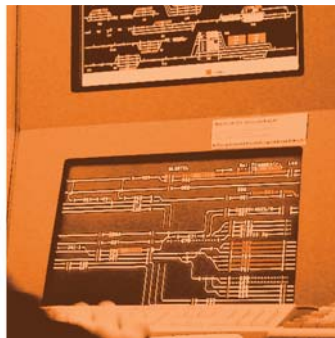


White Paper



Railway Data Networks –
Demands for data networks with maximum availability
in railway control and safety technology

Table of content

| | |
|--|-----------|
| 1. Basic facts | 3 |
| 2. Demands on control and safety technology | 4 |
| 2.1. Explanation of CENELEC EN-50126 | 5 |
| 2.2. Explanation of CENELEC EN 50159 | 5 |
| 2.3. Operating licence | 6 |
| 3. Safety and availability of the control and safety technology | 6 |
| 3.1. Safety | 6 |
| 3.2. Availability | 7 |
| 3.3. The limits of redundancy | 8 |
| 4. Trends in the railway sector | 9 |
| 4.1. Increasing demand for bandwidth | 9 |
| 4.2. Powerful network infrastructure | 10 |
| 5. Conclusion | 12 |

Railway Data Networks

Railway network operators are constantly faced with the challenge of enhancing the technical and commercial aspects of network operation. Standardisation of transmission procedures has created the conditions for optimising data networks. As a result, control and safety technology in railways is increasingly using the data communications technology already available, instead of proprietary technology.

The high level of automation in today's, and in particular tomorrow's rail technology, is only possible when extremely reliable information transmission systems are used. Furthermore, network topologies must be able to fulfil the extensive requirements for reliability.

The CENELEC standard EN 50126 and in particular the standard it spawned – EN 50159-1:2001 for closed transmission networks – are the basis for safety-critical communication in today's safety systems in control and safety technology.

But the use of new technologies for economical management is still in its infancy. Previous attempts to launch innovative technologies, such as Local Area Networks (LAN), Wide Area Networks (WAN), IP technology and GSM-R are a start, but have not yet produced effective results.

Till today, in control and safety technology, only physically separate networks or SDH paths are accepted. Other mechanisms to separate networks in accordance with EN 50159-1, like VLAN tags or MPLS labels, are not recognised yet so that an entire system can be authorised. To be able to use advanced data technologies in future, the foundations for transmitting via open network structures have been established in the EN 50159-2 standard.

1. Basic facts

European railway companies are coming under pressure to operate their companies more economically. This applies particularly to regional railways that appear on the one hand to be threatened frequently by high operating costs and a lack of investment on the other. At the same time, an integrated concept for effective and economical data communication of the different railway services is playing a key role.

Today's data communication in control and safety technology does however sometimes place different demands on the applications concerned, with in some cases diverse levels of safety and physically different transmission technologies. To date this meant that separate networks were usually set up for individual groups of applications. Hot axle box detectors, axle counters, track vacancy detection systems and switch blade detectors are for example all part of control and safety technology.

Because of the different parameters and the history of the development of control and safety technology, nowadays separate cables for traditional modem technology and line-bound non-switched synchronous multiplex systems can exist alongside each other. In other words these are network concepts that have proved to be highly reliable, but from a commercial point of view have to be looked at critically.

One answer would be to use a standard, integrated data network for all data communications and therefore avoid operating parallel networks and isolated solutions.

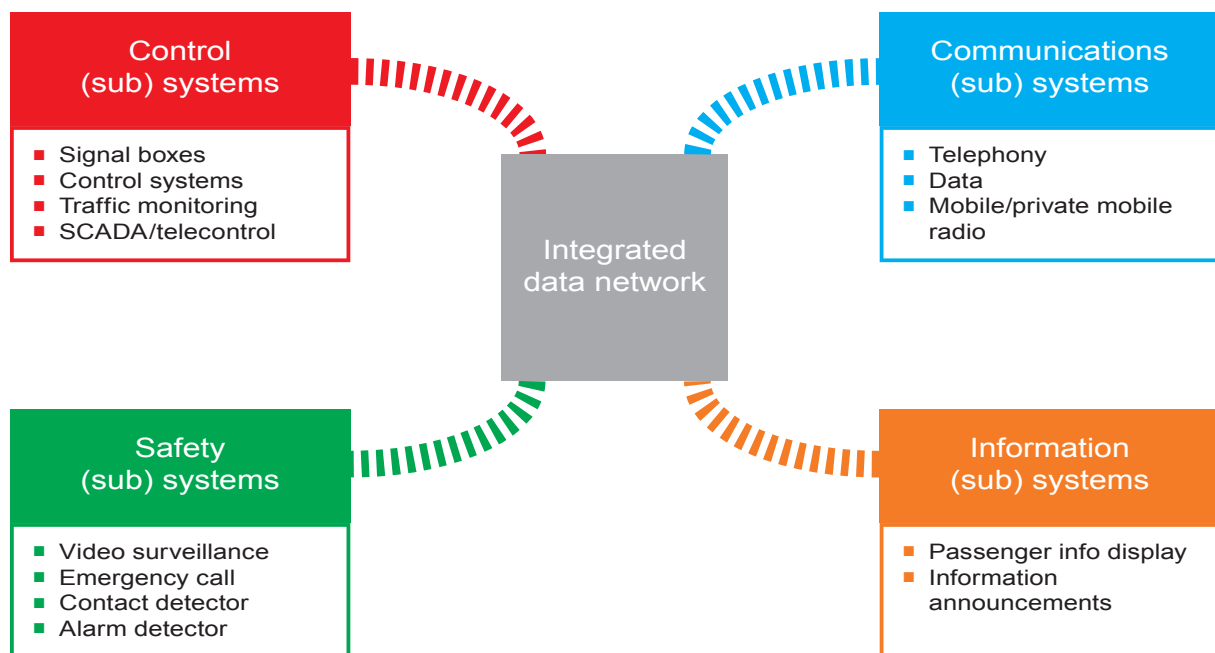


Figure 1: All service applications via one single data network

The integrated data network is the backbone for efficient and smooth-running mobility of passengers and goods.

Previous attempts to develop and launch innovative IP technologies for these types of integrated data networks in control and safety

technology have not been very effective till now. Railway companies believe that the risk involved in launching and using these types of technologies today is too high.

2. Demands on control and safety technology

The technical end systems introduced in railway companies, particularly for control and safety technology, have very long product cycles in comparison to industrialised automation technology solutions for example.

If components from the standard market are used to implement railway operation systems, a discrepancy occurs between the product life cycles of the components purchased and the expected product life cycles of the technical systems in railways.

When introducing new technologies and procedures for operating track-bound traffic, the exact conditions and the environment in each individual application must be taken into account, in order to make safe and at the same time economical operation possible.

As a result, control and safety technology for railway operation is increasingly using data

communications technology. Transmission reliability and quality of service play a vital role.

The European Committee for Electrotechnical Standardization (CENELEC), defined norm EN-50126 and in particular the follow-up norm EN 50159-1:2001 for closed and accepted transmission networks. These standards are the foundation for safety-critical communication of the safety systems in control and safety technology.

The safety systems require an operating license if they are to be used in railways. This operating licence is always the final step in an extensive authorisation procedure. The operating licence is issued by each country in accordance with CENELEC EN-50126.

2.1. Explanation of CENELEC EN-50126

CENELEC stands for Comité Européen de Normalisation Electrotechnique (French).

The CENELEC standard EN-50126 is the key standard for safety-critical communications outlined in this paper. It provides information for specifications and confirmation of RAMS in all phases of the product life cycle.

RAMS stands for:

- Reliability
- Availability
- Maintainability
- Safety

Implementation of the CENELEC standard EN 50126 is carried out in four project phases (concept, systems definition, risk analysis, establishing the requirements). An independent expert checks directly with the railway network operator that all these phases are adhered to.

The purpose of the technical equipment, used for control and safety technology, is to ensure that risks are minimised should a human error occur. The prerequisite is that technology is fully functional when the error occurs. The demands produced as a result (e.g. disclosure of errors and prevention of authorisation for trains to continue if the technology does not work) must be taken into account when developing the system. Terms such as safety and availability of transmission networks are brought to bear (see also the chapter on Availability and safety in control and safety technology).

The CENELEC norm EN-50126 and in particular the subsequent follow-on norm EN 50159-1:2001 for closed transmission networks are the basis for safety-critical communication of the safety systems in control and safety technology.

2.2. Explanation of CENELEC EN 50159

EN 50159-1 (part 1)

The standard's main aim is to provide for safe communication in closed networks. For this to happen, the following conditions must exist:

- Only authorised access is possible,
- the maximum number of subscribers that can be connected is known and
- the transmission medium is known and cannot be altered.

EN 50159-2 (part 2)

The second step was to abolish the conditions required for closed networks when defining safe communications in open networks. This means that the following conditions for an open network were agreed to:

- Different transmission paths and technologies,
- messages can be stored at will and
- possible unauthorised access to the communications network.

These extensive demands require protection from unauthorised attack and therefore additional applications, such as encryption procedures and management of the crypto key.

In this case, less important are possible direct attacks on physical parts of the system, such as direct local tapping of data lines. It is more important to prevent unauthorised and deliberately destructive anonymous connection with powerful computers. This is easy in an open data network with a large number of subscribers that cannot be controlled. As attacks by Internet hackers on inadequately protected computer systems at banks, military organisations etc show, this is a highly dangerous, social phenomenon to be taken seriously.

2.3. Operating licence

To be able to operate technical telecommunication elements in safety-critical railway applications, an official licence is required.

The railway network operator requests the licence. The licence is given after confirmation is provided that the part works satisfactorily, also taking into account properties, such as for example availability, environmental properties and ease of maintenance, based on defined parameters.

The application software must not interfere with non-safe signalling components or

components that are responsible for safety. This has to be guaranteed and ascertained by the components responsible for safety. This prevents faults spreading in safe signalling components.

Operating licences or type inspections are carried out differently in each country. One of the aims of European standardisation is to make a mutual recognition of the operating licences at different railway companies possible.

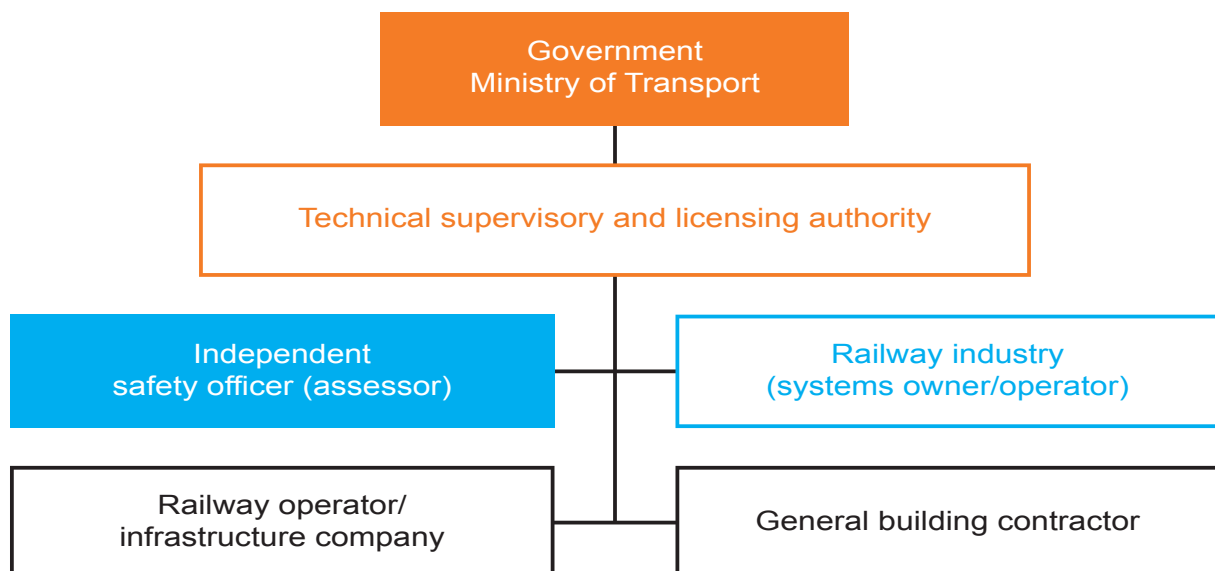


Figure 2: Overview of the parties involved in the operating licence process

3. Safety and availability of the control and safety technology

3.1. Safety

Safety is an objective that must be fulfilled by law. Better security cuts the risk of injury to people, damage to the machinery and the environment (e.g. all planes are grounded).

A financial bonus is that lower insurance premiums are charged. Safety is achieved by:

- Monitored redundancy (fail-stop systems),
- effective redundancy (persistent systems) or
- protective redundancy.

The extreme demands on reliability and availability of complex telecommunications systems can only be fulfilled, if during the definition, development, manufacturing and usage phase, steps are taken to guarantee quality and reliability.

A gauge for reliability is the MTTF: Mean Time To Fail (average life cycle), e.g. 100 years.

This gauge measures the probability that a system will remain fully functional during a given period.

3.2. Availability

Availability is a financial objective. Higher levels of availability increase productivity and output (e.g. all trains are running to schedule).

The gain is underlined by higher levels of productivity. Availability is achieved thanks to better maintenance and functional redundancy so systems can carry on working.

To increase availability, transmission networks and their systems used in control and safety technology are redundant. Availability can also be increased by other steps, such as for example carrying out maintenance.

All equipment is redundant that would not be needed if there were no errors. There are also systems where redundancy is integrated automatically, as well as systems where redundancy can be seamlessly introduced after repairs have been carried out (interruption-free systems).

A transmission network can be classified into three groups as regards its availability for example in minutes per year and in percent as follows:

- 99.98% unprotected
(unavailable for approx. 1.75 hours per year)
- 99.999% protected
(unavailable for approx. 5 minutes per year)
- 99.9999% secure
(unavailable for approx. 32 seconds per year)

Depending on the level of availability, the railway application can be connected to the transmission node (SAP: Single Access Point) with a single or double level of redundancy.

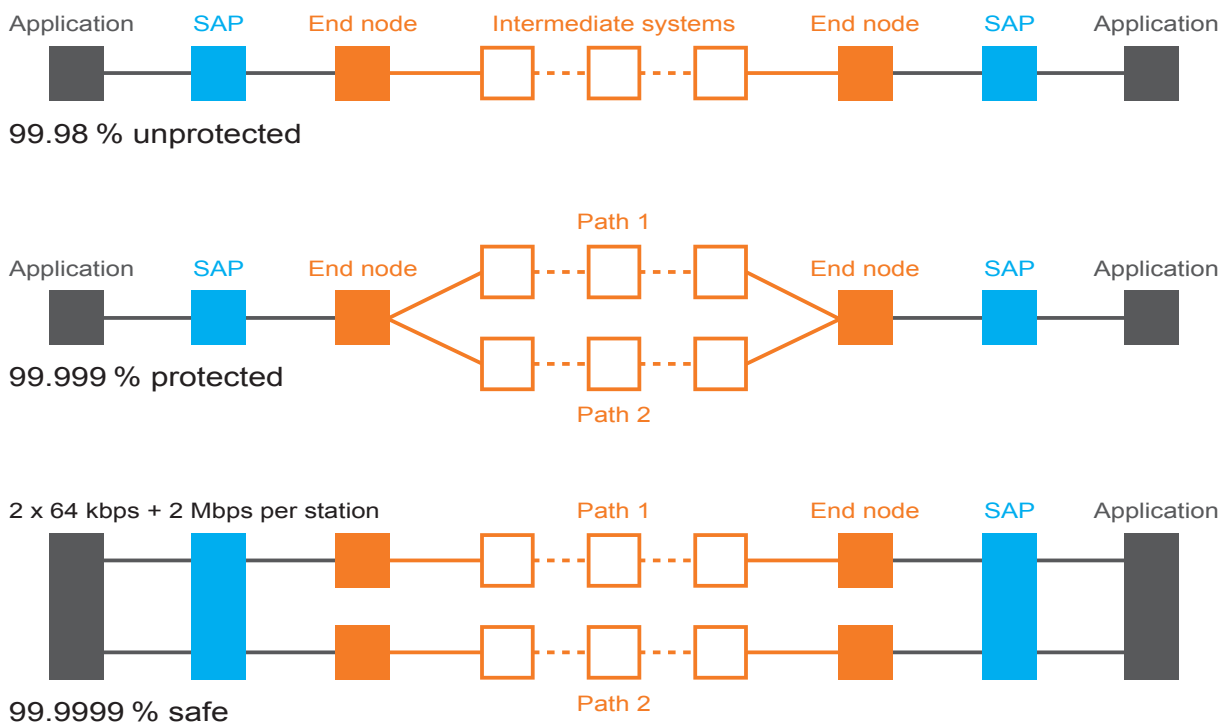


Figure 3: Availability categories

At the same time the percentages, calculated from the reliability figures for the individual elements (MTTF) for the whole of the network topology, can indicate the probability of a whole system actually performing as stated.

Whether systems and their individual components will have to be deployed with single or double redundancy, depends primarily on the level of availability of the railway application.

A summary is provided here of the most frequent railway applications, subdivided according to how available they are required to be.

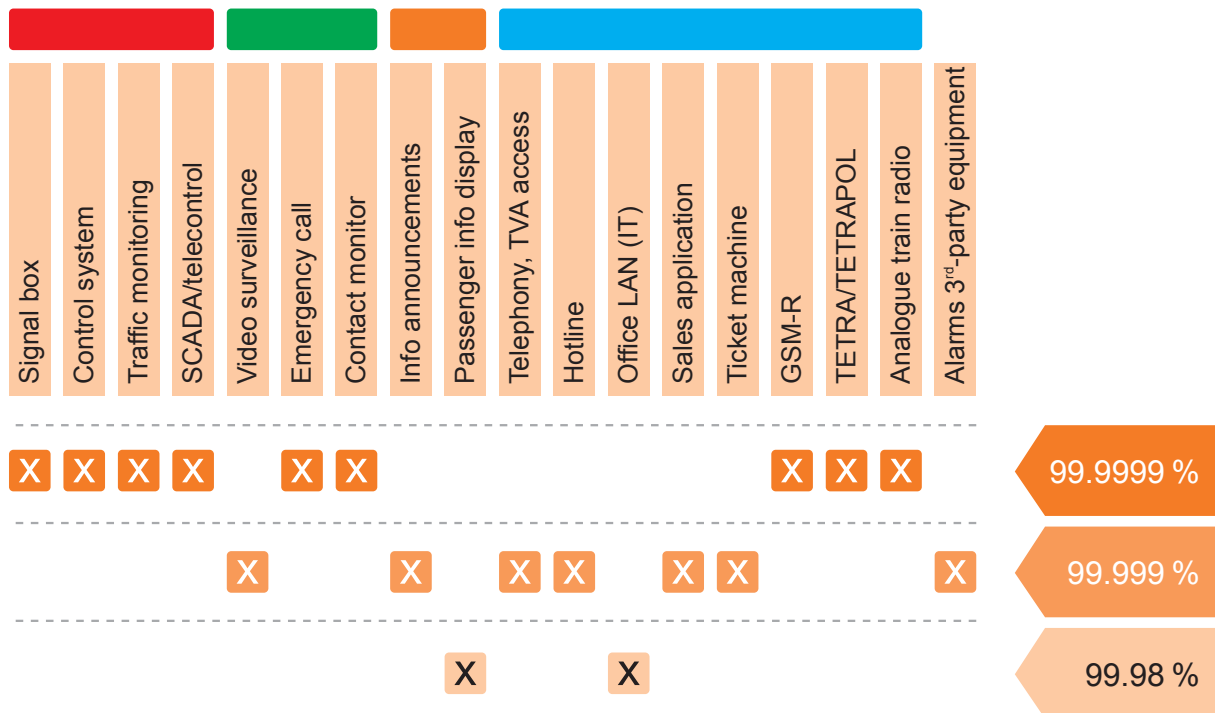


Figure 4: Probability of failure according to individual railway applications

3.3. The limits of redundancy

Thanks to redundancy and error tolerance, availability only depends on the probability of a second failure, before the first one is repaired. However, availability is therefore not infinite.

The only definite factor in a doubly-redundant system is that it is twice as expensive and fails

more than twice as often. As a result reliability and availability targets must be clear before redundant solutions are looked at.

4. Trends in the railway sector

4.1. Increasing demand for bandwidth

Heterogeneous network technology in control and safety technology systems has grown for several decades. Nowadays, there is pressure to modernise and consequently cut costs and increase performance. Signalling applications usually transmit far less data volume than the other IT applications that are more technology driven. However, due to increasing demand in control and safety technology for flexibility and

for increasing capacities in control and operating systems, systems management, (remote) diagnosis, maintenance services etc, requirements for data transmission capacity are constantly on the increase.

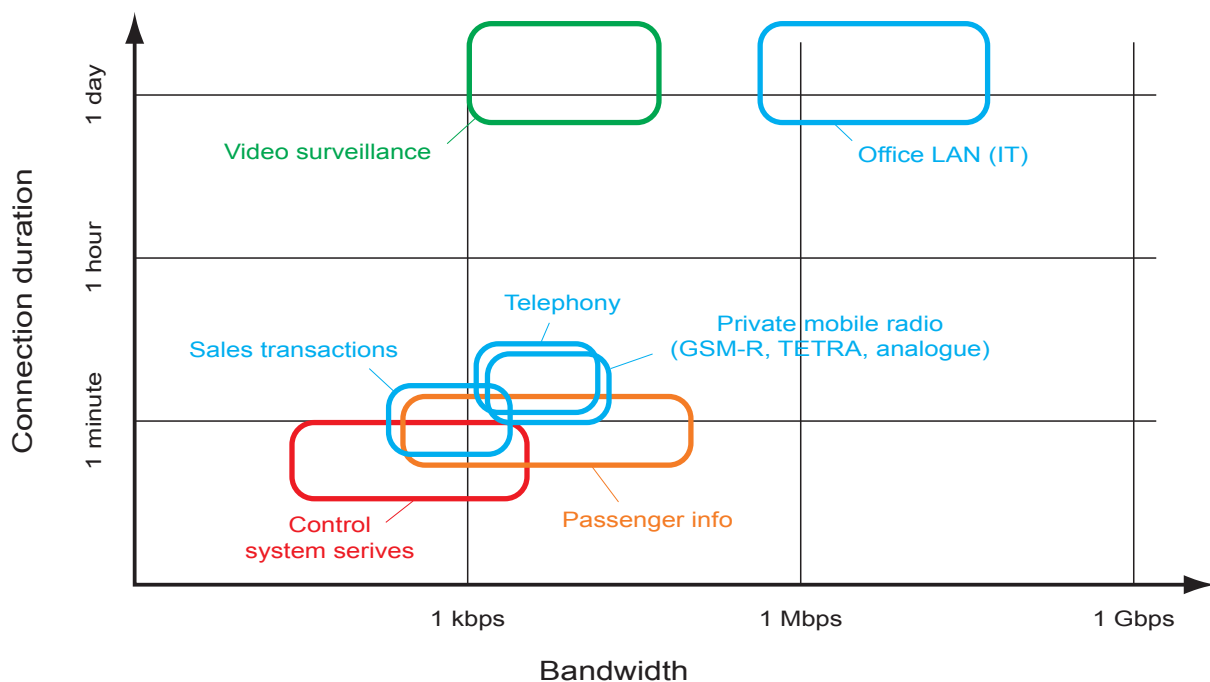


Figure 5: The individual railway applications' bandwidth requirements

The days where, as has been the case up till now, a 64 kbps channel was sufficient between two locations, will soon draw to close. This will happen once communications transmitted separately till now, or new remote transmission (e.g. Radio Block Centres etc from the operating centres), or entirely new services (such as maintenance service centres) will be switched to joint network connections to save costs. Sooner or later, a major operator should be able to transmit WAN connections at a standard 2 Mbps between large nodes, such as operating centres and sub-centres. Then with increasing data volumes, enough bandwidth would be available for some time to fulfil

real-time demands for time-critical applications using the current TCP/IP basic protocols, leaving a reserve at the same time for other applications.

Otherwise, if a bottleneck occurs in a 64 kbps channel, additional protocols that set priorities will have to be used, which will cause delays to subordinate applications.

4.2. Powerful network infrastructure

From the perspective of control and safety technology, two evolutionary paths are becoming obvious.

One of the trends is the development towards large systems that integrate networks and services (convergent networks is the term). The other trend is the increasing usage of processes to safeguard closed sections of networks within large networks (network security). Systems that integrate services mean for example that real-time services, such as voice and live video services are transmitted via IP networks, which these days still tend to be designed for computer data communication that is not time critical. At the same time safety and control technology systems (e.g. rail IP) are also to be transmitted. The customary TCP/IP protocol family (including UDP, a protocol providing faster transmission when data loads are heavy, but which does not prevent transmission faults), does not yet offer any satisfactory methods of always guaranteeing quick through-put times and error-free transmission. Should an interruption occur, convergence times of less than ms (type 50 ms) have to be adhered to at back-up level.

In control and safety technology, Quality of Service (QoS) and fast convergence rates are important. Today, standard solutions from the Metro-Ethernet-IP environment are not yet good enough to be used in control and safety control.

Nevertheless, these technologies do definitely have potential as regards data transmission capacity. As a result, two routes are being pursued. A protocol called Multi-Protocol Label Switching (MPLS) will be added to the basic IP transport functions. MPLS technology adds an additional marker (a label) to the IP data packages during transmission in the data network. Based on this information, routers with MPLS capability take into account different priorities and service categories in the individual data packages and, depending on their service category, allocate them qualitatively different routes through the data network. With regard to configuration management, MPLS is considered very time consuming and therefore complex to operate and maintain.

Another procedure called Next Generation SDH (NG-SDH) opts for the tried and trusted TDM-based SDH infrastructure using Ethernet over SDH (EoS). With Ethernet over SDH, packet-enhanced Ethernet technology is combined with the real-time enhanced TDM process from the Synchronous Digital Hierarchy (SDH). By combining both technologies, the advantages are fully exploited and the disadvantages prevented. Implementing the EoS technology includes flexible broadband management with dynamic broadband allocation to communications demands, physical separation of networks, the interruption-free transmission of data, as well as the integration of the Ethernet interfaces in SDH.

EoS offers network operators an interesting alternative to MPLS, especially as real-time behaviour exists and the Quality of Service (QoS) can be modified. Furthermore, NG-SDH enables consolidation of all services in a single data network with high levels of availability.

Other protocols, such as Provider Backbone Transport (PBT), are to take into account the specific parameter as well, as mentioned above. They are being pushed by renowned manufacturers, but have not yet been tested properly in practice.

The table below summarises the properties of the different transmission technologies we have discussed.

| | Maturity | TDM support | Protective mechanisms and capacity | Configuration | Operation and maintenance |
|----------------|--|-------------|--|---------------------------------|--|
| NG SDH | SDH ~ 15 years NG SDH ~ 5 years | Native | Path and section protection (pre-configured) <50 ms | Fully developed, simple | Many functions, efficient |
| METRO ETHERNET | ~ 1 to 3 years | Emulation | Spanning tree, Ethernet protection, switching, link aggregation <50 ms | Few functions, no end-to-end | OAM standardisation in final phase |
| MPLS (IP) | ~ 6 years | Emulation | alternative routes (pre-configured) <50 ms | Complicated traffic engineering | High level of complexity |
| PBT | No practical experience gained yet, technology too new | Emulation | alternative routes (pre-configured) <50 ms | Similar functions to SDH | No practical experience gained yet, technology too new |

Figure 6: Properties of the different transmission technologies

To date, the developments of the different transmission technologies were also driven by the assumption that the demand for transmission capacity would rise sharply. The hierarchical levels of the SDH technology introduced range from 155 Mbps to 10 Gbps. And with advanced wavelength multiplex technology of up to 40 Gbps, the optical networks, some of which have already been and will be implemented, exceed this figure and are likely to do so in the future.

With the advent of Local Area Network (LAN) technology, control and safety technology has the SDH base already installed in the transport network. With EoS-capable network components, SDH systems will become NG-SDH capable.

This allows Ethernet-based services in control and safety technology to be transmitted safely. The initial transmission capacity of 10 Mbps to a current standard of 100 Mbps to 1 Gbps (already common in many cases) are not a problem.

It is also possible to transmit the traditional two-wire copper line by using symmetrical DS technology with $n \times 5.7$ Mbps in TC-PAM 32 Ethernet services up to 100 Mbps.

5. Conclusion

From an ICT standpoint, data communication in control and safety technology will remain a special case as regards:

- Data rates that are currently still relatively low,
- particularly high demands regarding safety and
- relatively long user system innovation cycles.

The directions ICT developments are heading, are however inevitably reflected in the way control and safety technology is used. This is evident in the current proliferation of LAN/WAN technology in the cross-over to IP.

Control and safety technology network designers are facing conflicting priorities of compatibility with the legacy systems, different demands nationwide from the railway operators for new solutions, international standardisation trends in control and safety technology, as well as affordable, but never totally adequate standard solutions from the global market in information and telecommunications technology.

Because the length of innovation cycles varies, it is always a problem to identify when a new ICT trend is here to stay and likely to become a trendsetter in the future, so that adopting it into control and safety technology, with its time-consuming testing and licensing processes, is economical.

Finally, networks must be designed for implementation as an entire control and safety technology system that will receive a licence. As a result, KEYMILE has opted to supply its integrated and advanced multi-service access system UMUX to its railway customers worldwide.

Publisher

KEYMILE GmbH

Wohlenbergstrasse 3
30179 Hanover, Germany

Phone +49 511 6747-0
Fax +49 511 6747-450
Internet www.keymile.com
Mail info@keymile.com