



VAN

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

Virtual Automation Networks

Work Package 7

Cooperation of private and public networks

Task 7.1

Status and Analysis

Deliverable D07.1-1

Report on analysed public network
technologies

Document type	: Report
Document version	: Draft
Document Preparation Date	: 17.07.2006
Classification	: WP7 internal
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
1.0	Initial version	ifak	17.07.2006
1.1	Revision concerning board level review results	ifak	04.09.2006
1.2	update regarding review report	ifak	09.01.2007

Final approval	Name	Partner
Review Task Level	Lutz Rauchhaupt	ifak
Review WP Level	Thomas Werner	ifak
Review Board Level	Axel Klostermeyer	Siemens

Executive summary

The objective of Workpackage 7 is to investigate, identify, and develop feasible combinations of mixed private and public communication solutions as the VAN overall networking concept. Furthermore, new aspects arising with the expected utilisation of a heterogeneous network infrastructure shall be addressed which go far beyond the state of the art. In particular, on the fly switching of used infrastructure networks e.g. between best matching wireless technologies or on the fly switching of the service provider without interfering manufacturing or process control is a demanding challenge.

Within the first Task 7.1 "Status and Analysis" public network solutions and telematic systems currently implemented have been analysed in detail. Furthermore, the deficiencies of these basic technologies concerning the VAN requirements have been worked out and as conclusion new enhancements have been identified.

The current document represents the report on analysed public network technologies. The basis of the analysis is the description of requirements of wide distributed automation applications in chapter 1. This chapter starts with short descriptions of three characteristic use cases which require data communication via public networks. The systematic analysis of these use cases resulted in a number of attributes which characterise wide distributed automation applications. These attributes are used to assess the different technologies which are described in chapters 3 - 5. The technologies are grouped in Wireless Technologies (chapters 3), Wired Technologies and Routing (chapters 4) and Telematic Systems (chapters 5). In chapter 6 deficiencies and required enhancements of the described technologies are summarised.

This document is the result of a close cooperation of following project partners: SIEMENS AG, ifak Magdeburg (ifak), Teleport Sachsen-Anhalt GmbH (TSA) and University of Magdeburg, Center Verteilte Systeme (CVS).

Due to professional experiences and orientations of the participating partners, the main editorial competency of the respective chapters was given to SIEMENS AG (Requirements on Wide Area Networks), TSA (Service Level Agreement, Wired Technologies and Routing), ifak (Wireless technologies), CVS (Telematic Systems).

The document structure and compilation was performed by ifak.

Contents

Executive summary	3
Contents	4
List of figures	6
1 Requirements on Wide Area Networks	7
1.1 Use case description	7
1.1.1 Utility application	7
1.1.2 Maintenance of manufacturing application	7
1.1.3 Logistic application	10
1.2 Requirement Summary	11
1.3 Attributes of wide distributed applications	12
2 Service Level Agreement	15
2.1 Motivation	15
2.2 Service classes	16
2.3 Method of measurement	16
2.4 Typical quantitative values	17
2.5 Management	18
3 Wireless technologies	19
3.1 General Packet Radio Service (GPRS)	19
3.2 Universal Mobile Telecommunications System (UMTS)	21
3.3 Worldwide Interoperability for Microwave Access (WiMAX)	22
4 Wired technologies and routing	25
4.1 Analogue	25
4.2 ATM	25
4.3 DSL	26
4.4 ISDN	26
4.5 MPLS – Multiprotocol Label Switching	27
4.6 SDH	28
5 Telematic systems	29
5.1 General Terms	29
5.2 IEC - International Standard Protocols	30
5.2.1 IEC 61850 - Communication networks and systems in substations:	30
5.2.2 IEC 60870	30
5.2.3 TASE.2	31
5.3 Non IEC Standards/Protocols	31
5.3.1 Low level network protocols	31
5.3.2 Network communication standards	32
5.4 Wired Proprietary Protocols	32
5.4.1 RP 570/571	33
5.4.2 ADLP-80	33
5.4.3 ADLP-180	33
5.4.4 Sinaut 8FW	33
5.4.5 SEAB 1F	33
5.4.6 SEAB 1W	33
5.4.7 GEADAT 90	34
5.4.8 GEATRANS F 202	34
5.4.9 Harris-5000/5500/6000	34
5.4.10 CDC	34
5.4.11 SAT 1703	34

5.4.12	Telegyr 809.....	34
5.4.13	Indactic 23	34
5.4.14	Indicat 33/41	34
5.5	Wireless Protocols.....	35
5.5.1	VoWLAN - Voice over WLAN	35
5.5.2	GSM - Global System for Mobile Communications:.....	35
5.5.3	GPRS - General Packet Radio Service:.....	35
5.6	Selection of Telematic Systems	35
5.6.1	MicroSCADA	35
5.6.2	SINAUT ST7.....	35
5.6.3	digiCONTROL	36
5.6.4	Telecontrol Systems.....	36
5.6.5	PivoTrack™	36
5.6.6	ServiceFleet 3.0.....	36
5.6.7	AQASYS™ 5.2	36
6	Deficiencies and required enhancements	38
6.1	Wireless technologies	38
6.2	Wired technologies and routing.....	39
6.3	Telematic systems.....	39
7	Conclusions.....	41
	Glossary	43
	References	47

List of figures

Figure 1: Requirements on availability and reliability of wide area networks	15
Figure 2: GSM / GPRS Network Device	20
Figure 3: How WiMAX works	23
Figure 4: Schraml telecontrol system	37

1 Requirements on Wide Area Networks

The first chapter is related to the requirements of Wide Area Networks (WAN). This chapter starts with three use cases. These use cases describe three totally different areas where a WAN is used in an automation network. This includes a utility, a maintenance and a logistics application. Furthermore, requirements on use of WAN are identified and attributes are used to categorize the applications later on. The last subchapter defines metrics for service level agreements.

1.1 Use case description

1.1.1 Utility application

Utility applications monitor and control a number of widely distributed process stations to a limited amount of control centers or among one another via a wide area network.

The following requirements concerning the use of WAN shall be met (references in brackets to requirements summary in chapter 1.2):

- Provision of WAN service [RQ-7]
Adopt to the local existing WAN infrastructure, depending on environmental conditions (region, climatic influences, maintenance and service)
- Minimized system downtime [RQ-6]
Provider shall provide hotline and notification service (prescheduled WAN service measures) to minimize impact on utility application.
- Provision of appropriate WAN interfaces [RQ-8]
Stations need to provide appropriate WAN interfaces to connect to the WAN
- High level of availability of the control system [RQ-2]
Transmission of Data shall be secured against loss due to unavailable WAN service by appropriate means (buffering on local stations if the WAN connection fails, redundant transmission, etc.).
- Protection against unauthorized access (Data security) [RQ-5]
Security issues apply, unauthorized access to the system shall be inhibited.
- WAN use shall be optimized regarding cost [RQ-1]
- Data transmission shall be optimized regarding limited WAN bandwidth [RQ-4, RQ-11]
- Urgent data shall be transferred immediately for up-to-date data in the control centre [RQ-11]
- Reconfiguration during runtime [RQ-13]
It must always be possible to add new stations and to reorganize them and remove them at any time without impact on existing stations.

1.1.2 Maintenance of manufacturing application

The power of having information when you need it facilitates sound asset management decisions that add value to the top line, trim expenses, and reduce waste. The contribution to the bottom line is significant, making development of an asset information management network a sound investment. The resulting network that integrates and synchronizes the various maintenance and reliability applications to gather and deliver asset information where it is needed when it is needed is called e-maintenance, which is a subset of e-manufacturing, and e-business.

Industry has a growing set of smart industrial devices with embedded intelligence. Just like humans, they need online services (i.e., for condition monitoring, remote diagnostics, maintenance, etc.) It's the goal of the e-maintenance to answer this need.

On the other hand maintenance operations ceased to be a "necessary evil" and are currently considered as a part of a global EAO (Enterprise Asset Optimisation) policy implemented by a growing number of industrial organizations.

The general objective to support a global maintenance activities is to provide a platform, which would implement three main functions:

- Continuous assessment of Equipment health:
which consists in continuous remote monitoring of the system by the mean of a set of selected measurement & events, observed through their evolution
- Maintenance and Repair Operation process management:
this process groups logistic actions aiming at improvement of efficiency of field operations means of remote access to technical documentation and knowledge stores for maintenance agents, on-line usage of modeling packages, decision help tools and human experts
- Comprehensive data presentation and synthesis:
which involve direct information delivery to actors of both tactical and strategic operations (including supervisory and decision level, asset management panel and maintenance contract management).

According to [Pro03a] and in more detail information handled within overall maintenance processes are

- Management information
 - number and volume of orders; status of current orders; orders expected for the future
 - work hours and resources spent for an order
 - status of the budget; profitability of the maintenance activities
 - indications on customer satisfaction and availability of the maintained equipment
 - self-explaining functionalities –few hours training before first use
 - exact definitions for all types of information available on demand
 - up-to-date information in aggregated form, which is easy to read
- Information for contract management
 - information on customer: name of customer etc.
 - terms of the contract: price, period of execution, date of delivery to the customer, warranty
 - situation at the workshop during the period when the work order shall be executed and during the following weeks: which share of the resources has already been booked; what type of work will be done; who are the customers; what do they pay etc.
 - information when resources and spare parts are available in the workshop (information to be presented in graphical form or as tables)
- Information for project management
 - There also is a need for flexibility. It must be possible to launch a work order without having all necessary information and resources available.
- Diagnostic support
 - corrective maintenance: verification of error reports by customer and identification of the reasons of failures
 - preventive maintenance: each preventive maintenance intervention includes a systematic search for errors on a more or less detailed level
 - check lists adapted on the needs of the output devise
 - Diagnostic support for maintenance
 - context-related data from maintenance history, mainly for identification of the reasons of faults / errors if the reasons are not obvious
 - interactive manuals, based on manufacturer's documentation
 - functionalities of a retrieval tool for historic data
 - working with a set of predefined queries for different purposes,
 - loggings from condition monitoring systems and of error messages, both with context data; diagnostic reports; intervention reports

- interactive manual
 - display of the available documents in a list and direct access to them
 - alternative ways to access documents by index and by graphical interface
- Intervention support
 - By analyzing the types of information which are suitable to support interventions and also available in electronic form (or to be made available in electronic form), we see that it is similar to the information used for diagnostic support.
- Diagnostic report and intervention report
 - document maintenance interventions
 - diagnostic report
 - a predefined report structure (skeleton to fill with contents)
 - optional text modules, which can be completed by free text entries,
 - information coming from the work orders and the maintenance history,
 - guided dialogues where the operator has to answer by multiple choice
- Maintenance history
 - basic data describing the maintained equipment (only as far as interesting for maintenance)
 - all error reports from the customer
 - all error messages from condition monitoring, as well as aggregated measurement values, together with context data
 - diagnostic reports and intervention reports

As it can be seen this information can be spread within a plant or even distributed over different locations including use of VAN technologies. The following scenarios, as presented by the PROTEUS project results [Pro03a], are focused on the needs to access the information mentioned above through a common portal with the consequence that all information must be communicated through this portal independent from the underlying communication systems.

The main goal of the maintenance process is to provide the right resources at the right time for the right intervention. I.e. the maintenance operator must have the right tools, spare parts and maintenance script, for doing the intervention at a favourable moment, considering the production schedule and the maintenance schedule. All the infrastructure should help user to reach all the information he needs.

The maintenance area manager must keep an eye on the maintenance contract clauses. He has to check the value of the performance indicators imposed by the contract. One way of improvement is to help the maintenance area manager to follow these indicators. Through the portal the maintenance area manager should be able to manage all his resources, (i.e. spares parts, human resources, specific tools and lifting tools) to make his planning and schedule intervention.

The portal should allow user to be link with the SCADA system and provide an easy access to online info for each relevant equipment.

In the field of the spare parts management, user should be able to access to a tool which helps him to optimise the composition of stock, by taking account of the constraints imposed by the criticality of the equipment, the procurement lead times. Another prospect for improvement is the management of the spare parts by holding account of the stocks of store located in different geographical places.

The user should be able to access to the History of its plant and access to all the e-doc.

The operator can make use of streaming MPEG content about topics selected, leading to a form of on-site e-learning [Pro03a]. Video can also be up-streamed to provide distant experts or management with information.

Several technical constraints can be derived from scenarios and requirements presented [Pro03b]:

First the user constraints impose that the different actors (ERP, CMMS, ...) within a maintenance platform must communicate via a global networking facility such as Internet. Therefore widely used routing and transport layers must be used. Both co-operation models of application processes, Client-Server and Publisher-Subscriber should be supported to fit the scenarios.

As it also can be seen from the scenarios a broad range of bandwidth is needed (real-time data delivery to multimedia streaming). Timing related QoS are less critical than in control applications.

1.1.3 Logistic application

Logistic applications are mainly characterized by three attributes:

- the real time expectations are mainly focussed on the guarantee that a certain event happens at a predictable point in time while high speed communication is usually negligible
- they are often spread between multiple legal business entities, organized in a supply chain so every transaction has to be traceable and auditable
- as they often are related to material and information flows in any B2B scenario a monetary flow is also involved which raises an especially high standards in terms of security, in particular regarding authentication, authorization and normally also confidentiality

Logistic applications are - even if not in the central focus of VAN - notably well suited for public network communications. They usually span wide distances, are often involving mobile and hence wireless applications and are under pressure to cut costs constantly.

As obvious from the above for the intended use case we focus on the logistics between customer and supplier while the same attributes may also be true in internal logistic situations in a single enterprise.

Because of the commercial figures related to this area of business several organisations have been founded to address topics of interoperability and cooperation. One of those, the GS1 with its head quarter in Brussels, has especially addressed issues like

- GLN (Global Location Numbering),
- GTIN (Global Trade Identification Number),
- GRAI (Global Returnable Asset Identifier),
- GDSN Global Data Synchronization Network)

and similar aspects that are focussed on global harmonisation and interoperability of logistic systems.

The use case would normally imply an indirect communication as the ERP level is normally directly involved and the communication would pass the order management process.

Hence we care for the special just in time, periodic delivery based on an established contract. Material has to be delivered directly to the plant and progress information will be provided to the ERP system simultaneously. The supplier collects transfer related data via mobile links and provides them according to the service level agreement transparently to the customer.

It is expected that mobile communication allows for exact tracking of positions of the delivery system (truck), transfer of alert messages in the case of complications (truck breakdown) and access to carriage composition.

Important information items that have to be provided to the automation system include the projected real delivery time, availability from alternative delivery sources and material properties (concentration or temperature) in case of raw materials (as opposed to parts delivery).

Decisions for the production process which may be derived from this information flow are production speed control, priorities for different production lines, use of buffer reserves and escalation as a result of missing transmissions (short communication interruption due to tunnel travelling to loss of communication because of car crash).

The timing constrains are highly dependent on the transport distance, the dynamics of the particular production process and the projected damage in case of control mistakes.

Cycle times for the chosen example are about 10 minutes, the acceptable transmission delay has been fixed to less than 60 seconds.

The customer demands digitally signed data transmissions with a timestamp and generally encrypted transfers for confidentiality.

The transmission path is designed via mobile technologies from the transport vehicle to the suppliers premises and is being retransmitted in a controlled and documented way to the customer. The customer controls his processes without implicit feedback to the supplier, explicit information

containing demand changes, delay inquiries and planned maintenance schedules are provided in the same channel.

1.2 Requirement Summary

The following table summarizes the requirements of the use cases.

Table 1: Requirements on wide area networks

ID	Requirement
RQ-1	Reasonable cost for public connection
RQ-2	Level of availability of the network (medium, high) <ul style="list-style-type: none"> • Quality • Media redundancy • System redundancy (non-stop systems)
RQ-3	Transmission of realtime data
RQ-4	Reserved Bandwidth for transmission
RQ-5	Protection against unauthorized access (Data security)
RQ-6	Provider service (Hotline, Notification Service)
RQ-7	Independency of environmental conditions <ul style="list-style-type: none"> • Provision of service depending on Region/Area (rural areas, metropolitan areas) • Climatic influences (flooding, tidal flooding, heavy rainfall, snow fall) • Maintenance and service measures without impact on operation
RQ-8	Use of existing WAN interface
RQ-9	Well-defined responsibilities if WAN subnets belonging to different operators
RQ-10	Selective distribution of data <ul style="list-style-type: none"> • To one destination • To multiple or all destinations
RQ-11	Selective generation of data
RQ-12	Protection against data loss <ul style="list-style-type: none"> - packet loss - connection loss (partner not available)
RQ-13	Reconfiguration during runtime (dynamic adding / removing nodes)
RQ-14	Support of different data types
RQ-15	Support of data consistency
RQ-16	Interoperability between equipment from different vendors
RQ-17	Support of transmission of WEB-Services

ID	Requirement
RQ-18	Mobility
RQ-19	Availability where wired infrastructure not available

1.3 Attributes of wide distributed applications

General description of attributes derived from requirements. The numbering leaves gaps to make it easier to add further attributes.

ID	Subject	Reference
1	Fees/Models for calculating fees	
1.1	Fees according to number of connects and time units	RQ-1
1.2	Fees according to time units	RQ-1
1.3	Fees according to volume of data	RQ-1
1.4	Flat rate fees	RQ-1
1.5	Fees for options	RQ-2, RQ-3, RQ-4, RQ-5, RQ-6
20	Attributes of WAN interface	RQ-16 RQ-2 RQ-3 RQ-4 RQ-8
20.1	interface type:	
20.2	transmission speed	
20.3	Throughput	
20.4	transmission delay	
20.5	bit error rate	
20.6	Redundancy	
20.7	Security	
30	Redundancy	
30.1	No redundancy supported, single route (Data source → communication element (e.g. CP) → one data	RQ-2

ID	Subject	Reference
	route → communication element → data sink)	
30.2	Media redundancy: Multiple communication paths, single devices	RQ-2
30.3	System redundancy (multiple communication paths, multiple devices)	RQ-2
40	Distribution of data	RQ-10
40.1	1:1 relation (static or dynamic)	
40.2	1: n relation: The same information will be sent to n destinations: <ul style="list-style-type: none"> • Static or dynamic registration initiated by data destination or source • Acknowledged or unacknowledged 	
41	Generation of data	
41.1	The source specifies the transmission criterion uniformly for all destinations.	RQ-11
41.2	The source specifies the transmission criterion individually for each destination.	
41.3	Each registration specifies its transmission criterion individually.	
41.4	Event-oriented generation of data (at each value/information change, dependent on threshold settings or program controlled)	
41.5	Cyclic generation of data	
80	Criteria for Data Transfer	RQ-1
80.1	Directly linked to data generation	
80.2	Buffered data transfer (Conditionally, Time driven, Cost driven) <ul style="list-style-type: none"> • All data buffered (no data loss) • Only latest data is forwarded (data may be lost) 	RQ-10 RQ-12 RQ-13 RQ-15
110	Data Types	
110.1	Process data	RQ-14
110.1.1	Messages	
110.1.2	Commands	
110.1.3	Setpoints	
110.1.4	Parameters	

ID	Subject	Reference
110.1.5	Archive values	
110.2	<p>Organizational data</p> <p>Organizational data means all data required by a distributed system to allow the system to inform itself of the existence and status of its partners and to be able to control and monitor dynamic sequences.</p>	<p>RQ-2</p> <p>RQ-5</p> <p>RQ-6</p> <p>RQ-7</p> <p>RQ-10</p> <p>RQ-12</p> <p>RQ-13</p> <p>RQ-15</p>
110.3	<p>System data (upload, download, ...)</p> <p>System data includes all data necessary for system functions such as uploading and downloading, reconfiguring, diagnostics etc.</p>	RQ-13
110.4	<p>Picture data (camera)</p> <p>The extent to which picture data will be transferred in automation in future should be considered. The transfer of picture data may well be advantageous in widely distributed processes or when mobile process subscribers are involved.</p> <p>Example: Automation detects a fault: With the detection of default, a camera takes a picture and transfers this as an "attachment" to the event.</p>	RQ-14
110.5	Audio data	RQ-14

2 Service Level Agreement

As agreed in other deliverables and parts of this project there often is only a contractual basis in the guarantee of transmission attributes because no technical means can be taken when using heterogeneous, public and shared network paths. The major part of these contracts consists of the description of services that can be achieved for a given monetary scenario.

A Service Level Agreement (SLA) itself is a formal written agreement in the case of VAN made between two parties: The infrastructure provider and the client, usually responsible for an automation task via public networks. Generally, a SLA contains clauses that define a specified level of service, support options, sometimes incentive awards for service levels exceeded and usually penalty provisions for services not provided.

In the following we want to further describe the attributes that SLAs usually can define and typical quantitative limits. We here concentrate on IP based parameters because the VAN architecture is focussed on on IP.

2.1 Motivation

Few enterprises today question the need to manage their IT resources using service level agreements. And no wonder: as companies of all types increasingly rely on IT to meet their business goals, more are compelled to create SLAs which define in specific terms what an IT department or service provider is expected to deliver.

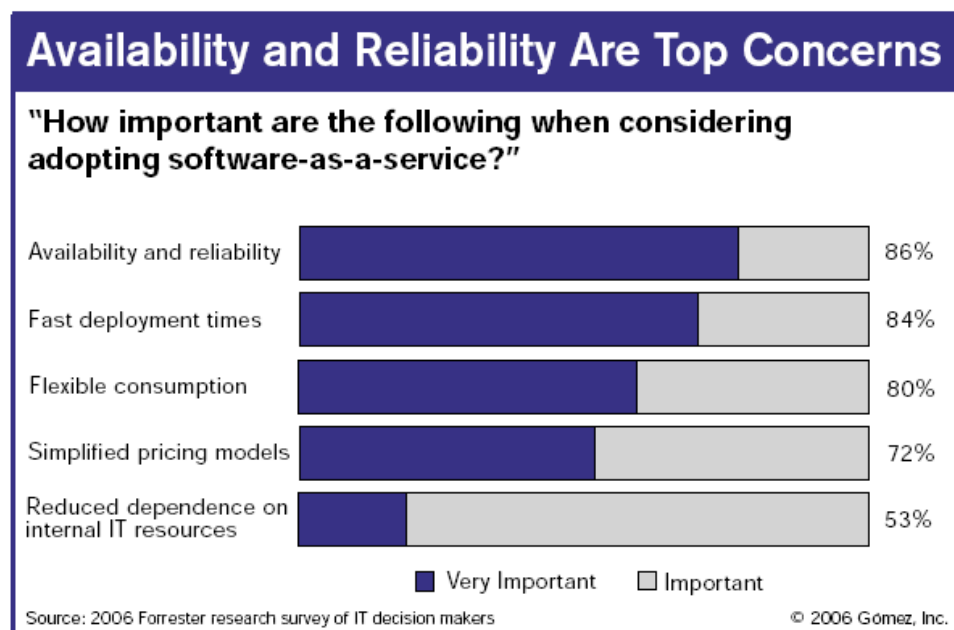


Figure 1: Requirements on availability and reliability of wide area networks

A good SLA addresses five key aspects:

- What the provider is promising.
- How the provider will deliver on those promises.
- Who will measure delivery, and how.
- What happens if the provider fails to deliver as promised.
- How the SLA will change over time.

While there are many potential benefits of creating SLAs, too many companies rush in to set them up and then fall short in their everyday management. Many fail to define and adhere to a standard monitoring approach to be used across the enterprise and, as a result, inadvertently prolong the frustration and fingerpointing among IT, line of business and third-party vendors. This is especially true in between IT and telecommunications and even more IT and automation.

Others neglect to measure their most critical business processes from the end device perspective, by far the metrics with the most relevance to service management. By not routinely tracking IT performance against valid automation system requirements, they continue to churn out SLA "reports" with limited rational value.

Because SLA monitoring can surface performance issues which otherwise go unnoticed, communication between IT and automation generally gets enhanced. Consider an aging IT infrastructure that's due for an upgrade. SLA metrics can objectively document a need for improvement, thereby smoothing the way for alignment of activities between office IT and automation management that otherwise might have been held out of context with the business. And with performance out in the open, companies can motivate their IT organizations and strategic third-parties to step up to mutually-defined performance targets and create better alignment between IT resources and automation requirements

The earliest SLAs were often one-sided and punitive and, like other forms of negative reinforcement, typically limited in effectiveness. But in today's more successful performance environments, neither party wants the other party to fail. Each stakeholder should be motivated and committed to the best business partnership for all. Building trust is an integral part of these relationships and both parties must understand each other's vision and objectives.

However, in the event of frequent breaches, operators of automation networks must be prepared to document and demand remuneration from the service provider and if the problem persists, to find a new provider. Several of today's top providers of content delivery networks and acceleration services are committed to guaranteed performance levels. Many edge out competitors in the pre- and post-sales process by demonstrating consistent and ongoing adherence to services levels where the need for a trusted third party measuring service is required

2.2 Service classes

Usually it is possible to buy different service classes which then allow the service provider to purchase more exclusive capacities. These classes also define some less technically relevant parameters such as access to second level support and a greater level of transparency concerning the progress in problem solving situations.

Typically these service classes are related to the purpose they are intended for or just provide several stages of link attributes. Stage classifications tend to be abstract terms like "Premium", "Platinum" or simply "advanced". As these wordings do not by themselves reveal the associated QoS no suggestion can be given here. Typical applicative classifications could be "Voice" (low jitter, variable bitrate, moderate throughput, moderate packet loss), "Crypto" channels (low bit error rate) or "Corporate" (high bandwidth, flatrate between locations, possible private transfer network).

In most cases one should carefully evaluate what is available in standard levels before investing effort into a specific set of parameters. Predefined sets of parameters are deployed throughout the whole infrastructure and mismatches when using alternative routing are less likely.

One goal of the VAN project should be to cause infrastructure service providers to create sophisticated service levels for the automation industry and especially for VAN. These could concentrate on the typical message size, individual priorities and predefined feature sets for backup lines. As these services are often consolidated from other suppliers as well, it is crucial for a process like this to make the service provider aware of the specific and sometimes unique requirements related to automation networks.

2.3 Method of measurement

IT, especially in an isolated automation environment, has traditionally gathered metrics based on the state of equipment located behind the firewall or on a network not connected at all. Unfortunately, this type of reporting cannot reliably measure the true state of a distributed automation application or network. For example, a measurement taken from an internal router may report greater than 99% availability, even when sensors on dialup connections cannot access the application at all. While basic data center monitors may indicate a company's homepage is live, service management may still be blind to any number of potential application problems that prevent communication partners from completing their intended goals, including middleware issues, service provider glitches or Internet backbone congestion that are all hiding behind that 99% figure. Unfortunately, a service

provider's own SLA reports may also mask the true health of an application via a public network. That's because many reports focus inappropriately on overly-specific technical aspects of application delivery rather on the actual end-to-end experience.

At provider side

The usual way in service provisioning is for the service provider to use the built-in functionalities provided by the technical components used for provisioning. These have counters for most of the events like repetition counters, FEC error counters and layer 2 problems.

Special consideration has to be given the information path when the service provider encounters problems providing the contracted parameters.

Depending on what has been defined in the specific SLA the reporting procedure for actual violations of QoS may include the proactive information towards the client about the fact and the measures taken. Otherwise an information is provided for the first level support to answer requests accordingly. The weakest but least expensive occurrence of service is only driven by customers reporting problems with the creation of tickets and repair attempts thereafter. This is only mentioned here but usually not acceptable in an automation application.

VAN measurement

The architecture of VAN and the underlying IP stack allows devices to measure the achieved QoS attributes end to end. In combination with the built-in communication options a VAN device could then report a violation of the expected parameters to enable the system to react accordingly.

The task to measure link parameters constantly will be especially important for the security infrastructure devices and VAN access points as they usually terminate connections between VAN domains or segments.

QoS dedicated agents

The detection of slow degradations in the service quality or the measurement of more complex quality profiles is very unlikely to be realised in a generic VAN device but should instead be implemented in a specific profile, which could be applied in gateways and infrastructure devices. Intended are SLAs based on metrics obtained from an independent monitoring source offering open visibility on how the SLA tests work. That's because when measurements are called into question, complete visibility is required as to what is being measured and how those measurements are being taken. These should come from VAN specific devices which could be analysed and even calibrated. This hardly would be possible with devices being part of the production process.

Fully documented and understood, SLAs backed by a credible source are more meaningful when shared internally between IT and automation or externally with service providers and partners. SLAs that are "black box" in nature - that is, provide little insight on the method behind the metric -- should be avoided at all cost.

Experience shows that most third party service providers will readily agree to correlate their own metrics with additional sources. Service providers and IT departments who are confident about their performance levels are typically receptive to the use of such independent measurements. In fact, market leading service providers are beginning to use SLA guarantees as a sales and marketing tactic.

One task for the VAN consortium or further advancing development activities should be to create functions for devices like VAN access points or security infrastructure devices to provide comparable and reliable metrics on given communication links.

2.4 Typical quantitative values

The following values have been taken from a service level contract offered by one of the largest providers in Germany, hence the special mentioning of Germany as a traffic source.

The measurements have been taken using a packet size of 100 Bytes and are one way data. They represent monthly average values. The individual measurements were conducted with 1000 packets in a bulk transfer.

Table 2: Typical quantitative values for packet loss

	Europe	USA	Japan
Germany	0,19%	0,19%	0,19%
Europe	0,04%	0,04%	0,04%
USA		0,04%	0,04%
Japan			0,04%

In the table above it is easily to be deduced that a loss-free link can not be achieved in public networks. High quality links are however comparable to LAN qualities and should be complemented with link protection measures usually implemented in VPN stacks.

It has to be mentioned that the values given here are already above average, the acceptable average packet loss for an MPLS link and basic availability in Germany for instance is 1.06%.

Table 3: Typical quantitative values for transmission delay

	Europe	USA	Japan
Germany	39 ms	108 ms	180 ms
Europe	24 ms	93 ms	165 ms
USA		45 ms	121 ms
Japan			6 ms

Transmission times in the table above which are less than ten milliseconds imply that a transfer technology is used that does not require the additional burden of fragmentation and reassembly and also recalculation of header field in every step of the transmission. This is on an IP based technology only achievable by the consequent migration to IPv6. The transmission times between end points in Japan for this carrier are most certainly applying the next generation internet protocol end to end.

Table 4: Typical quantitative values for jitter

	Europe	USA	Japan
Germany	22 ms	22 ms	22 ms
Europe	12 ms	12 ms	12 ms
USA		12 ms	12 ms
Japan			12 ms

2.5 Management

In general it is to be expected that an established service provider uses one of the common tools for SLA management. Typical applications suites in this context would be IBM Tivoli, Remedy, Managed Objects etc.

This is even more true in applications within automation environments.

Gartner research notes the greatest indirect cost associated with web application performance problems as the cost of finding, not resolving, the issue. Poor problem identification, an inability to quickly perform root-cause analysis to identify and isolate an issue, hampers the problem management process. Transparency of all known problems and the immediate availability to the trouble shooter is a crucial aspect in case of an emergency.

3 Wireless technologies

This chapter describes wireless wide area technologies most interesting for VAN. This includes the packet oriented communication (GPRS) via the current mobile phone standard GSM, UMTS the emerging technology of the 3rd generation mobile phone and WiMAX a wireless broadband technology under development. Direct communication via satellite or via trunked radio systems are not considered in this project.

3.1 General Packet Radio Service (GPRS)

GPRS is a packet data overlay onto existing GSM networks. As a global standard, it is expected to be widely deployed on GSM networks.

Usually, GPRS data are billed per kilobytes of information transmitted while circuit-switched data connections are billed per second. [GPRS01] For GPRS are different calculating models available. In principle you can choose between two models. Either you pay for the volume of data or you can use a flat rate. The fees for these presented models depend regionally on the Provider.

The theoretical limit for packet switched data is approximate 160.0 kbit/s (171 kbit/s). This limit can be only achieved when using 8 time slots and capability class 4. A realistic bit rate is 30–80 kbit/s, because it is possible to use max 4 time slots for downlink and 2 time slots for uplink. A change to the radio part of GPRS called EDGE allows higher bit rates of between 160 and 236.8 kbit/s. The maximum data rates are achieved only by allocation of more than one time slot in the TDMA frame. Also, the higher the data rate, the lower the error correction capability. Generally, the connection speed drops logarithmically with distance from the base station. This is not an issue in heavily populated areas with high cell density, but may become an issue in sparsely populated/rural areas.

GPRS offers difference data services (GSM):

- point to point for internetworking with the Internet (IP protocols) and X.25 networks
- point to multipoint for point-to-multipoint multicast and point-to-multipoint group calls

GPRS use the same nodes as GSM. At a high level, GSM is a mobile telephony network based on the cellular concept. Users can place and receive calls without being fixed to a specific location or wired to a physical connection. To supply this capability, a GSM network consists of three basic components:

- *Subscriber Terminal Devices* — Today, these devices are typically cell phones, but there are other devices such as personal digital assistants (PDAs) with various input/output capabilities. All have integrated radio transceivers.
- *Radio Base Station Network* — Cellular networks are composed of small, low-powered, terrestrial radio cells that typically range in coverage area from tens of kilometers in sparsely populated rural areas to less than 500 meters in densely populated urban areas. The frequencies used by the network are reused again and again in different cells throughout the network to increase network capacity.
- *Network Switching and Services Infrastructure*— The traffic to and from the radio network is concentrated at a set of switching nodes that interface to other fixed public or private networks. These nodes handle the call setup, channel resource allocation, and the administration of subscriber services. [GPRS02]

To efficiently handle packet data, GPRS adds two new components to the (GSM) network:

- the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). These nodes interact with the Home Location Register (HLR) node to obtain subscriber profile and authentication information.
- The SGSN is connected directly to the base station network and controls access, tracks user mobility, and implements various security functions. The GGSN is a gateway to external data networks and provides services such as authenticating external network access, quality of service (QoS), and tunnelling. External networks may include the Internet, private intranets, or legacy X.25 networks. The GGSN also supports roaming by routing incoming traffic to the appropriate SGSN where the user is located. [GPRS02]

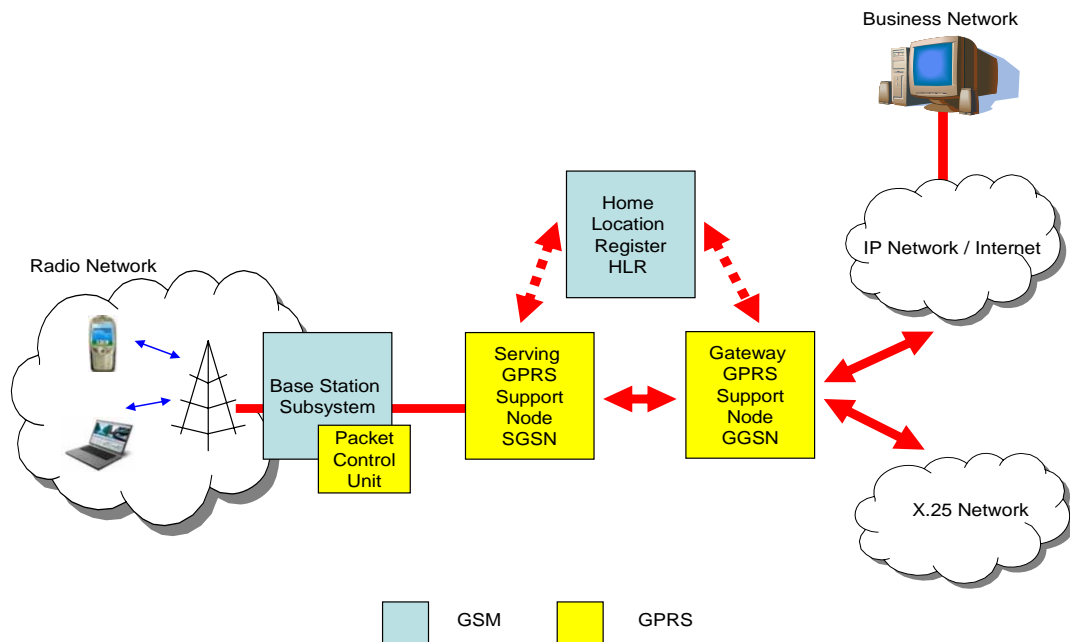


Figure 2: GSM / GPRS Network Device

GPRS and robust connectivity

GPRS improves data transmission integrity with a number of mechanisms. First, user data is encoded with redundancies that improve its resistance to adverse radio conditions. The amount of coding redundancy can be varied, depending on radio conditions. GPRS has defined four coding schemes—CS1 through CS4. Initially, only CS1 and CS2 will be supported, which allows approximately 9 and 13 Kbps in each time slot. If an error is detected in a frame received in the BSS, the frame may be repeatedly retransmitted until properly received before passing it on to the GPRS core network. [GPRS02]

GPRS and Security

GPRS builds on the proven authentication and security model used by GSM. At session initiation, a user is authenticated using secret information contained on a smart card called a Subscriber Identity Module (SIM). Authentication data is exchanged and validated with records stored in the HLR network node. GPRS enables additional authentication using protocols such as RADIUS before the subscriber is allowed access to the Internet or corporate data networks. GPRS supports the ciphering of user data across the wireless interface from the mobile terminal to the SGSN. In addition, higher-level, end-to-end VPN encryption may take place when a user connects to a private corporate network.

GPRS Applications

GPRS enables a variety of new and unique services to the mobile wireless subscriber. These mobile services have unique characteristics that provide enhanced value to customers. These characteristics include the following:

- **Mobility**—The ability to maintain constant voice and data communications while on the move
- **Immediacy**—Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session
- **Localization**—Allows subscribers to obtain information relevant to their current location

The combination of these characteristics provides a wide spectrum of possible applications that can be offered to mobile subscribers.

In general, applications can be separated into two high-level categories: corporate and consumer. These include:

- **Communications**—E-mail; fax; unified messaging; intranet/Internet access

- Value-added services—Information services
- E-commerce—Retail; ticket purchasing; banking; financial trading
- Location-based applications—Navigation; traffic conditions; airline/rail schedules; location finder
- Vertical applications—Freight delivery; fleet management; sales-force automation
- Advertising [GPRS03]

An advantage from GPRS is not the data throughput but the small response times (few milliseconds). [GPRS04]

In general GPRS supports all Data Types.

The devices have mostly a bit rate between 30–80 kbit/s, because it is possible to use max 4 time slots for downlink and 2 time slots for uplink. (not all 6 time slots at the same time). Usually the devices can only use 5 time slots at the same time.

Most of the Software GPRS-Modems for mobile telephones or PDAs run only with drivers for Windows. Driver for Linux, Mac or other OS are missing.

The external interfaces for GPRS devices (modems) are: USB, RS232, Compact Flash Slot, PCMCIA, Bluetooth, Ethernet.

3.2 Universal Mobile Telecommunications System (UMTS)

UMTS combines three important things. The W-CDMA air interface, GSM's Mobile Application Part (MAP) core and the GSM family of speech codecs. [UMTS01]

For UMTS are also different calculating models available like GPRS. In principle you can choose between two models. Either you pay for the volume of data or you can use a flat rate. The fees for these presented models depend regionally on the provider.

Like other real-world W-CDMA implementations, UMTS uses a pair of 5 MHz channels, one in the 1900 MHz range for uplink and one in the 2100 MHz range for downlink. A major difference of UMTS compared to GSM is the air interface forming Generic Radio Access Network (GRAN). It can be connected to various backbone networks like the Internet, ISDN, GSM or to a UMTS network. [UMTS01]

UMTS supports up to 1920 kbit/s data transfer rates, although at the moment users in the real networks can expect performance up to 384 kbit/s - in Japan upgrades to 3 Mbit/s are in preparation. [UMTS01]

Problems and issues with UMTS

Some of the rollout problems operators faced included:

- overweight handsets with poor battery life;
- problems with handover from UMTS to GSM, connections being dropped or handovers only possible in one direction (UMTS->GSM) with the handset only changing back to UMTS after hanging up, even if UMTS coverage returns;
- initially poor coverage due to the time it takes to build a network;
- for fully fledged UMTS incorporating Video on Demand features, one base station needs to be set up every 1000 – 1500 m. While this is economically feasible in urban areas, it is impossible in less populated suburban and rural areas;
- competition for broadband access from Wi-Fi;
- lack of significant consumer demand for 3G [UMTS01]

In general, applications can be separated into two high-level categories: corporate and consumer. These include:

- Communications—E-mail; fax; unified messaging; intranet/Internet access
- Audio and video telephony
- Value-added services—Information services

- E-commerce—Retail; ticket purchasing; banking; financial trading
- Location-based applications—Navigation; traffic conditions; airline/rail schedules; location finder
- Vertical applications—Freight delivery; fleet management; sales-force automation
- Advertising [UMTS01]

UMTS supports the same Data Types as GPRS.

The devices (modems) have mostly a bit rate of max. 384 kbit/s.

The external interfaces for UMTS devices (modems) are Compact Flash Slot, PCMCIA, Bluetooth, USB, Ethernet.

High Speed Downlink Packet Access (HSDPA)

HSDPA is one of the transfer methods of the UMTS standard. It allows downlink data rates of 1Mbit/s to a max. of 14.4Mbit/s (under laboratory terms). Therefore it enables the transmission of large data such as videos or games between the base station and the mobile device also combined with lower latency especially for VoIP service. This technology is based on an optimised scheduler (AMC – adaptive modulation and coding) within the base station that continuously and efficiently arranges the amount of data by the adaptation of channel coding and modulation method. The transmission time interval (TTI) is shortened to 2ms. The channel quality indicator (CQI) informs about the current channel quality and is input for the scheduler of the base station. HSDPA does not support soft handover between cells. If this technology is available by mobile telecommunication providers special fees for that service can be expected.

3.3 Worldwide Interoperability for Microwave Access (WiMAX)

WiMAX is a wireless technology that can connect IEEE 802.11 (Wi-Fi) hotspots with each other and to other parts of the Internet and provide a wireless alternative to cable and DSL for last mile broadband access. IEEE802.16 provides up to 50 km of linear service area range and allows connectivity between users without a direct line of sight. Note that this should not be taken to mean that users 50 km away without line of sight will have connectivity. Practical limits from real world tests seem to be around 5 to 8 kilometers. The technology has been claimed to provide shared data rates up to 70 Mbit/s, which, according to WiMAX proponents, is enough bandwidth to simultaneously support more than 60 businesses with T1-type connectivity and well over a thousand homes at 1Mbit/s DSL-level connectivity. Real world tests, however, show practical maximum data rates between 500kbit/s and 2 Mbit/s, depending on conditions at a given site. [WiOv01]

It is also anticipated that WiMAX will allow interpenetration for broadband service provision of VoIP, video, and Internet access—simultaneously. Most cable and traditional telephone companies are closely examining or actively trial-testing the potential of WiMAX for "last mile" connectivity. This should result in better pricepoints for both home and business customers as competition results from the elimination of the "captive" customer bases both telephone and cable networks traditionally enjoyed. Even in areas without preexisting physical cable or telephone networks, WiMAX could allow access between anyone within range of each other. Home units the size of a paperback book that provide both phone and network connection points are already available and easy to install. [WiOv01]

At this moment calculating models are not available, because WiMAX is in the test phase.

A WiMAX system consists of two parts:

- A WiMAX tower, similar in concept to a cell-phone tower - A single WiMAX tower can provide coverage to a very large area -- as big as 3,000 square miles (~8,000 square km).
- A WiMAX receiver - The receiver and antenna could be a small box or PCMCIA card, or they could be built into a laptop the way WiFi access is today.

A WiMAX tower station can connect directly to the Internet using a high-bandwidth, wired connection (for example, a T3 line). It can also connect to another WiMAX tower using a line-of-sight, microwave link. This connection to a second tower (often referred to as a backhaul), along with the ability of a

single tower to cover up to 3,000 square miles, is what allows WiMAX to provide coverage to remote rural areas. [WiOv02]

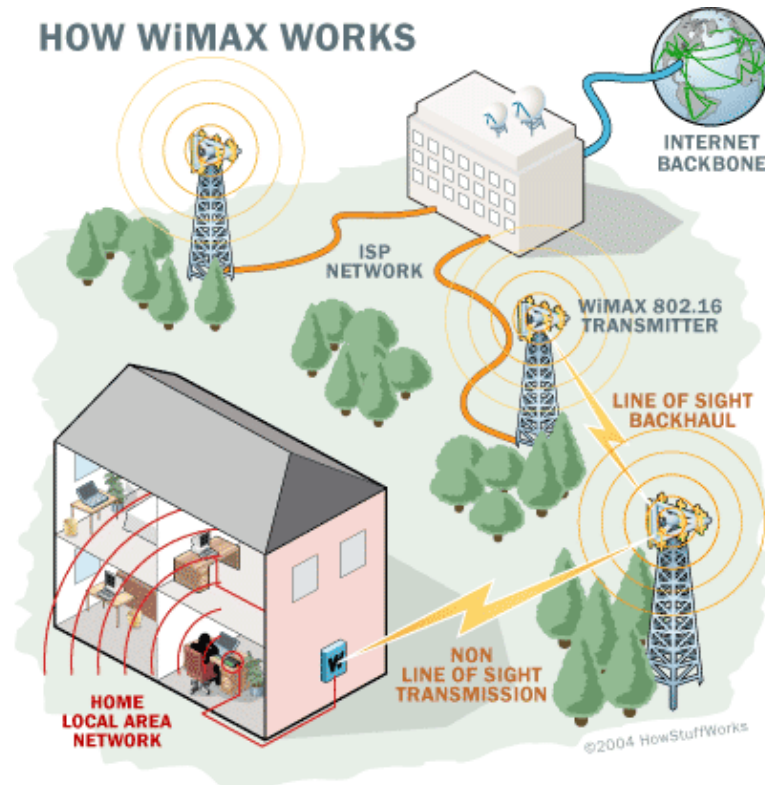


Figure 3: How WiMAX works

What this points out is that WiMAX actually can provide two forms of wireless service:

- There is the non-line-of-sight, WiFi sort of service, where a small antenna on your computer connects to the tower. In this mode, WiMAX uses a lower frequency range -- 2 GHz to 11 GHz (similar to WiFi). Lower-wavelength transmissions are not as easily disrupted by physical obstructions -- they are better able to diffract, or bend, around obstacles.
- There is line-of-sight service, where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. The line-of-sight connection is stronger and more stable, so it's able to send a lot of data with fewer errors. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz. At higher frequencies, there is less interference and lots more bandwidth.

WiFi-style access will be limited to a 4-to-6 mile radius (perhaps 25 square miles or 65 square km of coverage, which is similar in range to a cell-phone zone). Through the stronger line-of-sight antennas, the WiMAX transmitting station would send data to WiMAX-enabled computers or routers set up within the transmitter's 30-mile radius (2,800 square miles or 9,300 square km of coverage). This is what allows WiMAX to achieve its maximum range.

In general WiMAX should be support all Data Types (data, video, audio,).

Examples for topologies:

- can be used as a point to point
- cellular overlay technology

Beyond these metro area rollouts, WiMAX is like Wi-Fi in that you can "roll your own". Several vendors have some form of product, usually in a pre-standards-compliance stage so multivendor interoperability within a single network segment can't be reasonably expected. Several companies are planning rollouts of compliant chipsets in FPGAs and ASICs which will shrink the digital electronics suitable for PCMCIA and MiniPCI type of form factors. It is planned to embed WiMAX into the system processors and board architectures for laptop, PDA and other devices. The ability to embed multi-mode WiMAX/WiFi/cellular into consumer and IT products should create a compelling argument for WiMAX's acceptance. [WiOv01]

The introductions of WiMAX into mobile devices like PDA, Notebook, SDA, Mobil telephon is planned for 2006.

4 Wired technologies and routing

In this chapter the wired technologies most commonly used for public networks are described with the focus on how these technologies influence the behaviour of the transmission path. Usually a direct influence on the configuration and topology which the service provider applies is impossible but still projections are possible based on this information.

4.1 Analogue

The so called plain old telephony network (POTS) has been designed to transfer voice communication. This defines the frequency range that can be transported and additional services that can be offered.

Classic Telephony is circuit switched and so creates a completely electrically connected path from end to end of the communication line. This also means that this requested capacity is available exclusively during a phone session.

The secondary use of these lines for data transfer purposes has started in the 1950s in the US for military purposes (distributed air defence systems) and became widely available in the 60s. Transfer rates started at 300 Bit/second (Baud). The connection to the telephone network was established by acoustic coupling at the handset. Later on so called smart modems got directly connected to the physical lines and improved the options for bandwidth and signalling drastically.

The highest available transfer rates on an analogues modem are achieved now at 56Kbit/s, based on 64KBit for digital transmissions minus some overhead for in band signalling, which is realized in ISDN with the separate D channel.

Today the development of analogues modems has nearly stopped due to the wide availability of alternative access methods such as ISDN (the network of the telecommunication providers being fully digital today), DSL and cable modems. Analogue connections today are still the most widely deployed access connections in industrial countries but will become a less important solution for end users.

Typically the attribute of being circuit switched today is only a simulated behaviour to the customer, the transfer on the voice channels today is as data (sometimes already using Voice over IP) and is reconstructed at the switch that the communication partner is connected to. That is also the reason why additional modulation schemes can not be expected to yield high data transfer rates.

An analogues dialup connection imposes another disadvantage: Line setup takes 2 to 4 seconds which is mainly suitable for store and forward connections and adds a rarely acceptable delay for ad hoc transfer of data.

4.2 ATM

The cell switched asynchronous transfer mode ATM has been developed as a networking standard that uses the synchronous transport technologies (DSH, PDH) and extends them with additional features. ATM does not only support circuit switched transfer but also packet switched ones like IP and frame relay. Contrary to the robust and simple Ethernet (hence layer 2) or TCP/IP (layers 3 & 4) which react unpredictably under heavy loads ATM provides guarantees regarding effective bandwidth, delay and jitter and by that offers many quality of service attributes.

The task to combine multiple data streams of different types has been accomplished in converting both type of bit streams – synchronous and packet based – at the interface to a new stream carrying ATM cells of a constant size (53 Bytes). These cells then are for instance carried in the user data sections of SDH formatted data streams. Asynchronous in ATM means that sender and recipient may use different clock rates and the receiving party is responsible for re-clocking if required.

In its original concept ATM was considered the key technology for the broadband-ISDN which should provide the carrier backbone for the plain old telephony system. Hence ATM defines the complete layers 1 to 3 of the OSI reference model and implements many telecommunication specific technologies and conventions, due to telcos having been the strongest driver for the development of ATM.

Today ATM offers a wide range of support for applications in the telecommunication and internet backbones, is used as modulation schema in DSL modems and offers application specific transfers using ATM abstraction layers (AAL) without the need to deal with low level protocols.

ATM is being distributed, enhanced and standardized by the ATM forum.

Today ATM has lost some of its significance in favour of easier and cheaper deployable technologies such as MPLS, but still is heavily used in backbones, hidden from the awareness for the end user.

Typically it is rarely possible nor desirable to attach end user equipment to ATM networks directly. The technologies visible for customers are the classical Ethernet or E1/T1 connections. These then are connected to the opposite end point by establishing switched or permanent virtual circuits (SVC/PVC), which then allow to apply all necessary definitions, mainly related to QoS.

4.3 DSL

The basic structural difference between DSL and traditional data connections via telephone lines (POTS) or ISDN is that the actual DSL connection is not established between two end points but instead is established between the subscriber and the telecommunication switch unit. Coming from the DSL router of the subscriber the analogue DSL signal gets demodulated at the switching unit in so called DSLAM, digitized and transferred via a broadband backbone connection to a provider. Based on the higher transfer capacity in the backbone connection compared to a telephone channel in the subscriber line more bandwidth can be provided by better modulation schemes and the use of wider transfer frequency ranges.

One major drawback of ADSL (asymmetric product for private customers) is in the behaviour described above. Multiple subscriber lines are usually terminated at the switching unit and hence the upstream (direction from subscriber to the provider) has to follow a time consuming access control in order to avoid data destruction via collisions. In the case of SDSL these obstacles are removed in exchange for substantially higher costs mainly to cover the loss of overbooking capacity at the provider site.

The availability of DSL connections depends on copper structures to the end customer and the provided backbone structure which usually deployed depending on the customer/business potential in a given region.

The only flavour of DSL that is suitable for automation applications which require a defined timing behaviour is SDSL in association with a good SLA. Here Service levels starting from 99,7% are possible and managed services with 24/7 support are offered.

The use of cheap ADSL is limited to applications where the availability requirements allow the periodic interrupting by the service provider at night, varying transfer speeds are acceptable and repair works may take days.

4.4 ISDN

The integrated services digital network is an international standard for digital telecommunication networks. It was designed to transfer and mediate classical telco services such as Telex, Datex-L, Datex-L and of course voice. These service networks formerly existed separately with gateways where appropriate.

The end user experienced the introduction as a telephony standard providing additional features and higher bandwidth (two separate voice channels) and faster connecting and transferring internet access.

In principle ISDN is available in two connection setups: BRI (for the end user, two voice channels) or PRI (for connecting PaBX's with 30 voice channels).

The main feature that is interesting in the context of automation systems is that the B channels (the payload channel as opposed to the D channel which is solely used for signalling) are bit transparent and synchronous so that any line code can be transmitted. In order to increase the throughput channels can be bundled to a multiple (up to 30) of 64KBit/s which then requires the attached device to be able to keep these bundled B channels synchronized. The interesting feature is that in most cases a 2MBit connection is the end point of a channel in a synchronous digital hierarchy (SDH, see there) and hence provides the synchronous transfer end to end.

Due to the fact that ISDN based communication setups establish a (virtual) circuit switched connection a point to multipoint configuration is impossible or is implemented at one endpoint in a conference setup (which is not feasible for data communications as echo cancellation mechanisms destroy bit transparency). Hence for every communication path a separate connection has to be

established. If an ISDN channel is in the connected state and there is less traffic to be transferred than the channel bandwidth allows the surplus capacity is padded.

4.5 MPLS – Multiprotocol Label Switching

This network protocol is used for a fast forwarding of data packets between network nodes. It gives every packet a label with forwarding information in a very short form. So the MPLS routers don't analyse the normal header but just that label. These labels then are used as an index to find the new label and the target of the next hop for that packet in a table of the device. Once this structure is established, the routing with these labels is very fast. These techniques are applicable to any network layer protocol (that's why 'multiprotocol'), but mostly it is used in conjunction with IP network protocol.

MPLS in general has been explained in several deliverables, so we will concentrate here on the qualitative opportunities provided with MPLS rerouting and traffic engineering.

So, what is the difference in QoS to classical IP networks? Like ATM MPLS directs traffic solely based on a label assigned by the interface at the ingress point. A path through the MPLS network is called a Label Switched Path, or LSP. Traffic engineering and fast rerouting use the labelling capabilities in MPLS to create "tunnels" for creating alternative paths for IP traffic. The labels contain the information needed to guide data packets toward their destinations along the desired paths.

Normally, traffic on an IP network travels along the shortest path to a destination. This characteristic is very important to the scalability of the Internet since it permits routing to be largely an automatic process. However, the shortest path is not always the fastest path or the best one for that data. Traffic engineering provides a way for data to circumvent this rule. Traffic engineering allows data to be directed through a specific path-one that is more efficient but not necessarily the shortest. It allows network managers to implement traffic management policies to ensure optimal traffic distribution and improve overall network utilization, helping save money while improving performance. Customers like the automation industry can take advantage from having a basic knowledge about this when negotiating contracts.

Fast rerouting is a cousin to traffic engineering. It allows the network to direct traffic extremely quickly to a new route if a node or link fails. Rerouting is done fastest if it can be done locally-at the first point in the network where the failure is detected. This is because in wide-area networks the time to get notification of a failure halfway across a continent can significantly delay rerouting. Still it would be beneficial to request and demand these notifications from the infrastructure service provider for restructuring to avoid longer usage of expensive alternative paths.

With MPLS traffic engineering, rerouting can be done locally. At each node bypass tunnels are created to bypass links and adjacent nodes. When a link or node fails, traffic is directed along these bypass tunnels. This avoids longer interruptions of traffic connections. To illustrate the power of rerouting the fastest available rerouting algorithm – MPLS Fast Reroute - has been evaluated more carefully. It shows that it is possible to avoid packet loss totally with switchover times (experienced as additional packet jitter) between 1 and 100 ms. The most important disadvantage in this scenario however is, that packets might arrive at the egress of the MPLS link out of order. Additional means have to be established to accomplish this.

More generally one can think of traffic engineering and fast rerouting as exceptions to the rule of how IP networks route data. If these exceptions aren't carefully controlled, one also can create routing loops. The task was to find a way to integrate traffic engineering directly into the IP network's standard routing. The standard routing calculation (called Shortest Path First or SPF) was modified to take traffic-engineered tunnels into consideration and decide when (and when not) to route traffic over the tunnels. At the time of writing this deliverable technology to offer these link attributes is already widely available and deployed.

Traffic engineering enables more efficient packet transport and overall better quality of service (QoS), as well as maximizing network capacity. The development of traffic engineering and fast rerouting also offers a huge cost-savings to network operators. Previously, service providers had to run an ATM or Frame Relay network layered below their IP network to have traffic engineering and used SONET for fast reroute capabilities. Now with such features available directly in IP routers, service providers don't have to run these other infrastructures.

The QoS improvements and recovery times provided by MPLS allow service providers to offer a new type and quality for SLAs dedicated to specific target groups such as the automation industry.

[Source: RFC 3031]

4.6 SDH

SDH implements a synchronous time multiplex technique that provides a multiplex hierarchy similar to PDH. When developing SDH the goal was to make the best achievable usage of a fibre optical cable transfer capacity. Contrary to PDH the clock on single connection segments is kept synchronous in very narrow margins. PDH allows clock deviations of up to 50 ppm while SDH requires a more than ten times better accuracy. The basic principle is very simple: bit streams of a bit rate for R from n sources are combined via synchronous multiplex to a bit stream of a rate $n * R$.

Different to PDH an SDH system allows based on its totally synchronous behaviour to derive a multiplex signal directly from the multiplex signals of all underlying multiplex layers. The transfer of asynchronous data streams such as ATM or PDH is also possible (called cross connect) and unused bandwidth is then padded in order to keep frames rate and clock synchronised.

The following are the most common hierarchy levels.

Table 5: Bit rates of different SDH levels

Hierarchy level	Nominal bit rate	Bit rate payload	Bit rate overhead
STM-0	51,84 MBit/s	49,536 MBit/s	1,728 MBit/s
STM-1	155,52 MBit/s	148,608 MBit/s	5,184 MBit/s
STM-4	622,08 MBit/s	594,824 MBit/s	20,736 MBit/s
STM-16	2488,32 MBit/s	2377,728 MBit/s	82,944 MBit/s
STM-64	9953,28 MBit/s	9510,912 MBit/s	331,776 MBit/s

SDH reserves about 5% of the gross data rate for OAM (Operations, Administration and Maintenance).

SDH has been standardised by the ITU-T (.707, G.793, G.803) and has formerly been derived from Sonet, a system that has been developed by AT&T and others since 1985. The differences between Sonet and SDH nowadays are very small and both concepts are interoperable. As PDH has proven to be of limited use at bitrates beyond 100MBit/s SDH had been chosen as the primary transfer system for B-ISDN¹.

The simplified layer model for SDH can be described as follows.

Physical interface	Usually fibre but in principle also radio or even a satellite link
Regenerator section	Refresh of attenuated and disturbed signals in clock and amplitude
Multiplex section	Combine (plesiochronous and) synchronous signals to higher bitrate streams, inserting and extracting data streams (so called mapping)
Virtual container section	VC-4 for 140MBit/s stream (E4) insertions and extraction, VC-3 handles mapping of 34MBit/s and VC-12 is used when providing E1 access lines (2MBit/s)

The principal method of mapping common telecommunication bandwidth channels into a high capacity multiplex is applicable for data communications as well. Unfortunately capacities are then often spent in vain as for a 100MBit/s Ethernet IP link a 155MBit/s STM-1 Signal is required. The next generation SDH enhancements (such as VCA and LCAS, which are not further explained here) allow for a transmission of packet oriented data streams simultaneously with bit synchronous signals and newer recovery mechanisms (such as implemented in GMPLS) precalculate replacement paths dynamically in case they are needed.

The future of SDH is defined by multiservice platforms as a transfer layer of IP and Ethernet and in the same multiplexed data streams for packet and circuit switched services.

¹ B-ISDN was an approach for wideband ISDN but development and the expensive deployment stopped in favour of packet switched technologies following the markets demands.

5 Telematic systems

This chapter gives an overview of various protocols and standards involving within the field of telematic systems. The IEC standards are relevant for Europe and are mainly focused within the following chapter. Further global standards are available e.g. ISA, however they have similar characteristics.

5.1 General Terms

The term Telematic is derived from telecommunication and informatics (computer science). By this telematics describes interconnected information processing systems using telecommunication systems for their data exchange.

In automation telematics covers a wide range of methods and techniques to get remote access and control possibilities to industrial devices, machines and plants. The remote access is based on nowadays used communication technologies as telecommunication technologies and a steadily rising part of Internet technologies. General distinguished techniques of telematic are Telecontrol, Teleservice, and Teleengineering [Lang00].

Telecontrol

Telecontrol means the remote access to control and automation devices for monitoring and controlling of processes. This includes acquiring, transmitting and displaying of all necessary information. For this a telecontrol system is typically monitoring inputs/outputs signals in remote locations. Telecontrol systems are strongly influenced by electrical power supply networks but it is also important in gas- and water supply networks. Priority objective of telecontrol systems are economic monitoring and controlling of each single distributed component.

A classical layout for a telecontrol system is one central unit connected with different outstations via transmission lines. Both, central unit and outstations are equipped with sensors and actuators.

Another term sometimes used in the same meaning as telecontrol is telemetry – internationally called TEMEX (Telemetry Exchange). Telemetry focuses on remote controlled measurement, but also covers controlling and monitoring of technical systems via public telecommunication networks and is thus just another term for telecontrol

Teleservice

Teleservice covers the services of remote maintenance, diagnostics, failure handling and start-up of any distributed industrial or other automation system.

Teleengineering

Teleengineering is the geographical distributed development and engineering of the various parts of a complex industrial automation system. [KLUß01], [SCHU95],[AUD00],[TKIF01]

Further terms that have a close link with telematics are listed and described in the following:

VMI - Vehicle Management Information:

Vehicle Management Information or Fleet Management systems are systems for tracking the position, speed, travelled distance etc. of vehicles with GPS or any other similar system. This information are transmitted to and managed in a central system.

SCADA - Supervisory Control and Data Acquisition:

This term covers a broad range of system used in industrial and engineering applications to monitor and control distributed systems from a master location.

RTU – Remote Terminal Unit:

The Remote Terminal Unit connects a control system to physical equipment such as switches, pumps, and other devices and monitors and controls these devices. Today the differences between PLC and RTU vanish more and more.

5.2 IEC - International Standard Protocols

5.2.1 IEC 61850 - Communication networks and systems in substations:

IEC 61850 [IEC61850] is the most recent standard for communication networks and systems in substations. This standard describes the architecture of the cooperation and data transmission in a substation automation system (SAS). It defines the communication between Intelligent Electronic Devices (IEDs) in a substation and its related system requirements. It is a kind of successor of the IEC 60870-5 protocol. The data model in this standard is object oriented. It also introduces an XML-based language (Substation Configuration description Language - SCL) offering a vendor-independent method of describing devices and their configurations. This protocol is based on Manufacturing Messaging Specification (MMS). It defines the mapping to communication services for transmitting data using CSMA/CD (ISO/IEC 8802-3) over TCP. [IECN01], [IPSP01]

5.2.2 IEC 60870

The IEC 60870 is a series of signal orientated standards which applies to telecontrol systems and equipment for monitoring and control of remote and geographical distributed processes. These standards are getting obsolescent and will be removed by the above mentioned IEC 61850 standard.

These systems comprise all kind of equipment for acquisition, transmission and display the necessary process information. There are two main aspects which defines the efficiency of a telecontrol system:

- the integrity of the transmitted data
- the speed of the data transmission

These aspects are influenced by several factors like bandwidth, traffic load, transmission quality, coding and encryption schema, and computer power of communication node [IEC 60870-1].

The IEC 60870 consists of six parts. The parts one to four give a general introduction and describe the operation conditions, the interface structure and performance requirements, the actual transmission protocol standard is described in the parts five and six.

IEC 60870-1: General considerations:

This part gives an introduction to the general aspects and the general layout and specification of telecontrol systems.

IEC 60870-2: Operating conditions:

Specifies classes for environmental conditions under which telecontrol equipment has to operate.

IEC 60870-3: Interfaces (electrical characteristics):

Defines the interface conditions to be fulfilled when connecting together the various elements of equipment needed to constitute a telecontrol system and enabling the user to manage such a system.

IEC 60870-4: Performance requirements:

Deals with those characteristics which affect the performance of telecontrol systems and relates the characteristics to the application and processing functions. Establishes a set of rules to assess and specify the performance requirements of telecontrol systems; where feasible, performance classes have been specified for each of the properties covered.

IEC 60870-5: Transmission protocols:

Covers all aspects of the data transmission, like general transmission frame formats; coding, formatting and synchronizing of data frames; definition of link layer transmission procedures; the general structure of application data; rules for defining information elements; and a set of basic application functions (to reside beyond the application layer).

IEC 60870-5-101: The companion standard 60870-5-101 defines the data transmission with serial interfaces like V.24, V.28, X.24 or X.27.

IEC 60870-5-104: The companion standard 60870-5-104 combines 60870-5-101 with the TCP/IP transportation protocol.

IEC 60870-6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations:

It is a report to define the application context and the organisation of standards. It describes the standards and their functions within the OSI reference layers. It wants to create functional profiles of services. [IECN01]

5.2.3 TASE.2

The IEC standard TASE.2 (Telecontrol Application Service Element), also referred to as IEC 60870-6-503, enables the exchange of time-critical information between control systems via WAN and LAN. It is a very wide spread protocol supported by many telematic/telecontrol systems. TASE is identical to the ICCP protocol. ICCP stands for "Inter-Control Center Communications Protocol" and was defined by EPRI (Electric Power Research Institute). The standard TASE.2 was published by the IEC as an open standardised interface for process data communication. It was intended to network control stations. [IPSP01], [IEC60]

5.3 Non IEC Standards/Protocols

5.3.1 Low level network protocols

Low level protocols are protocols which always deal with "low-level", physical interaction of the hardware. In telecommunication branch, protocols that are allocated within this layer are used for communication control in a telecommunication network. This protocols use signals for controlling the communication. That's why it is called signaling.

Signaling refers to the exchange of information between call components required to provide and maintain service. Signaling protocols are process regulations to encode, decode and interpret control messages. Several protocols are arranged in so called layers (OSI 7 Layer Model) that serve to cover the different net requirements. Together they form a signalling system.

The IETF established a working group called Next Steps in Signaling (NSIS). This working group is responsible for standardizing an IP signaling protocol with QoS signaling as the first use case. This working group will concentrate on a two-layer signaling paradigm. The intention is to re-use, where appropriate, the protocol mechanisms of RSVP, while at the same time simplifying it and applying a more general signaling model. There are several protocols developed within this working group. [IETF01]

5.3.1.1 GIMPS - Generic Internet Messaging Protocol for Signaling

The Protocol was renamed in 2005 by the NSIS group to GIST (General Internet Signaling Transport).

5.3.1.2 GIST - General Internet Signaling Transport

The General Internet Signaling Transport (GIST) protocol is currently being developed at the IETF NSIS working group. It is the base protocol supporting a variety of signaling applications to be run on top of it. This protocol defines the stacks for the routing and transport of per-flow signaling messages along the path taken by that flow through the network. The solution uses existing transport and security protocols under a common messaging layer, the Generic Internet Signaling Protocol (GIST), which provides a universal service for diverse signaling applications. GIST does not handle signaling application state itself, but manages its own internal state and the configuration of the underlying transport and security protocols to enable the transfer of messages in both directions along the flow path. The combination of GIST and the lower layer protocols provides a solution for the base protocol component of the 'Next Steps in Signaling' framework.

This specification concentrates specifically on the case of "path-coupled" signaling, which involves network elements which are located on the path taken by a particular data flow, possibly including but not limited to the flow endpoints. GIST manages its own internal state and the configuration of the underlying transport and security protocols to ensure the transfer of signaling messages on behalf of signaling applications in both directions along the flow path. [IETF02]

The draft was developed within NSIS.

Note: This protocol changed name from former GIMPS to GIST (General Internet Signaling Transport) in 2005.

5.3.1.3 CASP - Cross-Application Signaling Protocol

CASP is a modular protocol for establishing network control state along a data path between two nodes communicating on the Internet. The signaling problem addressed by CASP is the same as the

overall problem being addressed by the NSIS activities. The CASP framework is defined as a modular protocol, which includes a general purpose messaging layer (M-layer), which supports a number of client layers for particular signalling applications. [IETF03]

This draft was developed within NSIS.

5.3.1.4 RSVP – Resource Reservation Protocol

The RSVP protocol is one of the most important signaling protocols within the internet protocol stack. This protocol describes the mechanism to reserve resources across a network for multicast or unicast data flow. So it can deliver a specific quality of service (QoS) along requested network paths. This can be rate-sensitive or delay-sensitive quality requirements. This kind of protocol is applied for networks with limited bandwidth or for real time data streams where dropouts can have serious consequence (e.g. robotic telemetry). The further development of RSVP is accomplished by the NSIS group. [RFC2205]

5.3.1.5 RTP-Realtime Transport Protocol

RTP is a real time transport protocol that provides an end-to-end network transport of real-time data, and multicast such as audio, video or simulation data, over multicast or unicast network services. RTP can run over ATM, IP and IPX. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery. RTP and RTCP are designed to be independent of the underlying transport and network layers.

5.3.2 Network communication standards

The basis for a telemetric system is the ability to transport the necessary data between all participating partners. There are several network communication standards

5.3.2.1 DNP3 – Distributed Network Protocol:

The development of DNP3 was a comprehensive effort to achieve open, standards-based interoperability between substation computers, RTUs (Remote Terminal Units), IEDs (Intelligent Electronic Devices) and master stations (except inter-master station communications). It is based on standards of the IEC (especially the 60870 series) but with additionally functionality. It can be used via serial communication but supports also TCP/IP based operation.

DNP 3.0 commands a very powerful application layer, which allows the decoding of data without the use of implicit parameters. It supports a variety of representation modes for information objects, offering a high degree of interoperability on the application layer. This was achieved at the cost of greater complexity, which makes implementation more difficult and demands much more time for implementation and testing. [IPSP01],[DNRP01]

This protocol was developed by Harris, but now it is under ownership of the DNP User Group.

5.3.2.2 SISA/QD2

'SISA' stands for 'Supervisory and Information System for local and remote Area' and refers to a communication network for controlling and monitoring telecommunication facilities such as SDH, PDH multiplexers. SISA/QD2 is hierarchically organized network dispatching information between network elements (NE) and corresponding operation systems (OS). Its physical interface is called QD2.

SISA/QD2 was standardized by the FTZ (German Telecommunication Engineering Authority, now ZZF) as per the FTZ standard N 13-5. [IPSP01]

5.4 Wired Proprietary Protocols

The following protocols are an assortment of proprietary protocols for communication of devices (mostly) from one special vendor. The application of vendor specific protocols is common in this field. Often they are developed before an international standard was agreed and, because of the long lifecycle of automation devices and techniques, are still in use, or these protocols are adaptations of existing standards to specific environments.

5.4.1 RP 570/571

The RP 570/571 protocol was developed by ABB at the beginning of the 1990's and enables the coupling of control stations and substations. IEC-TC57 (IEC 60870-5-1) is used for physical layer encoding. [IPSP01]

5.4.2 ADLP-80

The ADLP-80 was developed by ASEA (ABB) for communication between a SCADA system and RTUs. Its physical layer uses a specific PCM encoding type consisting of a 4-bit start code and one or more 14 or 19-bit words. ADLP-80 operates in half-duplex mode following the master/slave principle. A master can communicate with up to 15 RTUs, an RTU only responds to an explicit request from the master. [IPSP01]

5.4.3 ADLP-180

The ADLP-180 protocol was designed by ABB for communication between the SINDAC control system and COLLECTOR 100, 300 and 400 substations. It represents an upgrade from its predecessor ADLP-80. The difference to ADLP-80 is in the use of standard mode (UART compatible) for data encoding on the physical layer. [IPSP01]

5.4.4 Sinaut 8FW

The Sinaut 8FW protocol was up to the beginning of the 90's the standard protocol used by Siemens for coupling controls stations and substations before being replaced by IEC 60870-5-101 and later by SINAUT ST7 EthernetTCP/IP based system. There are several variants of this protocol in use:

- Sinaut 8FW PDM for physical layer encoding based on the PLM method (Pulse Length Modulation)
- Sinaut 8FW PCM for physical layer encoding based on the PCM method (Pulse Code Modulation) with start bit, data bits, parity and stop bit. This protocol variant used the FT1.2 telegram format standardized in the IEC TC57 (IEC 60870-5-1) protocol.
- Sinaut 8FW DUST follows the 3964R procedure on the physical layer mainly used in process automation (SPS).

In addition to those basic variants already mentioned, there are other versions which differ in their functional scope and telegram length. This is why the range of functions needs to be specified in each case. [IPSP01]

5.4.5 SEAB 1F

The SEAB 1F protocol (also known as Modnet 1F) developed by AEG enables the coupling of control station and substation belonging to the Geadat 120 product line. SEAB simply refers to the expression 'serial installation bus' which also describes a possible topology of this protocol based on half-duplex operation. In other words, up to 128 substations can be operated by one control station in party line mode. Also worth mentioning with respect to Seab 1F is that handshake signals normally employed in modem control are used to implement end of telegram recognition. These signals have to be controlled actively by the respective transmitting station, which demands highly accurate timing of these signals during communication. But the physical connection can still be realized via a normal RS232/V.24 interface, either directly or via a special designated AEG modem connection of the UEM201 type. This means that data can be exchanged via the telecommunications network, if the required automatic calling modules have been installed. [IPSP01]

The SEAB 1N deviate was developed to enable communication over Ethernet networks.

With the liquidation of AEG all its proprietary protocols are not longer enhanced.

5.4.6 SEAB 1W

The SEAB 1W protocol (also referred to as Modnet 1W) developed by AEG is primarily based on the widely known IEC 60870-5 standard using the FT1.2 format class for the link layer. It supports unbalanced data transmission (master/slave principle) and enables the coupling of several substations to a single line.

Only a small part of the full range of functions supplied by the IEC was implemented, and previously varying parameters, such as the number of address bytes, have now been clearly specified for the first time. Minor changes were made, for instance in the way time stamps are encoded. [IPSP01]

5.4.7 GEADAT 90

Developed by AEG, the GEADAT 90 protocol is based on the serial bus SEAB. Unlike SEAB, GEADAT 90 has been designed for point-to-point operation. It supports baud rates of up to 600 Baud. It has a limited function scope. [IPSP01]

5.4.8 GEATRANS F 202

Developed by AEG for communication between control stations and substations, the GEATRANS F202 protocol uses the PLM mode (Pulse Length Modulation) for data encoding. [IPSP01]

5.4.9 Harris-5000/5500/6000

Developed by Harris (GE Harris), Harris-5000/5500/6000 supports communication between a SCADA system and RTUs of the same denomination. It has been widely used in North America and comes in several variants. The main difference between these versions is the extended address range in Harris-6000. It operates in half-duplex mode based on the master/slave principle. One master can communicate with up to 63 RTUs, while each RTU only responds to explicit requests from the master. Harris-5000/5500/6000 does not support quality identifiers, transmission of time stamps is however possible. [IPSP01]

5.4.10 CDC

Developed by the EMPROS company, the CDC Type I protocol enables communication between control stations and RTU 44-500 or 44-550 substations. The physical layer operates in a proprietary PCM mode.

The CDC Type II protocol enables communication between control stations and RTU 8890 substations. The physical layer operates in a proprietary PCM mode with 42 and 122-bit words. [IPSP01]

5.4.11 SAT 1703

The SAT 1703 protocol was developed by the SAT company (VA TECH SAT) and enables the coupling of control stations and substations. The FT1.2 format as specified in the IEC 60870-5-1 (TC57) standard is used for the link and physical layers. [IPSP01]

5.4.12 Telegyr 809

Developed by the Landis & Gyr company, the telecontrol protocol Telegyr 809 enables the coupling of control stations to Telegyr 809 substations. The link and physical layers of this protocol use the FT1.2 format specified in the IEC 60870-5-1 standard. [IPSP01]

There are other proprietary Telegyr XYZ standards to connect to other Telegyr systems

5.4.13 Indactic 23

The Indactic 23 protocol was developed by ABB and is used to link up RTUs and control stations in the energy industry. Siemens, too, has developed compatible controller boards to enable connection of their own systems with ABB systems. The telegram frame of the protocol complies with DIN 19244, format class FT1.2 which also applies to the IEC870-5-101 protocol. In multi-point operation up to 254 substations can be connected. Indactic 23 always uses half duplex communication. [IPSP01]

5.4.14 Indicat 33/41

The Indactic 33/41 protocol was developed by the BBC company (ABB) at the beginning of the eighties. It found high resonance in the energy industry for the automation of transformer stations enabling the communication between a control station and several RTUs. It is often referred to as "Indactic 33", so it is easily confused with the Indactic 2033. Indactic 2033 is derived from Indactic 33/41.

Data transmission is based on the half duplex communication mode. The control station continuously sends synchronization signals even when there is no data ready to be dispatched. The RTUs on the other hand only respond to an explicit request from the control station. Up to 15 RTUs can be connected to a single communication line. Data is encoded in 16-bit words with 8-bit use data which together make up a telegram. [IPSP01]

5.5 Wireless Protocols

Detailed information of wireless protocols can be found in D01.1-1 and Deliverables of WP3.

5.5.1 VoWLAN - Voice over WLAN

VoWLAN (Voice over WLAN) is a method of sending voice information in digital form over a wireless broadband network. Essentially, VoWLAN is VoIP delivered through wireless technology. The technology is sometimes called "VoWi-Fi" or "Wi-Fi VoIP" because it uses the IEEE 802.11 set of specifications (informally known collectively as Wi-Fi) for transporting data over wireless local area networks and the Internet. Major barriers to VoWLAN include inconsistent voice performance and the need for quality of service (QoS); slow and unreliable encryption and authentication; and the proprietary nature of current products. [VoWL01]

5.5.2 GSM - Global System for Mobile Communications:

GSM is a standard for wireless communication to transport any kind of data. It is used mainly for mobile phones. Some telecontrol systems use GSM for remote communication. Details will be worked out in WP1 and WP3.

5.5.3 GPRS - General Packet Radio Service:

- GPRS is an extension of the GSM standard. It is used for a higher data transmission rate. Details will be worked out in WP1 and WP3.

5.6 Selection of Telematic Systems

5.6.1 MicroSCADA

ABB: MicroSCADA is a system for monitoring, local and remote control applications via LAN, or remotely on a portable workstation via a dial-up modem or a GSM mobile phone connection. It is suitable for electrical and non-electrical process applications.

MicroSCADA is a microcomputer-based, programmable and distributed supervisory control and data acquisition (SCADA) system. MicroSCADA runs on every commercially available PC-computer.

MicroSCADA is programmable because all application programs and most system configuration programs are built with SCIL (Supervisory Control Implementation Language). The control system can communicate with the widely distributed process through a communication system. The common platform technology, which MicroSCADA is based on, is used for building applications and systems.

MicroSCADA-based electrical application areas are power transmission and distribution. It is also well suited for other process areas. District heating, water purification and distribution, waste water treatment, oil and gas distribution can be mentioned as non-electrical application areas. The main MicroSCADA-based application systems are Substation Automation Systems for power transmission and distribution substations. There can also be Network Control and Distribution Management Systems for power distribution. [MSCP01]

5.6.2 SINAUT ST7

Siemens: SINAUT ST7: is an innovative and versatile system for fully-automatic monitoring and control of process stations that exchange data via WAN (Wide Area Network) with a control center or among one another (cross connection). Based on the SIMATIC S7 automation system with additional hardware and software, SINAUT ST7 encompasses matched hardware and software modules for WAN communication. The following industries are included in the main areas of application [TCSM01]:

- Water/waste water
- Oil and gas
- District heating
- Traffic engineering

- Mining

5.6.3 digiCONTROL

Hereschwerke: digiCONTROL, (also digiMATIC): The digiCONTROL system is a universal control and comprehensive telecontrol system in the environmental field. [TCDC01]

5.6.4 Telecontrol Systems

E.D.&A: Telecontrol Systems: Telecontrol Systems® fill the need for a mutual communication between systems. Via these Telecontrol Systems® one system gets in touch with another to transfer measured values and tasks. This happens automatically without any kind of human intervention. Devices can communicate wired and wireless (GMS) via the TeleController. (Use Cases: monitoring of vending machines, monitoring and registration of mobile machines as fork-lift trucks, refrigerated vehicles, monitoring of pumps, energy meters, tank and silo levels, real-time measurement of energy consumption a.s.o.). [TCSY01]

5.6.5 PivoTrack™

Tamtron Group: PivoTrack™ is a complete tracking system based on standard technologies (SMS, GPS and GSM) to track vehicles and even personnel. A location server named Nexus and its' database is the heart of this system. The server system communicates with GSM-GPS units, called Trackbox, who is needed to answer position requests from the server via SMS. The SMS contains precise position, the unit has retrieved from GPS-satellites. (Use case - railway company; monitoring waggons). [PTTS01]

5.6.6 ServiceFleet 3.0

Euro Telematik: The open architecture of ServiceFleet 3.0 is easy to integrate in an existing IT-infrastructure. Addicted to special needs, different modules can be implemented. The telematic basis (called ET FleetServer) allows a universal, digital communication between headquarters and vehicle or stationary terminals. [SFET01]

- The stationary terminals are connected with the telematic basis via LAN, WLAN or WAN. The implemented OTI (Open Telematik Interface) allows a standardized communication.
- The mobile elements are connected via WWAN or WLAN with the ET FleetServer. Different data services can be connected with the server.

The ET FleetServer uses a variety of software e.g. Oracle, MS-SQL, XML, IP, Mobile IP, GSM, GPRS, UMTS, GPS, Windows and .NET

5.6.7 AQASYS™ 5.2

Schraml: The AQASYS™ technic is a data based process control system for using in water supply systems and sewage plants. For data handling the Process server / Central device can communicate wired (serial/network) a wireless (GSM / WLAN IEEE802.11) with other applications. The remote control centre is used as data buffer store, for data handling, alerting, telediagnosis and as communication device. [ASRS01]

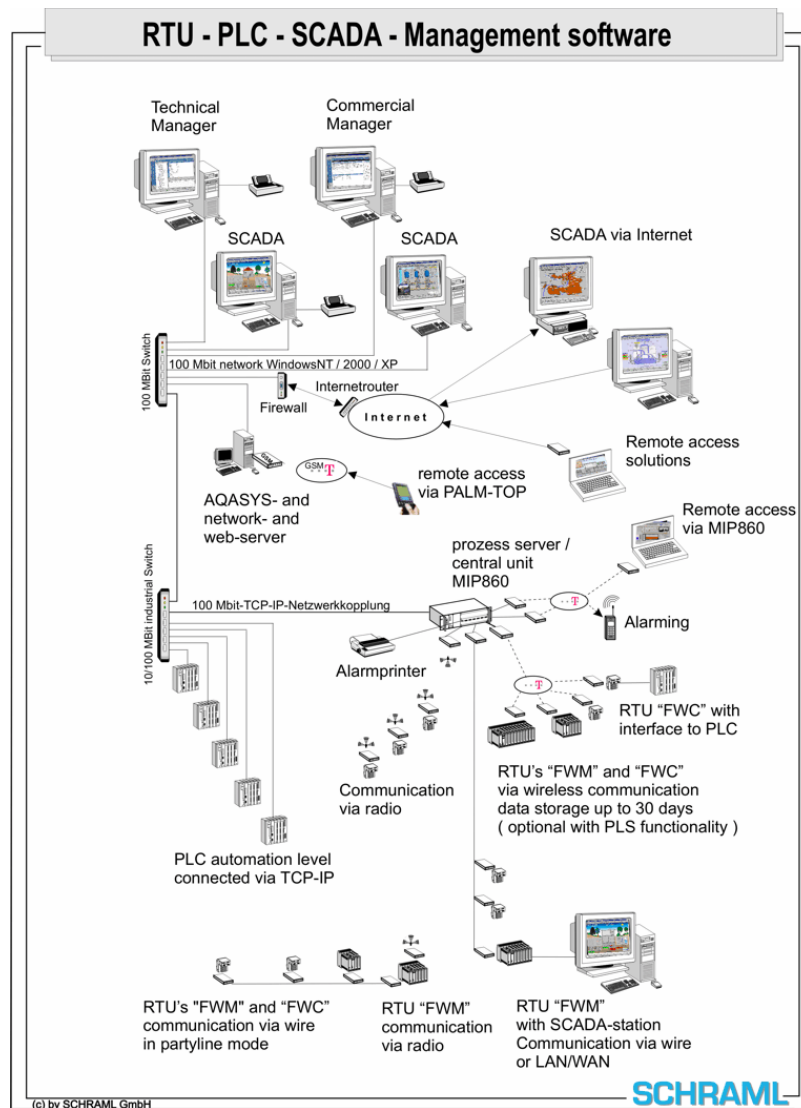


Figure 4: Schraml telecontrol system

6 Deficiencies and required enhancements

Automation networks require deterministic behaviour for realtime control. It must be predictable for every event which serves as an input for an automation application control loop when the corresponding output action shall be completed in a given amount of time for every occurrence. The automation application needs to detect irregularities and handle them, in worst case the application has to enter a safe state.

The deterministic level of mixed private and public networks compared to today's private automation network is low due to divergent technologies and responsibilities of the individual subnetworks. As a consequence and as shown in the different use cases, dependencies between public and private networks are minimized today. Use cases are restricted to primary non-realtime use (maintenance, logistics applications) or adapt to restricted communication capabilities by specific protocols (utility application, telematic systems).

For future applications, an increased deterministic level of mixed private and public networks is required to enable distributed realtime control applications:

- End to end Quality of Service between automation devices, also under on the fly switching of network technologies or service providers
- Convergence of LAN and public network technology for smooth interoperability

Also, local automation devices must be enabled to communicate in a global environment with a lower deterministic level. Telecontrol functionality may be added to accomplish this task, event-driven communication may play a more important role in future private networks besides cyclic processing of data.

6.1 Wireless technologies

Wireless wide area networks are used in distributed automation applications where no wired communication infrastructure is available or to integrate mobile components (logistic, transport) of the application. Even though solutions based on mobile phone systems are available today there are still some deficiencies to consider.

In principle providers of mobile systems do not allow to operate a remote device (in place of a mobile phone) as an server. Measures are necessary to overcome the problem of addressing remote stations (which get their IP address dynamically by the provider) by a central station on request. Solutions are known. However, these solutions are proprietary stand alone solutions and not part of an overall concept related to the needs of automation applications.

Even though mechanisms to prioritise messages are specified in mobile phone standards they are not yet provided by the providers. A first measure to get an idea of the time behaviour could be an online timing analysis. Bases on that the current status of a connection could be assessed.

In mobile parts of an automation system (e.g. transport systems) the relation to a certain location get lost. That is why such applications urgently need a location awareness solution. For that information of the mobile phone system could be used. The subject location awareness will be investigated in detail in task 3.3.

It has to be mentioned that wireless communication via mobile phone systems is mostly visible at one side only. After delivering the message into the network of the provider it can not be said which network are passed and how the second partner is connected to the network. For VAN it could mean that the second partner not necessarily has to be connected to public network. It is also possible that it is a PLC in an Ethernet or an I/O device in a fieldbus system at a factory floor. This is the reason why communication solutions based on mobile phone or mobile broadband systems shall not be focused on the basis technology or on devices but on the overall VAN approach. This implicates as well

- the integration into VAN architecture
- the integration into VAN device architecture and
- the integration into VAN engineering.

6.2 Wired technologies and routing

The development in the wide area sector is focussed on providing more capacity and the addressing of newly arising demands.

The capacity is mainly defined by bandwidth requirements hence the tendency to provide broadband access even to the private end user is putting high pressure on the backbone operators and their equipment. Even though automation applications usually are not demanding high volumes of data to be transferred, the faster transmission is still beneficial. This is because the same datagram of a given size will be transmitted in a shorter time (it takes longer between the first and the last byte of a packet to be serialised into a slow channel than into a very fast one), given that priorities are set correctly. More available bandwidth also allows more extensive data protection, redundancy and encryption. The drawback is mainly in the economic region. The installation of new media for higher bandwidths together with higher service fees does is often not justifiable.

The change in the quality of user traffic is even more interesting for automation scenarios. Upcoming new services in the end user market such as triple play over IP (data, voice and video via the same infrastructure) have very similar expectations towards the underlying networks (low jitter, relatively isochronous transfer, a wide range of QoS features). Internationalisation and closer cooperation between companies are another driving factor as this triggers service providers to offer products addressed to virtually private networks instead of sole access to the internet. These VPN offers are based on MPLS, sometimes ATM PVCs and Carrier Ethernet and allow the definition of a service quality not available on a public infrastructure before.

As most of the wired technologies are designed to carry data (apart from exotic approaches like powerline transmission) there are not many deficiencies that can be identified which are not already addressed. One main problem when connecting to large public infrastructures is that on the last mile despite all measures that are being taken in the meshed distribution network there is no physical redundancy and so the customer access stub is a single point of failure. The access to more stable redundant topologies like meshed networks or double ring structures is usually limited to those running these infrastructures. Here additional measures for increasing the availability of these network access scenarios have to be taken.

Another limitation of wired systems is that the user has nearly no influence to the attributes of the transmission. Other than wireless links where it is possible in principle² to avoid a disturbed part of the spectrum by changing carrier frequencies or adapting transmission power levels this is impossible with most wired systems. Here the increase of bit error rates can only be compensated with stronger FEC which reduces payload throughput drastically. If the disturbance even has the character of an interruption usually this particular infrastructure is then not usable at all at this point in time.

6.3 Telematic systems

Today a flood of sectoral telematic systems, technologies and protocols most of them proprietary do exist. But there is a clear trend and demand to open standardised technologies and systems. Regarding this, the introduction of the IEC 61850 standard gives a good opportunity for a migration to open standardised technologies.

Telematic systems usually use standardised telecommunication paths via public networks for their remote data exchange. Also telematic is faced with steadily increasing demands. With higher requirements on the applications side and extended functionalities as telediagnosics, telesupport and telecontrol the requirements concerning the data transmission are expanding. An important requirement is the predictability and a guarantee of the contracted network behaviour i.e. the Quality of Service (QoS). Concerning to the rising requirements security and safety become more importance to guarantee a secure remote data exchange.

It is unlikely that telematic or automation systems can really influence the development of public networks since, compared with telecommunication and IT applications as voice and video transmission, Internet and so on, automation only produces a very small share of the entire public network load. So for observing the transmission path's status two general approaches seem to be

² meaning for instance in the range of legal possibilities, regulation of the use of frequencies is limiting these options.

possible. The first approach is to collect and analyse on the application side the previous and actual status of the transmission to deduct the future behaviour. The second approach bases on a providing of QoS data that are used already for network internal purposes by the provider to the user. For this the definition of interfaces to public networks is necessary. Also a mix of both approaches could be useful.

7 Conclusions

Wide area networks are already partially used in current automation applications. The reason is for instance the increasing global operation of enterprises. Private networks are not sufficient anymore or too expensive to gather all production related information of remote factories or substations of an enterprise. Furthermore, substations often are far away of any wired communication infrastructure or the installation conditions (e.g. in mountains) are difficult and therefore out of question. In addition mobile substations or transport systems with a wide operation range have to be included into the overall automation concept. In that case only global wireless communication systems such as mobile phone systems can be used.

That is why public wired or wireless networks have to be used besides to private network infrastructures. However, the potential of further application is remarkable. Following for instance the trend of decentralisation of power generation (small power plants using renewable energy sources on-site) such concepts require extended communication capabilities. An efficient operation of such systems demands very simple, cost effective substations on one side and a central station which is able to process the complex algorithms of a number of substations. It is obvious that such a concept needs a capable network which connects all the substations to the central station. Furthermore, different technologies (wired, wireless, telematic) have to be used depending on the special use case. The data communication is very demanding concerning real time, throughput, security and probably safety.

As described in chapter 6 not all of these requirements can be fully met today. Up to now the influence of the automation industry to telecommunication providers is limited. However, the activities of providers in the field of machine to machine communication (M2M) seems to lead to a change of their policy. One result of the VAN project should be to show the opportunity of VAN solutions for telecommunication providers. New business models could be developed based on the results. Even though automation applications using wide area networks represents a small business section this section is stable over a long time since the life cycle of relevant systems are very long. The VAN project should be to cause infrastructure service providers to create sophisticated service levels for the automation industry and especially for VAN. These could concentrate on the typical message size, individual priorities and predefined feature sets for backup lines.

The nature of public networks causes that providers are not able to describe the communication paths which a packet sent by an automation application takes. Probably several technologies (wired and wireless) with different characteristics are used. Furthermore it is not possible to have access to the provider's communication parameters which could give information about the quality of the current used path. Even more the measured parameters can hardly be used to get the needed information for automation applications. That is why the architecture of VAN should enable devices to measure the QoS attributes end to end. Functions should be created for devices like VAN access points or security infrastructure devices to provide comparable and reliable metrics on given communication links. In that way can be assessed if a QoS promised by a service level agreement is maintained.

One of the key prerequisites for a broader use of wide area networks is that the integration into and the cooperation with automation networks is seamless. And this has to be valid for different types of communication networks. The VAN approach is that the required solutions for real time behaviour, security and safety do not exist insulated for one network but is unique for all technologies which are relevant for the described VAN use cases. Even if the addressed communication solutions do not support the required capabilities today the VAN project should provide the measures and specification to be prepared for more advanced technologies. As described in other deliverables preconditions for a realisation of the VAN approach is the capability to transmit IP traffic and to support WEB services.

Based on the analysed network technologies the integration concept can be developed in WP 7.2. This concept will consider interfaces which can be used to access public networks. Therefore, application service elements of GPRS and UMTS for wireless access as well as ISDN and DSL for wire line access will be taken into account for further investigations. Technologies which may be used within the communication paths such as SDH, MPLS or ATM will be regarded as far as it is reasonable within the VAN approach. This prerequisites a direct access to a related interface or indirectly provided status information which can be used to control the traffic via public networks.

Because of the general tendency to migrate all infrastructure services to the use of TCP/IP, native interfaces lose importance. Therefore the focus of workpackage 7 is based on interfacing to public network structures via one general technology which is IP. IPv4 is currently state-of-the-art and globally available. IPv6 is the designated successor.

Nevertheless the knowledge about the underlying technologies provides a valuable insight in the possible set of reachable attributes that a certain link or a given backbone technology can provide. The discussion about actual service levels and the evaluation of the asserted link features can not be performed without major experiences or a descent understanding of the underlying technologies and the problems that arise from interconnecting them.

MPLS or SDH interfaces are not considered as a replacement for service level agreements, they are not even planned to be part of VAN at all (especially a native MPLS access is not expected to be offered by any service provider). Instead the SLA definitions are the one and only mean to describe the quality of a link and to fix expectations on both sides of a service relation. Deliverable D07.1 is determined to establish a common understanding about state-of-the-art in public networks and the technologies used.

In accordance with WP4 the requirement of the transfer of isochronous realtime data via public networks (D01.2-1 R7.16) will no longer be followed. Other parts of the project clearly indicate realtime over UDP to be the transport means for real time data and Web Services to be used for the VAN specific messaging.

Based on these definitions, together with the WAN knowledge gathered in this workpackage, it is now possible to define VAN related SLA descriptions including automation traffic classes.

The next steps in work package 7 are

- the definition of application related topologies based on the selected technologies including redundant communication paths
- the identification of VAN device types within the defined reference topologies
- the definition of the building blocks relevant for data communication via wide range private and public networks

The basis for the listed specification work is the VAN system and device architecture specification described in deliverable D02.1-1. The specification requires cooperation with WP 4 concerning the real time behaviour, with WP 5 concerning a safety related reliable communication, and WP 6 concerning security functions and parameter. QoS and security aspects will be addressed in the future deliverables of workpackages 6 and 7. After the specification an application programming interface has to be specified in preparation to the implementation of the pilot system in work package WP 9.

Glossary

AAL	ATM Abstraction Layer
ADLP	Automated Data Link Protocol
ADSL	Asynchronous Digital Subscriber Line
AMC	adaptive modulation and coding
ASIC	Application Specific Integrated Circuit
ATM	Asynchronous Transfer Mode
B2B	Business to Business
BRI	Basic Rate Interface
CASP	Cross Application Signalling Protocol
CMMS	Computer Maintenance Management Systems
CSMA/CD	Carrier Sense Multiple Access/Collision Detect
CQI	channel quality indicator
DIN	Deutsches Institut für Normung
DNP	Distributed Network
DSL	Digital Subscriber Line
DSLAM	DSL Access Multiplexer
EAO	Enterprise Asset Optimisation
EDGE	Enhanced Data rates for GSM Evolution
EPRI	Electric Power Research Institute
ERP	Enterprise Resource Planning
ET	Euro Telematik
FEC	Forward Error Correction
FPGA	Field Programmable Gate Array
FTZ/ZZF	German Telecommunication Engineering Authority
GDSN	Global Data Synchronization Network
GGSN	Gateway GPRS Support Node
GIMPS	Generic Internet Messaging Protocol for Signalling

GIST	General Internet Singling Transport
GLN	Global Location Numbering
GPRS	General Packet Radio Service
GRAI	Global Returnable Asset Identifier
GSM	Global System for Mobile communications
GTIN	Global Trade Identification Number
HLR	Home Location Register
HSDPA	High Speed Downlink Packet Access
ICCP	Inter-Control Centre Communications Protocol
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
ISA	Instrument Society of America
ISO	International Standards Organisation
IT	Information Technology
ITU	International Telecommunication Union
LAN	Local Area Network
LSP	Label Switched Path
M2M	Machine to Machine
MMS	Manufacturing Messaging Specification
MPEG	Motion Picture Expert Group
MPLS	Multi Protocol Label Switching
NSIS	Next Steps In Signalling
OS	Operating System
OSI	Open Systems Interconnection
OTI	Open Telematik Interface

PaBX	Private Automatic Branch Exchange
PCM	Pulse Code Modulation
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PDH	Plesiochronous Digital Hierarchy
PDM	Pulse Density Modulation
PLC	Programmable Logic Controller
PLM	Pulse Length Modulation
POTS	Plain Old Telephony Network
PRI	Primary Rate Interface
QoS	Quality of Service
RP	Rendezvous Point
RTCP	Realtime Transport Control Protocol?
RTP	Realtime Transport Protocol
RTU	Remote Telemetry Unit / Remote Terminal Unit
RVSP	Resource Reservation Protocol
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SCIL	Supervisory Control Implementation Language
SCL	Substation Configuration description Language
SDH	Synchronous Digital Hierarchy
SDSL	Synchronous Digital Subscriber Line
SGSN	Serving GPRS Support Node
SISA	Supervisory and Information System for local and remote Area
SLA	Service Level Agreement
SMS	Short Message Service
SPF	Shortest Path First
SPS	Speicher Programmierbare Steuerung
TASE	Telecontrol Application Service Element

TDMA	Time Division Multiple Access
TEMEX	Telemetry Exchange
TTI	transmission time interval
UMTS	Universal Mobile Telecommunications
USB	Universal Serial Bus
VAN	Virtual Automation Network
VMI	Vehicle Management Information
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WP	Work Package
W-WAN	Wireless Wide Area Network
XML	Extensible Mark-up Language

References

- [anPM01] aperto networks PacketMAX, URL: <http://www.apertonet.com/products/pmax.html> [Access 09.06.2006]
- [ASRs01] AQASYS - SCADA and RTU systems URL: <http://www.schraml.de/index.htm.en> [Access 09.06.2006]
- [DNPR01] Distributed Network Protocol, URL: <http://www.dnp.org/> [Access 09.06.2006]
- [GPRS01] Overview General Packet Radio Service, URL: http://en.wikipedia.org/wiki/General_Packet_Radio_Service [Access 09.06.2006]
- [GPRS02] Overview General Packet Radio Service, URL: http://www.dell.com/downloads/global/vectors/2002_gprs_overview.pdf [Access 09.06.2006]
- [GPRS03] Overview GSM GPRS UMTS, URL: http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/cm/mmq_sq/cmxcgs_m.pdf [Access 09.06.2006]
- [GPRS04] Overview GPRS GSM modem, URL: <http://www.gsm-modem.de/gps/gsm-modem-module.html> [Access 09.06.2006] [IECN01] IEC- norms, URL: <http://www.iec.ch/> [Access 09.06.2006]
- [IETF01] Next Steps in Signalling, URL: <http://www.ietf.org/html.charters/nsis-charter.html> [Access 09.06.2006]
- [IETF02] Internet Draft GIST, URL: <http://www.ietf.org/internet-drafts/draft-ietf-nsis-ntlp-09.txt> [Access 09.06.06]
- [IETF03] Internet Draft CASP, URL: <http://user.informatik.uni-goettingen.de/~fu/paper/draft-schulzrinne-nsis-casp-01.txt> [Access 09.06.06]
- [IPSP01] Standard Protocols, URL: http://www.ipcomm.de/protocols_en.html [Access 09.06.2006]
- [Lang00] R. Langmann, Internet in der Industrieautomation, A&D Newsletter, issue 6/2000, pg. 76, publish-industry Verlag, München, www.aud24.net
- [MSCP01] MicroSCADA Pro, URL: <http://www.abb.com/global/abbzh/abbzh251.nsf!OpenDatabase&db=/global/seapr/seapr035.nsf&v=99716&e=us&c=F865830D0F3BA17BC225697300330CD6> [Access 09.06.2006]
- [PTTS01] PivoTrack TAMTRON SYSTEMS, URL: <http://www.pivotex.com/asset.html> [Access 09.06.2006]
- [RcRM01] Redline Communications RedMAX, URL: <http://www.redlinecommunications.com/> [Access 09.06.2006]
- [SCCW01] SEQUANS Communications Chip for WiMax, URL: <http://www.sequans.com/site/sqn2010.html> [Access 09.06.2006]
- [SFET01] ServiceFleet Euro Telematic, URL: http://www.euro-telematik.de/servicefleet/sf_technik.htm [Access 09.06.2006]
- [TcdC01] Telecontrol with digiCONTROL, URL: <http://www.hereschwerke.ag/english/produkte/digicontrol.php> [Access 09.06.2006]
- [TcSM01] Telecontrol with SIMATIC S7, URL: http://www.automation.siemens.com/net/html_76/produkte/060_produkte.htm [Access 09.06.2006]
- [TcSy01] TELECONTROL SYSTEMS, URL: <http://www.telecontrolsystems.de/en/home/> [Access 09.06.2006]
- [TKIF01] tekomp informations, URL: <http://www.tekom.de/> [Access 09.06.2006]
- [UMTS01] Overview Universal Mobile Telecommunications System, URL: http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System [Access 09.06.2006]
- [VoWL01] VoIP over WLAN, URL: <http://www.mobilein.com/VoWLAN.htm> [Access 09.06.2006]

- [WiKI01] WiMax Kaiserslautern, URL: <http://www.wimax-kl.de/> [Access: 09.06.2006]
- [WiOv01] Overview WiMax, URL: <http://en.wikipedia.org/wiki/WiMAX> [Access 09.06.2006]
- [WiOv02] Overview WiMax, URL: <http://computer.howstuffworks.com/wimax.htm/printable>
[Access 09.06.2006]
- [WsWP01] Wavesat WiMax Portfolio, URL: <http://www.wavesat.com/products/index.html>
[Access 09.06.2006]