	06-07-21
0.4	Trends in real time included	CVS	06-07-21
0.5	Engineering content updated	SCHNEIDER	06-07-24
0.6	Cooperation of Pub. & Private contents added	IFAK	06-08-07
0.7	Safety contents added	PHOENIX	06-08-14
0.8	Exec summary and Conclusions added	CARTIF	06-08-14
0.9	Introduction review	BUT	06-08-23
1.0	Executive Summary review	CARTIF	06-08-24
1.1	Deliverable review	BUT	06-08-25
1.2	Security chapter included	TSA	06-08-29

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 second version of a rolling deliverable, which is devoted to update and complement Trends in VAN-related technologies. As it was stated in the first version of this document, the main objective of version 2 is to provide continuous information about the status and evolution of several technologies related to VAN.

For easy tracking of what is new, the document follows the same chapter structure as the previous version, and only new information is included in it. It is not a progressive document. Due to this reason, the previous version should be considered as a reference, in order to obtain a global, widespread view of the matter of the document.

As the report deals with a several sorts of technologies, and their respective evolution changes with different latencies, chapters' contents differ in a significant way. The scheduled frequency for the updates may be too short for representative evolution changes in some technologies, but it is strictly required anyway to ensure correctly tracking others with fast growth expectations.

As in the previous version, the document is structured in 10 chapters. Chapter 1 is the main introduction (BUT), chapters 2 to 8 directly deal with VAN project main technical figures, which correspond to VAN technical work packages: Wireless in industries (Siemens), Real time considerations (CVS), Safety (Phoenix), Security (TSA), Co-operation of private and public networks (Ifak, TSA), and Engineering tools (Schneider). Chapter 9 is a summary of collected conclusions from all the chapters (Cartif).

Since wireless technologies (Chapter 2) continue being the most dynamical, and their trends should be observed closely to market evolution, a specific chapter (3, Siemens) deals with these figures. Also, other market figures are considered in the rest of the chapters.

Chapter 4 introduces newly emerging trends in real-time technologies. It summarizes already previously started trends and confirms the predicted evolution. A new actuator/sensor fieldbus IO-Link is shortly introduced. This chapter also contains market analysis in this field.

With regards to the safety topic, chapter 5 (Phoenix), in this deliverable it is specified in more detail, basic terms, definitions and their interpretation in terms of functional safety. Functional safety of control systems is one of the most significant phenomenons of recent industrial automation, particularly in Europe (see the market analysis in the Chapter 5).

The security chapter 6 (TSA) is devoted to the commercial development of IT-security technologies, also concentrates in the status of the Ipv6 spreading. The chapter shows a status of cryptography (quantum cryptography and web services security) and ends with topics not directly related with automation systems like phishing or spam.

The trends in cooperation of private and public networks (chapter 7, IFAK) are focused in different topics like VoIP services, Gigabit Ethernet technology or the worldwide infrastructure Metro Ethernet.

Chapter 8 (Schneider) is dedicated to engineering tools for the VAN project, shows the progress of new specifications and standards that are being updated like OPC, FDT/DTM, and the trend of different technologies presented in the first version of the deliverable like Plug and Play, SNMP or Web Services.

The deliverable ends with some concluding remarks, further work and links with other work packages.

Contents

1	INTRODUCTION [BUT]	7
2	TRENDS IN WIRELESS TECHNOLOGIES	8
2.1	EVOLUTION	8
2.2	MATURITY	10
2.3	CONCLUSIONS.....	10
3	MARKET APPROACH IN WIRELESS TECHNOLOGIES	12
4	TRENDS IN REAL TIME PROPERTIES OF INDUSTRIAL COMMUNICATION SYSTEMS	14
4.1	INTRODUCTION	14
4.2	MARKET TRENDS FOR INDUSTRIAL REAL TIME COMMUNICATION	14
4.2.1	<i>Trends on relevant layers and protocols</i>	14
4.2.2	<i>IO-LINK</i>	15
4.3	TIME SYNCHRONISATION.....	15
4.3.1	<i>IEEE 1588 Version 2</i>	15
4.3.2	<i>External Time synchronization</i>	16
5	TRENDS IN SAFETY OF INDUSTRIAL COMMUNICATION SYSTEMS	17
5.1	DEFINITION OF SAFETY FOR INDUSTRIAL COMMUNICATION.....	17
5.2	BLACK CHANNEL PRINCIPLE	18
5.3	SAFETY MARKET	19
5.3.1	<i>Safety Fielbus Market</i>	19
5.3.2	<i>Safety PLC Market</i>	20
6	TRENDS IN SECURITY OF COMMUNICATION SYSTEMS	22
6.1	COMMERCIAL DEVELOPMENT.....	22
6.2	DEVELOPMENT OF IPV6	22
6.3	CRYPTOGRAPHICS.....	23
6.3.1	<i>Quantum cryptography</i>	23
6.3.2	<i>Web Services Security</i>	24
6.4	TRENDS NOT DIRECTLY RELATED TO AUTOMATION SYSTEMS	24
6.4.1	<i>Phishing and Spam</i>	24
6.4.2	<i>Bot-nets</i>	25
6.4.3	<i>Survivability</i>	25
7	TRENDS IN COOPERATION OF PRIVATE AND PUBLIC NETWORKS	27
8	TRENDS IN ENGINEERING TOOLS FOR VAN GOALS	30
8.1	INTRODUCTION	30
8.2	OPC.....	30
8.3	FDT/DTM.....	30
8.4	PLUG-AND-PLAY	31
8.5	SNMP AND MIB	31
8.6	WEB SERVICES	31
8.7	CONCLUSIONS ABOUT ENGINEERING TOOLS	31
9	CONCLUDING REMARKS; FURTHER WORK AND LINKS WITH OTHER WORK PACKAGES	33
	GLOSSARY	35
	REFERENCES	37

List of figures

Fig. 1 Selected IEEE 802 Wireless Standard Working Groups (cf. [For06a], p. 2)	8
Fig. 2 Different wireless technologies (cf. [For06a], p. 2).....	9
Fig. 3 Requirements on wireless field devices (cf. [For06a], p. 4).....	10
Fig. 4 Forecast volumes of UWB-enabled end-equipment split by UWB PAL (cf. [IMS06], p. 3).....	13
Fig. 5 Shipments of Industrial Ethernet devices by protocol [ARC]	14
Fig. 6 Allocation of the average probability of dangerous fault in the entire system.....	18
Fig. 7 Safety Layer Architecture.....	19
Fig. 8 Growth for machine automatic safeguarding equipment in Europe and North America.....	20
Fig. 9 Distribution of Ipv6 allocations	23
Fig. 10 Distribution of e-mail quantities from an email system's point-of-view	25
Fig. 11 North American and Asia/ Pacific VoIP Service Revenue Forecast [InfoRes2].....	27
Fig. 12 Worldwide Metro Ethernet Manufacturer Revenue Forecast [InfoRes2].....	28
Fig. 13 Worldwide Metro Ethernet Manufacturer Revenue by Technology [InfoRes2]	29
Fig. 14 Interrelations of trend reports along VAN project.....	34

List of tables

Table 1 ISA SP-100 Wireless Usage Classes (cf. [For06b], p. 21).	9
Table 2 External clock synchronisation.....	16
Table 3: Development of Safety Fieldbus Market (Source: Venture Development Corp)	19

1 Introduction

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

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

Many market research institutes expect that the world market with wireless devices will grow over a next five year horizon. This grow encompasses Wi-Fi, Wi-MAX, ZigBee a Bluetooth technologies and also UWB technology which promises throughput in hundreds Mbps, but till now, there are still open issues in its standardization outside the US.

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

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

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

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

Previously mentioned aspects allow penetration of office technologies, which are based on the Ethernet, into the automation domain based on fieldbus systems. Merging both the domains allows "vertical integration" between office automation and process automation domains, encompassing both wired and wireless technologies, the Internet and telecommunications systems. This trend requires solving safety, security and real-time issues more then used in solutions of existing Industrial Ethernets with an important stress on interoperability of heterogeneous elements of industrial automation systems. These issues are in the scope of the VAN project.

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

To keep the goals of the VAN project up-to-date, the trends in relevant technologies from a technical and market point of view are looked into.

2 Trends in Wireless Technologies

The following two chapters address the evolution, maturity and forecasted future development of wireless technologies in the industrial environment. This document updates the information provided by the deliverable "Trend Screening Report on VAN Relevant Technologies – Version 1".

2.1 Evolution

The broad landscape of standardization working groups (see Fig. 1) and the increasing willingness of suppliers to participate confirm the future importance of wireless technology. Member companies target "a joint solution that will enable industrial plants to use a single wireless network architecture to support a wide range of applications from low-rate monitoring to process control to wireless worker functions" (cf. [IWB06b]).

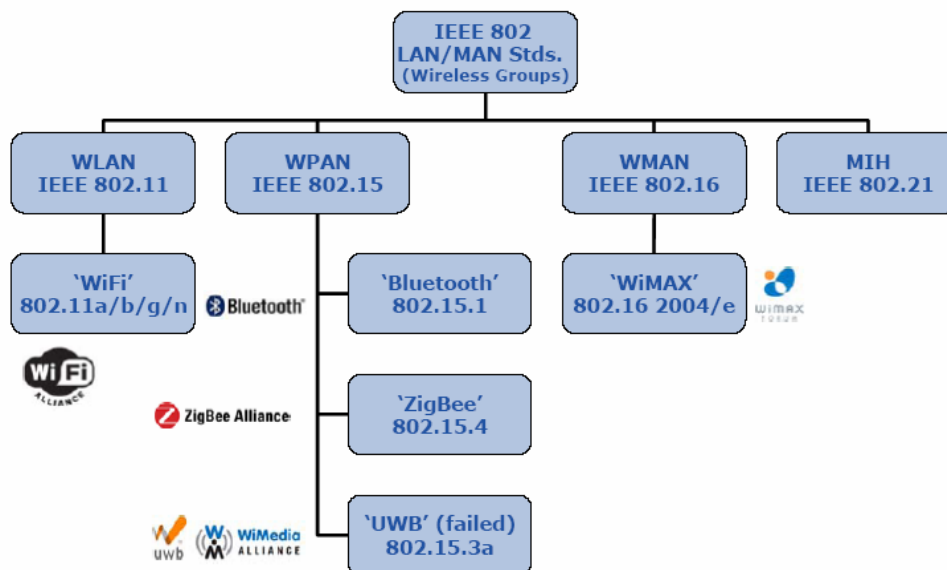


Fig. 1 Selected IEEE 802 Wireless Standard Working Groups (cf. [For06a], p. 2)

The IEEE recently announced the approval of IEEE 802.11e, the mobile WirelessMAN standard that will facilitate the global development of mobile broadband wireless access (BWA) systems. "The IEEE 802.16 WirelessMAN standard continues its evolution as a platform upon which the broadband wireless industry can build high-performance, cost-effective fixed, and now mobile, broadband access systems," said Roger B. Marks, Chair of the IEEE 802.16 Working Group on Broadband Wireless Access (cf. [IWB06a]).

ISA-SP100 Committee announced to form two new standards working groups, SP100.14 and SP100.11: "The SP100.11 working group will strive to provide a wireless connectivity standard for applications in classes 1-5, and possibly class 0 (see Table 1) as well. The SP100.14 working group seeks to provide a wireless connectivity standard for monitoring applications" (cf. [ISA06]).

The standardization of IEEE 802.15.3a (UWB) suffered a setback. Both the WiMedia Alliance and the UWB Forum are working on a standard but their propositions are incompatible (cf. [Gol06]). Another barrier for the widespread utilization of UWB is "the existence of conflicting regional regulations governing UWB devices" (cf. [For06a]). UWB is currently accepted only in the U. S. and is therefore not globally proved. But nevertheless the innovation is going further: Within the scope of the

European project "PULSERS Phase II" UWB should achieve data rates of at least 1 GBit/s (cf. [Gol06]).

The ARC Advisory Group (cf. [For06b], p. 12) sees the industrial wireless sensor market trends as follows: radio frequency technologies will migrate to IEEE 802.15.4 for battery-powered devices and IEEE 802.11 for mains-powered devices. Furthermore sensors will have the following multiple network layers: proprietary, ZigBee, Wireless HART, IPV6 and ISA SP100.

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

Importance of message timeliness increases ↑

Table 1 ISA SP-100 Wireless Usage Classes (cf. [For06b], p. 21).

These activities show the motivation of organizations to push and support the use of wireless technology in the market. But there also critical views concerning this diversity of activities: Merritt is talking about "The next Fieldbus War, perhaps. And some end users are getting tired of it" (cf. [Mer06]).

According to Forbes (cf. [For06b]) the customer is application driven, that is, the application is the source of value not the technology. At present, many wireless technologies compete with each other for use in applications (cf. [For06a], p. 8). The sharp distinctions and boundaries between wireless technologies shown in Fig. 2 do not exist in reality.

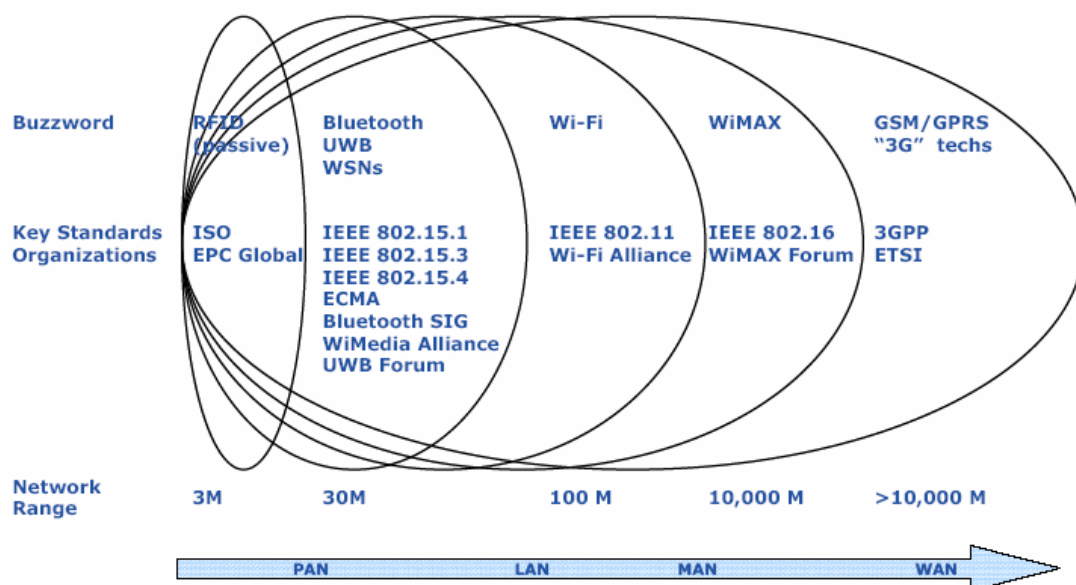


Fig. 2 Different wireless technologies (cf. [For06a], p. 2)

Forbes (cf. [For06a], p. 3) points out further out that, "The concept of coexistence is fundamental to the planning and deployment of wireless systems. In this context, coexistence is defined as the ability to share a single medium of communication. All wireless technologies share a single medium – free space." For customer's purposes sensors, manufacturing automation, production operations, real-time location, wireless data, and voice communication all must use the same spectrum and coexist (cf. [ARC06]).

From the suppliers' point of view "The industrial requirement is an open standard which ensures users utilise the technology for an extended lifecycle," said Satoru Kurosu, vice president of marketing for Yokogawa Industrial Automation Business, "The goal is a single, general purpose industrial wireless standard which can support multiple applications" (cf. [IWB06b]).

2.2 Maturity

Suppliers of wireless automation devices consider WLAN and Bluetooth as mature in the market: These technology standards were stable; their capability was known and field-tested. Furthermore the interference problems between WLAN and Bluetooth were solved, whereas a coexistence of ZigBee with other radio systems in the same frequency band was still problematic (cf. [Wec06]).

Due to special requirements for system availability in the industrial environment and the concerns shown in Fig. 3, the possibility for the use of wireless technology in applications seems to be limited. In the opinion of Merritt (cf. [Mer06]), "Wireless is a fine way to monitor data and transmit set-point information, but it may not be suitable for real-time control when response is critical. Too many variables can upset the timing of wireless transmissions, including other wireless traffic, interference, electrical noise, and so on."

Fig. 3 shows that wireless field devices must simultaneously satisfy many interacting requirements.

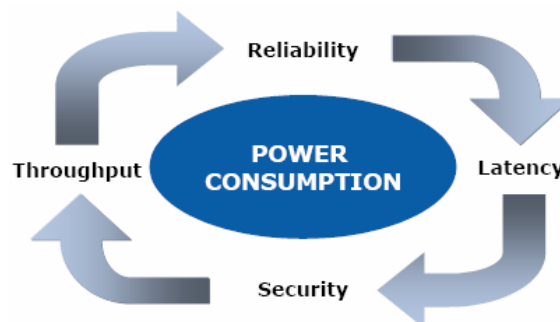


Fig. 3 Requirements on wireless field devices (cf. [For06a], p. 4).

A recently published market study by IMS confirms these concerns: "IMS Research consulted manufacturers and users for its study and concluded that there is a strong requirement for wireless communications in industry, but growth is forecast to be limited to certain applications including monitoring, data collection and programming" (cf. [Mor06]).

2.3 Conclusions

As shown in the last chapter there are still a couple unsolved problems concerning the use of wireless technology in the industrial field. According to Merritt (cf. [Mer06]) there is no doubt that these problems will be solved one day, and wireless Ethernet will prove to be a dominant force in fieldbus. Whereas Chand (Chief Technology Officer at Rockwell Automation) predicts that "wireless will flourish for certain applications but widespread deployment of wireless in industrial automation would be negated by the need for mobile radios and power limitations, as well as customer concerns: "When we ask our customers 'what are your fears about wireless?' they say 'interference, coverage, environmental compatibility and security'" (cf. [Dav06]).

The industrial wireless communications report published by IMS supports this opinion. The study forecasts high growth rates for wireless enabled industrial automation products. But Morse (cf.

[Mor06]), market analyst at IMS, points out that "Although high growth is forecast, progress will be restricted by concerns over the reliability and security of wireless communications. There will have to be a considerable period of confidence-building before wireless is commonly used for applications where there are safety issues".

In this context the Quality of Service (QoS) discussion seems to gain importance for the acceptance of wireless networks. Panousopoulou et al. (cf. [Pan et al 06], p. 5) evaluated the trends on QoS for wireless networked controlled systems and came to the conclusion that "In the control-related case, a sufficient QoS definition remains an unsolved challenge".

But even if the QoS question will be solved experts do not assume that wireless will replace field buses: "Wireless is a complementary technology to HART and field bus, and represents just the physical layer of communication stack" (cf. [Mer06]).

3 Market Approach in Wireless Technologies

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

The world market for wireless communications in automation is forecast to grow at an average of 28.1% per year over the next 5 years, according to IMS Research: "Wireless communications is not widely used within the automation environment at present, but a proliferation of new products is being introduced currently" (cf. [Mor06]).

Indeed the pace of innovation in wireless networking is relentless (cf. [For06a], p. 3). Known exhibitions for automation technology like Hannover Fair and SPS/IPC/Drives confirm the trend to wireless communication. At Hannover Fair 2006, 40 companies exhibited wireless automation devices (cf. [Mer06]). "Wireless in Automation" remains also a main focus at SPS/IPC/Drives 2006 in Nuremberg, Germany.

From the regional point of view Asia-Pacific is projected to grow at a rate higher than either EMEA or the Americas. This is true for most of the seven product sectors considered for the report (cf. [Mor06]). Considered products are Wireless Access Points, Sensors and Transducers, Industrial PCs and HMIs, Programmable Logic Controllers, Drives, Rugged Mobile Computers and Wireless Enabling Accessories.

Growth is also predicted for the ZigBee and UWB markets. In-Stat expects "skyrocketing growth" for IEEE 802.15.4: "On an aggressive basis, 802.15.4 nodes/chipsets could grow by a Compound Annual Growth Rate (CAGR) of 200% from 2004 to 2009" (cf. [InS06b]). The research firm estimates a market volume in terms of unit shipments for ZigBee products of 150 Mio. (cf. [Seu06]). The Chairman of the ZigBee Alliance, Bob Heile says that "Over the past year, in excess of 2 million ZigBee radio chips were sold – more than other radio technology in this space" (cf. [Zig06]).

The UWB Forum reinforced its commitment to the commercialization of UWB technology worldwide, following a meeting of the Institute of Electrical and Electronics Engineers (IEEE) (cf. [UWB06]).

Due to a study of In-Stat (cf. [InS06a]), "manufacturers will begin shipping Ultrawideband (UWB) chipsets in 2H06 and shipments are expected to ramp up with a total of 289 million chipsets shipping in the year 2010. PCs will be the initial and largest volume market for UWB wireless chipsets, with PC vendors shipping over 125 million desktop and laptop PCs with UWB capability by 2010."

IMS Research (cf. [IMS06]) reveals that a number of UWB enabled products are expected to incorporate multiple Protocol Adaptation Layers (PAL). Fig. 4 shows the UWB market split by PAL: "During the forecast period 2005 to 2011 WUSB will be the first UWB PAL to come to market and is expected to be the most popular. IP over UWB is expected to target more specialised markets and is particularly suited to home networking and the home entertainment environment. IMS Research has predicted that Bluetooth over UWB-enabled products will hit the market in 2008. The introduction of Bluetooth into this market will be a substantial volume driver for UWB-enabled products. Cellular terminals are expected to be the dominant application, accounting for around 50% of Bluetooth over UWB shipments in 2011."

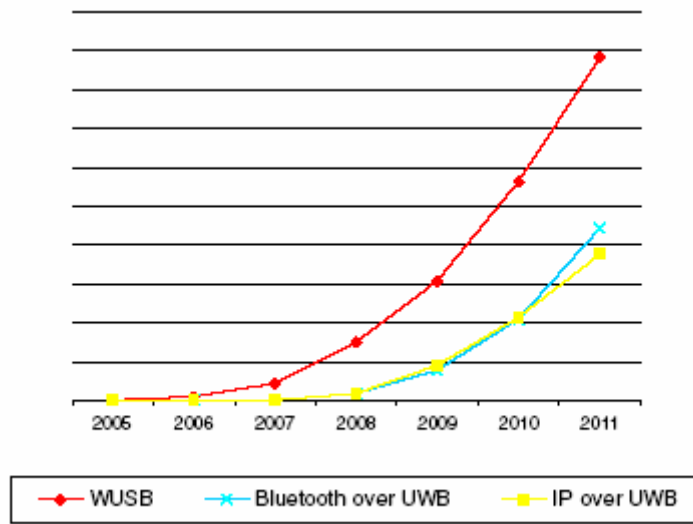


Fig. 4 Forecast volumes of UWB-enabled end-equipment split by UWB PAL (cf. [IMS06], p. 3).

4 Trends in Real Time properties of Industrial Communication Systems

4.1 Introduction

Within this chapter new aspects and market trends in context with real time technologies are described. The focus of the following description is to update the existing Deliverable D01.3-1.V1. In Version 1 the prediction of growth of Industrial Ethernet devices is described. The adduced ARC study "Industrial Ethernet Devices Market Outlook study" from year 2005, prognoses a growth of 51.4 percent of industrial devices up to 2009. A comparable ARC study from year 2003 prognoses nearly the same growth already for the year 2007. So, the outlook of growing sales markets for industrial Ethernet was shifted through the years [ARC04]. But, nevertheless the market for industrial devices and thus also for real time communication increases. According to ARC study from 2005 the following figure [ARC04] shows the real shipments of Industrial Ethernet devices in 2004 sorted by protocol. Modbus TCP protocol (managed by Modbus-IDA) and EtherNet/IP managed jointly by ODVA lead this list. This is due to the fact that these protocols exist longest. Considered on a long term there will be a change instead of Modbus TCP, Profinet will adduce the list of device shipments together with EtherNet/IP.

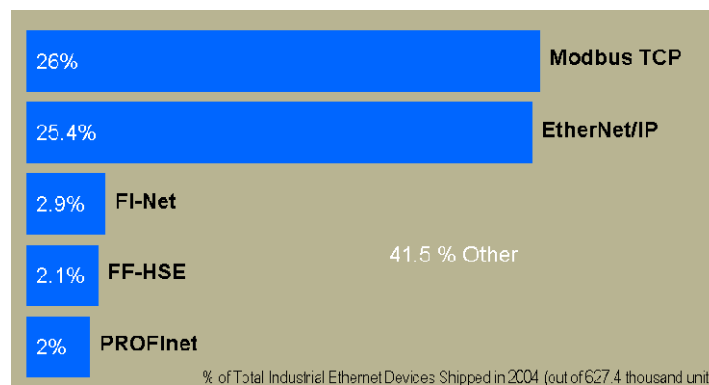


Fig. 5 Shipments of Industrial Ethernet devices by protocol [ARC]

Decreasing prices, rising performance and components which fulfil industrial requirements penetrating rapidly the different levels of automation hierarchy. A current trend which appears in automation is the so called "Commercial off-the-shelf" technology. A lot of Ethernet based appendages with different standards are carried into the industrial surrounding field. The borderlines for the use of Industrial Ethernet are not foreseeable, so far. Everything moves and the further developments are going on.

4.2 Market trends for industrial real time communication

4.2.1 Trends on relevant layers and protocols

With scope of real time, essential definitions for real time in automation with measurable range of values are not solid specified. For high real time requirements the weak point of Ethernet is the low prediction of communication (determinism problem). From this point of view specific field buses are better solutions up to now. In higher hierarchies of the communication, Industrial Ethernet can emphasis its advantages. To use the current benefits and for further development in real time communication the automation industry is faced with IT layer technology. The physical layer specification IEEE802.3xx enables a faster data exchange with the 10 Gigabit version and the 100 Gigabit version expected earliest in year 2010. So, the physical layer is provided for the growing

requirements of data exchanges and data rates and will be not the bottleneck in future industrial networks. Another layer which can influence the Industrial Ethernet environment is the present and wide spread network layer Ipv4 (internet protocol). A new version Ipv6 is designed and specified to deliver a solution for higher requirements. This version implements QoS and introduces traffic classes (service and priority field) and a flow label field. These fields make it possible to insert different entries into the header. These entries let the router know the importance of a data package within a flow. The service class shows the router which Quality of service a flow needs. With the focus of real time aspect and in combination with bandwidth reservation protocols this protocol can provide higher real time utilization in automation. With the capabilities of Ipv6 the QoS parameters like jitter, packet loss rate and data transmission rate will be enhanced. This influences the possibilities of real time communication over WAN and public networks in a positive way.

The technology is available and implemented in some products but penetration to market is slow, because the providers are switching very slow to this new protocol and there is no "Flag day" for switching to this new version defined.

For real time communication different protocols with different architectures are distinguished (see D01.3-1-V1 p. 30). The CIP Sync resp. CIP Motion extension for EtherNet/IP which allows motion control is published within Version 3.0 of Common Industrial Protocol (CIP) specification and Version 1.2 of Ethernet/IP specification in May 2006.

4.2.2 IO-LINK

A new developed standard for connecting actuators and sensors is called I/O Link developed by a working group within the PNO. IO-Link is a serial point-to-point connection oriented on IEC 60947-5-2. It supports a cyclic communication mode with deterministic time behaviour. To exchange process data 2 ms cyclic time are sufficient. For extreme high switching operations a special real time gate can be implemented [IOLINK].

4.3 Time Synchronisation

4.3.1 IEEE 1588 Version 2

In Deliverable D01.3-V1 an example of CIP Sync implementation using the standard IEEE 1588 is shown. This IEEE 1588 standard is very important for real time communication in automation. Thus, the following describes the further development of version two of IEEE 1588 with its new specifications. The temporary release date is planned for spring 2007. Interesting enhancements given by a statement from the NIST organisation are:

- Enhancements for increased resolution and accuracy
 - sub-nanosecond timestamps allowed
 - shorter sync intervals
- Shorter frame and/or Ethernet layer 2 mapping
- Master clock redundancy
- Security extensions
 - Authentication of grandmaster
- Mapping to other protocols
 - DeviceNet
 - MPLS
- Annex D modifications for variable Ethernet headers
 - Tagged frames
 - QoS

- IPv6
 - Increased system management capabilities
 - Transparent clock
 - Time scale supports both TAI and UTC

The concept of transparent clock can be an interesting part for real time communication. If a clock does not depend on the quality of all preceding clocks the cascade effect in cascading Transparent clocks is much better than cascading Boundary clocks. For further descriptions of IEEE1588 version 2 are written in Deliverable D04.2-1.

4.3.2 External Time synchronization

To reach real time communication in distributed automation systems an external time synchronisation is needed. Different technologies, for example DCF77 or the IRIG-X time code are used to synchronise the time behaviour between longer distances. With satellite navigation systems GPS established since the mid of the 1990s higher accuracy clock synchronisation has been possible. The Navstar-GPS system allows a clock accuracy of 10^{-14} seconds. With GPS clocks used in industry a time offset to GPS time of about 50ns can be reached. Another satellite navigation system that is still in development is the so called "Galileo" system which will reach the full operational capacity in 2010. One service of this system is to provide a precise time signal of 30ns according to the UTC (Coordinated Universal Time). The following table shows a comparison of technologies which are currently used and can be used for clock synchronisation in industrial automation. For detailed information see Deliverable D04.2-1.

Clock Synchronisation Technology	Possible accuracy	Warranted Availability	Background
GPS	50 ns	95 %	Military
Galileo	30 ns	99.5 %	Civil
DCF77	50 μ s – 100 μ s	99.7 %	Civil (contract until 2013)

Table 2 External clock synchronisation

5 Trends in Safety of Industrial Communication Systems

5.1 Definition of Safety for Industrial Communication

Safety in general

Safety in general means: freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment and destruction/ damage of production plants.

The main points are:

Safety = Freedom from unacceptable risk

Risk = Combination of the probability of harm occurrence and the severity (costs) of that harm

Motivation → The aim is to reduce the risk to an acceptable risk

Comparison of Safety and Security

For clearness of differences between safety and security terms, we will introduce a short summary of objectives, risks and the respective range connected to these terms

Safety forms a protection against unintended damages which are typically caused without human intervention. For instance, these are environmental accidents or component drop-outs. The consequences of these accidents can be foreseen and the probability of such an accident appears with specific probabilities. The range of damage can be estimated in advance.

Security forms a protection against intended damages typically caused by criminal behaviour of humans. For instance, these are spying or terrorist attacks. The targets of the attacks are the weak-points of the system which are not known in advance and the state of emergency changes rapidly. The range of damage is immense. The intruder aims at causing maximal damage.

Functional safety according to IEC 61508

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

For example, an over-temperature protection device, using a thermal sensor in the windings of an electric motor to de-energise the motor before it can overheat, is an instance of functional safety. But providing specialised insulation to withstand high temperatures is not an instance of functional safety (although it is still an instance of safety and could protect against exactly the same hazard). Neither safety nor functional safety can be determined without considering the systems as a whole and the environment with which they interact.

Safety as a system aspect

The typical allocation of the average probability of a dangerous fault in the entire safety system is depicted in Fig. 6. The communication portion, e.g. over the "VAN cloud", has an amount of 1% of the entire system and is assigned to the controller. The safety loop of the system starts from sensor to controller to actuator, all of them connected via an industrial communication system to each other (i.e. via fieldbus).

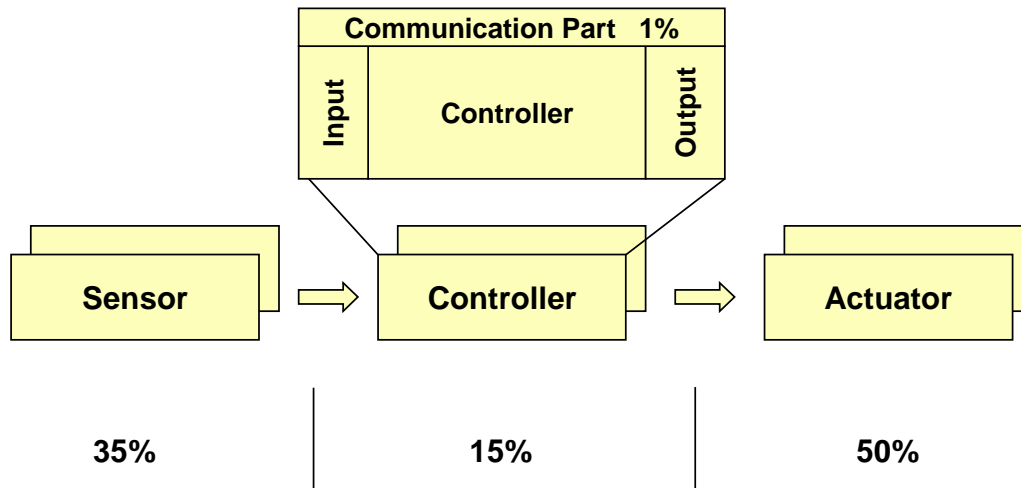


Fig. 6 Allocation of the average probability of dangerous fault in the entire system

5.2 Black Channel Principle

A basic principle of safety communication technology is the implementation of a so called Safety Layer as an additional protocol stack layer consisting of all countermeasures against the possible transmission errors. This Safety Layer typically is a kind of firmware layer, running on top of a standard communication layer. A SIL capable Safety Layer has to be implemented in a SIL capable environment (e.g. 2 channel Hardware, special qualified compiler, etc).

The Safety Layer must consist not only of measures against possible transmission errors on the physical layer of communication.

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

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

On this basis, safe communication is performed by

- A standard transmission system and an
- Additional safety transmission protocol on top of this standard transmission system.

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

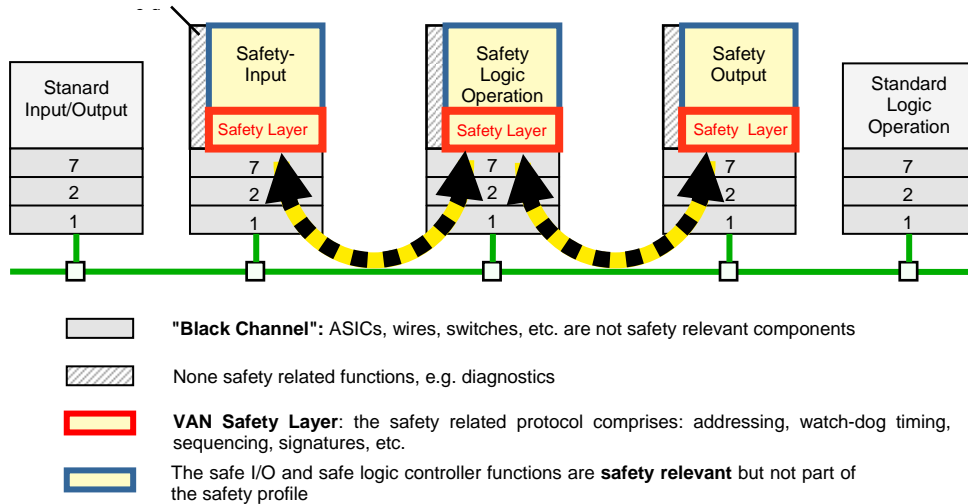


Fig. 7 Safety Layer Architecture

Safety applications and standard applications are sharing the same standard communication systems at the same time.

This principle delimits the certification effort to the "safe transmission functions". The "standard transmission system" does not need any additional certification. Transmission is performed via electrical or optical conductors

5.3 Safety Market

5.3.1 Safety Fieldbus Market

The major safety networks based on fieldbus technology are:

- Profisafe
- AS-I Safety
- DeviceNet Safety
- Interbus Safety

The estimated market share and its development is shown in Table 3

	2002 Share	2006 Share
Profisafe	70,2 %	48,3 %
AS-i Safety	18,7%	25,5%
DeviceNet Safety	0	13,1%
Interbus Safety	0	2,2%
2002 market = 7.1 Mio USD		
2005 market = 56.5 Mio USD		

Table 3: Development of Safety Fieldbus Market (Source: Venture Development Corp)

Market figures for Industrial Ethernet based networks could not be collected.

5.3.2 Safety PLC Market

Another market study by Venture Development Corporation (VDC) projects the most rapid growth for machine automatic safeguarding equipment in Europe and North America will be for programmable safety systems (safety PLCs).

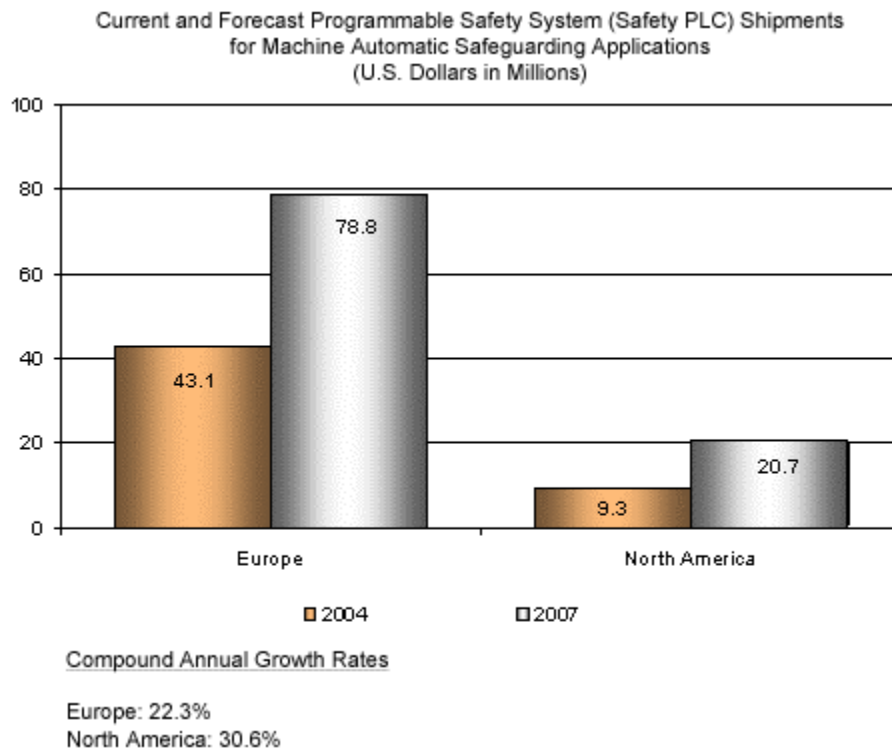


Fig. 8 Growth for machine automatic safeguarding equipment in Europe and North America

The overall machine automatic safeguarding equipment markets are forecast to grow at compound annual growth rates (CAGRs) of 7.4% for Europe, and 12.5% for North America between through 2007. However, the small programmable safety system portions of these markets are forecast to growth at significantly higher rates of 22.3% and 30.6% respectively. This difference is primarily due to the European market's level of maturity, as well as its further adoption of programmable safety systems for these applications.

There are concerns about the reliability and safety in the use of safety buses/networks for machine automatic safeguarding, particularly when safety and non-safety data is handled by the same bus/network. Nevertheless usage is expected to grow significantly over the forecast period, as the use of safety PLCs grows and reliability of operations with safety buses/networks becomes proven. Usage is particularly attractive when machines and controls become more complex (i.e., for example, requiring many emergency stops and/or safety gate switches with multiple actuators).

Benefits resulting from use of safety PLCs and buses/networks include:

- Allowing greater integration of machine controls
- Capability for better and easier diagnostics where intelligence is provided down to device levels
- Faster and easier maintenance
- Greater flexibility in machine controls
- Less wiring to be installed, fewer connections to be made
- Reduction in cost of commissioning
- Reduction in installation and reconfiguring costs

- Reduction of design costs.

6 Trends in Security of Communication Systems

6.1 Commercial development

Security technologies generally have gained additional market share due to the fact that the overall desire for security increased and at the same time the awareness for threats has been raised by companies and organisations. According to the Gartner Group the total security software market revenue grew nearly 15 percent to \$7.4 billion in 2005. Symantec was the overall market leader, with more than 32 percent of the market share.

At present about ten percent of the enterprises world-wide have reached a high level at IT-security. This is the result of an analysis in IT-security in enterprises, performed by the market study and consulting company Gartner. Until 2008 already 20 percent are expected (2005: five per cent). These companies use secure technologies efficiently and effectively, so that resources could be used purposefully against again emerging dangers. However many enterprises are still busy with the defence of routine attacks due to small budgets and should increase their IT-budget. In the opinion of Gartner in the next years many enterprises will have to increase their security budgets.

At the same time Microsoft Windows, TCP/IP, Ethernet, Web browser or Wireless spread rapidly in automation applications. The increasing interconnection makes the formerly isolated network segments more vulnerable. Here protection solutions are required, which exclude interruptions of the processes by viruses, worms or simply only unauthorized accesses from within the network. And also the amount of external attacks against those networks grows intensely. First security appliances for the industrial employment make a secure transmission possible up to the individual plant or the automation equipment. According to a current study of the PA Consulting Group a prominent international management, system and technology consultation, 49% of the viruses and worms, which struck automation plants, came over the internal enterprise network. In the opinion of these advisors the process automation moves more into the view of hackers. 13% percent of the analysed incidents between 2001 and 2005 are identified as sabotage. In average the damage caused by a security incident is quoted as 1,5 Million Euros.

6.2 Development of IPv6

IPv6 is advancing in many ways, primarily in the backbone section of large infrastructure providers but today in many products from ISPs it is possible to get a natively routed IPv6 address range coexisting on an IPv4 access link. The importance of IPv6 in the context of security has been illustrated in other documents in this project but is immanently related to the close integration of IPsec into the stack, the clean hierarchical routing and native support for QoS.

The largest visible development in the research area may be the GÉANT2 network (<http://www.geant2.net/>), which is the successor of GÉANT and will offer access speeds of up to 32Gbit/s. This network will make use of dark fibres (in 18 of the 44 planned routes), which allows the use of several 10Gbit/s wavelengths exclusively (compared to buying fractions of the bandwidth which is then controlled by other infrastructure providers).

The success of GÉANT is another milestone in the adoption of IPv6 and correlates with the successful ending of other activities which are aimed to prove the suitability of IPv6 for productive use, such as the interlink of isolated IPv6 networks via IPv4 tunnels, known as the 6bone. Bob Fink (6Bone Project): "After more than ten years of planning, development and experience with IPv6, with efforts from all around the world, it is gratifying for me to see the 6Bone phase-out on the 6th of June 2006, having served it's purpose to stimulate IPv6 deployment and experience, leaving IPv6 a healthy ongoing component of the future of the Internet!". The 6bone project was necessary as long as native

IPv6 routing was not available on long distances but today carriers nearly only deploy hardware which is capable of routing both versions of the internet protocol concurrently.

The important role of the European Union in the use and distribution of the next generation internet protocol can also be illustrated by the amount of assigned IPv6 network ranges. IPv6 address space for use on the Internet is distributed through a system of hierarchically organised Internet Registries. As one of the five Regional Internet Registries (RIR's), the RIPE NCC allocates IPv6 address space to its members, the so-called "Local Internet Registries" (LIR's). The RIPE NCC service region covers Europe, the Middle East and parts of Asia. The following figure is there to show the share of RIPE NCC and hence the importance of this European institution.

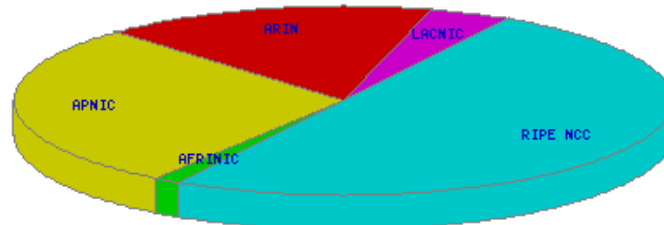


Fig. 9 Distribution of IPv6 allocations

One of the focus areas of RIPE NCC's activities is the securing of routing information. This is planned in form of digital certificates to help authenticate the use of IP address blocks and AS Numbers. In 2006 the RIPE NCC will design and implement the process and technology to enable the RIPE NCC to issue such certificates. The RIPE NCC will also work with the RIPE community to further evaluate particular technical proposals and technology designed to improve routing security. These could include improved routing configuration tools, possibly based on certificates, and BGP protocol enhancements, such as SBGP and SoBGP. As VAN concentrates its name resolution strategies on DNS and the resulting IP addresses an observation of these activities and their implications appears reasonable.

6.3 Cryptography

6.3.1 Quantum cryptography

Despite the efforts put into the development of cryptographic mathematics the only proven secure encryption method is the one time pad. Nearly every other system used today relies on the huge computation resources necessary to calculate a key that successfully decrypts a given message. With the increasing availability of CPU power that formerly was restricted to supercomputers the length of the keys used has to grow as well.

Two major phases of encrypted communication heavily rely on this: the key exchange, where - usually based on an asymmetric key pair (public and private key) - a symmetric key only valid for this session is negotiated and the actual transmission where based on this symmetric key payload is transferred. Only in cases when timing is not crucial at all and messages are small asymmetric encryption is used directly for the encryption due to its enormous calculation costs. In both cases the security can only be considered as "nearly" secure.

Based on quantum physical effects a completely new scenario is possible today and becomes more widely available. Because it is possible to create photons that are interlocked and transmit these to both ends of a communication channel. By observing the physical attributes like the polarisation of one of these particles the attributes of the other one are defined as well. An eavesdropper in between would have to intercept such a photon but then would change its attributes resulting in a mismatch of key information and hence a detection of this intrusion. This is therefore considered as an absolutely secure way to generate keys either to be continuously used as a one time pad or to exchange session keys, depending on the data rate required.

The problem until recently was to reliably create single photons that then could be split into two interrelated photons, having these useful features. But in 2006 some advances have been made

especially at the Toshiba Research Labs in Cambridge and allow the use of semiconductors (instead of attenuated lasers) which makes quantum key servers commercially available.

The achievable key rate heavily depends on the distance to be covered. On short distances (few kilometres) it is possible to generate keys in a frequency that allows for instance every frame of a video to be encrypted with a separate key, while at the maximum range of currently about 120 km it takes several seconds to create one 256Bit key. A concatenation of these sections appears feasible, if the relay station can be considered as secure.

It can be expected that service providers will create meshed structures of "totally secure" communication channels which will allow new application scenarios also for automation industries.

6.3.2 Web Services Security

Three more specifications have been established by the Organisation for the Advancement of Structured Information Standards (OASIS), dealing especially with WS Security. In general OASIS members are defining many of the infrastructure standards that enable Web services as well as the implementation standards that are used in specific communities and across industries. With the introduction of WS-Trust, WS-Secure-Conversation and WS-Security-Policy the WS-Security suite becomes more useful also in a VAN context.

WS-Trust describes a universal token service that may further uncouple the provider and the web service client and by introducing a central component for checking and transforming security assertions (described in SAML) the changes in security mechanisms (probably required because of new threats) do not influence the provider and client program.

WS-Secure-Conversation introduces a security context on message level and hence extends approved concept in the transport layer. The implications of not having to create a new temporary key for every consecutive message are obvious and it is also possible to have more than two communication partners to use the same security context which has been established once in the beginning of this "conversation".

WS-Security Policy provides an extensive vocabulary to describe security requirements of a web service. This is described as a list of alternative ways to communicate with a provider and the client may choose the most appropriate one for this session. Every alternative here is a complete and valid set of requirements. In WS-Security Policy all allowed assertions are described such as protection assertions, token assertions and security binding assertions. These policies are usually referenced in the WSDL of the according service.

These extensions provide an effective approach to construct more robust and sustainable security applications and environments and isolate the volatile security mechanisms from productive and stable application frameworks. VAN aims at the heavy use of web services and therefore the implementation of a security token service and the other mechanisms mentioned above may be beneficial.

6.4 Trends not directly related to automation systems

6.4.1 Phishing and Spam

Even though realtime communication in an automation system is not directly related to email its expanding usage also has influences to all other communication channels such as automation networks. The following picture shows the percentage of useful emails according to the annual report of the German federal office for information security.

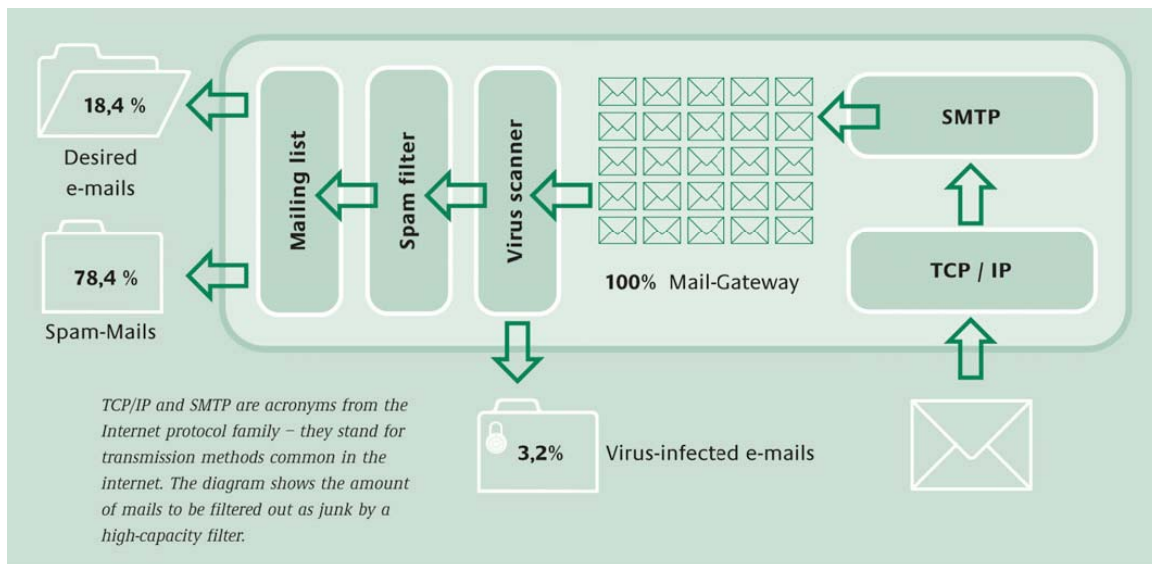


Fig. 10 Distribution of e-mail quantities from an email system's point-of-view

Apart from the sheer number of unwanted emails a substantial new tendency seems to be spear fishing which describes the targeted use of false identities to access company information and gain access to commercial scenarios, for instance in B2B relations. This has certain relevance as after a first very careful phase of high security awareness the introduction of VAN equipment will become a standard operation and hence potentially be vulnerable to identity theft and abuse.

6.4.2 Bot-nets

In the recent past Bot-nets have become serious threats to internet security. The term "Bot" stems from the term "robot" and is used for an application that can process orders independently. It is fed onto an unsuspecting user's computer, being controlled and misused by a third party for their own purposes. A bot-net is a remotely controlled network of PCs connected via the internet which in the hand of cyber criminals may be used for their own intentions. Malicious programs infect an individual computer, put it under their control and integrate it into the bot-net. It shows no detectable damage but waits for orders from outside which activate it to the ends of the attacker.

The increasing use of standard operating systems in automation environments, namely the Windows platform allows this type of malicious software in a scenario with increasing degree of internet-working to invade domains that have not been considered as vulnerable formerly. The implications of such a "sleeper" incident seem obvious without further illustration.

6.4.3 Survivability

In recent years a new trend has been settled in operating networks which is based on the awareness that absolute security can not be reached in complex technical systems. That's why many efforts are spent to design networks that are capable to maintain an operational status even in the presence of a problem similar to a biological organism, staying alive in case of an infection or injury.

Cert.org defines the derived term "survivability" as the capability of a system to fulfil its mission, in a timely manner, in the presence of attacks, failures, or accidents. The term system is used in the broadest possible sense, to include networks and large-scale systems of systems. In particular, the focus of survivability is on unbounded networked systems where traditional security precautions are inadequate. This hence is applicable to public networks in the sense that we intend to use them in a VAN context.

These types of networks (like any public network such as the internet) are characterized by multiple administrative domains with no central authority, an absence of global visibility (i.e., the number and nature of the nodes in the network cannot be fully known), inter-operability between administrative domains is determined by convention, widely distributed and inter-operable systems, users and attackers can be peers in the environment and the network cannot be partitioned into a finite number of bounded environments.

The trend introduces one new aspect, which apart from resistance (protective measures such as firewalls), recognition (intrusion detection) and recovery (backup and redundancy strategies) also demands adaptation and evolution to reduce effectiveness of future attacks (adaptive filtering, new signatures etc.).

7 Trends in Cooperation of Private and Public Networks

VoIP Service

VoIP service revenue doubled in North America, Europe, and Asia Pacific from 2004 to 2005, and will continue to boom for at least the next five years, according to a new report by Infonetics Research [InfoRes1]. The report also found that a combined \$120 billion will be spent in the three regions on VoIP services between 2005 and 2009. The facts are:

- Between 2005 and 2009, VoIP service revenue will grow from:
 - \$2.6 billion to \$13.3 billion in North America
 - \$2.3 billion to \$12.7 billion in Europe
 - \$4.2 billion to \$12.9 billion in Asia Pacific
- Percent of VoIP service revenue coming from residential vs. business customers:
 - 51% in North America
 - 72% in Europe
 - 83% in Asia Pacific
- The number of worldwide VoIP subscribers is expected to almost double 2005 to 2006, when it will top 47 million
- Vonage leads in North American residential/SOHO VoIP subscriber market share, but is down from 34% in 2004 to 27% in 2005, resulting from fierce competition from cable MSOs, traditional telecommunications, and low-cost new entrants
- Cable companies continue pushing to increase VoIP subscriber share: Cablevision and Time Warner Cable each have double-digit share and combined have 39% of all North American residential VoIP subscribers
- AT&T, Comcast, and Cox are the only other providers with North American VoIP subscriber share greater than 3%

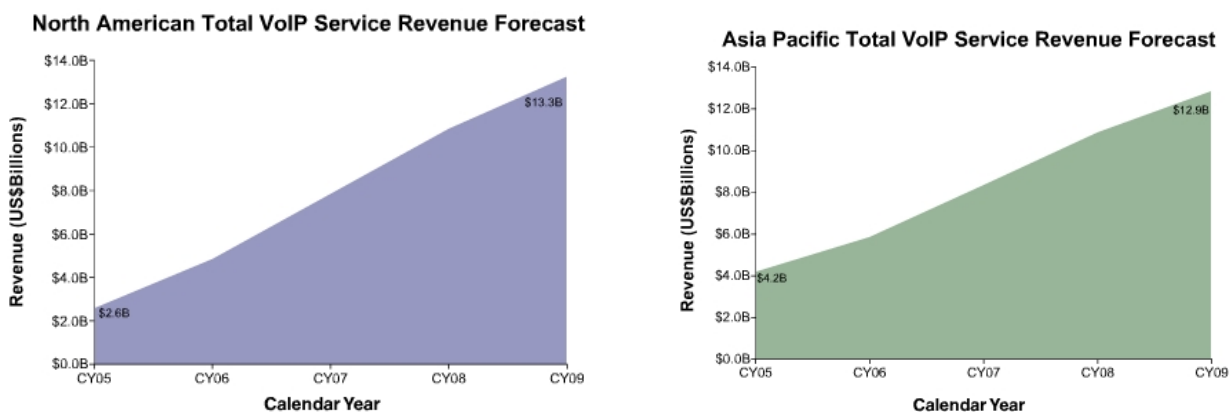


Fig. 11 North American and Asia/ Pacific VoIP Service Revenue Forecast [InfoRes2]

Gigabit Ethernet

End-user spending on Gigabit Ethernet switches is expected to increase by a compound annual growth rate of 1.8% in the next five years. Sales of these switches will account for 70.7% of all spending in 2010, Gartner predicts [ZdnetRes1].

Metro Ethernet

Worldwide metro Ethernet equipment revenue nearly doubled between 2004 and 2005, from \$2.6 billion to over \$4.9 billion, and is expected to triple to \$15.5 billion by 2009, according to Infonetics Research's Metro Ethernet Equipment report [InfoRes2].

Ethernet is becoming an increasingly integral part of metro networks, with equipment spending accumulating almost \$49 billion over the five-year period between 2005 and 2009. Every year Ethernet will account for a larger portion of metro CapEx, led by phenomenal growth in carrier Ethernet switches and routers, a growing mainstay for providers to deliver Ethernet services." The facts are:

- Metro Ethernet port shipments are projected to skyrocket in the next few years, increasing more than 30-fold between 2004 and 2009; the majority of ports sold will be VDSL copper ports
- Revenue in nearly all metro Ethernet equipment categories grew at a fast rate in 2005, with CESR, EPON, Ethernet access devices (EADs), and Ethernet over copper/cable posting triple-digit growth
- Worldwide between 2005 and 2009:
 - CESR revenue will more than double, representing 32% of the metro Ethernet equipment market by 2009
 - EADs will grow 647%, strongly influenced by Ethernet services uptake
 - Ethernet over copper and cable will grow 853%, driven by healthy VDSL deployments in Asia and North America
 - RPR revenue will grow 226%
- North America accounted for 34% of all metro Ethernet equipment revenue in 2005, Asia Pacific for 33%, EMEA for 30%, and CALA for 3%

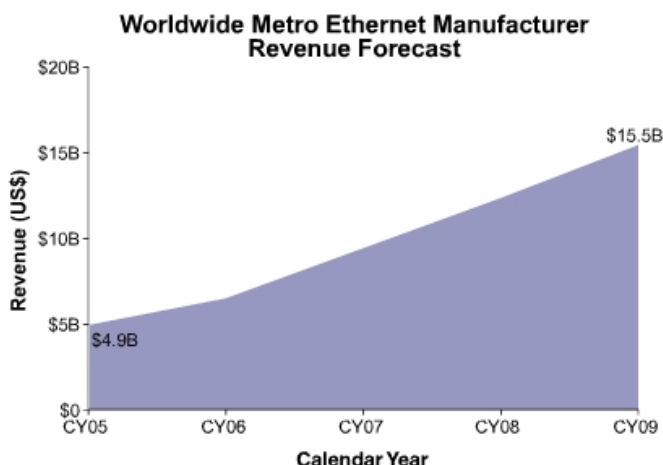


Fig. 12 Worldwide Metro Ethernet Manufacturer Revenue Forecast [InfoRes2]

From the technological viewpoint there are different techniques for Metro Ethernet. The forecast, depicted in the following figure, shows the migration goes from Synchronous Digital Hierarchy (SDH) to Carrier Ethernet.

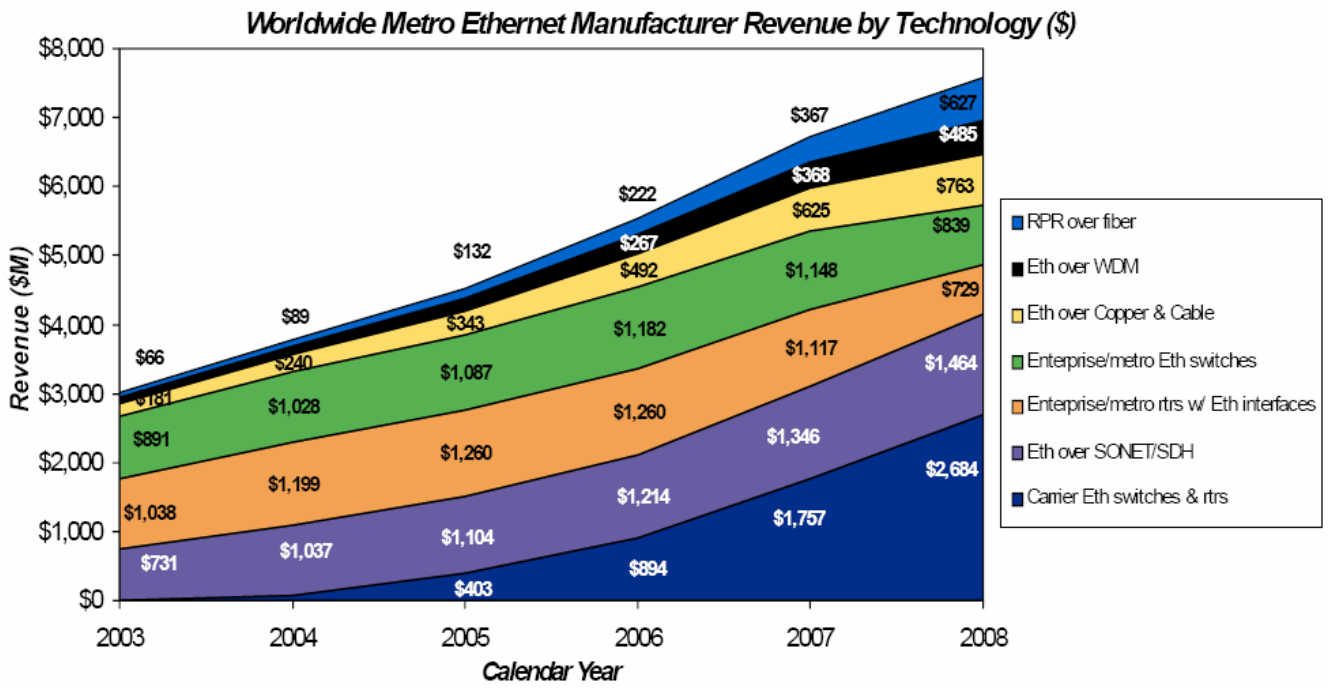


Fig. 13 Worldwide Metro Ethernet Manufacturer Revenue by Technology [InfoRes2]

8 Trends in Engineering Tools for VAN goals

8.1 Introduction

The technologies relevant for VAN-related engineering tasks have already been identified in the first version of the trend screening report. In the meantime no additional technologies have been discovered in available engineering tools for management of automation systems or data exchange across heterogeneous communication networks. In addition to the overview and the description of evolution and maturity for the technologies described in the first version of this deliverable the following chapter will supplement updated information on advances for each technology which are relevant with respect to the VAN project.

Analogously to the investigations made for the first version of the trend screening report the analysis has to follow a qualitative approach due to the fact that no dedicated research on market trends for the engineering tools is conducted. The market analysis is rather dedicated to the primary products of the vendors, i.e. they are focused on devices and systems. Since engineering tools have to support these devices and systems, the tools and technologies for engineering have to follow the market trends of the vendors' primary business offerings.

8.2 OPC

The preparation of the OPC-UA specification for the new Unified Architecture design is proceeding. The specification is divided into 11 parts, which are scheduled to be released until the end of 2006. Parts 1-8 are already available as release candidates for the final review. Moreover, the OPC foundation is developing code based deliverables for the OPC-UA design in order to aid in the creation of OPC-UA applications and to speed adoption. The code base deliverables include a communication stack built on TCP and SOAP, a binary encoder and decoder, a programmers API, a reference client and server implementation as well as proxy and stub components to convert between the existing OPC protocols based on COM technology and the new OPC-UA protocols based on Web services [OPCUA].

Beside the advances with the specifications there is an "Early Adopter Development" program and there are special conferences dedicated to concepts, architecture and implementation of OPC-UA [DEVCON]. Also, more than ten automation vendors have already announced their intentions to support the OPC-UA specifications in their software products.

8.3 FDT/DTM

The FDT specification is divided into a central part for the description of the basic FDT concept with the basic interfaces and separate annexes for specifications related to individual communication schemas. This approach allows adding annexes for further fieldbuses without the need for new releases of the complete specification. The annexes for the fieldbuses Profibus, HART and Foundation Fieldbus had already been listed as released specifications in the last version of this deliverable. In the meantime the annex for Interbus was completed by the FDT group. The development of the specifications for AS-I, Modbus, Profinet I/O and DeviceNet are still in progress.

The FDT group has submitted the specifications to IEC and ISA for international standardization. IEC has established the working group SC65C WG14 and it has released the FDT specification with annexes for Profibus, HART, Foundation Fieldbus and Interbus as "Publicly Available Specification" IEC PAS 62453 in May 2006. Also, ISA has founded the working group ISA SP103 in USA in January 2006 to represent the interests of the American industry and to act as review committee for standardization. [FDT1]

The number of vendors and tools supporting FDT/DTM is growing continuously. Also the number of members of the FDT group is strongly growing. In the first half year of 2006 another 12 international companies have joined the FDT group. The global origin of the new members ranging from Europe to USA and Asia-Pacific clearly shows the rising recognition of the FDT technology in the market worldwide. [FDT2]

8.4 Plug-and-Play

The UPnP technology is still focused on entertainment and consumer electronics in home networks, applications for home automation as well as printing and computer networking in office environment. Devices for use in industrial environment are not targeted.

The number of members in the UPnP Forum has grown to almost 800 vendors.

8.5 SNMP and MIB

As already described in the first version of this deliverable SNMP is a well settled protocol, which is widely used over several years and supported by various vendors. Therefore, no significant changes emerged, which are relevant to be reported in this deliverable.

8.6 Web Services

Web Services are heavily employed in the office domain and for IT business. The penetration in these areas is continuing and standards are complemented for new fields of application.

Due to limited resources of the devices in the industrial domain the usage of fully fledged Web services is not reasonable, but the DPWS specification shows an alternative, lightweight approach, which is also fully compliant with basic Web service technologies and specifications. A new release of the DPWS specification was published in February 2006 [DPWS06]. As it was also mentioned in the last version of this deliverable DPWS will be natively integrated and an API will be available under Windows Vista. The strong support of Microsoft for this technology was affirmed by a dedicated presentation and a hands-on lab during the last WinHEC conference [WINHEC].

8.7 Conclusions about Engineering Tools

The evolution of the technologies and tools for engineering showed no unexpected changes since the release of the first version of this deliverable.

OPC is well established and widely used. The UPC-UA specification for combination of UPC-UA with Web services is well proceeding and the OPC foundation facilitates adoption of this new technology be diverse activities. Since the specifications are to be released not before end of 2006 the acceptance and the impact on engineering tools can not be evaluated for the time being.

FDT/DTM is clearly spreading out and it is supported by increasing number of engineering tools. Moreover, the acceptance obtained by international standardization bodies also shows the upward trend. These trends in the last months confirm the relevance of FDT/DTM for the VAN project.

The UPnP technology has also made noticeable progress. But there are no activities focused on the automation sector. Therefore, this technology seems not to be significant for engineering tools in the automation environment. Due to particular importance of plug-and-play techniques in the VAN architecture, future development of this technology has to be observed.

SNMP and MIB are widely used and supported by most industrial network components. Due to the widespread usage in the engineering tools of the office domain, the architecture for VAN devices already incorporates SNMP as one access point to VAN devices. Although, no significant changes are expected over the next years, this technology has to be further observed.

Clear trend in evolution of engineering tools is in the direction of XML based data representation and web services based data exchange. VAN follows this trend, and web services are an integral part of the its architecture, making it mandatory to further observe enhancements and improvements for this technology. Although, there is a strong push for DPWS from Microsoft it is still not obvious, whether DPWS will be accepted and whether this technology will prevail in the automation domain. Anyway, significant impact can only be expected after the release of Windows Vista operating system with native support of DPWS in 2007.

9 Concluding Remarks; further work and links with other work packages

Next, a summary of conclusions is presented as list of key topics to watch, improvements needed by the different technologies involved in the project, and further work:

- The widespread deployment of wireless in industrial automation would be negated by the need for mobile radios and power limitations, and the fears of the customers about interference, coverage, environmental compatibility and security. Also, the reliability and security of wireless communications, is still an open issue in industrial automation products.
- Reports published by IMS forecasts high growth rates for wireless enabled industrial automation products, But this progress will be restricted by concerns over the reliability and security of wireless communications (cf. [Mor06]).
- For the control-related case, a sufficient QoS definition remains unsolved. The new version Ipv6 is designed and specified to deliver a solution for the higher requirements. This way the router should know the importance of a data package within a flow.
- The usage of the so called "Commercial off-the-shelf" technology appears as a current trend in automation.
- With regards to physical layer specification, the 10 Gigabit version and the 100 Gigabit (2010), should cope with the growing requirements of data exchanges and data rates, so they won't become the bottleneck in future industrial networks.
- In the Gigabit Ethernet market, the end-user spending on switches is expected to increase by a compound annual growth rate of 1.8% in the next five years
- It is very important to watch the new connection standards like for example I/O Link, a serial point-to-point connection developed standard for actuators and sensors.
- The IEEE 1588 standard V2 release (spring 2007) will contain interesting enhancements: increased resolution and accuracy, security extensions and transparent clock, just to mention a few.
- To reach real time communication in distributed automation system external time synchronisation is needed, for example by means of satellite navigation systems. The so called "Galileo" system which will be reach the full operational capacity in 2010, should provide a precise time signal of 30ns.
- The usage of PLC safety systems is becoming of great importance with significantly market growth rates. Also the use of safety buses/networks for machine automatic safeguarding is becoming very useful specially due to the complexity of machines and controls.
- The overall machine automatic safeguarding equipment markets shows an increase of 7.4% for Europe, and 12.5% for North America between through 2007 (measured in compound annual growth rates, CAGRs). However, the small programmable safety system portions of these markets are forecast to grow at significantly higher rates of 22.3% and 30.6% respectively.
- IPv6 is advancing in many ways, primarily in the backbone section of large infrastructure providers. Today even in many products from ISPs it is possible to get a natively routed IPv6 address range coexisting on an IPv4 access link.
- Survivability trend introduces a new aspect, which apart from resistance (protective measures such as firewalls), recognition (intrusion detection) and recovery (backup and redundancy strategies) also demands adaptation and evolution to reduce effectiveness of future attacks (adaptive filtering, new signatures etc.).

- The world-wide Metro Ethernet equipment revenues nearly doubled between 2004 and 2005, and is expected to triple by 2009.
- The increasing number of engineering tools that supports FDT/DTM confirms the relevance of this technology for the VAN project.
- Due to particular importance of plug-and-play techniques in the VAN architecture, future development of this technology has to be observed.
- Web services are an integral part of the VAN architecture, making it mandatory to further observe enhancements and improvements for this technology, like for example DPWS strongly pushed by Microsoft.

In Fig. 14 the relationship between the different versions of the trend screening report and the deliverables from other work packages is presented.

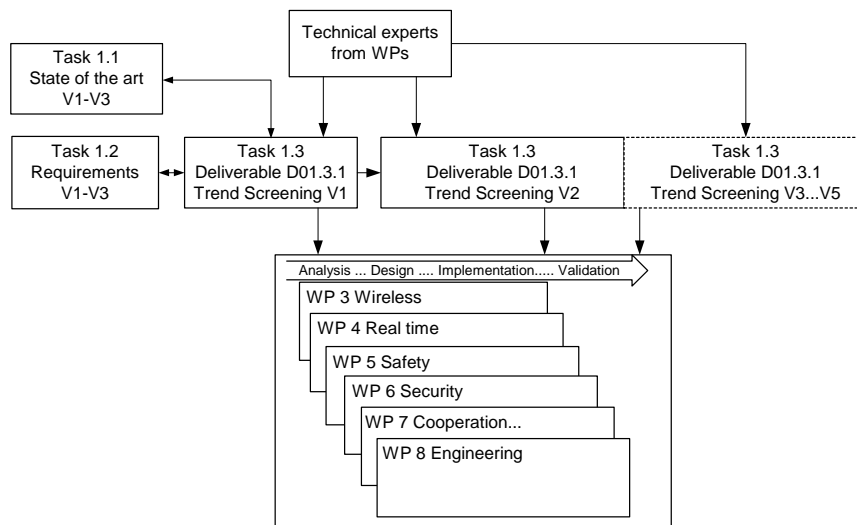


Fig. 14 Interrelations of trend reports along VAN project

Glossary

API	Application Programming Interface
AS Numbers	Autonomous System Numbers
B2B	Business to Business
BGP	Border Gateway protocol
BWA	Broadband Wireless Access
DPWS	Devices Profile for Web Services
DTM	Device Type Manager
EMEA	Europe, Middle East and Africa
FDT	Field Device Tool
HART	Highway Addressable Remote Transducer
HMI	Human-Machine Interface
IEC	International Engineering Consortium
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol security
IPv6	Internet Protocol version 6
ISA	Instrumentation, Systems, and Automation Society
ISA SP100	ISA's Wireless Systems for Automation Standards Committee
ISA	International Federation of the National Standardizing Associations
ISP	Internet Service Provider
LAN	Local Area Network
MAN	Metropolitan Area Network
MIB	Management Information Base
MIH	Media Independent Handover
NIST	National Institute of Standards and Technology
OPC	OLE for Process Control
OPC-UA	OPC-Unified Architecture
PAL	Protocol Adaptation Layer
PAN	Personal Area Network
PAS	Publicly Available Specification
PULSERS Phase II	Pervasive Ultra-wideband Low Spectral Energy Radio Systems Phase II
QoS	Quality of Service
RIPE NCC	RIPE <u>Network Coordination Centre</u>
RIPE	Réseaux IP Européens

RIR	Regional Internet Registries
SAML	Security Assertion Markup Language
SBGP	Secure Border Gateway Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SoBGP	Secure Origin Border Gateway Protocol
TCP	Transmission Control Protocol
UPnP	Universal Plug-and-Play
UTC	Coordinated Universal Time
UWB	Ultra Wide Band
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WS	Web services
WSDL	Web Services Description Language (WSDL)
WUSB	Wireless Universal Serial Bus

References

- [ARC05] ARC Advisory Group: Study from 2004 "Industrial Ethernet Market Analysis and Forecast Through 2009" July 21th, 2006
- [ARC06] ARC, ARCwire Industry Newsletter for the Week Ending May 5th, 2006.
- [Dav06] S. Davies, Interview – Problem Solver, In: Computing & Control Engineering, April/May 2006,
<http://www.ieepublishing.co.uk/oncomms/sector/computing/magazine.cfm?PrintVersion=true&issueID=112&articleID=CB5C35D2-D600-EBD3-83D90BEE9FD659E0>.
- [DEVCON] Conference DevCon 2006, Munich, October 2006
<http://www.opcfoundation.org/Default.aspx/DevCon/DevCon.asp>
- [DPWS06] Device Profile for Web Services, February 2006,
<http://specs.xmlsoap.org/ws/2006/02/devprof/>
- [FDT1] Press Release of the FDT Group, FDT Technology well on the road to standardization, July 2006, http://www.fdtgroup.org/demo/en/01e_news/ne-01_pr.html
- [FDT2] Press Release of the FDT Group, FDT Group announces strong membership growth in 2006, July 2006, http://www.fdtgroup.org/demo/en/01e_news/ne-01_pr.html
- [For06a] H. Forbes, ARC Strategies – Emerging Wireless Technologies in Manufacturing, February 2006.
- [For06b] H. Forbes, ARC Webcast – Emerging Wireless Technologies in Manufacturing, July 12th 2006.
- [Gol06] Golem.de, Geplant: Mehr als 1 Gigabit/s drahtlos über Ultra Wideband, <http://www.golem.de/0604/44977.html>, April 27th, 2006.
- [IMS06] IMS, Popularity of UWB Protocol Adaptation Layers, IMS Research News, June 2006.
- [InfoRes1] Infonetics Research, VoIP service revenue doubles in North America, Europe, Asia Pacific in 2005, CAMPBELL, California, July 26, 2006, online available:
<http://www.infonetics.com/resources/purple.shtml?ms06.vip.nr.shtml>
- [InfoRes2] Infonetics Research, Ethernet market on fire: tops \$4.9B in 2005, will triple by 2009, CAMPBELL, California, April 13, 2006, online available:
<http://www.infonetics.com/resources/purple.shtml?ms06.met.1.nr.shtml>
- [InS06a] In-Stat, Over 289 Million UWB Chipsets to Ship in 2010,
<http://www.instat.com/press.asp?ID=1678&sku=IN0601964RC>, May 30th, 2006.
- [InS06b] In-Stat, 802.15.4 Market Could Grow 200% By 2009 Reports In-Stat,
<http://www.instat.com/press.asp?ID=1356&sku=IN0501836MI>, June 8th, 2005.
- [IOLINK] IO-LINK <http://www.io-link.com>, July 21th, 2006
- [ISA06] ISA-SP100, ISA-SP100 Committee Announces Formation of Working Groups,
http://www.isa.org/Template.cfm?Section=Press_Releases5&template=/ContentManagement/ContentDisplay.cfm&ContentID=54465, May 18th, 2006.
- [IWB06a] The Industrial Wireless Book, IEEE 802.16e mobile WirelessMAN standard is official,
<http://wireless.industrial-networking.com/news/news.asp#234>, February 2006.

- [IWB06b] The Industrial Wireless Book, Major Companies join SP100 working group, <http://wireless.industrial-networking.com/news/news.asp#268>, May 2006.
- [Mer06] R. Merritt, Fieldbus Wars Continue, <http://www.controlglobal.com/articles/2006/127.html>, May 2006.
- [Mor06] J. Morse, IMS Press Releases: Substantial Growth Predicted for Wireless in Automation, <http://www.imsresearch.com>, May 23rd 2006.
- [OPCUA] OPC Foundation Web site, OPC Unified Architecture
http://www.opcfoundation.org/Default.aspx/01_about/UnifiedArchitecture.asp
- [Pan et al 06] A. Panousopoulou / G. Nikolakopoulos / A. Tzes / J. Lygeros, Recent Trends on QoS for Wireless Networked Controlled Systems, http://www.ist-hycon.org/HYCON-publications/CITSA_v15.pdf, 2006.
- [Seu06] F. Seufert, Wireless wird erwachsen – Flexible Funkkommunikation ergänzt das Kabelnetz mit wenig Materialaufwand und ist durch verteilte Intelligenz einfach zu i, In: SPS-Magazin, 4/2006.
- [UWB06] UWB Forum, UWB Forum Focuses on Commercialization of High-Rate Wireless Technology, http://www.uwbforum.org/index.php?option=com_content&task=view&id=122&Itemid=2, 2006.
- [Wec06] J. Weczerek, Sicher und zuverlässig funken, In: elektroAutomation, 4/2006, p. 106.
- [WINHEC] Conference WinHEC 2006, Seattle, May 2006, <http://www.microsoft.com/whdc/winhec/>
- [ZdnetRes1] ZDNet Research, 7/22/2006, online available:
<http://blogs.zdnet.com/ITFacts/wp-trackback.php?p=11363>
- [Zig06] ZigBee Alliance, ZigBee Alliance Sees Unprecedented Momentum Shaping 2006 – Acquisitions, Partnerships and Market Expectation for Certified Products Demonstrate Overwhelming Value of Standard, http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=7654, February 1st, 2006.