



VAN

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

Virtual Automation Networks

Work Package 1
Requirements and Trend Screening

Task 1.1
State of the Art

Deliverable D01.1-1-V2
State of the Art and Trends
in Safety, Security, Wireless Technologies
and Real-time Properties

Document type	: Deliverable
Document version	: Final
Document Preparation Date	: 08.09.2006
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
0.1	Initial structure	BUT	04.08.06
0.2	Added contributions from partners	Phoenix, IFAK, CVS, Siemens	28.08.06
0.3	Figure added	BUT	29.08.06
1.0	Final version	BUT	31.08.06
1.01	Glossary added, chapter 4 update + minor corrections elsewhere	BUT, CVS	08.09.06

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

Final approval	Name	Partner
Review Task Level	Petr Fiedler	BUT
Review WP Level	Frantisek Zezulka	BUT
Review Board Level	Axel Klostermeyer	Siemens

Executive summary

The D01.1-1-V1 was focused to description of relevant communication technologies used in industrial automation. The goal of the “V1” deliverable was to describe crucial technical features of each relevant communication technology – the deliverable was focused to technologies itself. The goal of this deliverable, the D01.1-1-V2, is to describe state-of-the-art from the point of view of automation applications, including existing application limitations caused by limited features and capabilities of state-of-the art technologies. The aim is to show capabilities and especially limitations of present communication solutions for automation systems and to show the potential technological advantage of VAN.

This deliverable is rather brief for the following two reasons:

- 1) From the date of release of the D01.1-1-V1 no technological significant breakthrough in the field of industrial communications has been done. The only exception is the real-time chapter, where new technologies are described. Instead this deliverable tries to show major limitations of present industrial communication technologies, and shows that many of these limitations will be addressed within the VAN project.
- 2) While within the time frame of D01.1-1-V1 it was necessary to form a common technological baseline for the project participants, the situation within the time frame of D01.1-1-V2 is such that all technical work-packages have been investigating and evaluating intensively existing technologies and approaches in their particular fields and tasks. These will eventually contribute to MS2 milestone (Detailed Specification of the used technologies, Concepts and Mechanisms; due month 24).

The structure of this deliverable follows the structure of the project work-packages – the chapters are focused to the communication architecture, real-time application requirements, use of wireless systems in automation, functional safety and security. Moreover in the introduction a short overview of development of industrial communication systems is given, which also clarifies why Ethernet and its industrial enhancements receive the major focus within VAN.

Contents

1	Introduction	6
2	Communication Architecture in Automation	8
2.1	State of the Art.....	8
2.2	VAN Enhancement.....	9
3	Wireless in Automation	11
3.1	State of the Art.....	11
3.1.1	Bluetooth.....	11
3.1.2	UWB	11
3.1.3	WLAN	12
3.1.4	ZigBee	12
3.2	VAN Enhancement.....	12
3.2.1	Bluetooth.....	12
3.2.2	UWB	13
3.2.3	WLAN	13
3.2.4	ZigBee	13
4	Real-time in Automation.....	14
4.1	State-of the art.....	14
4.1.1	Latest technologies for real-time in automation.....	14
4.2	VAN enhancements	16
5	Safety in Automation	17
5.1	State of the Art.....	17
5.2	Organization of Safety Measures.....	17
5.3	VAN Enhancements	17
5.3.1	Safety specification for open networks.....	17
5.3.2	Interoperability of existing safety networks.....	18
5.3.3	Wireless Safety solutions	18
6	Security.....	19
6.1	State of the Art.....	19
6.2	VAN Enhancement.....	20
7	Summary.....	21
	Glossary.....	22
	References.....	23

List of figures

Fig. 1.1: Hierarchical communication architecture7

Fig. 6.1: Hierarchical communication architecture19

1 Introduction

Traditional industrial control systems relied on discrete and analog devices, which were individually wired from the device to the controller. The real-time performance of the discrete system was limited mostly by performance of the controller and response time of the device. The real-time performance of the analog devices was also limited by the dynamics of the 4 - 20 mA current loop, which was the most typical analog interface.

The point-to-point wiring “topology” was difficult and slow to debug and maintain. The flexibility of such systems was extremely low. Moreover the information transfer was lacking any diagnostic or status information that could be used for monitoring of the “health” of the sensors and actuators in the field. For this reasons various industrial communications systems (a.k.a. fieldbuses) have been developed. The idea behind development of fieldbuses was to enable interconnection of control elements for centralised or decentralised control that would enable exchange of both process information and diagnostic information in real-time.

The extreme variability of services being integrated into the intelligent automation devices and wide range of communication solutions proposed by different vendors to handle this variability has caused strong heterogeneity in the field of automation systems. Experience with heterogeneous systems has shown that significant interoperability issues occur when heterogeneous systems have to exchange data.

The contemporary automation architecture is dominated by intelligent field devices that are connected to various networks and fieldbuses, often based on RS-485, CAN or other physical and link layer solution. Very often it is necessary to employ in the single plant several different communication subsystems, which meet specific requirements of the various tasks found in the plants. It would be desirable to use only one type of fieldbus in the whole plant; however there is no single fieldbus that would fit various requirements on transmission speed, inter-device distances, communication latencies and explosion safety. Utilization of heterogeneous communication systems is in most cases the only option. There have been various fieldbus integration efforts in the past, however these efforts were not successful and multiple competing fieldbus protocols have been accepted as international standards (e.g. IEC 61158 and EN 50170).

The need to use the heterogeneous communication technologies that are able to cover various application areas resulted in development of gateways, which are able of translating information between heterogeneous systems. A gateway between two networks has to “understand” both protocols, as it interprets data received from one network and translates them to data structures available on the other network. In many cases utilization of gateway based solutions is the only option available, however the inter-networking based on gateways often leads to interoperability issues as quite frequently the common data structures are subsets of the original data sets.

Communication networks found in today’s plants and processes can be divided into the following groups [LeBlanc00] according to their primary focus:

1. *Sensorbus* – low level networks used for connection of simple low cost sensors and actuators. The amount of process data being transmitted in a single message is expressed in bits rather than bytes. More complex devices (e.g. manipulator systems, injection moulding machines with robotic arms, NC machines) often contain a sensorbus.
2. *Devicebus* – general networks interconnecting smart field devices. The amount of process data and/or diagnostic data being transmitted in a single message is in the order of bytes. Devices interconnected via devicebuses can perform more detailed diagnostics and report more advanced diagnostic data. These communication systems have been the fast real-time solution before the industrial Ethernet appeared.
3. *Fieldbuses* – These systems support transmission of larger amounts of data in the order of kilobytes, however the data rate was sometimes lower than the data rates of devicebuses.

4. *Higher Control networks* – Targeted at high level communication between powerful PLCs or DCS controllers.
5. *Enterprise networks* – The network backbone for the company, predominantly Ethernet TCP/IP based systems.

Where it is not necessary to distinguish between different types of process networks, there the networks from groups 1 to 4 are generally called fieldbuses.

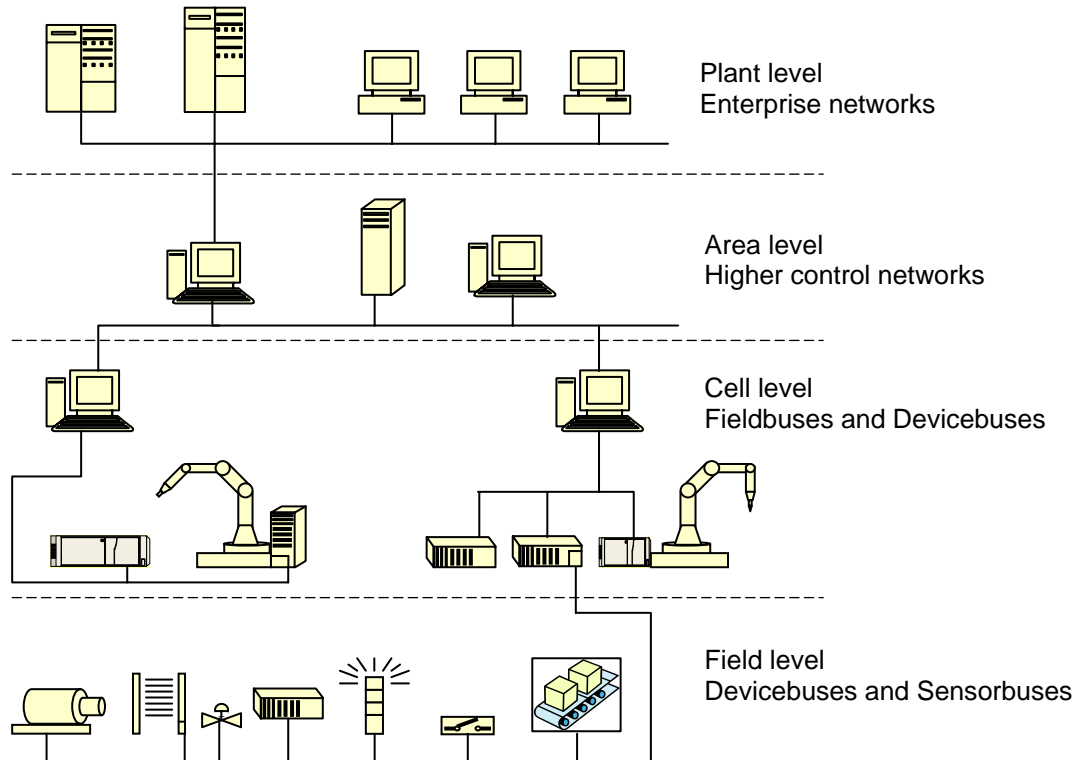


Fig. 1.1: Hierarchical communication architecture

The efficiency of the traditional fieldbuses was not sufficient for the fastest applications and many discussions used to be held if Ethernet was the right solution for a data exchange under deterministic conditions; the new developments like the switch technology enabling collision free star topology predestine the Ethernet as a network for hard real-time communication [2]. As a hardware technology Ethernet addresses nearly all requirements of the specialized industrial busses, with the advantages of widespread usage and lower cost due to high volumes [1]. Moreover standard Ethernet can be extended to achieve fast isochronous real-time communication, which is necessary for many networked motion control applications. These extensions at the link layer induce hard real-time deterministic performance by TDMA-like slots in such a manner that the industrial Ethernet not only suites even the most demanding real-time needs but even becomes the only standard option available.

The adoption of Ethernet at the process level enables simplification of the above described complex heterogeneous network hierarchy as it significantly reduces the overall heterogeneity.

2 Communication Architecture in Automation

2.1 State of the Art

The automation applications range from very simple systems that consist of a few interconnected devices (e.g. single manufacturing cell) to complex systems consisting of thousand of interconnected devices (building automation applications in large commercial buildings). For this reason there has been developed a broad range of communication standards and technologies that suite different application.

Architecture of each fieldbus has been optimized for specific range of applications with respect to limitations induced by properties of the used physical layer. During the process of selection of a fieldbus for a given application a set of technical criteria has to be observed. One of the most important parameter is the topology of the fieldbus.

Linear Bus Topology – with linear bus topology there are defined maximum length of the bus, maximum stub lengths and minimum distances between neighbouring nodes. Often the bus length can be extended by use of repeaters; however, the number of concatenated repeaters is always limited. Often the bus has to be terminated on one or both ends to prevent reflections. The requirement to have a single bus with stubs of limited length limits flexibility of the wiring. In automation applications the wiring is in most cases given by physical construction of the automated device or automated system and thus cannot be adapted to the properties of the bus. Although the bus lengths of most fieldbuses are in the order of hundreds of meters, sometimes it is not sufficient even for applications located in a single production hall or within a single production line as the stub lengths are limited to the order of few meters. The bus itself has to be wired to the proximity of each of the networked devices. For this reason often multiple fieldbus segments have to be used within one system. Most of the traditional fieldbuses use this topology.

Star Topology – Star topology is a topology with a central interconnecting element, where each network node is directly connected to the interconnecting element with a dedicated communication link. The central interconnecting element is in most cases an active networking element. In principle this topology allows more freedom when routing the wires as there is nothing like the limited stub length, the major limitation is the cable length between the central element and each of the nodes. Repeater can be used to extend this length; the maximum “distance” between two farthest nodes depends on media access method used. The major disadvantages of the star topology is the possibly higher length of cables used when compared with the linear bus topology (due to the dedicated cables to each node) and the presence of the central element, which presents possible single point of failure. The star topology is the most common topology for industrial Ethernet applications; there are industrial grade or even redundant hubs and switches available in the industrial Ethernet market today.

Tree (Multistar) Topology is an enhancement of the star topology where the central elements of different stars are interconnected. Ethernet allows for such interconnection.

Mixed topology - with networks that allow multiple physical layers below common higher layers it is often possible to combine different segments into a mixed topology, where linear bus and stars or trees can be combined. Mixed topology Ethernet networks existed in the past in the office environment, where linear bus and star (tree) topologies were combined.

Ring topology is a network where each node is connected to two other nodes so as to create a ring. The major advantage of a ring is possible very high speed bottleneck-free architecture; the major disadvantage is difficult ring management leading to high complexity of networked devices. Very attractive feature of the ring topology is the possibility to create double ring with full redundancy of the bus.

Free topology – some physical layers allow for undefined topology, where the only limitation is total length of the cable (capacitance of the cable). This is one of the most attractive topologies for automation, however very few physical layers allows for such topology. Moreover, such topologies impose low bit rates (usually below 200 kb/s).

Mesh topology is a topology in which devices are connected with many redundant interconnections between network nodes, in an ideal case each node is connected to every other node in the network with direct connection. With wired systems such topology is more theoretical than practical; however, with wireless systems this topology is very attractive as it provides high reliability due to redundant paths existing in the mesh. Advanced routing algorithms have to be used to fully take advantages of the mesh.

Other important technical parameters other than topology are:

Cycle time and network bandwidth – both has to suit the intended application. Standard IT networks are often designed to meet the average requirements, however for industrial applications the network traffic is often in bursts of messages and the network for control purposes has to be able to handle these bursts gracefully. Moreover during system faults and failures the peak network loads appear; the communication network has to handle these peaks without disturbing the real-time properties to minimize losses by well controlled shutdown of the systems affected by failures. Guaranteed time slots, prioritized messaging or other means of guaranteeing real-time performance even under the most severe network conditions are highly desirable for use with automation systems.

Address range – Traditional fieldbuses had very limited address space; the number of nodes allowed on the fieldbus was in the order of tens. Such limitation usually arose from the electrical properties of the bus – the maximum number of devices connected to a single bus segment was limited by the total impedance of the network, which is to be driven by each of the bus drivers. Applications that needed more network nodes had to consist of more than one bus segments. Such more complex topologies required implementation of network layer capable of structured addressing and/or routing. To bypass the need of routing such applications have often consisted of separated (both physically and logically) fieldbuses that were connected to either a common control system or to control devices connected to common high level control network thus forming hierarchical networked control structure.

Most of the traditional fieldbuses do not implement a network layer at all. Even most industrial Ethernet solutions do not define for real-time communication any network layer and the real-time domain has to be a single network segment where no routing across segments is possible. The few industrial networks with defined real-time network layer and capable of message routing have been deployed in applications where the time constants of the controlled systems were in the order of seconds if not minutes. However, in the past years there has been increasing demand for more complex networks and networked systems as the various process networks are used not only for direct process control, but for purposes like quality control, quality assurance, statistical process control, e-Kanban, lean production etc., i.e. applications that need both complex data acquisition across the process as well as optimization of the processes across the plant. Traditionally the interconnection of various fieldbuses was done using gateways (for hierarchical interconnection) or the data acquired from various fieldbuses were gathered at the area level (MES) or plant (ERP) level using technologies like NetDDE and OPC. However such high-level interconnection is relatively slow. In any case interconnection of heterogeneous systems sometimes led to interoperability issues.

External access to the plant was performed in most cases by either at the MES/ERP level using TCP/IP connection without any real-time requirements or by dedicated phone line (i.e. modem connection) where the authorized external person connected directly to a device using modem and utilizing RS-232/RS-485 interface directly on the particular device. WAN based real-time access to the process was not at all a standardized solution.

2.2 VAN Enhancement

VAN will enable interoperable interconnection of various fieldbus systems including wireless systems, thus enabling mixed topology systems with guaranteed real-time performance. Moreover the VAN aims to enable hard real-time interconnection of multiple LANs based on IP addressing, which will enable both hard-real-time applications deployed across multiple LANs (LAN segments, IP subnets)

as well as more complex functional safety applications. Both of these are not possible with today's state of the art technologies. Another VAN enhancement will be inclusion of WAN based access to the process level with the defined possibility to utilize QoS based connection for assuring scaleable real-time over the WAN. This will enable remote debugging, commissioning and even (preventive) maintenance thus significantly reducing costs of unplanned shut-downs, which is extremely important especially in "just-in time" productions found in the automotive industry.

3 Wireless in Automation

Wireless technologies in general are not developed with automation application requirements in mind and consequently the focus is shifted more towards developing wireless devices for bigger markets such as the home and office.

Application areas for wireless technology in industry have a wide range of requirements and subsequently require more than one wireless technology solution. Therefore, in industrial wireless there are systems with different functionality as well as different parameters and interfaces.

One of the first (general) VAN enhancements will be to enable one single access point in order to access process and management data from different wireless technologies.

Secondly, due to the vast application areas for industrial wireless communications and because of the numerous characteristics of the different radio solutions, there are various possibilities of integrating these technologies to the overall network (e.g. direct connection, proxy connection) within the VAN framework.

The technologies within the wireless industrial communications field applicable for automation are outlined next with respect to the state-of-the-art, limitations and VAN enhancements.

3.1 State of the Art

3.1.1 Bluetooth

The current Bluetooth standard is V2.0 (Enhanced Data Rate (EDR)) with a potential data rate of 3Mbps. The next version of Bluetooth (with the first core known as Lisbon, and the second Seattle) is aiming primarily to increase security as well as usability.

One of these attributes of Lisbon includes simple pairing, which aims to simplify the pairing process from a user perspective and to improve the security.

The Seattle core will aim to adopt UWB technology (the WiMedia Alliance Multi-Band Orthogonal Frequency Division Multiplexing (MB-OFDM) version) to improve the data rate – potentially up to 480Mbit/s.

Current limitations include:

- Slow network start-up delays
- Restricted complexity for network topologies and number of active devices
- No dedicated industrial profile

3.1.2 UWB

UWB can enable new applications as well as enable enhancements for existing technologies. As an example, future versions of Bluetooth aim to use the MB-OFDM version of UWB. UWB's primary feature is its high data rates at low power due the large bandwidth employed.

- As a consequence of this, one of the limitations is the effective low range, which is typically less than 10 meters.
- Another very important limitation from the automation perspective is the lack of a single global standard.
- Furthermore UWB is not yet available worldwide and consequently you have to deal with different local regulations (standards of regulation bodies)

3.1.3 WLAN

WLAN is a relatively mature technology and most of its impact can be seen in the home and office. There are various (current and developing) sub-standards within the 802.11 standard that address specific issues regarding security, performance enhancement and commissioning and management issues. From the perspective of industrial automation, the rapid evolving standards within WLAN could be seen as a concern to industrial automation vendors due to support for longer product life cycles. However, the 802.11 standards organizing bodies continue to ensure maximal interoperability amongst the various sub-standards.

- A primary concern of WLAN for industrial automation communications is security. However, the 802.11i task group aims to address these security issues but for industrial automation, network security will always be an area of concern.
- Additionally, WLAN mobile applications in industrial automation suffer due to poor battery life performance and WLAN points for industrial automation in general will be mains powered.

3.1.4 ZigBee

The market for ZigBee in general is still very immature and even more so from the perspective of industrial automation. ZigBee shows much promise (low power, low cost and dense mesh networking capabilities) for wireless sensor networking applications.

However, the limitations of ZigBee for industrial automation include:

- Low data rate (250Kbps) which could be restrictive for certain applications
- The lack of an industrial automation profile
- Single channel operation only (which additionally, can only be changed by the ZigBee coordinator)
- Reduced mobility because in a mesh topology the ZigBee network expects 100% duty cycle from the routers which means the routers should ideally be mains power
- No beacon mode for mesh networks
- Remote updates (e.g. access to change and read remote node MIB attributes) not supported by ZigBee and must be implemented at the application layer.

3.2 VAN Enhancement

In general, VAN enhancements could facilitate the integration of homogenous and heterogeneous wireless networks and could improve the effective range and redundancy of the network. VAN could additionally facilitate effective diagnostics of various wireless systems using a single engineering client. Possible VAN enhancements for specifically chosen wireless technologies are introduced below.

3.2.1 Bluetooth

- Enable more complex Bluetooth network topologies by joining multiple Bluetooth networks together
- Facilitate the interoperability of various versions of Bluetooth across various networks
- Select appropriate application profile for industrial automation applications or even develop a proposal for a suitable profile

3.2.2 UWB

- Due to the lack of a single global UWB standard, VAN could be used for convergence opportunities by bridging divides that could exist from the standards disparity.

3.2.3 WLAN

- Extend range and merge different standards of WLAN networks

3.2.4 ZigBee

- Provide a bridge between different ZigBee networks (as well as other networks e.g. proprietary wireless networks).
- Facilitate the integration of different types of homogenous networks e.g. combine a beacon-enabled star network (where low latency requirements are important) to a mesh network (where reliability and redundancy is more important) together using VAN solutions.
- Develop a proposal for a suitable automation profile.

4 Real-time in Automation

This chapter considers updates and new developments important for real-time communication compared to Version 1 of this document. The first part gives an overview about changes within the last month in real-time communication.

4.1 State-of the art

4.1.1 Latest technologies for real-time in automation

One surprise at the Hanover Fair 2006 was the introduction of a new Ethernet-based fieldbus – Varan. Another surprise at the Hanover Fair 2006 was the introduction to the automation audience of two new non-Ethernet based actor sensor buses – I/O Link and Componet. As primal intention in both cases the development of a low-cost alternative resp. complementary I/O bus to existing Ethernet fieldbuses with a comparatively low data transmission volume, was given.

The future has to show, whether this intention will give the “right to exist” for these buses for a longer period of time and not only as a short-term solution for the reuse of existing cable installations. Because the experience shows that the standard Ethernet components (COTS) are subject to a permanent price declining and by this also Ethernet based fieldbuses are expected to participate from this, but costs of Ethernet ports still seems not to be acceptable at the low-cost sensor actor level.

In the following the 3 new protocols will be shortly described.

Furthermore the new 10 Gigabit IEEE standard 802.3an will be discussed.

VARAN

As a successor of the DIAS-Bus a new fieldbus communication system called VARAN - Versatile Automation Random Access) developed by the Austrian company Sigmatec was presented on HMI 2006. This Ethernet based bus system - the physical layer is compatible with IEEE802.3 - was developed for machine automation applications. It is a non-proprietary, wired data network technology for LAN'S and also supports the use of TCP/IP. The address allocation is realized via the bus. The master – slave bus system can administrate more than 30,000 participants. The structure of this system can be built up in a mixture of star-, line- or tree topology. The synchronization of all bus participants is covered by the bus manager. Ethernet cross traffic is also possible and is realized by the bus manager in free time slots. Important features of this system are:

- The protocol is totally solved as hardware solution. Implementation will be with FPGAs, ASICS are not necessary but a possible option.
- Needs special network components.
- All important sent messages get verified and repeated within the same bus cycle if a failure during transmission occurs.
- Jitter less 100 nanoseconds and data transfer rates less 2 μ s for a 16 Bit value. One data access is restricted on a length of maximum 128 Byte.
- All received messages are confirmed by the receiver.

It was announced that this technology will be completely laid open. In July 2006 the VARAN-Bus-user organization (abbr. VNO) was founded. Scope of this organization is a fast penetration of the market.

IO-Link

IO-Link is a newly defined standard which specifies the communication between actuators/sensors and I/O devices. It was defined by a working group under the roof of PNO (Profinet User Organisation). With it the last meter to actuators/sensors is realized via serial point-to-point connection with standard sensor actuator cables. The interface is oriented on IEC 60947-5-2. Different communication modes are defined. The non cyclic mode can be used for parameter data e.g. for the start-up phase. For the transfer of process and service data a cyclic mode with typical 2 Byte input and 2 Byte output data and maximum 32 Byte input/output data is defined. The time behaviour in this mode is deterministic with cycle times of 2ms at 16 Bit of process data. There is also a cyclic switch mode where actuators/sensors can be connected classically (no communication but switching signals). First prototypes for PROFINET, PROFIBUS and Interbus will be presented at SPS/IPC/Drives in 2006. First products will be available in spring 2007. At the moment the specification is finalized and the standardization with IEC is in progress.

CompoNet

The ODVA published in April 2006 a new actuator-sensor concept called "CompoNet" formerly known as "Project CipnetSA". This new member of the CIP network was developed for special applications with low end sensors and actuators. CompoNet allows an efficient and rapidly bit and byte data transfer using implicit (I/O) messaging in a time slot technology. The focus of this technology lies on high speed communication between master controller and its connected slaves. A single master controls the network and supports a maximum of 256 bit slaves I/O (128 input nodes/128 output nodes) and 128 word slave I/O (64 input nodes/64 output nodes). The ODVA published the first edition of CompoNet™ Specification on August 21st 2006.

IEEE 802.3x

For real-time communication the kind of used wires and possible transmission speed are an important factor. Fast Ethernet connections (100Base-T) with 100 Mbps are meanwhile wide spread and standard on factory floors. 1000Base-T specified in IEEE 802.3ab with a 1Gbit/s connection is typically used in backbone systems. But the advancement goes on. The IEEE institute with its working groups specifies actually a new standard called IEEE802.3an, in which - the 10GBase-T group standardized a 10Gbit Ethernet technology for unshielded twisted pair wiring. On June 8, 2006, the IEEE Standards Association (IEEE-SA) Standards Board approved IEEE P802.3an. But at the moment the standard is not steady and thus not ready yet for the use in automation branch.

Further research groups still working on enhancements which are of interest for real-time communication in automation. Such a group is the 802.3ap – Ethernet Backplane group. Increasing numbers of plug in cards within switching or routing chassis also lead to an increasing variety of manufacturer solutions for the backplane connection, from this the target of the group derives to define a compatible, standardized and inexpensive manufacturer-spanning backplane solution – based on Ethernet. Within the group two types of 10Gbit/s interfaces are defined: (10GBASE-KX4 and 10GBASE-KXR; (release is scheduled for September 2006).

The 10GBase-LRM group works on a 10Gbit/s- Ethernet specification for classic multimode fibre.

The advantage of a faster connection seems clear: a typically used 100 Mbps network needs about 120µs to transmit the maximum Ethernet frame size of 1522 bytes. With a 10 Gbps network it takes only 1.2 µs [IAONA]. So, the transmission speed will be increased and thus is unlikely to become the bottleneck for future real-time applications.

4.2 VAN enhancements

The following table is taken from deliverable D04.2-1 and shows up the existing and non-existing real-time (RT) solution fields with the deducted VAN activities (yellow marked fields).

Table 4.1 : Real-time Communication Grid [D04.2-1]

		Type of Communication (Industrial)		
		Non-RT	RT	IRT
Communication Space	LAN	- Required: Yes - Exists: Yes - Example: all Ethernet fieldbuses - Utilization: engineering, parametrisation, web & OPC servers	- Required: Yes - Exists: Yes - Example: Profinet IO, Powerlink - Utilization: cyclic process data, signalling, alarms	- Required: Yes - Exists: Yes - Example: Profinet IO (IRT), Sercos III - Utilization: motion control, high-speed applications
	Inter-LAN	- Required: Yes - Exists: Yes - Example: Profinet CBA, etc. - Utilization: parametrisation, SW update, MES, Recipes	- Required: Yes - Exists: No - Example: Profinet (RT over UDP) - Utilization: resource reservation, cell synchronisation, alarm handling	- Required: No - Exists: No
	WAN	- Required: Yes - Exists: Yes - Example: Profinet CBA, etc. - Utilization: remote monitoring, telecontrol, telepresence	- Required: Yes - Exists: No - Example: Profinet (RT over UDP), MPLS - Utilization: vast applications with fast spreading media, alarm handling	- Required: No - Exists: No

According to the table above VAN will provide enhancements in following fields of real-time communication:

- VAN will develop solutions for real-time communication over inter LAN and WAN connections. Real-time over Inter LAN and WAN networks is a new concept. VAN will use two approaches to realize this concept.
 - The first approach is real-time communication over Inter- LAN and WAN networks with RT over UDP. The advantage of this approach is the use of the routable UDP/IP protocol.
 - The second approach for real-time communication over Inter- LAN, WAN and public networks is the use of a private VPN tunnel. An established VPN Tunnel can also be used to transport layer 2 protocols and thus enables the integration of existing real-time communication technologies which are using layer 2 addressing and are not routable by themselves.
- Another enhancement developed by VAN will be a solution for telecontrol within the VAN architecture. This solution will fulfil the special requirements for real-time communication which are needed for telecontrol. Such requirements are:
 - non permanent RT-communication connections together with
 - an according local data logging with time-stamping and
 - alarm handling.

Benefits of VAN solution

With the VAN enhancements for real-time following benefits will be achieved. A common solution for all required communication types in automation (see Table 4.1) will be provided. Unlike other approaches the VAN RT solution will be part of an all-embracing concept which provides scalable real-time, safety and security strategies.

5 Safety in Automation

5.1 State of the Art

Safety applications are very conservative from the technology point of view. The clear reason is that no risk at all shall be taken in order to guarantee the safe operation of a plant, a machine or any other technical system. Therefore only very reliable and well known technologies are used in safety relevant applications. That is why until now most of the safety applications for automation systems are still parallel wired using relay based control. Thus, a typical automation system consists of IO devices connected via a fieldbus with a PLC and a separate parallel wired safety system.

But, implementing the safety system in such a manner is very cost intensive. Therefore manufacturer of automation systems were forced to investigate in the serial transmission of safety data via fieldbuses. Hereby the main requirement is to use the same wire (serial bus system) as for the transmission of non-safe standard data. All of the fieldbus systems now offer this functionality and the first applications based on this new automation philosophy have been installed. From the view of safety this is state-of-the-art.

Wireless communication systems are increasingly used in industrial applications. Mobile applications can save significantly costs and allow high flexibility in the plant design. The systems available today are sufficient stable for the transport of standard (non-safe) data. However, the communication layers have not been developed for usage in safety application. Therefore, only proprietary wireless solutions for safety application exist today.

5.2 Organization of Safety Measures

The task of safety technology in general is minimizing the risk of hazards. On basis of a risk analyses the developer of a plant has to find the right mixture of technical and organizational measures for error avoidance, error detection and error handling. The more technical measures are integrated in the safety system the less organizational measure are required. But the more complex the technology is the higher is the risk of failures.

Therefore a safety application needs to be accepted by:

- the technical and maintenance staff
- the financial department
- and mainly by the certification and test institutes

The first to points indicate that a company needs to agree on technique and costs of the solution chosen. This is of course valid for most of industrial application. But for safety applications it is very crucial that the institutes give their approval. Otherwise, it is allowed to start.

5.3 VAN Enhancements

The state-of-the art of safety applications contains many points for improvements. Herein lays the motivation for VAN. This section lists some possible enhancements for safety application which might be created within the VAN project.

5.3.1 Safety specification for open networks

In the focus of the VAN-project is the safety relevant communication and not the safety control units, safety device, etc. The serial communication of safety relevant signals is nowadays accepted in so

called closed networks. These are the fieldbuses with safety extensions, e.g. PROFIsafe or INTERBUS Safety. The advantage of a closed system is the possibility to define the borders and limits of a system and to proof and test the complete system. For example the INTERBUS Safety system is proved on so called basic sample plant with the maximum of connectable devices of 126.

In the emerging industrial Ethernet solutions the systems are not closed any more. The automation and IT communication networks are connected to each other. Therefore an access from the Internet directly to an Ethernet field device is possible, if the network configuration (IP router settings, etc.) allows this. This leads to new safety requirements for the communication networks, new error reasons arise, new error avoidance measures are necessary.

Most of the Fieldbus organizations are meeting this challenge currently and defining or modifying the safety layers. But, there are still open issues regarding true open networks. For example, the evaluation report of the certification institutes on the new PROFIsafe V2 does exclude the cyclic data exchange over IP router.

VAN should investigate in this open issue and find out solutions. Having solutions would be a huge benefit for the customer for the design of automation applications based on industrial Ethernet.

5.3.2 Interoperability of existing safety networks

As mentioned already, different fieldbuses were developed for different purposes regarding speed, size of data transmitted, inter-device distance, etc. These fieldbuses are not compatible to each other although they are standardized in IEC-61158. Of course, also the safety fieldbuses are incompatible. Unfortunately, the same is valid for industrial Ethernet communication networks. This leads to difficulties in the design of the plant's architecture, because different communication networks are normally used.

In VAN solutions should be investigated to create solutions for establishing the interconnectivity between different safety networks.

5.3.3 Wireless Safety solutions

Within the VAN project open wireless solution for safety applications should be investigated. This would give industrial application a higher degree of flexibility saving costs and installation time. Safe data via a wireless connection can be transported as part of the communication network or from the sensor/actor to an IO module.

6 Security

6.1 State of the Art

The implementation of open Ethernet standards in the plant network as well as the availability to connect to the Internet and remote access has increased the potential for attacks into the plant. There is the potential for an attack from the outside as well as the inside. Outside attacks are usually considered deliberate with intent to harm whereas an inside attack can be deliberate or the consequence of human error.

When dealing with network security, there are two concurrent defense approaches used in the IT world – “Hard Perimeter” and “Defense in Depth”. The hard-perimeter approach focuses on an impenetrable “wall” around the system, the wall is in most cases represented by a single security point (e.g. firewall), which separates the trusted and distrusted network segments. Despite the simplicity this approach faces problems like single point of failure (failure of a single security device is compromising the whole secured network segment) and inability to prevent attacks from inside of the trusted segment. On the other hand the defense-in-depth approach replaces the single security point by a multi-level security philosophy, which is applied across the whole network in a form of multiple security zones with varying security policies [Tange05]. Some of the currently installed security mechanisms and solutions used in the automation industry include the use of passwords to restrict access to devices and applications. Firewalls are used to separate the automation network in protected cells as well as a demarcation point between the plant and the office network. VPN technology is used as a standard for remote access to a network as well to secure data communication between two or more automation cells.

The above mentioned technologies have been successfully implemented in a typical IT network. This does not always translate into immediate success for the plant network. The plant network requires above all high availability and low latency, whereas the office network can be sustained with limited availability and high latency.

Traditionally the security in the fieldbuses (e.g. IEC 61158) has been considered only in terms of access protection on some objects and devices. Primary goal of such protection was not protection against intentional misuse of the communication facilities and networked devices [ChH04]. The security measures were there to prevent accidental erroneous use by trusted users as well as to protect device configuration, device parameters, application data and application software from incompetent interventions by device operators. The communication at the field level was quite often not connected to the outside networks. If it was connected to the outside (e.g. to the office LAN), it was protected by a single security point, i.e. simple “hard perimeter” approach was used. However the figure below, which provides a snapshot of attacks that occur from the outside or inside in both Europe and North America, shows the need and the importance of “defense-in-depth” approach.

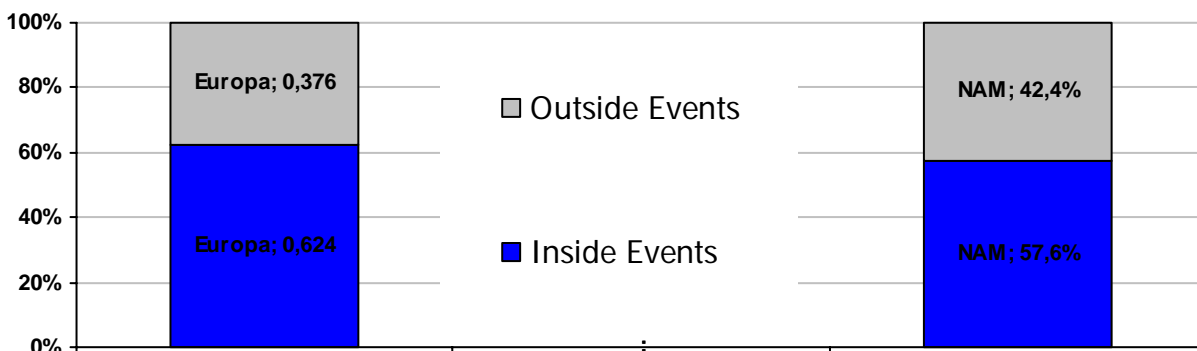


Fig. 6.1: Hierarchical communication architecture

The majority of the recorded attacks were “Inside events”, i.e. events where the simple and traditional “hard-perimeter” approach is useless (study performed by Consultic Marketing & Industrieberatung GmbH, Germany). Moreover as distributed manufacturing applications become more and more diverse, complex, integrated and interconnected into other kinds applications and communication systems, possibility of both internal and external attacks to the security of the networks increase as well [ChH04].

6.2 VAN Enhancement

The implementation of current security technologies such as Intrusion prevention or intrusion detection is an area of interest for the plant network as well as Network Access Control (NAC) technology. The implementation of NAC is an extra layer of security where user access and device access is compared to an existing set of policies to ensure that both user and device are current with regards to a device being up to date with patches and virus software. If the device is deemed not to be up to date then it is quarantined until it reaches the level set forward by the established policies. Such “defense-in-depth” approach used throughout the VAN will bring significant security enhancement to the plant floor.

7 Summary

The traditional fieldbuses (usually based on RS-485 or CAN buses) with limited data rates became bottlenecks for the fastest applications as the speed of automation devices has been constantly improving. On the other hand the recent developments of the Ethernet enabled to use Ethernet based networks for hard real-time communication. Isochronous extensions enabled to use these networks even in motion control applications, which require fast truly isochronous real-time data exchange. For both technical and economical reasons the Ethernet and its industrial variants become popular choice for both office and the plant floor. However the hard-real-time communication based on Ethernet is limited to single LAN operation.

VAN is taking the full advantage of recent industrial Ethernet developments; moreover VAN aims to enable hard real-time interconnection of multiple LANs, which will enable both hard-real-time applications deployed across multiple LANs as well as more complex safety applications. Both of these are not possible with today's state of the art technologies. Another VAN enhancement will be definition of scaleable real-time connections, which aims to enable access to the process level using WAN connections with defined QoS characteristics. This will enable remote debugging, commissioning and even (preventive) maintenance thus significantly reducing costs of unplanned shut-downs. This feature will be attractive especially for just-in-time productions found in automotive and other industries, where the production relies on broad range of subcontractors.

With the VAN enhancements for real time a homogeneous solution for all required communication types in automation (see Table 4.1, pg. 16) will be available. Unlike to other approaches, the VAN solution will be part of all-embracing concept providing scalable real-time, safety and security strategies.

Another important aim of VAN is the integration of homogenous and heterogeneous wireless networks into the common VAN architecture – this could improve both the effective range and redundancy of the industrial control networks and also enable new, more flexible solutions.

All the intended aims of VAN will be complemented with matching security architecture based on “defence-in-depth approach”, which will bring significant security enhancement to the plant floor. Such in-depth security approach is necessary as the recent surveys show that more that 50% of all security incidents are inside events, where the “hard-perimeter approach” fails.

Glossary

CIP	- Common Industrial Protocol
EDR	- Enhanced Data Rate
IP	- Internet Protocol
IRT	- Isochronous Real-Time
LAN	- Local Area Network
MB-OFDM	- Multi-Band Orthogonal Frequency Division Multiplexing
NAC	- Network Access Control
NC	- Numerical Control
PLC	- Programmable Logic Controller
QoS	- Quality of Services
TDMA	- Time Division Multiple Access
UDP	- User Datagram Protocol
UWB	- Ultra Wide Band
VPN	- Virtual Private Network
WAN	- Wide Area Network
WLAN	- Wireless LAN

References

- [ChH04] M. L. Chavez and F.R. Henriquez, SDL Specification of a Security Architecture for WorldFIP, Proceedings of the 14th International Conference on Electronics, Communications and Computers, IEEE Computer Society, ISBN 0-7695-2074-X, 2000 , available from <http://csdl.computer.org/dl/proceedings/conielecomp/2004/2074/00/20740149.pdf>
- [CISCO] <http://www.cisco.com/global/DE/verticals> (2006-08-22)
- [IAONA] Iaona Handbook 3rd Edition; Version 1.3, published 26th 2005
- [LeBlanc00] C. LeBlanc, The Future of Industrial Networking and Connectivity, Dedicated Systems Magazine, Issue on Networks, 1Q of 2000, pp. 9 - 11.
- [ODVA] <http://www.odva.org/index.htm>
- [Petig00] M. Petig, The way to distributed PLCs, Dedicated Systems Magazine, Issue on Instrumentation & Automation, 2Q of 2000, pp. 30 - 32.
- [PROS] <http://www.technikreport.at/produktion/automatisierung-mechatronik/produkte-systeme-anwendungen/schnelle-reaktionszeiten-mit-profisafe/1293> (2006-08-22)
- [Tange05] M. Tangermann, The IAONA Handbook for Network Security, version 1.3, Industrial Automation Open Networking Alliance e.V. pp. 21-22, Germany, 2005