INDUSTRIAL NETWORKS*

Žarko Čučej, Dušan Gleich, Mihael Kaiser, Peter Planinšič

University of Maribor, FERI
Smetanova ulica 17, 2000 Maribor, SLOVENIA
zarko.cucej@uni-mb.si

Abstract. *Remote control as well as remote supervising systems are the backbone nowadays producing systems. Both are enabled by different kind of computers and especially microcontrollers connected by different data networks. These networks, industrial networks as their common name is, differ from other data networks in at least in the following:* ***(i)*** *shape of traffic,* ***(ii)*** *available processing capabilities for data interpretation and validation are usually very limited, and* ***(iii)*** *the most important from them is the expected data error renaissance as well as "on time" delivering of correct data. In this article a brief overview of the industrial network issues is given.*

1. INTRODUCTION

The future scenarios of distributed automation require more mechanisms for the local remote distribution of automation functions by various reasons. For example [1]:

- centralized supervisory and control of decentralized technological plants,
- remote control, configuring, commissioning, parameterizations, maintenance of distributed automation systems,
- including remote experts or external knowledge for the plant operation and maintenance.

The resulting automation system has to offer location-based and context-sensitive services to guarantee suitable local and remote functions for different user needs (tele-operation, tele-service) and requires a real-time data transmission, safety and security mechanisms [2, 3].

All this is enabled by appropriate communications between entities involved in distributed automation. Their profiles determined by communication models depend primarily on automation dynamics demands, shape of communication traffics, geographical spreads of entities and so on. According to the hierarchy structure of factories or other systems with distributed automation, the needed communication can be divided into three groups (Fig. 1):

- **Backbones network** link system networks and large communication users. For them it is desirable that allow graduate increasing transfer capabilities on the same physical media.
- **System networks** are simpler than backbones networks. Usually they are implemented by local area networks. Through bridges, switches or router they are connected to backbone and to fieldbuses.
- **Fieldbuses** are specialized local area networks for control and supervisor remote production. They link smart sensors and actuators with PLC or (industrial) computers.

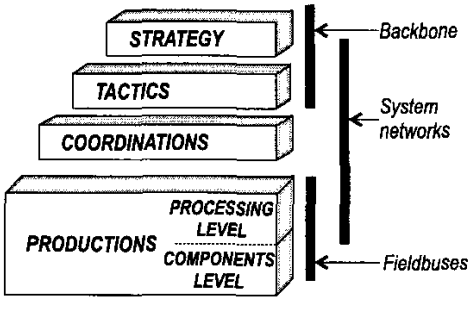

Figure 1: Typical production hierarchical structures and to them adopted data networks

Aforementioned networks differ between each other in the bit rate capability, concepts of work, traffic shape and the most important in the offered services. Meanwhile, backbones and the most of the system

*Invited presentation

networks are not very different from the general data network (because their typical uses are in office flours), part of the system networks and the Fieldbuses has specifics tied to production or other automatized system dynamics. For example, fieldbuses offer less services, are unappropriate for file transfers, but provide hard real-time operation in processing and elements level.

2. LOCAL COMMUNICATIONS

While the major concern of general data Local Area Networks (LAN) is a data throughput, in the industrial local area networks it is reliability, responsiveness and predictability [4]. The development of these networks started around 1980 when smart sensors began to be developed and to be used in digital control [5]. Today, there are many standards on the market; they were developed for different purposes (within cars, buildings, for motion control, process control, etc.) and by different companies [6].

2.1. Available Technologies

Local industrial networks mostly operate on low-cost, twisted pair cables. Today, for many of these networks, optical fiber is considered a new medium. There are also some types of industrial networks that have developed from the opposite directions - they have started with the optical fiber, and then added the use of copper cable to their standard.

2.1.1. Fieldbus systems

Fieldbus systems and sensor networks have been standardized. Nowadays, the Fieldbus transmission technology has been completed by a radio front end (realized by the European project RadioFieldbus) [7–9]. This technology requires additional protocol mechanisms and contains the scheduling of real-time and non real-time traffic. Other important supplements of the legacy fieldbus systems are strictly synchronous communication systems, especially within the motion control area and automotive applications, e.g. TTP, Interbus, hardware-based synchronization mechanisms, PROFIdrive. A summation of the characteristics of some of the popular control networks is given in the Table 1 and briefly presented in the following paragraphs.

Table 1: A summation of the basic characteristics of some popular fieldbuses

Network	Speed	Max. # of nodes	Arbitration	Cable type	Primary application
BITBUS	375 kb/s	32 or 250	Master/Slave	Twisted pair	Intelligent I/O modules, Process Control
World FIP	31.2Kb/s, 1Mb/s, 2.5Mb/s	64 or 256	Bus Arbiter	Twisted pair, copper wire, optical fiber	Real-time Control, Process/machine
Profibus	9.6,..., 1500kb/s	32 or 127	Hybrid medium access	Twisted pair, optical fiber for inter-PLC communication,	Factory automation
CAN	1 Mb/s	30/segment 2048 (A)	CSMA/CD enhanced (bit arbitration)	Twisted pair	Sensor/actuators, automotive
Lon Works	1.25 Mb/s	32000	Predictive CSMA Collision Avoidance	Twisted pair, coaxial cable, fiber optic cable,..:	Appliance control
SERCOS	2-4 Mb/s	256	Ring management	Plastic Optical Fiber	Motion Control
MACRO	100 Mb/s	256	Ring management	Glass Optical fiber, twisted pair	Motion control

2.1.2. LonWorks

LonWork [10] is intended to provide solutions to the problems of designing, building, installing and maintaining control networks. Intelligent nodes communicate with each other using the LonTalk protocol. LonTalk has implemented all seven layers of the OSI model.

The LonWork is worth considering in the executable level of communication. It supports a large number of network nodes and it is hierarchical in the nature. It is defined for fiber optic interface and has gained a larger user base. The speed of the network is not very high (1.25 Mb/s), but at executive and zonal level where commands are not time-critical in nature, this is not a critical factor.

The LonTalk is an open protocol. Echelon – the company that has designed the LonTalk protocol – has allowed the companies to port LonTalk to the processor of their choice. Beside the expected features, such as media access, acknowledgments etc., it also includes more advanced services like sender authentication, priority transmission, mixed data rates, foreign frame transmission, etc.

2.1.3. Controller Area Network: CAN

CAN is one of the most popular Fieldbus protocols [5, 6]. CAN is a high integrity serial data communication bus for real-time applications. It was developed originally for use in cars, but today it is used in other industrial automation and control applications. It uses carrier sensing multiple access/carrier detection scheme (CSMA/CD) [11, 12] with the enhanced capability of nondestructive arbitration to provide collision resolution. Priority of the message is determined by the value of its identifier. Data messages do not contain addresses; instead, the identifier labels the content of the message.

Originally CAN has been developed as an event driven communication system. Recently, time driven (so called Time Triggered CAN: TT CAN) has been developed and introduced to the marked.

2.1.4. Serial Real-time Communications System: SERCOS

SERCOS is designed primarily as a multi-axis motion/machine control standard that provides open controller-to-intelligent digital drive interface specifications [13, 14]. It was accepted as an international standard, IEC 1491, in 1995.

As a multi-axis motion standard it is capable of synchronizing communication nodes. It can support up to 254 digital drives connected to the higher level controller. The network operates at 4 Mb/s speed. Communication cycle time is set during the initialization. Predetermined cycle times are: 0.062ms, 0.125 ms, 0.25 ms, 0.5ms, 1ms or any multiple of 1ms. It utilizes plastic optical fibers. It has a ring master-slave structure. The master initiates a communication cycle by sending a Master Synchronization Telegram (MST). Each slave node uses the MST to resynchronize its clock so that it can calculate the exact time it could reply. The one-byte data that is a part of MST indicates if the ring is in initialization or communications phase. A good characteristic is its physical layer, since it is desirable to use plastic optical fiber because of its EMI immunity and lower cost.

2.1.5. Motion And Control Ring Optical: MACRO

MACRO is a non-proprietary digital interface developed by Delta Tau Systems for the connection of multi-axis motion controllers, amplifiers and I/O by a glass optical fiber or twisted pair ring [15, 16]. Because it is less known in Europe, brief description of it works follow.

MACRO utilizes a physical layer of the Fiber Distribution Data Interface (FDDI) determined in standard ANSI X3T9.5, 4B/5B Non-Return to Zero, Invert on Ones (NRZI) data encoding [11, 17] and transmits data at the speed of 125 MHz. Such high-speed capabilities are achieved by implementing most of the communication protocol in hardware.

MACRO protocol allows multiple master nodes, as well as the slave node to become a master node in a case of a ring break. Nodes have two states: active, which can accept data, and passive, which just passes the data on. Communication is initiated by the active master node, sending data down the ring. The node, to which the data frame is addressed, accepts the frame and substitutes the received packages with its own data and sends them around the ring back to the master. By this the necessary number of the transmitted frames is halved.

The optical fiber is defined as a physical layer, but recent development in plastic fiber transmitters and receivers, as well as the second generation of Taxi chip [18] on which the physical layer is based, allows the use of a higher speed (up to 400 Mb/s) than specified by this protocol.

2.2. Ethernet

The LAN based on the Ethernet with TCP/IP stack has been standardized and widely introduced in the office domain and also in the automation domain, using shared Ethernet as well as Switched Ethernet. Ethernet has system-immanent limits regarding the real-time behavior, because most of the solutions use the TCP(UDP)/IP functionality and a middleware above TCP/IP stack scheduling only soft-realtime and the non-real-time traffic. Examples of this category are PROFInet of PNO Siemens [2,3], Interface for Distributed Automation: IDA of Schneider and Phoenix Contact., etc. [19], Ethernet/IP of ODVA and Rockwell [20], High Speed Ethernet HSE of Fieldbus Foundation and Emerson.

A lot of research activities are dealing with a middleware on top of the MAC layer of Ethernet scheduling the hard real-time, soft real-time and non real-time traffic [21–25]. These mechanisms are very important for synchronous data transmission in the Motion Control area. Examples of this category are Power Link (B&R, Lenze etc.), EtherCAT (Beckhoff), PEAC (ifak), and in the future PROFInet-IRT (PNO Siemens) [15, 26]. Investigations have shown that the switched Ethernet itself is not the bottle neck of the present automation applications. The present bottle neck is the communication stack within the end devices [5-7].

2.3. Wireless communications

The wireless digital communication is becoming more and more important for the automation domain. There are two main reasons for this:

- in automatization more and more applications are like mobile robots etc., where wiring is almost impossible,
- simple implementation, where wiring is very expensive.

Known approaches are: IEEE 802.11b; IEEE 802.11a; IEEE 802.11g; Bluetooth 1; IEEE 802.15 (Bluetooth 2, ZigBee); Radio Add-Ons for Wired Systems; Ultra Wide Band Systems. Wireless LANs based on IEEE 802.11 standard has been introduced in the workshop floor, too. The wireless approaches based on Bluetooth and ZigBee are partially interesting, especially ZigBee as a future supplement of the fieldbus systems.

Many papers deal with several aspects of wireless communications, see [27–38]. Their pivot points are reliability and security. Harsh noise environment and the multiple propagation claim to be carefully addressed in their development. Security issues arise, because received signals can be easy interfered by anyone. Both above mentioned problems are considered in the European Radio Fieldbus project RFieldbus [7]. It reached the following targets:

- supporting real time communication,
- offering flexible multi-cell network architectures,
- managing inter-cell mobility with PROFIBUS procedures,
- taking benefit from multi-path propagation,
- linking wired and wireless segments,
- using available radio technology.

3. WIDE AREA COMMUNICATIONS

In the recent times remote tasks such as tele-supervisory, tele-operation, tele-service, etc. have became more and more important. They are enabled by using Wide Area Networks (WANs). There the stock of the existing communication technology is broader:

- all appearances of the Internet (mostly with the best effort QoS)
- public digital wired telecommunication systems (ISDN, DSL etc.)

- public digital wireless telecommunication systems (GSM, GPRS or/and UMTS-based)
- private wireless telecommunication systems, e. g. trunk radio systems.

Using these technologies within the automation domain there are many private protocols over the leased lines, tunnelling mechanisms, etc. Most of the wireless Radio Networks can be used in the non real-time applications, some of them in the soft real-time applications. The behavior of the end-to-end connection via these telecommunication systems depends on the recently offered quality of service and cannot be guaranteed in many cases.

3.1. Virtual Automation Network

In order for Internet and other public networks to be exploited for automatization, a Virtual Automation Network (VAN) should be formed. It is a heterogeneous network consisting of wired and wireless LANs and WANs telecommunication systems [1]. It means that remotely distributed application programmes cooperating to fulfil a control application are connected via this VAN accessed by the remote connection endpoints (Fig. 2).

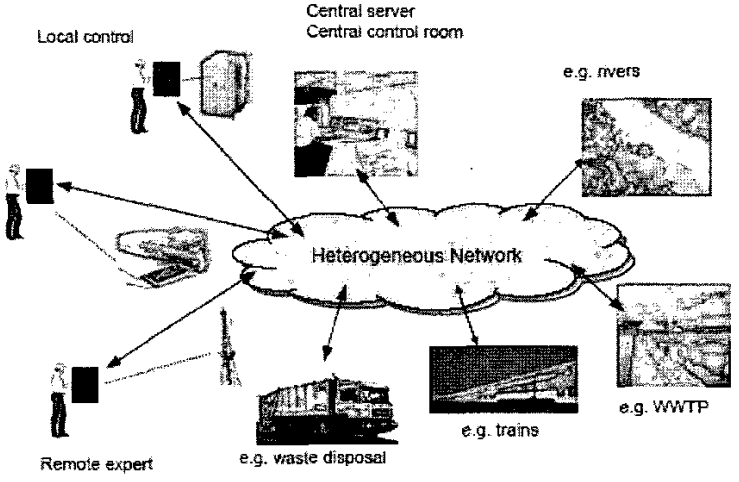

Figure 2: VAN over WAN

The end-to-end connection through a heterogeneous network has to guarantee the privacy, required real-time behavior, security, and safety. Due to strong requirements within the automation domain, the virtual Private Networks VPN known from the office domain do not satisfy enough the above mentioned mechanisms.

3.1.1. Real-time Behavior of VAN

There are different levels of real-time behavior within a VAN depending on the level of the enterprise network. The data packet transmission in the industrial automation application has to have the highest priority. Using WANs, the actual offered mechanisms support mainly the best effort QOS and privilege the video and audio stream transmission. There is a need for offering QOS levels which give suitable response behavior of the data packet transmission. The IPv6 approach offers the real-time mechanisms.

Since the Internet or other telecommunication systems are general-purpose communications systems, the infrastructure and business model preconditions for the selection of requested QOS within a spectrum of available communication services of various providers have to be developed. This means, in analogy to the "switched" Ethernet in LANs a WAN switching mechanism has to be developed for this selection, i.e. choosing dynamically the network type and/or network provider, which guarantees the required QOS.

3.1.2. Functional Safety of VAN

Caused by the distribution of data via the communication networks the safety of these networks becomes more and more important regarding the functionality of an automation system. For that reason special safety buses were developed and existent Fieldbuses were or are going to be extended with the safety layers [39, 40].

IEC 61508 [41] defines Safety Integrity Levels (SIL) for electrical, electronic and programmable electronic devices, which contain the permissible residual error probabilities and error detection rates. It is necessary to prove that the used VAN safety codes fulfil these requirements - especially for different types of communication media. The results should be introduced in the proposed new IEC standardization activities on "Profiles for functional safe and secure communications in industrial networks" [42].

To meet the defined SIL (see IEC 61508), the Residual Error Probability (REP) $\leq 10^{-7}$ errors/h should be for SIL 3 [3]. The communication part requires a REP of $\leq 10^{-9}$ errors/h for SIL 3 (1% of 10^{-7}; the other 99% are required for sensors, PLCs, actuators, etc.). Other requirements are easy integrated into the existing approaches and compatibility with the installed basis.

One principle to make safe communication is to consider the communication channel as *Black Channel* [1]. This means that all safety related functions will be realized on the top of the communication layers. With this principle, an existing communication system can be used as it is – and with the existing components like ASICs, cables, connectors, repeaters, links, etc.

3.1.3. Security

The protection of safety-critical and infrastructure systems against the electronic and communication network based attacks becomes more and more important [43–46]. Security criterions are:

- confidentiality of information, i.e. protection against access by unauthorized third parties;
- information integrity, i.e. detection of unauthorized modification of the message contents with a specified level of confidence;
- timeliness of the message delivery, i.e. detection of any unauthorized message retiming, resequencing or replay of prior messages;
- authentication and authorization of communication peers.

Nowadays, two common defence approaches are discussed: hard perimeter, which does not make sense for VAN, and defence in-depth, which has several zones/shells placed around the protected automation object. Many arguments are given why the defence-in-depth with multiple, staged, complementary security mechanisms is the more suitable approach [43–46].

4. NEW EMERGING TECHNOLOGY

All technologically high developed countries have research programs for 21 century. Important part of them are so called next generation communications. Here the development is going in more directions, from services to communication processors to new transmission media materials, which enable higher data transfer rate, lower end-point connection cost, etc. One of such projets in Japan is Keio University 21st Century COE (Center of Excellence) Program "Optical and electronic device technology for access network". One of the important results is high bandwidth, large-core Graded-Index Plastic Optical Fiber (GI-POF) for use in giga bit data communication area. Perfluorined (PF) polymer based GI-POF networks can support higher transmission rate than silica fiber network (of course at the much lower costs) due to their small material dispersion of PF polymer compared to silica [49, 50]. This make GI-POF attractive for future industrial networks at least for following reasons:

- very low bit error rate compare to other optical networks
- high mechanical flexibility (bending locus can be five times smaller than at the silica fiber)
- the visible light source can be used (important for secure maintenance).

As it is stated in [49], GI-POF together with Responsive Multi-threaded (RTM) processor as control and communication processor core is intended for use in robots (humanoids, etc), cars, video conferencing systems, home automation, office automation, intelligent rooms/buildings, amusement systems, i.e. for all systems, which can not be controlled by a single CPU.

Demonstration networks in Keio University campus like Giga-House Town Project has many elements typical for hard real time control like on-line medical care, house automation, real-time video, etc. Together with all-optical switches it presents a promised base for a development for new generation of the industrial network with more simple network and smarter end terminals.

5. VERY FAST SERIAL BUSES FOR DEVICES

Recently we are also witnessing of introduction of a very high speed serial buses for interconnecting personal computers components like SATI, etc. We can expect that semiconductor technology, which enables the design serial buses with a bit rate up to 2,4 Gb/s, will be shortly used in control and automatization domain. There are many devices like power electronic converters of any kind, which with introduction of the communication system in their building blocks can be significantly simplified in design and use [47]. For this purpose up to now the modified MACRO fieldbus is used [16, 48], which enables payload bit rate up to 85 Mb/s and a jitter within a few % of a bit duration.

6. CONCLUSION

Industrial networks are a fast growing (tele)communications field. Recently, development in the general data networks have a strong influence on the classic division of industrial network and their development. More and more general data LAN and WAN are used for automatization and remote control. In such their applications they should be adopted to those needs.

The existing VPN technology has some useful features, but doesn't support the important VAN features such as definition and specification of the compliance classes, management, as well as test infrastructure. The most serious problem at VAN seems to be the free choice of telecommunication service providers that choose the actual needed QoSs, since there are not any legal instruments for the required contracts and any online switch mechanisms.

We are also wittiness of further development of data networks where the issues of the industrial network are considered. New ultrahigh speed communications systems, projects like Giga-Hause Town Project, clearly indicate this direction.

REFERENCES

[1] Neumann, P.; Virtual Automation Network, IEEE conference ICIT'03, Maribor 2003, Proceeding, pp. 994 – 999

[2] Sauter, T.; P. Neumann: Feldbus, Internet und Mobilkommunikation wachsen zusammen. VDE Kongress, Dresden 2002, (Band 2), Seite 245-250

[3] Neumann, P.: Merging Fieldbus and Telecommunication Systems in the Industrial Automation Domain. IEEE AFRICON 2002, 6th AFRICON conference in George, ZA, Proceedings Vol.1, pp.197

[4] Frequently Asked Questions about LonWorks Networks, http://www.lonworks.echelon.com, Echelon - The LonWork Company, 1997.

[5] The History of Fieldbus, Fieldbus Tutorial-History, http://rolf.ece.curtin.edu.au/-clive/Fieldbus, 1997.

[6] Selecting the Right Fieldbus, Gespac, 1997. http://www.gespac.com/html

[7] Decotignie, J.-D.: Wireless Fieldbusses – A Survey of Issuses and Solutions. 15th Triennial World Congress of the International Federation of Automatic Control, Barcelona 2002

[8] Rauchhaupt, L.: RFieldbus a Survey. 5th IFAC International Conference on Fieldbus System and their Applications (FET 2003), Aveiro, Portugal, 2003, Proceedings, pp. 105-114.

[9] Rauchhaupt, L.: System and Device Architecture of a Radio Based Fieldbus – The RFieldbus system. 4th IEEE International Workshop on Factory Communication Systems, 27.-30.08.2002, Västeras, Proceedings pp. 185-192.

[10] Blomseth, R.; Capolongo, W.; Dolin, B.; Lund J.: The LonWorks Networks Services (LNS) Architecture Technical Overview, `http://www.lonworks.echelon.com`, 1997.

[11] Bertsekas, D.; Gallager, R.: Data Networks, Second Edition, New York: Prentice Hall, Inc, 1992.

[12] CAN Specification, version 2.0, Robert Bosh GmbH, 1991.

[13] SERCOS (IEC 1491), Developer's Kit, SERCOS N.A., March 1997.

[14] Berardinis, L., SERCOS Lights the Way for Digital Drives, Machine Design, August 1994.

[15] Delta-Tau Data Systems, Inc.: Motion and Control Ring Optical, Specification, May 1998. http://www.macro.org

[16] Milosavljevic, I.: "Power electronic system communications" MSc. thesis, 1999, Virginia Tech, Blacksburg, Va, USA. http://scholar.lib.vt.edu/theses/available/etd-021299-141947/unrestricted/IMTHESIS.PDF

[17] Stalings, W.: "Network standards", Addison-Wesley, 1996.

[18] Taxi chip: CY7C9689A Datasheet, Cypress, 2003. http://www.cypress.com/products/datasheet.cfm?partnum=CY7C9689A-AC

[19] IDA Group: IDA - Interface for Distributed Automation, Architecture Description and Specification. Revision 1.1, November 2002.

[20] Jasperneite,J.: Leistungsbewertung eines lokalen Netzwerkes mit Class-of-Service Unterstützung für die prozessnahe Echtzeitkommunikation. Shaker Verlag, Aachen 2002. ISBN 3832208321.

[21] Agarwal, Anjali and Kang Bin Wang: "Supporting Quality of Service in IP multicast networks" in Computer Communications, Volume 26, Issue 14, Pages 1533-1540.

[22] Caponetto, R.; L. L. Bello; O. Mirabella: Experimental Assessments of Fuzzy Smoothers for Ethernet Networks. 15th Euromicro Conference on Real-Time Systems, Porto 2003. Proceedings, pp. 57-60

[23] Carpenzano, A.; Caponetto, R.; Lo Bello, L.; Mirabella, O.: Fuzzy Traffic Smoothing: an Approach for Real-Time Communication over Ethernet Networks. 4th IEEE International Workshop on Factory Communication Systems. WFCS'02, Västeras.

[24] Alves, M.; Tovar, E.; Vasques, F. : Ethernet Goes Real-Time : a Survey on Research and Technological Developments. Techn. Rep. HURRAY-TR-0001, Polytechnic Institute of Porto, Jan. 2000.

[25] Bonaccorsi, A.; Lo Bello, L.; Mirabella, O.; Neumann, P.; Pöschmann, A.: A Distributed Approach to Achieve Predictable Ethernet Access Control in Industrial Environments. FET 2003, 07.- 08.07.2003, Aveiro, Proceedings, pp. 173 – 176.

[26] Feld, J.: Real-time Communication in PROFInet V2 and V3 Designed for Industrial Purposes. FET 2003, 07.-08.07.2003, Aveiro, Proceedings, pp. 291 – 296.

[27] Skvarla, Carol: Wireless Technologies and Services in the U.S.: Overview. 2002-11-21, Gartner Group

[28] Wireless LAN Policies for Security & Management. 2003-03-21 , AirDefense, Inc. , Whitepaper

[29] Rammig, R.: Security in Wireless Networks (Report Summary) 2003-09-12, Siemens AG, CT IRC TIS , TechnologyReport

[30] Understanding the Layers of Wireless LAN Security & Management. 2003-05-07, AirDefense, Inc. Whitepaper

[31] Hiller, K.: Wireless LANs: An Overview 2002-10-17 , Gartner Group, Analyst report

[32] Klein, M.: Executive Briefing: Wireless Network Security. 2002-12-19, InterlinkNetworks,Inc. Whitepaper

[33] Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte. 2003-09-10, Bundesamt fuer Sicherheit der Informationstechnik, Whitepaper

[34] Beutlich, B.: Wireless Security - Extending Access to the Road Warrior. 2003-07-28, Rainbow Technologies, Whitepaper

[35] Girard, J.: Secure the Enterprise Against WLAN Attacks, 2003-09-10, Gartner Group, Analyst report

[36] Ensuring Wireless Security with 3G: Deliver secure mobile services, 2002-07-29, Lucent Technologies, Whitepaper

[37] Puzmanova, R.: WLAN and WPAN technical overview: Wireless Personal and Local Area Networks. In Computer Communications, Volume 26, Issue 18, Axel Sikora (Ed.); Wiley, New York, 2003, 216 pages, ISBN 0-470-85110-4.

[38] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA): Funkgestützte Kommunikation in der Automatisierungstechnik (Radio based communication in industrial automation), VDI/VDE Richtlinie 2185, 2002

[39] Redmill, F.; Anderson, T.: Components of System Safety. Springer Verlag, Berlin-Heidelberg-New York, 2002.

[40] Reinert, D.; Schaefer, M.: Sichere Bussysteme für die Automation. Hüthig Verlag Heidelberg, 2001.

[41] IEC 61508: Functional Safety of Electrical/ Electronic/Programmable El. Safety-Related Systems

[42] IEC 65C/307/NP: Digital data communications for measurement and control – Profiles for functional safe and secure communications in industrial networks, New Work Item Proposal, 2003

[43] Naedele, M.: IT Security for Automation Systems, Motivations and Mechanisms. Automatisierungstechnische Praxis 45 (2003), H. 5, S 84-91

[44] Palensky, P.; T. Sauter: Security considerations for FAN Internet connections. International Workshop on Factory Communication Systems, 2000

[45] Naedele, M.; Dzung,D.; Stanimirov, M.: Network Security for Substation Automation Systems. In Computer Safety, Reliability and Security. Proceedings Safecomp 2001, LNCS 2187. Springer, Berlin 2001

[46] Fritz, R.; Halang, W.: Sichere Abwehr von Viren. 2002, ISBN 3-89577-266-6

[47] Čučej, Ž.: Power Electronic Buliding Blocks: a surway. Elmar 2003, Proceedings, Zadar 2003.

[48] Čučej, Ž.: Power Electronic Buliding Blocks: Control and Communication issues. Elmar 2003, Proceedings, Zadar 2003.

[49] Toshiaki Makabe (CEO leader) Proceedings of the International Symphosium on *Optical and Electronic Device Technology for Access Network*, December 5, 2003, Tokyo International Forum, Japan

[50] Minoru Obara (Editor) 21st Century CEO Program: *Optical and Electronic Device Technology for Access Network*, Interim RAs Research Progres Report (2002-20003), Volume 2. Keio universiti Yokohama, Japan