

7. Operation

Introduction

In this chapter there are discussed issues, which influence to a considerable extent the operation of the telecommunication networks and - from the perspective of the user of the network - are determining the quality of the network.

For all telecommunications services the time ratio in which a service is available for the user with the stipulated quality is an important feature. The continuous service usage and availability of the systems that realise the services could be obstructed or made impossible by network failures. The user's reaction, if a service is not available in a given time, can be different. Beside the bad perception about the service, in some cases the users may suffer particular financial or economic loss due to the lack of (or in quality degraded) telecom services. The Service Level Agreements (SLA-s) usually prescribe those tariff and compensation conditions according to which the service provider shall compensate the user in case of a service outage. Therefore, it is recommended for the telecom provider to plan the availability level of the service in advance. Availability planning always means considering of several aspects and can be carried out only by probability calculations. It is the consequence of the nature of events affecting the availability is random, but the processes can be properly modelled by mathematical tools. After all, the reliability analysis is a preliminary step before the economical decision on to what extent it is worth to invest money in availability improving technologies and/or enhancing the operation and maintenance conditions.

In the last decade more and more services are added to the traditional telephone services and the demand for transfer of high bandwidth data is increasing. The ability to deliver voice, video and data at higher speeds is becoming a critical requirement. Now, the telecommunications networks have to integrate different computer networks with different bandwidth demands. Their different nature of the traffic also generates new requirements for Network Operators and Service Providers.

In order to be able to carry different kinds of data at a faster rate, quite new technologies and significant improvements to the existing technologies and protocols have been and still are being introduced. The complex and diverse equipment and service portfolio, their rapid change makes the planning, installing and maintaining of the controlling networks, very sophisticated. This problem can be solved only by proper and adequate automation.

Telecommunications Network Operating Organisations have invested significant amount of time, money and human resources into building up their complex telecom networks that need to be maintained, as well. In order to maximise its efficiency and productivity, the telecom network is to be controlled and managed from the following three points: network elements, services and traffic.

Proprietary (vendor-specific) network management cannot provide interoperability among diverse technologies, equipment and networks deployed by different manufacturers and proprietary management solutions having different features and different level of management capabilities. Theoretically, the gap can be over-bridged by human resources, however, the speed that can be provided in this way is often not fast enough to provide the contracted level of service for the customer.

As the communications industry continues to evolve with deregulation and liberalisation, service providers are under increased pressure to deliver a broadened set of services at a competitive price. As a result, service providers must deliver these services in a cost-efficient and timely manner. The ability to manage effectively these networks has become a key point in retaining existing, as well as acquiring new market share. However, the complexities surrounding today's networks present challenges in achieving of the effective network management goal.

Traffic management in telecom networks deals with the controlled use of network resources to prevent the network from "having a bottleneck". In particular, when more traffic should be transmitted on the network that they can effectively handle, network performance will be degraded. Traffic management controls traffic generated by calls entering in and flowing through the network, and prevents the network from overload.

Telecommunication installations and equipment accommodated in them may vary by their design and destination, but they are common in one: all of them inevitably need electric power. In most cases, the public electricity network supplies this energy. In some particular cases it happens that the electric power supply is not available for the telecommunication system. Here, according to the local conditions, alternative energy sources provide for the feeding of such installations. Due to the fact that in such cases the energy is discontinuously available, these systems are supplemented with interim auxiliary energy storing batteries. In Hungary – with the exception of some special cases – the electric energy is available all over the country.

However, the continuity of the electric power supply cannot be always ensured, for a shorter or longer time interruptions (failures) may occur due to the outage of the mains, or due to the transient phenomena, disturbing the operation of the powered equipment. Telecommunications equipment must work also under such circumstances. During the powering of the telecommunications equipment with energy, the main goal is to provide for the possible most safety and reliable feeding; therefore it is necessary also the generation and storage of the energy in a telecom building.

In the interest of proper functioning of equipment in the given environment, i.e. without the degradation of its performance, it is necessary that the different equipment and their operational environment are made electromagnetic compatible. *The electromagnetic compatibility (EMC) refers to such a professional field, the object of which is to eliminate or at least to possibly minimise the “mismatch” between the equipment and their operational environment according to the accepted norms, standards and regulations.*

For the selection and implementation of a telecommunications system there are quite a lot financial and technical conditions to be taken into account. The first task of the planner/designer is to determine and specify the major functions of the system, i.e. to decide what is needed. This usually includes a technical analysis, a system planning, based on marketing survey. The Buyer issues a tender invitation on the basis of the large-scale and later the detailed system plan. By the thorough technical and financial assessment and evaluation of the received bids the most appropriate telecommunications system can be chosen. The system selection

means, therefore, such a technical/financial analysing and planning process, in the course of which the Buyer – with regard to the market conditions – brings into harmony his needs with his possibilities.

Csaba Kántor dr., Editor of the Chapter

7.1. Factors influencing the availability

Géza Paksy, author

József Wiener, reviewer

7.1.1. Importance of network availability

For all telecommunications services the time ratio in which a service is available for the user with the stipulated quality is an important feature. The continuous service usage and availability of the systems that realise the services could be obstructed or made impossible by network failures.

The user's reaction, if a service is not available, can be different. Private users may have bad perception about the service or can be disappointed. On the other hand, corporate users may suffer particular financial or economic loss due to the lack of telecom services. The service level agreement (SLA) usually prescribes the way and extent of compensation that the service provider shall make in case of service outages. Therefore it is recommended for the provider to plan the availability level of the service in advance. Availability planning always means considering several aspects and can be carried out only by probability calculations. It is because the nature of events affecting the availability is random, but the processes can be properly modelled by mathematical tools.

After all, the reliability analysis is a preliminary step before the economical decision on to what extent it is worth investing money in availability improving technologies and/or enhancing the operation and maintenance conditions.

7.1.2. Availability definitions

The quantitative measure of availability of telecommunication systems and networks is the *Availability* defined as follows:

$$\text{Availability (A)} = \frac{\text{error - free operational time}}{\text{total observation time}}$$

The availability is usually given for a year, or rarely for a month.

The un-availability rate (UN) can be calculated as follows:

$$\mu A = 1 - A$$

The availability of professional telecom systems falls into the range of 99.5...99.99%.

The availability of a telecom system depends on several factors that determine the reliability of the entire system. Since the system reliability depends on these factors, they are together called "dependability". Although the dependability itself has no measure, the parameters introduced in the following part have.

Reliability

The *Reliability* (R) parameter gives the probability that a device or equipment does not fail during a time period of t . In case of standard deviation, in addition to the expected reliability value, the reliability is also featured by the Mean Time Between Failures (MTBF) parameter.

The *failure rate* (λ) gives the average number of failures for a time unit. Its unit is FIT (Failure In Time):

$$1 \text{ FIT} = 1 \text{ failure} / 10^9 \text{ hours}$$

The relation between MTBF and λ is the following:

$$MTBF = \frac{1}{\lambda}$$

The effect of repair on availability

The *repair time* gives the mean time that is needed for eliminating a failure. This parameter is called MTTR (Mean Time To Repair).

The *repair rate* (μ) determines how many repairs fall into a certain time period (hour, month, year) in average.

Based on the parameters described above, the availability can be calculated as follows:

$$\text{Availability } (A) = \frac{MTBF}{MTBF + MTTR}$$

7.1.3. Effects of network failures on services

The service outages due to telecom network element failures have different effects depending upon the duration and type of the service. Short outages (some seconds) in line switched networks (e.g. PSTN) causes disconnections, but in packet switched networks it causes only some packet losses. Much longer outages (10-20 minutes) may result more serious problems in everyday life, sometimes indignation of the people may arouse (e.g. unavailability of cache machines, interruption in TV broadcasting, etc.).

The effects of various network outage times are summarised in the table below, giving a support to network planners for the network reliability calculations.

Most of the outages last 2 sec... 5 minutes. This is the domain where the service layers network management systems should act to repair the connections by rerouting or activating the protection systems.

Outage duration	Effect on service and users
< 50 msec	Minor quality degradation, certain fast line protections are activated; Audible clicks due to synchronisation losses in PSTN connections; Significant increase in bit error rate of data transmission;
50...200 msec	Some PSTN connections are disconnected. Some packets have to be re-sent in X.25 and TCP/IP systems;
200 msec...2 sec	Several PSTN connections are disconnected; Sufficient packet re-sending is required;
2 ... 10 sec	All PSTN connections are disconnected and it is impossible to re-establish them; X.25 and ATM connections are disconnected, disturbances occur in data link layer, re-routing functions are activated;
10 sec ... 5 minutes	All data transmission connections are disconnected;
5 minutes ... 30 minutes	Disturbances and congestion may occur in the traffic, causing slight effects on everyday private and corporate life;
> 30 minutes	Major network outages affecting numerous users; If the fault concerns the important telecom operators, it may have an impact on everyday life and business; The event becomes a news.

Table 7.1.1

7.1.4. Factors directly effecting network availability

Equipment reliability

The reliability of telecom equipment is determined by its individual active and passive components. These can be as follows:

- semiconductor devices, discrete or integrated circuit elements;
- passive electronic devices, such as resistors, capacitors, inductors, etc.;
- printed circuit boards, internal cablings, rack and subrack cablings, printed circuit back-planes;
- active and passive optical devices (e.g. optical transmitter and receiver diodes, WDM filters, optical switches, power splitters);
- dismantlable electrical and optical connectors;
- non-dismantlable electrical and optical connectors.

The manufacturers determine the reliability values of the individual elements by measurements. The figures rarely mean the probability of a catastrophic fault, rather the probability of being out of the specification range. In practice, the probability of an electronic device fault (λ) falls into the range of $(10...1000) \times 10^{-9} = 10...1000$ FIT.

The failure rate of the equipment, cards, units and ports of which the given configuration is made up, can be estimated by summing up the failure rates of their individual system components:

$$\lambda_s = \pi_e \cdot \sum_{i=1}^N \lambda_{si}$$

where:

N: is the number of system components;

λ_{si} : is the failure rate of the individual system component;

π_e : is the environmental failure rate multiplicative factor.

The manufacturers give the calculated λ_s figures for the delivered equipment, which are the inputs for the detailed reliability analysis of telecom networks.

Environmental conditions

The lifetime and failure rate of the telecom equipment is determined by the environmental conditions such as operating temperature and relative humidity. The current silicon based electronics technology requires +5...+40 °C temperature range and 80...85% humidity. The manufacturers have to ensure by serious planning that the temperature of the single components inside the equipment does not exceed the specified value. This can be achieved either by passive or active forced cooling.

Overvoltage and lightning protection

The inducted currents due to shortcuts of high voltage networks or power lines near to telecom equipment and cables are not allowed to cause permanent faults. Telecom networks must not fail if an atmospherical discharge occurs not directly through the network. The protection against such effects has to be thoroughly planned. (See details in Clause 7.8.)

Mechanical stresses

Telecom equipment and cables are exposed to considerable mechanical stresses. The equipment should be resistant against shaking. This is especially important in out-door equipment near to heavy traffic roads.

Probably the most frequent failure event is the cut of telecom cables due to external stresses. The failure rates can be decreased by clear signs in outer areas indicating the exact cable route, and by accurate registering of public utilities based on geospacious information systems (GIS).

7.1.5. Influence of transmission performance parameters on availability

The temporary or permanent degradation of performance parameters of the transmission routes, or a certain sections of it, interconnecting the service nodes, can make the whole connection unavailable. Insignificant transmission performance degradation is not considered to be a fault.

According to the ITU-T, a connection is considered unavailable if the transmission quality is severely decreased during 10 consecutive second. The

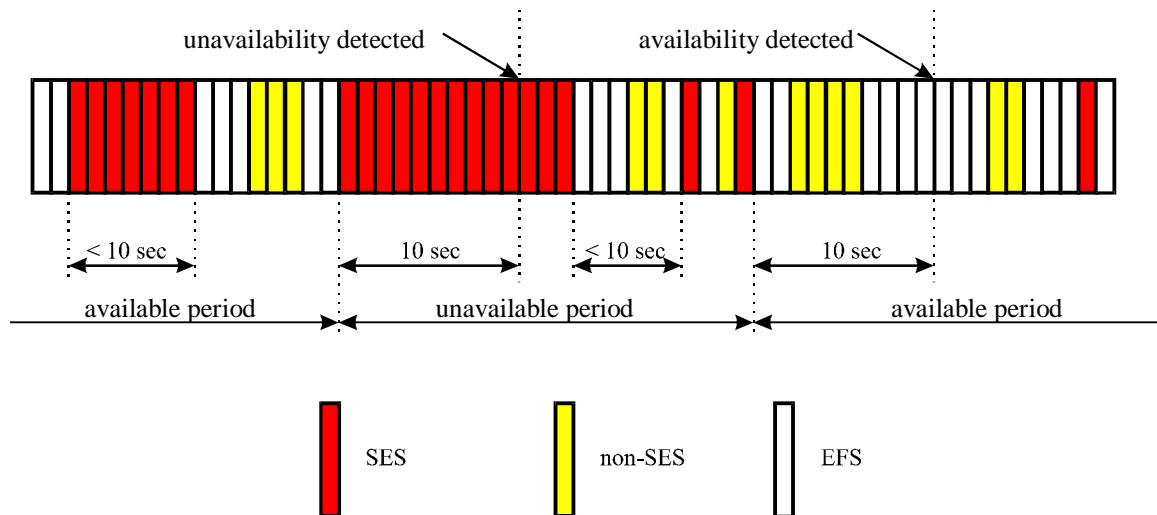


Figure 7.1.1

definition of severely errored statuses is different for various technologies and bitrates. For 64 kbit/s digital connections, the G.821, and for higher bitrates, the G.826 Recommendations are relevant. The determination of unavailability is depicted in figure 7.1.1.

The unavailable periods, determined by the above showed method, shall be added to the total accumulated system outages of the system. In order to minimise the number of the unavailable periods, the outage intensity is also specified. Please refer to the ETSI standard given in Bibliography.

Translated by Róbert A Horváth

7.2. Methods to increase reliability

Géza Paksy, author

József Wiener, reviewer

7.2.1. Network reliability analysis

The most suitable method for analysing the reliability level of a telecom network is based on mathematical modelling which allows us to determine the availability of the network relatively exactly. Such model is the continuous-time, homogeneous Markov chain. In this approach, the reliability model is given by a block diagram and a state-transition diagram, determining the relation between network elements and the reliability states of the network elements. For example, the figure below shows the model of a parallel, redundant optical network. The possible states of the system are 1, 2, 3 and 4. The state-transitions are indicated with lines interconnecting the different states. The system goes from faultless State 1 to State 2 or State 3 with the probability of λ_1 or λ_2 respectively. The system is available in State 2 or 3. In State 4 the system is unavailable, and the probability of this is $\lambda_1 \cdot \lambda_2$.

If a system contains K sub-systems, and each sub-system has m pieces of replaceable or on-site reparable components, then the Markov model has $2^{K \cdot m}$ states. In most cases, the failure rates of the components are orders of magnitude smaller than component failure detection, failure recovery and repair rates, therefore the model can be truncated to fewer states.

If the repair rate of the i th sub-system is μ_i , then the μ_i will appear on the relevant line.

P_j probability of state j can be calculated from the time the system spends in state j , provided $\sum P_j = 1$ and $j = 1, 2, \dots, K$. The P_j state probabilities are given as the result of a K element linear algebraic system. The state probabilities of simultaneous faults in large systems are so small that they can be neglected in order to reduce the computing time.

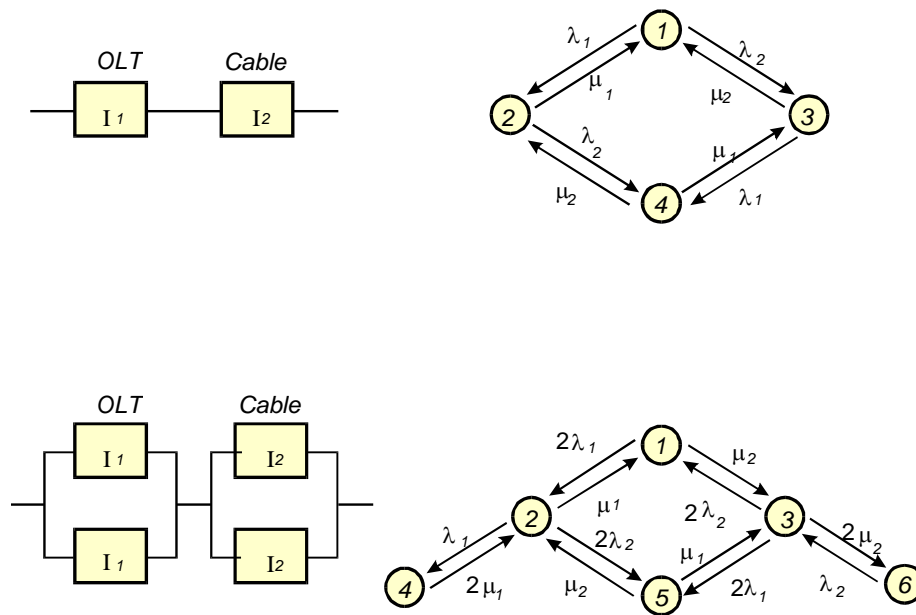


Figure 7.2.1

7.2.2. Network reliability level from economical point of view

The expected continuous availability of telecom services and the level of network availability are based on the agreement between the service provider and the user. For the service provider, the availability is not only a performance parameter but an important economical factor as well, since the increase of reliability is possible only with certain investments and additional operational costs. For profitable business, the network operator should make proper balance between expenses and incomes, that is:

$$\max\{LCR - LCC\},$$

where:

LCR: is the income during the network lifetime;

LCC: is the expenses during the lifetime.

The largest profit can be gained by minimising the present value of network:

$$\min\left\{C_I + \sum_i (C_{ii} + C_{mi})\right\} \cdot d_i,$$

where:

C_i : is the invested money necessary for a certain level of network reliability

C_{mi} : is the operational cost in the i th year

C_{ti} : is the lost of income due to network faults

d_i : discount rate in the i th year

C_t is the total loss due to network unavailabilities, directly influencing the income. This method gives us an unbiased figure for a certain availability level, rather than considering subjectively different availability values. Further advantage is that it is independent form the applied technology, and well suited for preparing different network plans.

The most critical part of the method is the estimation of C_t loss of incomes. Here is a simplified model for this:

Different effects of traffic outages on line switched and packet switched networks

In case of line switched traffic outage, the loss of income is:

$$C_t = \lambda_F \cdot MDT \cdot \alpha \cdot A \cdot E \cdot C_S,$$

where:

λ_F : is the fault rate (fault/year);

MDT : is the Mean Down Time (hour/year);

A : is the traffic in business hours (erlang);

α : is the ration of business hours and outage time;

E : is the probability of traffic congestion;

C_S : is the service income (income/erlang hour).

In case of packet switched traffic outage, the loss of income is:

$$C_{tp} = \lambda_F \cdot MDT \cdot \gamma \cdot \beta \cdot \varepsilon \cdot C_p,$$

where:

γ : is the packet transfer in business hours (packet/hour);

β : is the ration of packet transport during outage time and business hours;

ε : is the probability of packet loss during outage time;

C_p : is the economical consequence of a loss of packet (income/packet).

In case of leased line traffic outage, the loss of income is:

$$C_{il} = \lambda_F \cdot MDT \cdot n \cdot C_L,$$

where:

n : is the number of leased lines;

C_L : is the income from leased lines (income/erlang hour).

If a network segment is unavailable, the losses of income for the services operating on this network segment has to be added together.

The parameters in this model are presumed to be statistically independent from each others, and do not change in time. However, in reality, there may be some correlation between the business hours and the fault time.

After these calculations and the evaluation of the results, the required network reliability can be ensured by the measures considered to be economic.

7.2.3. Allocation of availability parameters to international connections

The resultant availability of long distance connections has to be provided jointly by the service providers that operate its sections. So that the operators use links with proper quality, ETSI elaborated a standard to allocate the availability parameters (EN 300 416). A 2500 km long leased line reference connection is determined as shown in the figure below:

PEP: Path End Point

TIC: Terminal International Centre

FS: Frontier Station

IB: International Border

ICPCE: Inter-Country Path Core Element

IPCE: International Path Element

NPE: National Path Element

CP: Customer Premises

The following categories are determined for the path lengths:

Path length, km	$L < 500$	$500 < L < 1000$	$1000 < L < 1500$	$1500 < L < 2000$	$1500 < L < 2000$
l	1	2	3	4	5

Table 7.2.1

According to the length categories, the availability ratios and allowed outage parameters of the constituent sections of the entire link can be determined by the following equations and table:

$$UR_{jS} = A_{jS} + i \cdot X_{jS} \text{ for standard category;}$$

$$UR_{jH} = A_{jH} + i \cdot X_{jH} \text{ for high quality category.}$$

Path element	Performance category	Mean value ($\cdot 10^{-4}$)		Worst case ($\cdot 10^{-4}$)	
		A_j	X_j	A_j	X_j
IPCE	standard	0	15	40	35
	high	0	3	8	7
NPE	standard	0	20	52	47
	high	0	4	12	9
ICPE	standard	0	20	52	47
	high	0	4	12	9

Table 7.2.2

If the connection consists of N independent sections, the following equations can be applied:

$$\text{Mean value: } U_{MN} = \sum_{n=1}^N u_{mn}$$

$$\text{Worst case value: } U_{WN} = U_{MN} + \sqrt{\sum_{n=1}^N (u_{wn} - u_{mn})^2}$$

where u_{mn} and u_{wn} are the unavailability ratios of the individual sections, provided the sections unavailability ratios are according to the Standard Deviation.

7.2.4. Possibilities to increase the availability

Referring to the parameters affecting the availability described above, the possibilities to increase it are as follows:

Network planning phase

- Choosing the most advantageous network topology, minimising costs; Careful selection of network interconnections; Multiple access of network nodes via alternative routes; Application of dual-homing;
- Application of various self-healing architectures;
- During implementation planning, the allocation of equipment to secure places; Ensuring high reliability power supply and the specified environmental conditions;

Realisation phase

- application of properly reliable equipment that meet the availability objectives of the system

During operation

- Application and operation of properly planned network management systems for prompt fault detection and fast network reconfiguration;
- Increasing the efficiency of maintenance activities by applying properly skilled staff; Minimising the number of faults due to human mistakes;
- Modernisation of out-of-date, overused equipment; Reconstruction of old networks; Application of new technologies;
- Accurate planning of fault elimination processes;
- Application of spare parts stock with appropriate quantities; Optimal distribution of the spare parts.

7.2.5. Planning the number of operational staff

In large networks significant savings can be achieved, if the optimal number of repairing teams is determined by knowing the expected failure rate (λ), in such a way that the sum of losses due to failures and the maintenance cost of the teams is minimal. The optimisation can be done as follows:

If the network repair rate is μ , and the deviation of average repair times is exponential, the $W(N)$ mean service outage time is as follows:

$$W(N) = \frac{\left(\frac{\lambda}{\mu}\right)^N \cdot \mu}{(N-1)!(N \cdot \mu - \lambda)^2} \cdot \frac{N}{N \cdot \mu - \lambda} + \sum_{k=0}^{N-1} \frac{1}{k!} \cdot \left(\frac{\lambda}{\mu}\right)^k \cdot \frac{1}{N!} \cdot \left(\frac{\lambda}{\mu}\right)^N \cdot \frac{N}{N \cdot \mu - \lambda}$$

The optimal number of teams (N_{opt}) is at the minimum of the sum of costs of fault repair and the income losses due to traffic outages, according to this formula:

$$N_{\text{opt}} = \min_N \{N \cdot C + \lambda \cdot W(N) \cdot F \cdot\},$$

where C is the annual cost of the maintenance of a team, and F is the income loss for a time unit.

The model can be refined by the priority orders of fault repairing of simultaneous faults, i.e. the higher priority traffic outages can be eliminated faster by interrupting the lower priority fault repairing activities.

It can be observed that using few repairing teams increases the loss due to traffic outages, while using too large repair staff causes unnecessary expenses on manpower. The size of operational equipment store can be optimised similarly.

The costs of repair and the maintenance staff can be reduced by several technical solutions, protections. In this case, the minimum of the sum of the investment cost of the network protection and the income loss due to the lack of protection has to be found. The technical solutions increasing the availability are described in Chapter 7.3.

Translated by Róbert A. Horváth

7.3. Network redundancy concept

(Editorial Chapter)

The structure of the network and the different self-healing solutions were discussed in chapter 4. In subchapter 4.1-4.4 traffic-routing methods were shown which can offer connectivity in the case of a single failure in any part or item of the system using meshed or double-ring networks. If there are at least four switching points in the networks then they can also transmit information from any source to the request sink in the case of more than one failures, but in this situation the quality will be impaired due to the higher congestion.

There are also appealing solutions where the redundancies are not only in the physical layer, but in the higher layer too, supporting the information transfer in the case of the outage of any section. Here we can use the intelligence incorporated in the third and higher layers offering a routing strategy fitted to the existing situation. This was also mentioned in chapter four, including the planning of it.

Modeling the network with graphs it is possible to have a proper view on the possible failure tolerances of the network. Here (1.10) you can see that extracting any path you can find several other possibilities to establish the requested connection. It has a further advantage namely mathematical model derived from the graphs gives a good background to calculate the optimal route of traffic transportation. In the course of planning and realisation it is possible to prepare the routing strategy for every failure. So in some milliseconds the rerouted networks can achieve any terminal points. More details can be found in 1.10 where the mathematical background was described by András Recski and Peter Laborczi.

Redundancies can be planned and realised not only in the network structure but also in the unit or equipment level. In the case of equipment reservation we have two possibilities. In the first case two equivalent units are working in parallel but the bit-stream is led on one of them. Only in the case of outage takes over the task the other one. There is no down-time so the user is not disturbed by the transition time. The maintenance staff will be informed about the failure immediately so they can change

the faulty unit. The engineering of this system is based on the availability requirements.

The goal of the maintenance organization is to minimize the down-time but in the same time the travelling time of the maintenance staff should be as low as possible. The number of the maintenance engineers, technicians is also a critical point because their salary is influencing the budget of the company. All this requirements can be fulfilled if the down-time of the network is much shorter than the fault-clearing time. This condition can be realised if they are in any position redundant units, transmission, paths, power supplies which can be switched on or if we are using network-structures which can be automatically transmit the traffic in any other way for example selfhealing networks.

The availability is the ratio of the operating time (T_0) to the whole calendary time (T). It is characterising the available time for telecommunications. The abbreviation of this ratio is ($A=T_0/T$). A must be near to 1 in general 0,999 offers a good service. In engineering or calculation to handle a number extremely near to 1 makes difficulties. Therefore the use of down time ratio is preferable

$$DTR=1-A$$

This can be used easier especially if we take in account that roughly there are 10000 hours (exactly 8760) in a year. So 10^{-4} DTR means that there is less than one hour downtime. 8 hour downtime equals 10×10^{-4} , which is an acceptable limit. If the telecommunication is a part of a technological process, and has critical task or purpose in it than lower limit should be defined.

The availability is influenced by the reliability and the fault-clearing time. For calculation purposes the reliability can be characterized by the failure rate or with other words with the average (meanvalue) of the time between two consecutive failures. We are using μ for characterizing this average the dimension of it is time. In some cases the use of n can be preferable the average number of failures in a given time intervall. It's dimension event/time. The fault clearing time is L . In the case of automatic overswitching it is in some minutes or less. If the operation can be restored only by local repair or change than the downtime is equal with the one way travelling time+ repair time

$$L=L_t+L_0$$

Using this letters

$$DTR=nL$$

If n is given in event/year and L in hours/ event, then $DTR=nL \times \frac{1}{8760}$, which is in general a small number. Therefore in the practice some times it is given in fit -5 which makes

$$DTR=10^9 \cdot \frac{n \cdot L}{8760} \cdot 10^5 n \cdot L \text{ (fits)}$$

For calculation the number of the maintenance staff or maintenance groups we must use the double of the travelling time, because in general before coming the next task, they return to the basis. If the maintenance is organized based on real time management using mobilecommunication, than the travelling time can be reduced. In that case it is possible to send that group to the next failure which is in the nearest position to the required place and they can reach it by car quite rapidly. This system is extremely usefull if in the car can be find hardware and spare unit for any possible failure or at least for the most often occuring problems. There are computer-programmes which support the optimizing the amount of spare units and the routing of the cars. The telecommunication network is based on the use of highly reliable equipments where the propability of two failures on the same day in a maintenance area is less than 10^{-4} so the consecutive fault clearing is acceptable.

If there is no automatically switched redundancy or self-healing structure than the engineering is based on $DTR=n(L_1 + L_0)$ overage workingtime should be minimum. From this can be calculated the optimal number of the maintenance group, the area belonging to one maintenance group minimizing the travelling time and giving a limit of three hour down-time. In general circles with 50-60 km radius makes possible an acceptable service. Depending of the amount of equipments can be defined the number of groups on this bases.

If there are new systems in the network on the territory the availability must be repland. The new plan must be fitted to the failure rate of the new systems and to the reduced fault-clearing time. If the network is overdimensioned than the failure is not causing disturbing traffic congestions so that the outage is not in close co-relation with the service impairment. In the acces network there is no alternative route and is

not possible overdimensioning so here a special fault monitoring can help in offering a service-level, defined by the SLA (Service Level Agreement).

In special cases (banking, technology supporting, ambulance, emergency services) the terminal can be connected to more than one switching center, so the failure of the access line or the local switching or routing point can be bypassed. Another method is to have simultaneously wire-line and wireless connection substituting each other.

Summarizing we can see that improvement of the network availability can be achieved by higher investments or maintenance costs. The customer can decide that which is minimum availability which is necessary for his job. Comparing it with the higher tariffs or rental price he can find the best compromise. Here it must be emphasized that cost (A) is not a linear function. (Figure 7.3.1)

7.4. Network Element Mangement and Network Management

József Wiener, author

Kornél Terplán, reviewer

In the last decade, more and more services are added to the traditional telephone services, and demand for transfer of high-bandwidth data like video has increased. The ability to deliver voice, video and data at higher speeds are becoming a critical requirement. Now, telecommunications networks have to integrate different computer networks with different bandwidth demands. The growing Internet, its different nature as of the traffic also generates new requirements for Network Operators and Service Providers.

In order to be able to carry different kinds of data at a faster rate, quite new technologies and significant improvements to the existing technologies and protocols have been and still are being introduced. Standards for Synchronous Digital Hierarchy (SDH), Asynchronous Transfer Mode (ATM), Digital Subscriber Line (xDSL) are well established, but implementations are at different stages at different Network Operators. Due to this facts and the rapidly changing demands, migration from the plain old telephone service (POTS) has to be realized very quickly.

Recently, fiber optics, wireless mobile communications have added their own complexity and speeds quite different from that of POTS. Telecommunication equipment shall be able to handle a variety of traffic in natures, speed instead of only voice.

The complex and diverse equipment and service portfolio, their fast change makes controlling networks, resources and services a very complicated task. This problem can be solved by using modern computer technology and by as much automatization as possible.

7.4.1. What is Network Management?

Probably anyone who has worked with a telecommunications network has a different concept on this subject.

Telecommunications Network Operating Organizations have invested significant amount of time, money and human resources into building their complex telecom networks that need to be maintained. Network Management can be identified as the process of controlling the telecom network in order to maximize its efficiency and productivity. This process includes data collection from the network (either manually or preferably automatically), processing the data and presenting it to the staff operating the network. As the importance of Service Management is increasing, Network Management shall also pre-process data for Service Management, and shall transfer it to higher levels (Service Management and Business Management) Systems.

During the last few years, there has been a major paradigm change in telecommunications. In many countries, deregulation led to strong, sometimes very aggressive competition amongst telecommunication service providers. Deregulation also allowed service providers to expand their activities outside their traditional areas, even beyond their own national borders. This globalization tendency has also increased competition.

Proprietary network management cannot provide interoperability between diverse technologies, equipment and networks deployed by different manufacturers and proprietary management solutions having different features and different level of management capabilities. The gap can theoretically be overbridged by human resources. However, the speed that can be provided by human resources is often not fast enough to provide the contracted level of service for the customer.

As it is known, there exists a so called "skill pyramid" (Figure7.4.1). This means that the higher skill is needed, the less staff is available. Also, the expenses of

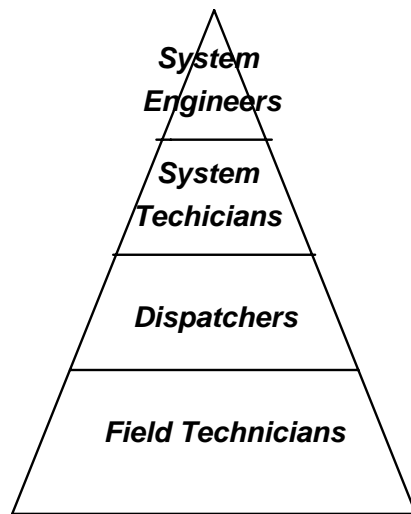


Figure 7.4.1. The Skill pyramid

training and salaries are increasing for the higher skill. The diverse and more and more complex technologies would need more skilled staff, but economic operations and efficiency would require less - no doubt that the requirements for more economic operations are the stronger ones, and companies can hire less skilled persons. Consequently, less and less staff shall run the bigger and bigger and more and more complex networks as well as services.

As a consequence, Network Management (NM) is becoming more and more critical. The essential idea behind NM is to replace human resources by computers in order to automate and speed up processes.

Proprietary network management solutions are usually working well with the manufacturers own equipment, but cannot provide interoperability between diverse technologies, diverse network management and service management solutions. This is driving the need for standard NM solutions important and urgent.

Legacy (proprietary) network management systems generate another problem, as high amount of money and human resources have been invested into these systems. It is difficult to discard solutions that are working and into which heavy investments were made.

This necessitates that legacy systems will coexist with the new standard network management solutions, and standardization work shall take into consideration this necessity.

7.4.2. Process Orientation

The Importance of Service

The core of a communications service provider is the service itself. The key objectives are 'more for less' - faster service introduction and provisioning, improved quality of service at a lower cost. These objectives can only be achieved through automation of customer care and operational support processes, and a strong automated linkage between the management of customer service offerings and the underlying networking assets. The level of customer service provided and the level of automation in the current environment of almost all Service Providers is much lower

than expected and lower than what providers need to remain competitive. Business process-driven approach

.Service Providers and Network Operators need to automate their business processes, which means information needs to flow from end-to-end across many different systems. All the activities, all the processes inside the Network Operator and Service Provider shall support the Business Processes; Network Management, Service Management, Marketing, Procurement, etc. shall collaborate with these Business Processes

A Business Reference Model

The Business Reference Model shown in Figure 7.4.2 is the basis for management. It illustrates the principal points of contact between a service provider, its customers, its suppliers and other service providers. A wide range of automation and integration opportunities exists among the business roles and relationships shown.

7.4.3. TMN (Telecommunication Management Network)

In telecommunications, and especially in the telecommunication industry, TMN (Telecommunications Management Network) is a loosely used term covering all kinds of network management solutions. In the strict meaning, however, TMN refers "only" to network management solutions that conform to the standards of ITU-T.

The legacy management solutions of telecommunication equipment manufacturers were good enough for limited services and limited geographic areas covered by their products. Because of the regulatory and protected environment, network operators & service providers had time and could control the introduction and implementation of new technologies and solutions.

The TMN model is a way to think logically about how the business of a service provider is managed. The TMN model consists of five layers, usually arranged in a triangle or pyramid (Figure 7.4.3). Business Management is at the top, Service Management is the second layer, Network Management is the third layer, and Element Management the fourth layer with the physical network elements is represented in the bottom layer.

The concept is that management decisions at each layer are different but interrelated. For example, detailed information is needed to keep a switch operating (at the element management layer), but only a subset of that information is needed to keep the network

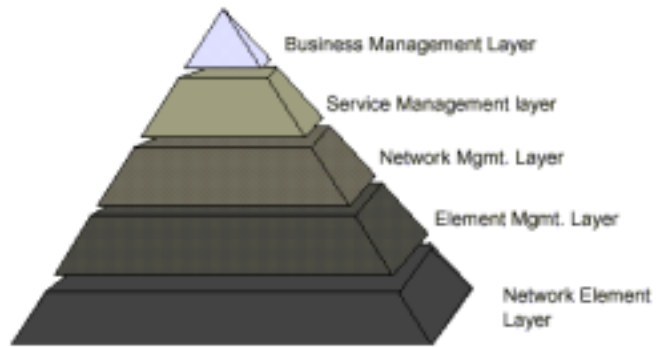


Figure 7.4.3. The TMN Model

operating (e.g. is the switch operating at full capacity). Working from the top down, each layer imposes requirements on the layer below. Working from the bottom up, each layer provides capabilities to the layer above.

TMN specifies a layered architecture for management of telecommunications networks. It deals with the monitoring, control and coordination of the resources in the network (resources are any components of the network, providing services - including equipment, software, hardware and customers). Some functions of TMN are:

- Remote management of systems components, hardware and software involved in providing services to customers - like voice, video, IN services, Internet, data communications, etc.
- Providing easy interfaces and easy interactions with customers in order to configure their services. This interface has to take into account the different skill levels of the end users as well as the operators.
- Providing automation in discovering and fixing problems. This also includes self-healing and self-correction in networks.
- Achieving seamless integration and management of legacy equipment and protocols with the new equipment and protocols.

Not only hardware, but also software is used to enhance the functionality of telecom equipment. This software and TMN (software) applications themselves have also to be managed.

7.4.4. Systems Management Functional Areas

To perform the management tasks, network management consists of five functional areas:

- **F**ault management covers the detection, isolation by diagnosis and analysis, and correction of problems in the network. Fault Management also covers reporting and problem tracking e.g. by Trouble Tickets.
- **C**onfiguration Management is used to keep track of resources in the network. This includes not only configuring equipment, but also covers areas such as view management, topology management, software management, inventory management and provisioning.
- **A**ccounting Management covers the usage of resources, controlled collection of data on the usage and charging for the usage.
- **P**erformance Management covers performance data collection, analysis of performance data and reporting of problems. Performance management is also concerned with the behaviour and evaluation of the effectiveness of resources.
- **S**ecurity Management function covers detecting and reporting security violations, creating, deleting and maintaining security-related services such as encryption, key management and access control. Distributing passwords and secret keys is also a function of security management.

These five areas are sometimes referred to as FCAPS, and the five categories are called Management Functional Areas (MFAs).

7.4.5. TMN Architecture and Functional Grouping

TMN needs an application architecture for the software of network element, network and service management software. Management functions are generally performed by distributed computing.

For the purpose of realisation, the ITU-T Telecommunication Network Management (TMN) information architecture shall be decomposed to a set of traceable requirements and explained in the form of possible to a way of considering practical implementation issues. This division makes possible the use of the standards in the industry as a set of requirements for componentized distributed computing in general.

Due to the endorsement of a layered TMN architecture in the industry, a telecommunications management building block

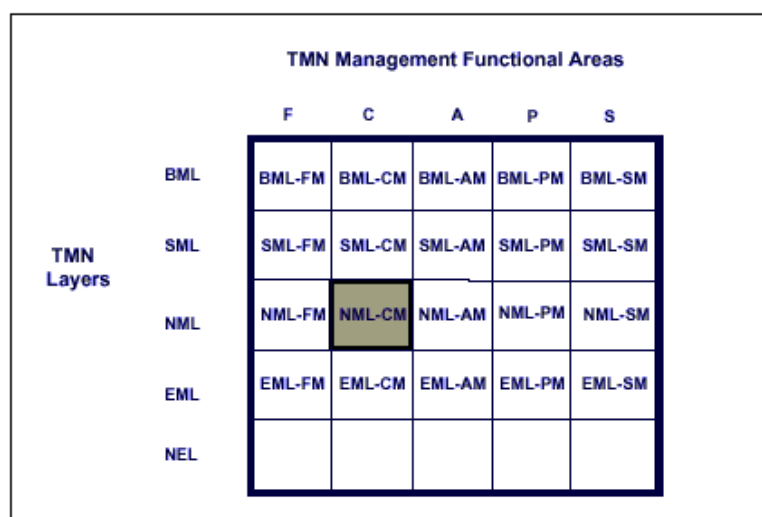


Figure 7.4.4. Layering and Grouping

must contain functions from only a single TMN layer and from a single TMN management functional area. This granularity requirement, constraining the maximum range of functionality of a telecommunications management building block, is here stated in terms of well-accepted layered architecture from the telecommunications management industry.

TMN formally requires a separation between the layers. These layers are separating the main areas of the business as operating the network (Network Elements & Element Management), managing the network (Network Management), Managing the Services provided for the customers (Service Management) and Managing the Business (Business Management). This well known layering is depicted on Figure 7.4.4.

In actual practice, it will often be found that each MFA would be implemented most conveniently as several building block types. For example, EML-FM contains element managers both for network alarm surveillance and for network test equipment. These element managers have different clients on the NML and different scaling and distribution issues. Implementing them separately makes it possible to deal with each of them in the most optimal manner.

7.4.6. TOM - Telemanagement Forum's Telecommunication Operation Map

The TMN model is simple, although its implementation is complex. The big number of standards now available that address the various interfaces between management systems sometimes makes it difficult to see and appreciate the whole picture. TMN Management Functions provides a structure and decomposition of functions for all of the layers. However, those ITU-T standards that specify information models and interfaces have been mainly concentrated on the management and connection of resources to the Network Element Layer. Until recently, little attention has been given to interface specifications and information models within the TMN. Consequently, it is difficult to apply the standards to a complete business case, such as for the procurement of a specific Operations Support System. It is also difficult to apply a customer centric focus on the processes that really respond to the customer needs.

The Telecom Operations Map (TOM), using the TMN model as a foundation, addresses operations support and management for any communications service from a top down, end-to-end process and customer oriented standpoint.

The TOM (Figure 7.4.5.) serves as the blueprint for process direction. It is also the starting point for development and integration of Business and Operations Support Systems (OSS). It consists of:

- A high-level view of Communications Operations processes, sub-processes and activities that is top down, customer-centric, and end-to-end focused;
- A high-level identification of the primary end-to-end processes of fulfillment, assurance, and billing, and sub-processes;
- Illustrative examples of process flows that show end-to-end processes;
- A more detailed view of the functions of each sub-process, including activities of each sub-process box, as well as its inputs and outputs to other sub-process boxes.

The Telecom Operations Map uses the layers of the ITU-T TMN model to organize core business processes, but divides the Service Management layer into 2 parts:

The first is Customer Care, the second is Service Development and Operations Processes. In the simplest sense, this division reflects differences between processes triggered by individual customer needs from those applied to a group of customers subscribed to a single service or service family. These processes are responsible for ensuring that the network and

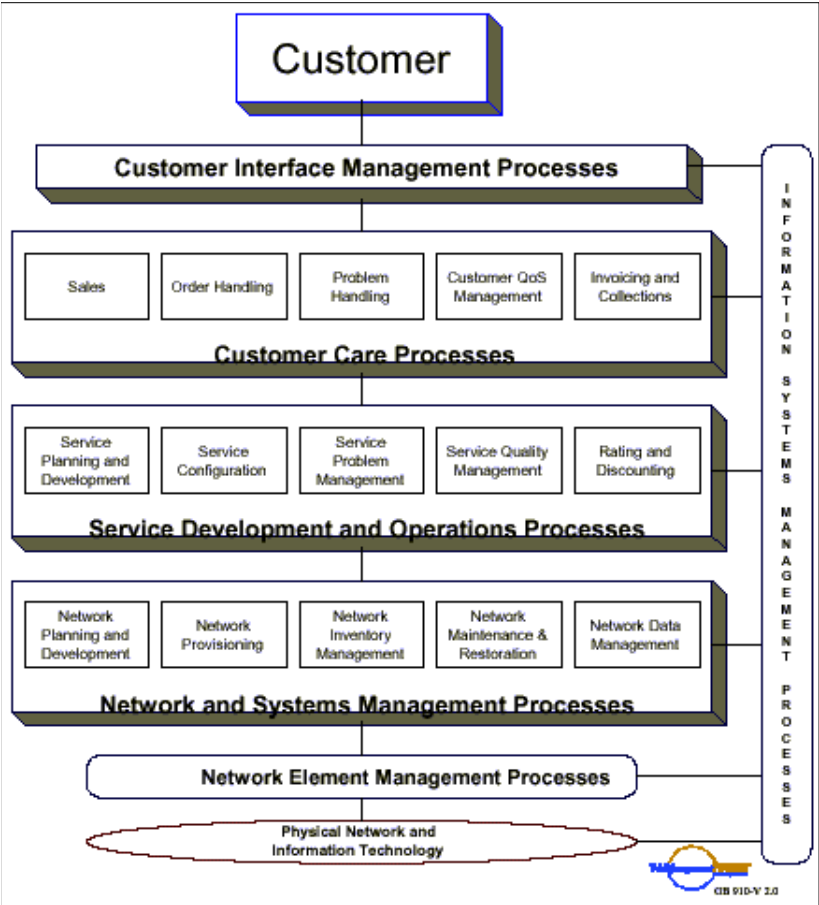


Figure 7.4.5. Illustration of TOM's Processes

information technologies infrastructure supports the end-to-end delivery of the required services.

Network and Systems Management is also the integration layer between the Element Management Layer and the Service Management Layer. Its basic function is to assemble information from the Element Management systems, and then integrate, correlate, and in many cases, summarize that data to pass on the relevant information to Service Management systems or to take action in the network.

7.4.7. Network Management Operations Map

As it was shown, Network Management Processes are part of the TOM. Network Management Processes are detailed further in the Network Management Operation Map. These processes and the relationship to TMN is shown on Figure

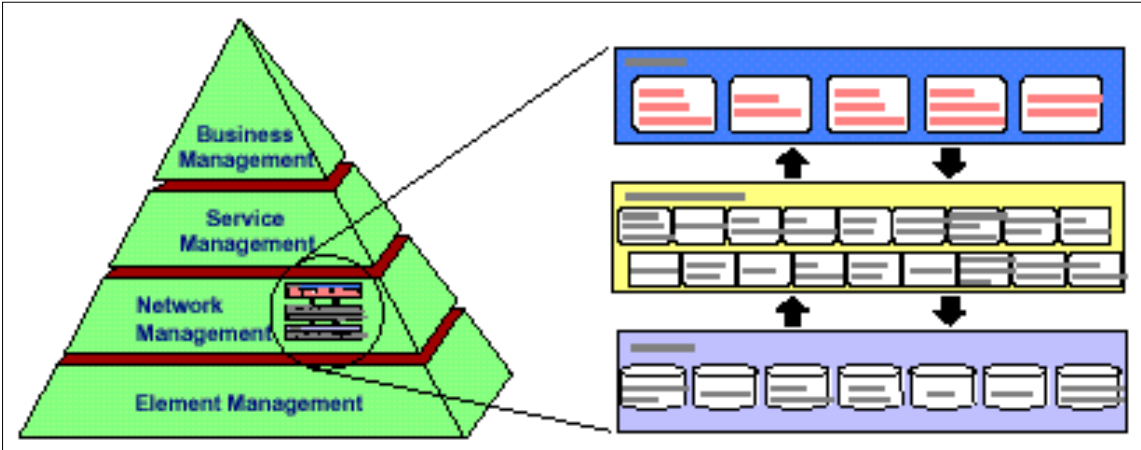


Figure 7.4.6.

Positioning the Network Management Detailed Operations Map within TMN

7.4.6

7.4.8. Element Management and Network Management

Element Management and Element management systems (EMS)

The telecom network consists of Network Elements (Equipment). *Equipment* or *Network Elements* (NEs) is the short term for the basic infrastructure, i.e. the hardware and software components of the network. In the usual case, equipment is vendor-specific to a large extent. For billing, this means that the raw accounting data

is delivered often in a vendor-specific format and reflects the functionality of the elements actually used.

The *Element Management System (EMS)* represents the hardware and software components used by the Service Provider or Network Operator to manage one or more Network Elements (NEs). The EMS provides management across a subnetwork or a single NE, typically across a single vendor equipment or collection of single vendor equipment. The NMS performs management functions across the Element Management Layer (EML) of the TMN. Some examples of these management functions include provisioning of NE resources and collection of NE faults.

Full separation of the MFAs on the EML is problematic with the current generation of network elements (NEs). Some NEs can connect to only one or two management facilities. This will require EML building blocks managing different aspects of an NE to share an element of common infrastructure. This common element will communicate directly with the NE then forward the information appropriately to the various EML building blocks according to their respective management interests. Additionally, the EML mediation function, which brings various NE management protocols from different vendors to a common view, might be performed most conveniently at a single point. This common single point of NE contact can be implemented either as an EML mediation building block, which will require open contracts, or as infrastructure, which can be vendor proprietary.

Network Management System (NMS)

The *Network Management System* represents the hardware and software components used by the Service Provider or Network Provider to manage their networks as a whole. The NMS provides an end-to-end network view of the entire network enabling management of the NEs contained in the network. These NEs managed across the network are typically provided by multiple vendors. The NMS performs management functions across the Network Management Layer (NML) of the TMN. Some examples of these management functions include connection management and circuit fault correlation.

Network Management is more than just a mediator between the EML and SML. Network Management processes have their own responsibilities; for example,

- Network Planning and Development (assuring complete infrastructure exists);
- Network Provisioning (implementing the infrastructure);
- Network Inventory, maintaining status of network assets;
- Management (implementation and administration of the physical network);
- Network Maintenance and Restoration (assuring availability and maintenance of the infrastructure) and
- Network Data Management (collects data to manage the network and provide billing records).

The important issue is that management responsibility will be placed at a level where adequate information is present, instead of shifting all responsibilities to Service Management.

The Network and Systems Management processes manage the complete service provider network and sub-network architecture.

NML-EML Interface

The composition of today's networks has contributed to the complexity of managing these networks. These networks are commonly composed of network elements provided by various vendors. The task of interoperability extends beyond the network element layer up to the management layers, to include interoperability between multi-vendor Element and Network Management Systems.

Service Providers have also taken advantage of technological advancements in transport network equipment. It is not uncommon for service providers to deploy next generation, multi-technology network elements, (or "hybrid NEs"), as these network elements provide new services and optimal network resource utilization. However, existing network management solutions that have been specified to date apply only to a specific technology.

There is an industry demand for a full-featured, commercially available, scalable and non-proprietary network management solution, where multi-vendor, multi-technology management systems

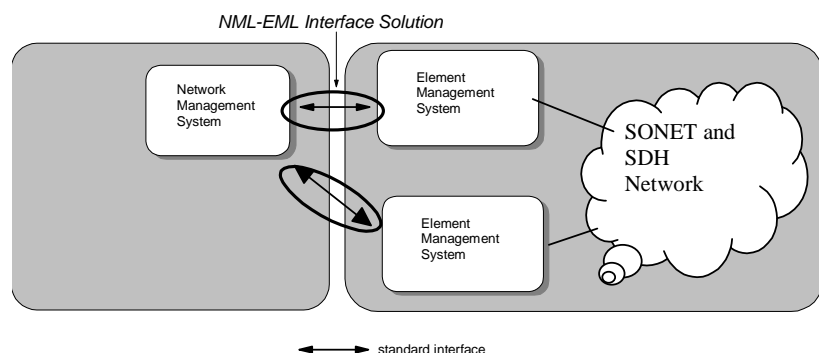


Figure 7.4.7. NML-EML Interface

interoperate in an open architecture environment.

The *NML-EML Interface* (Figure 7.4.7.) represents the communication data and exchange mechanism between the management system(s) that deploy the NML and EML functions of the TMN. A Network Management System (NMS) that performs NML functionalities may communicate with one or more Element Management Systems (EMSs) that performs EML functionalities via the NML-EML Interface.

Structuring the EML and NML Layers

Traditionally, Element Management level within the TMN Architecture has been used as the boundary for containing the technology specific management capabilities whilst giving a generic view of the network to the higher management layers (e.g., NML, SML etc.). Such a boundary is adequate for managing individual technologies but leaves much of the integration across technologies to be undertaken by the Service Providers/Network Operators. Increasingly, Service Providers/Network Operators seek solutions from the Equipment Suppliers in the form of complete Sub-Networks. Such Sub-Networks may consist of a range of technologies (Routers, Switches, etc. in an IP network) from multiple vendors.

In practice, the distribution of functionality may vary significantly between Element Management and Network Management Layers. One example is shown on

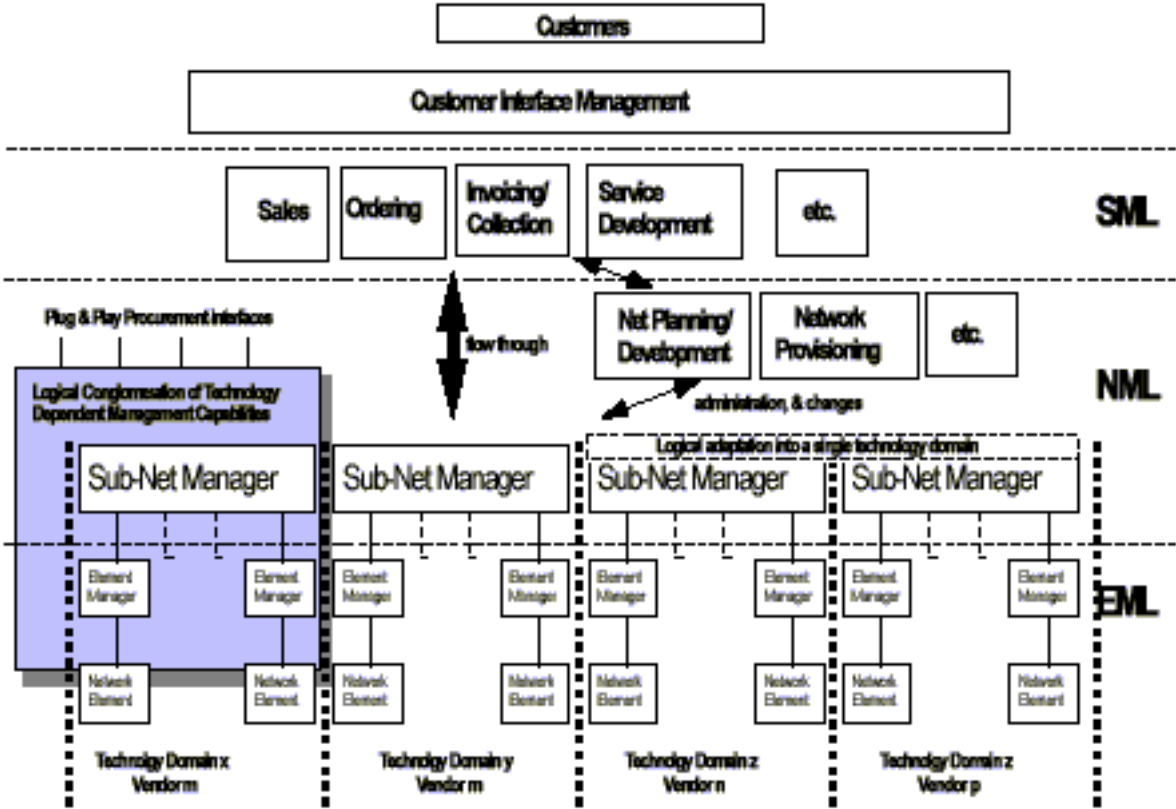


Figure 7.4.8. Structuring the Network Management Layer

Figure 7.4.8. The functional areas can be encapsulated as blocks of functionality within the TOM. The chosen functional blocks can reflect the distinction between generic and technology-specific management indicated above. The functional blocks shown in Figure 7.4.8. have been chosen to distinguish Network Management capabilities associated with Element Managers (at the node level) and Sub-Network Manager(s) (for some managed network area or domain).

The partitioning Network Management Layer into Generic and Sub-Network specific components and providing ‘plug and play’ type interfaces at the Sub-Network level can also be reached this way.

Note that this is only one possible structuring. Currently, there is no industry wide agreement on such a partitioning. Procurement by Service Providers of managed network technology is often based on a combination of Element Management and some aspects of Network Management packaged into this type of Sub-Network Management. This allows the managed Sub-Network domain to be accessed as a network area, rather than just a series of individual network nodes. The Sub-Network might be defined:

- on the basis that it employs a particular network technology (e.g. SDH or ATM), with its associated management, and is procured as a package;
- on the basis of geographical partitioning;

This can be done as specific areas of management functionality are supported, and different organizations have different needs.

7.4.9. Network Management Relationships

The following interactions impact Network Management processes and directly drive the need for interface specifications in the form of information agreements that may need to be automated.

Interactions with Service Management

This is one of the primary relationships for Network Management and acts as the main source of requests for information and actions to execute tasks. Service Management is responsible for managing the customers’ perspective for each individual service provided, normally against some type of contractual agreement.

Thus, its purpose is to ‘act on behalf of the customer’ for interactions with Network Management.

Interactions with Suppliers or with Supplier-provided Equipment

Most traditional Service Providers own and operate networks in order to deliver their services. Certainly, the service delivery chain will always include at least one Provider which takes on this Network Operator role. For these Provider/Operators, the network operations task is an internal business function rather than a point of external interface. However, since most Service Providers do not manufacture their own network equipment, they are reliant on the equipment suppliers, from whom they procure, to help them achieve their automation goals. The ability for devices to be configured in a common way, for example, or to provide alarm or performance data using common formats and terms, is critical to achieving the full benefits of service and network management automation. To get the most from automation efforts, procured equipment must be able to receive and act on common high-level instructions, and deliver performance and usage-related information in a common way, that meets the Providers' requirements.

Interaction with Customers

Most Service Providers see a need for automated management links with their Customers, at least with some types of Customers, and/or for some types of services. These interactions occur mainly with Service Management, which act as a proxy for the customers' needs to Network Management.

Interactions with Other Providers

World-wide alliances and regulatory actions are generating increasing volumes of interactions between Service Providers. Today, these often involve manual intervention, representing an unacceptable cost and often significantly degrading service quality to the Customer.

Some of the interactions between Providers may be similar in content to the interactions between a Provider and a Customer. However, it is likely that the volumes of transactions, the level of detail required, and the speed with which

information needs to be exchanged between Providers will dictate substantially different implementation agreements.

7.5. Service Management In Telecom Networks

József Wiener, author

Kornél Terplán, reviewer

As the communications industry continues to evolve with deregulation and liberalization, service providers are under increased pressure to deliver a broadened set of services at a competitive price. As a result, service providers must deliver these services in an cost-effective and timely manner. The ability to effectively manage these networks become key in retaining existing, as well as acquiring new market share. However, the complexities surrounding today's networks present challenges in achieving the effective network management goal.

7.5.1. Role of Service Management

The core of a communications services provider is service. The key objectives are 'more for less' - faster service introduction, improved quality of service at a lower cost. These objectives can only be achieved through automation of customer care and operational support processes, and a strong automated linkage between the management of customer service offerings and the underlying networking assets.

Both the level of customer service provided and the level of automation in the current environment of almost all Service Providers is much lower than expected and lower than what providers need to remain competitive. Many Service Providers are now actively engaged in re-engineering their business processes for maximum efficiency and effectiveness. The effective exploitation of this network infrastructure, whether directly operated or outsourced, is an integral part of the service delivery chain and directly influences the service quality and cost perceived by the end customer.

The idea is that the End Customer develops telecommunication service quality requirements necessary to operate their business. These requirements are brought to the Service Provider and the two parties begin to assemble the optimum set of SLA parameters and values for the services.

The two parties (Customer and Service Provider) may be an 'end' Customer and their Service Provider (SP) or two Service Providers, where one Service Provider has the Customer role buying support services from another Service Provider (e.g. who may be acting as a network operator).

The agreed-upon SLA requirements flow down through the organizations of the associated SP(s) and become the basis for internal management processes and QoS values. Customer satisfaction is improved by identifying the implications for supporting the service by the internal support infrastructure(s) of both the SP and the Customer.

7.5.2. Quality of Service (QoS)

By definition, Quality of Service (QoS) is the collective effect of service performances which determines the degree of satisfaction of a user of the service. The quality of service is characterized by the combined aspects of service support performance, service operability performance, service integrity and other factors specific to each service (ITU-T Rec. E.800).

The SLA QoS parameters support a contract between two parties. It is important to note that there is a distinct difference between the user/service QoS requirements defined in the SLA and the network level QoS.

Quality of Service (from SLA point of view) is the measure of the service quality defined for a service and provided to a customer. QoS is the definition of the performance parameters used to assess service quality. The parameters are usually associated with a specific service or service type. Traditionally, the term QoS is used to refer to performance related parameters. Some use QoS to mean the quality of service for all aspects of the service, e.g., network performance measures and Completion On Time, Call Pick-up Time, etc. QoS can be subjective, e.g., is a call easy to hear for voice, or objective, e.g., Cell Error Ratio for ATM.

Defining QoS is easiest with digital circuits. QoS for IP Services is getting a lot of attention, since it is a connectionless service that is hard to measure and since QoS for IP Services came from the IT arena, i.e. the "best effort" delivery model.

The SLA should include clear and unambiguous definitions of the following:

- The measurable QoS metrics and parameters that can be guaranteed by the SP for a specific service in terms that the Customer can understand and agree to.
- Service performance measurement method, measurement period, reporting period and reporting frequency.
- Customer and SP responsibilities, e.g. maintaining relevant hardware and software.
- SP procedures to be invoked on violation of SLA guarantees.
- Any conditions that affect operability/commitment to support.
- Selection of the type of reports associated with the service, specifying each report's contents, format, destination, conditions and delivery media.
- Service definitions for each service covered by the SLA.
- Process for handling the defined boundary conditions.
- Service cover time, i.e. the limits of SP support for different times of the day/week/month/year, etc.
- Dispute resolution procedures.

For any service the Customer should be able to select:

- Parameters to guarantee.
- Value ranges for the parameters.

7.5.3. Service Level Agreement

The SLA is a formal negotiated agreement (contract) between the two parties, and it is designed to create a common understanding about service quality, priorities, responsibilities, etc. SLAs can cover many aspects of the relationship between the Customer and the SP, such as performance of services, customer care, billing, service provisioning, etc.

Although an SLA can cover such aspects, agreement on the level of service is the primary purpose of a SLA. The focus is therefore on the management of the SLA and the Quality of Service (QoS) that is agreed upon in the SLA.

The parameter categories in the SLA are 1) technology-specific, 2) service-specific and 3) technology/service-independent. The Customer has two interests: 1) impact on the single user and 2) aggregate performance for a defined period.

An SLA, in many cases, is part of or an addendum to the contract with the customer. It defines the service provided and the set of metrics to be used to

measure the level of service committed against the level of service provided. Such service levels might include network performance metrics, installation completion on time metrics and intervals for new orders, availability, call pick up times at a work center, maximum periods of outage, average and minimum throughput, etc. The SLA also frequently defines trouble reporting and escalation procedures, reporting requirements and the general responsibilities of both parties.

7.5.4. Relationship to the Telemangement Forum’s Telecom Operations Map

Service providers must apply a customer-oriented and service management approach, using business process management methodologies, to cost effectively manage their businesses and deliver the service and quality customers require. To manage within a service

provider’s value chain, a common process framework is required. The TOM (Figure 7.5.1) uses the layers of the ITU-T TMN model to organize core business processes, but divides the Service Management layer into 2 parts: Customer Care and Service Development and Operations Processes. In

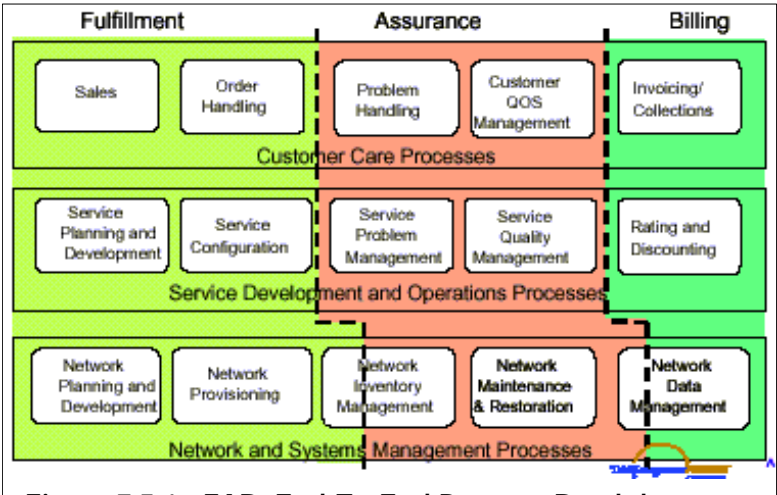


Figure 7.5.1: ‘FAB’ End-To-End Process Breakdown (FAB = Fulfillment, Assurance, Billing)

Note: The interface to element management systems and the physical network are not shown for simplicity.

the simplest sense, the division reflects differences between processes triggered by individual customer needs from those applied to a group of customers subscribed to a single service or service family. It also reflects the accountability for direct customer contact handling in Customer Care Processes and the critical need to focus on integration and automation of and in support of Customer Care Processes.

7.5.5. Service Development and Operations Processes

The Service Development and Operations Processes are on middle row of the TOM (See Figure 7.5.1).

These processes focus is on service delivery and management. Some of these functions are done on a one-time basis, like designing and developing a new service or feature. Other functions involve service capacity planning, the application of a service design to specific customers or managing service improvement initiatives, and are closely connected with the day-to-day customer experience.

Service Planning and Development Process

The process begins with the need for new service, feature, other concept/requirement, or a shortage of capacity. Triggers may come from customers, or from different departments of the company. It ends with introduction of the new service, feature, added capacity, including being able to sell, order, maintain, bill, report on and meet or exceed service quality, performance and cost targets.

This process encompasses:

- Designing capabilities to meet specified market need(s) at desired cost. This can be a new service, new feature, service enhancement, upgrade or maintenance related.
- Ensuring that the service (product) can be properly installed, monitored, controlled, and billed.
- Initiating appropriate process and methods modifications, as well as changes to levels of operations personnel and assuring required training is performed.
- Initiating any modifications to the underlying network or information systems to support the service requirements.
- Performing preservice testing to confirm that the technical capability works and that the operational support processes and systems function properly.
- Ensuring that sufficient capacity is available to meet sale forecasts.

Service Configuration Process

This process encompasses the installation and/or configuration of service for specific customers, including the installation/configuration of customer premises equipment. It also supports the re-configuration of service (either due to customer demand or problem resolution) after the initial service installation. Also,

reconfiguring the network to meet new demands and increase capacity may be part of this process, and such Service Configuration work would not be tied to configuring a specific customer instance for those cases. The aim is to correctly provide service configuration or re-configuration, including connection management activities, within the timeframe required.

Offering IP-based services, additional functions must be considered. Firewall, application services such as e-mail, web-hosting and their handling is important. Also, setting QoS and SLA parameters shall be performed.

Service Problem Management Process

This process encompasses reporting on service problems and trouble performance, isolating the root cause of service-affecting and non-service-affecting failures and acting to resolve them. Typically, failures reported to this process affect multiple customers. Actions may include immediate reconfiguration or other corrective action. Longer-term modifications to the service design or to the network or information technology components associated with the service may also be required. The aim is to understand the causes impacting service performance and to implement immediate fixes or identify quality improvement efforts required. The task include

- Isolate and resolve service problems
- Identify chronic failures
- Provide performance data
- Recommend service redesign, if appropriate
- Initiate escalation procedures
- Analyse service quality
- Generate reports about services

The process ends with the service problem rectified, improvements made, related development recommended or a decision made not to take action, and production of a root cause or other analysis reports.

Rating and Discounting Process

For a usage billed service, one of the essential activities of Rating and Discounting is to match usage to a customer record. As with other processes, some

providers provide rating and discounting functions for other providers as a service. For joint service arrangements, billing, invoicing, settlements and reconciliation between service providers may be involved.

The aim is to correctly apply charges, rate usage and to correctly apply discounts, promotions and credits. The process starts with registering a specific customer's identifiers for matching to usage and appropriate discounts, charges and/or credits. It ends with providing correct information for the billing invoice

7.5.6. Service Quality Management Process

This is a sub-process of the Service Development and Operations Processes, but due to its importance, it is discussed in this separate chapter.

This process supports monitoring service or product quality and cost on a service class basis in order to determine whether

- Service levels are being met consistently
- There are any problems with the service or product or any improvements are needed,
- The sale and use of the service is tracking to forecasts

This process also encompasses taking appropriate actions to keep service levels within agreed targets for each service class and to either keep ahead of demand or alert the Sales Process to slow sales. If improvements are required to the service or the infrastructure to maintain or improve service results, this process provides recommendations and tracks that approved developments are completed and/or that other required actions are completed. The aim is to provide effective service specific monitoring, to provide meaningful and timely performance information and to ensure service performance meets or exceeds commitments. This information can be used for specific customers (to internal management and customers, through the Customer QoS Process). The aim includes the monitoring, analysis, and reporting of service levels to meet SLA commitments or to meet standard commitments for the specific service or service class.

The Service Quality Management Process manages the service from first service to retirement of the service. Therefore, the process begins with Service

Introduction and includes the effective and efficient management and reporting of service results to meet or exceed the committed operations objectives.

The process include several sub-processes. Division of the process into sub-processes may depend on the Service/Network Provider. Two of them (Life-cycle Management and Maintaning SLA) are discussed in the following chapters.

7.5.7. The Life Cycle of the Service

To clarify the roles of the Customer and the SP, a Service and its SLA is divided into five Life Cycle stages: product/service development, negotiation and sales, implementation, execution, assessment. Each life cycle stage addresses specific operations processes in the *Telecom Operations Map* (Figure 7.5.1). The SLA Life Cycle provides a complete process description by delineating interactions between well-defined stages.

The Service Management processes form a longer periodicity lifecycle driven by the introduction, modification, and withdrawal of different service products (or ‘classes’ of service).

This lifecycle involves creating the specific policies, rules, process, and data templates used to configure and select service products the Customer Care process can utilize.

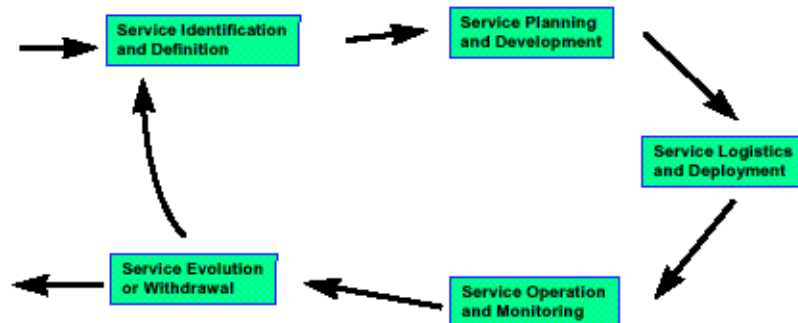


Figure 7.5.2
Typical Service Management Lifecycle

While there can be many combinations in how a particular company will segment and name their particular processes and methods, the overall lifecycle will generally contain many of the same steps. Figure 7.5.2. gives a typical view.

7.5.8. Maintain Service Level Agreements

Customers are interested first of all service-dependent metrics that are technology independent. This means, that technology-dependent metrics need not to

be included in the SLA, only if the service can exclusively be provided by one technology.

Service/technology-independent QoS parameters are those which are often (if not always) specified in a SLA. Examples include Percentage Availability, MTBF, MTTR, time to first yield, average call response time, etc. These are sometimes referred to as “operational performance criteria” and some are reportable by SPs to regulatory authorities on a regular basis, e.g. time to first yield.

Examples of service-specific QoS parameters

Some examples for service-specific QoS parameters are:

- **Voice telephony:** call connectivity and quality measures ABR/ASR/CCR/CSR/NER; network connection failures, Customer Affecting Incidents (CAIs), PSTN speech and 3.1 kHz audio loudness (speech level), attenuation, noise, crosstalk, echo, distortion; ISDN call set-up failures and delay, propagation delay (including differential delay between B-channels), G.821 error performance, premature release, release failure and delay, CLI reliability. With the increasing use of digital network technology, echo has become increasingly important, even for quite close destinations from a caller.
- **Voice over IP (VoIP):** delay and echo are two of the major hurdles to overcome.
- **Data:** BER, % EFS, errored PDUs, lost PDUs, UAS, Availability digital data parameters; loss, attenuation, group delay distortion, noise, impulse noise analog data parameters.
- **Facsimile:** image quality, character error rate, call cut-off, modem speed reduction, transaction time and availability.
- **Mobile telephony:** call completion rate, call dropout rate, noise, echo, distortion and availability.
- **Sound programme:** noise, crosstalk, stereo channel interference, distortion and availability.
- **Frame Relay Service:** It may include several parameters for access, plus per PVC parameters. For switched circuits, Customers negotiate other behavior based on the establishment of the SVC, Service Availability, Access Line Speed, Per VC Cell Rate (can be quite complex for non-real-time and real-time streams), Per VC Cell Propagation Delay, Per VC Cell Delay Variation, Per SVC Call Setup time, Per SVC Blocked Calls, Cell Error Ratio, Cell Loss Ratio
- **IP-VPN Service** - The following parameters may be part of the contract: Service Availability, IP Packet Transfer Delay, IP Packet Delay Variation (jitter), IP Packet Loss Ratio, IP Packet Error Ratio, Utilization.

Service Availability

Service Availability (SA) as a percentage (SA%) indicates the time during the contracted service at the Service Access Point (SAP) is operational. Operational means that the customer has the ability to use the service as specified in the SLA.

An event affecting the service at the SAP can be defined as an outage. The duration of the outage is outage interval. This concept is used for the unavailability percentage (UA%) and service availability percentage (SA%) calculations as follows (in the simplest case):

- $SA\% = 100\% - UA\%$,
- $UA\% = (\text{sum of outage intervals} / \text{activity time}) \times 100\%$.

Service Availability has three dimensions:

- Time dimension
- Site dimension
- Functional dimension

Time Dimension of Service Availability

Service availability is not only a simple sum of all the availability durations. In some cases, some time periods can be excluded from the calculations. An example is, if a shop is closed during the night, and no communication is needed at all, this duration can be excluded from the SLA calculation. An other example is, if the Service Provider and the Customer agree in a Maintenance Window, when the

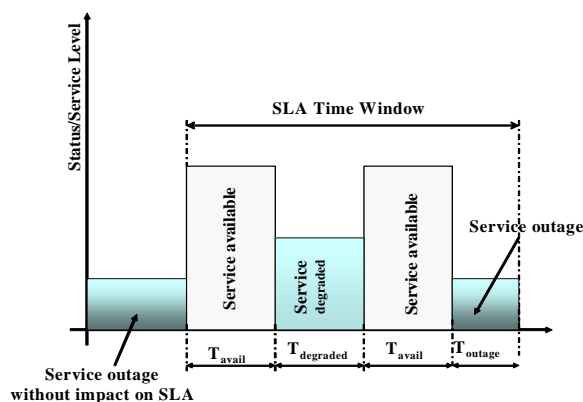


Figure 7.5.3. Time Division of Service Availability

Service Provider can perform scheduled maintenance work (conditions of having such Maintenance window shall also part of the SLA).

Figure 7.5.3. shows an example for this cases. There is also a situation on the figure, when the service is degraded for some reasons (e.g partial capacity or speed is available, performance degraded, etc.). Handling this situation in the SLA needs special attention from both parties. One possible solution is, eg. if this cases have some weights in the SLA calculations.

Site Dimension of Service Availability

Service Availability requirements may vary from site from site at a customer, depending on its importance, open/closed tiem, etc. This is shown on Figure 7.5.4.

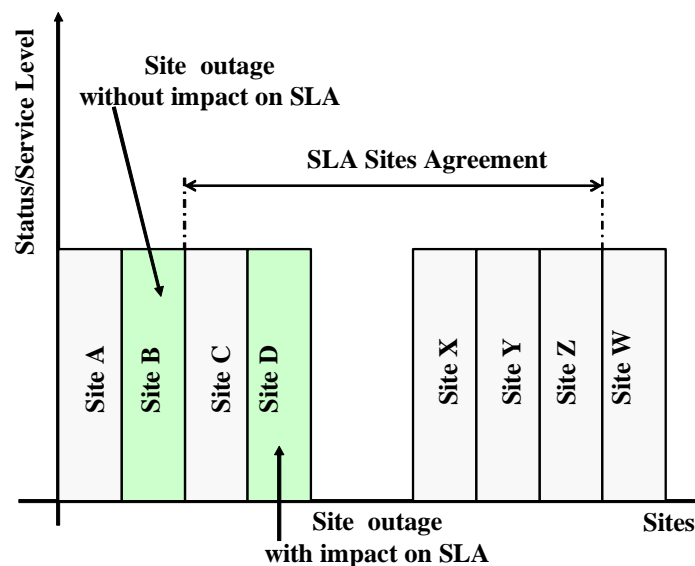


Figure 7.5.4. Site Dimension of Service Availability

Functional Dimension of Service Availability

Contracted and provided Service Availability may depend on the Function (Service) provided for the Customer. Some functions (Services) may be excluded from the SLA, others may have different weights when calculating the SLA (Figure 7.5.5)

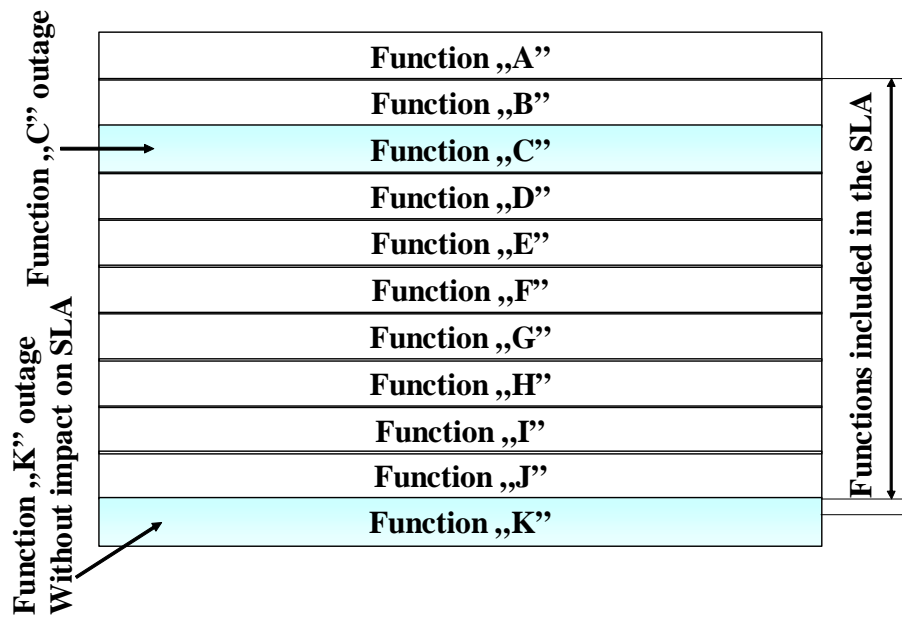


Figure 7.5.5. Functional Dimension of Service Availability

7.5.9. SLA Issues with IP-based Services

QoS is a key factor for the success of IP-based products and services. However, the approach is different from that of the traditional telecom services. This is due to the fact that it came from the IT world, and also as it is based (basically) on packet-switching.

Best Effort Service

This is basic connectivity with no guarantees. Although best effort service is the lack of QoS, it provides customers with a reference point on the nondistinct end of the spectrum. Also, best effort is suitable for a wide range of networked applications such as general file transfers and e-mail.

Differentiated Service

In this case, some traffic is treated better than the rest - faster handling, more bandwidth on average, lower loss on average. This is a statistical preference, not a hard and fast guarantee. With proper engineering, differentiated service can be provided and can be appropriate for a wide range of applications. Typically, it is

associated with grouping traffic into a small number of classes, each class receiving a particular QoS in the network.

Guaranteed Service

It means an absolute reservation of network resources for specific traffic. It usually concentrates on bandwidth. It implies reservation of buffer space along with the appropriate queuing disciplines to ensure that specific traffic gets a specific service level. Bandwidth is typically used for the other QoS attributes (jitter, delay) as the widest audience easily understands it. Bandwidth is often reserved down to the level of individual traffic flows, and this way particular flows have reserved resources. In other cases, aggregated flows may receive guaranteed service.

7.6. Traffic Management

József Wiener, author

Kornél Terplán, reviewer

The term traffic describes the flow of messages through a communications network, whether voice, data or video, analogue or digital. Traffic characteristics are influenced by many traffic metrics.

Traffic management in communications network deals with the controlled use of network resources to prevent the network from having a bottleneck. In particular, when more traffic are allocated to the network resources that they can effectively support, network performance for users degrades. Traffic management controls the user traffic generated by calls entering in and flowing through the network, and prevents the network from overload.

7.6.1. Traffic Control and Congestion Management

The operation by which user traffic is controlled is called flow control. Traffic control should assure that traffic does not saturate the network or exceed the network's capacity. Basically, there are three alternatives for flow control, both for traditional and new (emerging) technologies:

- **Explicit flow control:** This method limits the user traffic entering the network. The network limits this traffic by introducing an explicit control message, and either the user must stop sending traffic, or his traffic is forbidden to enter.
- **Implicit flow control:** This technique recommends that the user reduce or stop traffic sending to the network if network traffic exceeds a given value or network situation (e.g. problems in the net) needs control. One situation can be e.g. that the implicit flow control message is a warning to the user that the user is violating its service level agreement, and overloads the network or part of it.
- **No flow control (congestion control):** Flow control can be established by just discarding any traffic that is creating problems. This kind of control certainly provides perfect congestion management from the standpoint of the network, but may not meet the performance expectations of the user.

Based on these principles, different techniques can be used to control (to manage) the traffic. The actually applied techniques depend on the type of the

network and on several other parameters, some of them discussed later in this chapter.

7.6.2. Impact of Different Traffic Shapes

The way of performing the traffic control highly depends on the type of the technology, the network and the service provided on the network. Not so long ago, a phone call was, well, a phone call: people talked to each other. They still do, of course, racking up record POTS traffic, but this goes along with a growing amount of faxes, e-mails, data files, audio-messages, graphics and streaming video. And these newer forms of communications are being delivered over an equally wide selection of protocols — frame relay, ATM, IP, CDPD, GSM, as well as traditional TDM. This growing diversity of media and protocol types—which is (somewhat paradoxically) known as convergence is the governing principle of the broadband, multimedia era.

This diversity means different holding times, speed, sensitivity to delay, etc. i.e. different traffic patterns. For illustration, Figure 7.6.1. illustrates the nature and speed for different type of services and media.

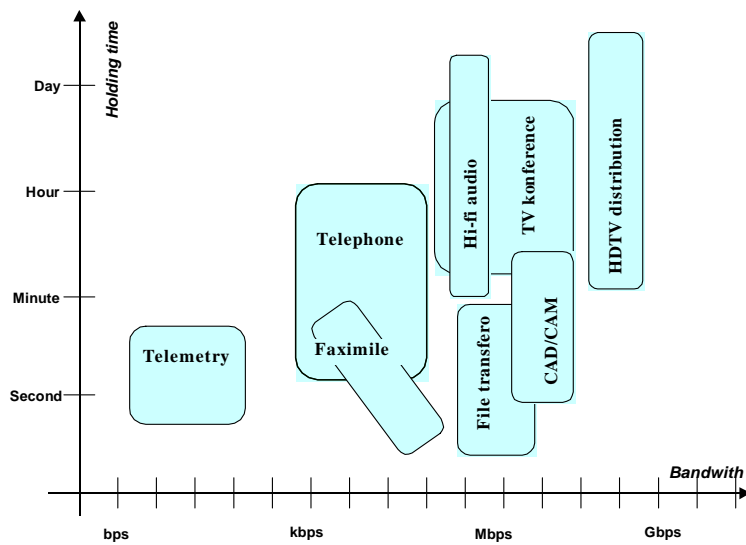


Figure 7.6.1. Traffic Characteristics for Different Telecomm Services

In the case of voice switches, control is applied at the input of the switch, but in the case of a router it can even be applied in the customer's router. It can easily be understood that different type of control can be effective at different speeds and

holding times, in case of circuit switched networks and packet switched networks, etc.

7.6.3. Traffic Management in Voice Network

In circuit-switched networks each connection is allocated a fixed amount of bandwidth, and a constant bit rate in the network is provided to communicating entities throughout the duration of the connection. For example, in a telephone network, each connection requires a 64 kbps channel. If a channel between the caller and the called parties exists, the connection is established, otherwise (e.g. if there is a congestion in the network) it is rejected.

Networks can be overloaded due to an unusually big number of call attempts, or network problems reducing the capacity of the network in some parts. An overload can be

- General network overload, when the entire network is saturated with calls, or
- Focused overload, when only a part of the network is overloaded - e.g. due to a radio-show, or any special event (catastrophe, visit of the pope, etc).

In order to control the network, abnormal conditions shall be detected, and some control methods shall be applied to the network. This action basically can be

- Protective control, when the amount of traffic entering the network is limited (the network is protected against extra load);
- Expansive control, when the extra traffic is re-routed from the source to the destination via areas that is not overloaded, and this way expanding the source-destination capacity of the network.

The theory of this kind of traffic management is well established, there are international (ITU-T) standards available, and there are several practical methods and systems performing such kind of Traffic Management.

The benefits of traffic control in the telephony network is shown by some real examples.

Fig 7.6.2. shows a situation when due to some exchange failures, the completed calls between two exchanges are dramatically reduced. The upper, „floating” curve shows the number of offered traffic (seizures), the „U-like” shows the completed calls. The area between the curves is clearly a loss for the Operator/Service Provider - the smaller the area is, the less the loss is. Without

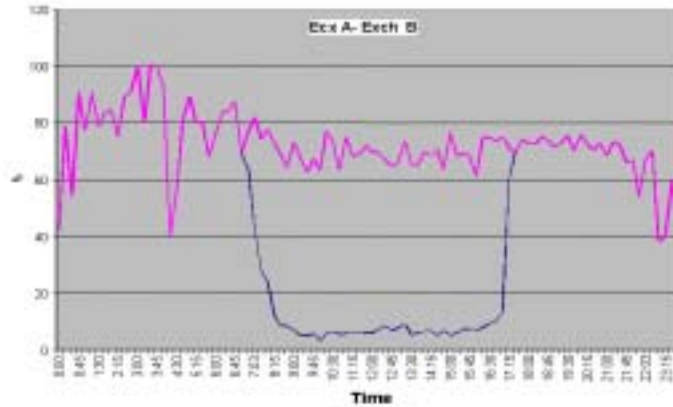


Figure 7.6.2. Traffic Management in Case of Network

Traffic Management, the problem would have been detected later, and the loss in revenue would have been significantly greater.

Figure 7.6.3 shows the impact of solar eclipse in 1999. A huge mass of people was moving to the area where the solar eclipse was best visible. As expected, people moving to, and being there generated an unusually big mobile traffic, that would overload both the mobile network and the trunks between the wireline and mobile net. In order to avoid the overload the networks, and to maximize the completed calls (maximize revenue), the following actions were introduced:

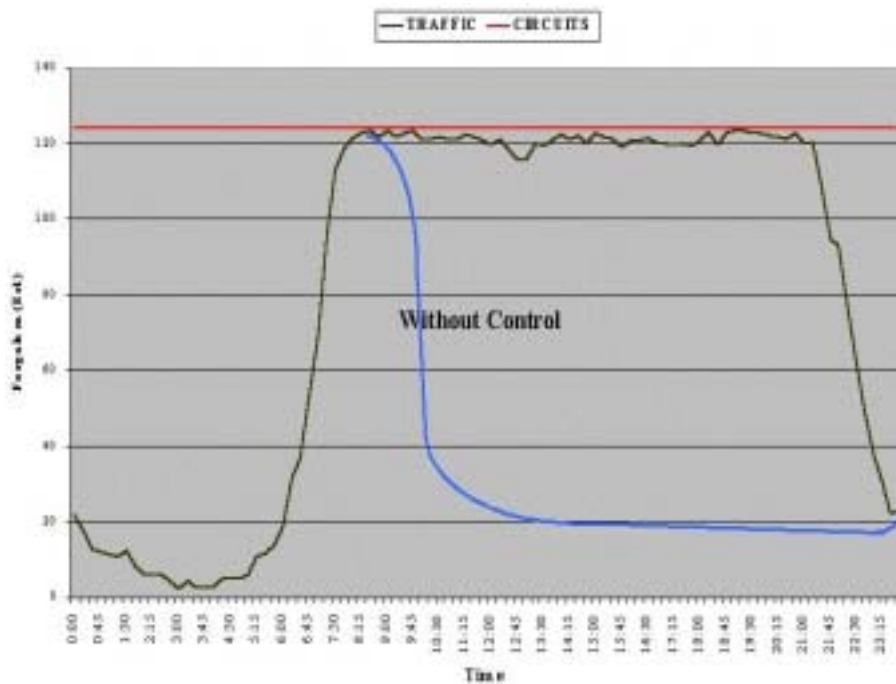


Figure 7.6.3. Traffic Management during the Solar Eclipse in 1999 (Traffic between two controlled exchanges)

- Some routes to and from the area of solar eclipse were rerouted (Expansive Control);
- In some exchanges call restriction control actions (namely in this case leaky bucket control) were applied.

The upper horizontal line on the Figure shows the maximum capacity between two affected exchanges (124 circuits, max 124 Erlangs). The slightly floating curve shows the real carried traffic; it is clearly shown that the applied control kept the traffic almost at a maximum. The dropping curve shows what would have happened if no traffic control had been applied: due to the tremendous amount of unsuccessful and repeated calls, the real (completed) traffic would have been only part of the maximum capacity. This effect is well known from the traffic theory and also from the practice.

7.6.4. Traffic Management in ATM Networks

ATM networks are expected to support a diverse set of applications with a wide range of characteristics. For the time being, there are no comprehensive measurements to satisfactorily address the characteristics of all type of traffic. Characteristics of voice sources are well known due to the studies performed in the last century. Constant Bit Rate (CBR) services are relatively easy to manage. The difficulty arises in choosing the (constant) bit rate to provide the desired service quality while minimizing the amount of bit rate used in the network.

Unfortunately, the behavior of data sources is not well-understood, and very often unpredictable. There is no typical data application, and no typical source behavior. Image and Variable Bit Rate (VBR) video data sources are relatively new areas, and the knowledge on their source behavior is limited.

In ATM networks, both flow control and congestion control can be used. But, flow control between the source and the destination does not help in reducing the possibility of congestion within the network. To minimize the effects of congestion, each node in the network shall regulate the traffic flow on its input links.

Some aspects of ATM networks that complicate the traffic control problem include the following:

- Various VBR sources generates traffic at significantly different rates - from a few kbps up to Mbps,

- A single source may generate multiple types of traffic with different characteristics,
- ATM networks have to deal with "traditional" performance metrics as call blocking and packet loss, as well as with cell delay variation, maximum delay and skewness,
- Different services have different QoS requirements at considerable varying levels,
- Traffic characteristics of various types of services are not well understood,
- As the transmission speeds increase, the ratio of call duration to cell transmission time increases. There are always a very large number of cells traveling in the network, and the large propagation delays compared with the transmission times, lead to long periods between the onset of the congestion and its detection by the network control elements.
- High transmission speeds limit the available time for on-fly processing.

Considering the high transmission speeds, the control algorithms should be as simple as possible to allow hardware implementations.

Congestion control mechanisms are classified as preventive and reactive control. Preventive control attempts to prevent congestions to occur in the network, The reactive scheme monitors the network for congestion, and if it is detected, sources are requested to slow down until the congestion is cleared.

In practice the efficiency of the control depends on the actual conditions, and a combination of the two principles should be used.

Resource provisioning

This is an important traffic management function for existing networks. Its major role is to provide an acceptable level of connection blocking performance. As the time is going on, several conditions may change in the network. Adding new resources or re-arranging VPs and the bandwidth allocated to them is some kind of traffic management.

Call admission control

When a new connection request is received at the network, the call admission procedure is executed to decide whether to accept or reject the call. Two questions should be answered:

- How can the required bandwidth by the new connection be determined?

- How can we make sure that the Service Level of the existing connections are not affected when multiplexing with the new connection?

The technique designed in response to these two questions, should work in real-time and should attempt to maximize the utilization of network resources.

Traffic shaping

For most VBR sources, during the active period, cells are generated at peak rate, while no cells are transmitted during the silent period. By buffering the cells during the peak period before they enter the network, it is possible to reduce the peak rate loading the network. So, the departure rate from the queue is less than the peak arrival rate of cells. Shaping can be done at the source equipment or at the network access point. With this technique good bandwidth saving can be achieved, but the amount of delay sets limitations.

Traffic policing

Traffic policing or usage parameter control is monitoring the network access points and should detect if the users stay within the connection parameters negotiated during the call setup phase. A policing function should detect a non-conforming source as quickly as possible, and take appropriate actions. When a non-conforming source is detected, the violating cells can be dropped, delayed, marked differently, etc. Most often used control schemes are the Leaky Bucket technique or different Windowing techniques.

Selective discarding

Policing schemes are designed to protect the network from non-conforming users. However, cells of non-conforming users can be marked, and admitted to the network. This is based on the assumption that these cells can be dropped when congestion occurs. Users may prioritize their cells before they are transmitted to the network. One cell can be either a high-priority or a low-priority cell. Then the buffer space at intermediate points can be used by incoming cells according to their priority.

Reactive congestion control mechanisms

Although preventive techniques reduce the buffer overflow probabilities, it is not possible to eliminate momentary periods of cell losses in the network. Loss cells

result in retransmission by the source codecs, thereby increasing the traffic, and resulting in a catastrophe as turning the momentary buffer overflow periods to sustained periods. Therefore, reactive control mechanisms are also necessary. These mechanisms have been used in low-speed packet-switched networks, but they are not so effective in ATM networks.

The following reactive mechanisms can be considered:

- End-to-End Notification Techniques: Once congestion is detected in an intermediate network node, the end nodes need to be notified to be able to react. Then, data sources can reduce their speed to reduce network load. There are three techniques proposed for congestion notification:
 - Estimation by the End Nodes: A source sends time-stamped probe cells along the connection to measure the one-way response time. When the destination node detects congestion (increased response time), it sends a notification to the source node.
 - Explicit Backward Congestion Notification (EBCN): In this scheme, each node in the network monitors the queues of its trunks. When the queue size reaches a predefined threshold, a notification is sent to all sources having path through the congested node.
 - Explicit Forward Congestion Notification (EFCN): Each line monitors the queues, and if its size reaches a threshold, all cells passing through that node is marked with a bit. The receivers know that there is congested node along that connections, but do not react very quickly. Only if the congestion is sustained, is a notification is sent to the sources.
- Adaptive Rate Control: The rate at which traffic is submitted to the network is varied by the source depending on the congestion control information. The proposed scheme is the EFCN to detect congestion.
- Incall Parameter Negotiation: This method is used to minimize the call setup overhead for traffic requiring transmission of only one or a few bursts. One alternative is to establish VPs between users of such services and defining a virtual network for them. In this case, it is relatively easy to manage the traffic inside the VPN.
- Dynamic Source Coding: The source may either reduce the traffic submission rate or mark cells that are not so essential as may be reconstructed from other cells. In case of Dynamic Source Coding, the source may decide which type of control is applied in case of congestion, depending on the traffic (delay-sensitive or not delay-sensitive).

7.6.5. Principles of IP Traffic Management

IP traffic management can be considered at various layers of the Internet Protocol stack. Lower layer solutions concentrate on the transmission of traffic from source to destination, but not considering applications and their properties.

At higher levels, the applications or other words their contents should be considered and more intelligent decisions should be taken. Some of the factors affecting the management decisions are:

- The amount of traffic from server to client is much higher than from client to server (asymmetric). This suggests that optimization is more important in one direction;
- The medium transfer size of web-documents is small, and short-lived. Due to the bursty nature they are more likely creating congestion;
- There is a difference in the usage of servers. Some top web-servers are accessed much more times than others (focused traffic).
- Some small number of large files consumes a big part of network and server bandwidth, and a significant number of small files are accessed only a few times.

Real-time traffic (distance learning, voice, streaming media) is becoming an increasingly proportion of web traffic. Management of this traffic should be supported. An effective management strategy should include admission control, bandwidth and buffer allocation solutions.

7.6.6. The Future of Call Control

Call Control Today

Today's call model is basic. The days of the very first call model—picking up a receiver and talking directly to a live operator working a plug-board switch—are long gone. Today, call control is the province of the Intelligent Network (IN). Service-control has been taken out of the switch and put on ancillary SS7 packet-networks to speed the development and deployment of new calling features.

But while these features may be new, they are also narrowband and voice-based. IN was designed expressly for the circuit-switched PSTN of 10 years ago when the Internet was still an R&D project and videos were what you rented from retail outlets. IN and SS7 are built on a triad of Service Switching Points (SSPs),

Service Control Points (SCP) and Signal Transfer Points (STPs), which oversees call completion in countless networks worldwide, aided by Intelligent Peripherals, under the overall control of Service Management Systems (SMSs). SSPs house stored programmed controls that instantly alert a CO's switch that it should consult the SS7 network before proceeding with call routing. Via a series of fast packet STP switches, the SSP then sends a query to the appropriate SCP about how to handle the call. A high-capacity database server, the SCP searches its files for instructions left by the SMS and replies. The switch then executes the forwarded call routine, often calling on an auxiliary IP to play announcements or collect Multifrequency Dial-Tone input from the caller.

In this model, call control is strategically placed in the SSP outright in a software-module called the call control function (CCF) that continually monitors a subscriber's line for points in calls (or PICs), trigger detection points (TDPs) and triggers. These are trip-wires that alert the SSP to temporarily suspend completion of the call.

Changing Call Control

Everything in the telecom world is converging—companies, markets, technologies—everything. It is believed, that for the full potential of this new world of communications to be realized, something else will have to change radically—the conceptual model dictating how calls are set-up and turn-down.

Even though it's the cornerstone of the entire PSTN, the call model in and of itself is changing. For example, in the new IN release, additional triggers - the SSP-IP interface busy and the no-answer trigger - as well as a new category of detection points - EDPs (event detection points)- are added (EDPs are a list of events such as busy, no answer, or terminating available resources.)

A Next Generation Call Model

It is likely that radical new changes will be needed to the call control model if the promise of broadband networking is ever to be fulfilled.

What may be needed is a model that accommodates a series of self-contained mini-calls within a call. The complexities entailed are an order of magnitude greater compared to the present model, requiring a two dimensional call model. Within a year

or two, the market will be demanding for network intelligence of this kind as competitive advantage among broadband service providers increasingly focuses on the ability to offer new services and not on bandwidth exclusively.

Innovative hardware and software vendors focussing on this issue will be rewarded handsomely, but that while each vendor will have a somewhat different solution, they will also all look for guidance for some recent work done by the International Telecommunications Union. What the ITU has done here is to put forth a new, four-plane conceptual map outlining a broadband compliant IN process. In the ITU model, each service is broken down into its constituent parts - generic blocks called SIBs (for Service Independent Blocks) and mapped to the plane immediately below. It is here in the Global Functional Plane, that the Basic Call Process (BCP) resides as a SIB. According to to the traditional IN call model, the BCP defines how calls not requiring any special treatment are handled. Not surprisingly, perhaps, it mirrors its predecessors almost PIC-by-PIC.

The Future of Call Control

The transformation of the old narrowband intelligent network into the broadband intelligent network of the next years will give a somewhat diminished role for the basic call model, which will now be just one building block among many. Instead, based on the ITU model, it will become the service-logic imparted by a string of SIBs and implemented in the distributed functional plane that controls the overall flow of a call through the physical plane. It will be a service logic, in effect, that gives equal footing to both caller-initiated and independent SCP- initiated calling sub-routines.

However, while intelligent networks are about to undergo radical change, it also indicates that at least the *forms* of the old infrastructure will be preserved. The sub-routines discussed above will continue to be implemented on SSPs (Service Switching Points), STPs (Signal Transfer Points) and SCPs (Service Control Points), but they will be a new breed of SSPs, STPs and SCPs, that vendors will have equipped with considerably more functionality. The venerable SSP will contain a Call Control Function (CCF) that both oversees call processing and provides network connection services; a Service Switching Function (SSF) that activates IN triggers during this call processing; a Specialized Resource Function (SRF) that ensures the

call processing software on a switch can communicate with the service control function on a SCP; and a Call Control Agent Function (CCAF) that supports caller interaction and user access to the network.

Such changes are not likely to be the last iteration of the call control function and that the ITU is not likely to be the only inspiration in this regard. Work is progressing on a uniform IN architecture for fixed-mobile at the European Telephone Standards Institute (ETSI). ETSI has already successfully ported traditional IN Functionality to GSM-based mobile networks via its Customized Applications for the Mobile Network Enhanced Logic (CAMEL) initiative. The International Telecommunications Information Networking Architecture (TINA) Consortium, is designing an architecture that is not backward compatible with the ITU's Intelligent Network Conceptual Model to promote open communications in distributed computing and processing environments, setting the stage for a standards showdown sometime in the near future. This is somewhat troubling as standards disputes have a nasty habit of derailing technological progress.

Probably unlikely that standards disputes could ever really destroy the market opportunities that innovative call control will lead to in the next few years. The huge revenue earning opportunities offered by the next generation intelligent network, means that both vendors and service providers have a very strong economic incentive not to let disputes get in the way of deployment.

7.7. Power supply

Zoltán Janklovics, author

György Varjú, reviewer

7.7.1. Power supply of telecommunication installations and their equipment

Telecommunication installations and equipment planted in them may vary by their design and destination, but they are common in one: all of them inevitably need electric power. In most cases, the public electricity network supplies this energy. In some particular cases it happens that the electric power supply network is not available (for instance in high mountains, far from inhabited areas) for the telecommunication installation. Here, according to the local conditions, alternative energy sources (e.g. solar cells, wind-electric generators, etc.) provide for the feeding of such installations. Due to the fact that in such cases the energy is discontinuously available, these systems are supplemented with interim ancillary energy storing batteries. In Hungary - with the exception of some special cases - the electric energy is available all over the country.

However, the continuity of the electric power supply cannot be always ensured, for a shorter or longer time interruptions may occur due to the outage of the mains supply, or due to transient phenomena, disturbing the operation of the powered equipment. Telecommunications equipment shall work also under such circumstances. During the powering of the telecommunications equipment with energy, the main goal is to provide for the possible most safety and reliable feeding; therefore care shall be taken also for the generation and storage of the energy. The power supply system, consisting of the following system technical elements, performs these tasks [7.7.1]:

- distributing unit of 0,4 kV AC (main distributor),
- stationary emergency (stand-by) generator,
- uninterruptible DC power supply system,

- uninterruptible AC power supply system.

In the past the power supply systems had been usually planted in separate rooms within the telecommunication installations (so called centralised power supply). Nowadays, the accommodation in the same room of the power supply units and the powered equipment is getting more and more widespread (decentralised, or switch-room power supply, however, the stand-by generator is installed even in such cases in a separate room).

System technical configuration of power supply and its system technical units

The central unit of the electric power supply system of telecommunication installations is the 0,4 kV receiving and distributing system (main distributor), to the input interface of which the primary and (eventually) the reserve network feedings, the stationary or mobile stand-by generators are connected. The different consuming appliances of the telecommunication installation are connected to the output of the main distributor. Among them the technological power supply units (uninterrupted DC or AC systems) feeding the telecommunications equipment are of great importance. The other consumers connected to the main distributor can be categorised into two groups: the group of authorised consumers to use Diesel (important consumers, for e.g. climatic appliances, which in case of mains outage, shall be powered from stand-by, emergency generators) and the group of unauthorised consumers to use Diesel.

A) AC distributing unit

The 0,4 kV distributing unit (switchgear), shortly the main distributor, serves for the reception and distribution among the individual consumers of the incoming low voltage (230/400 V) electric power. One characteristic feature of the main distributor of telecommunication installations is that in the interest of increasing the reliability of the feeding, reception of electric power is possible from several directions, i.e. ancillary feeding can also be implemented. In case of mains outage the required AC energy can be assured with the help of stand-by generators. The consumers of the installation can be powered in this case via stationary or mobile stand-by generators. These ones are connected to the main distributor. All consumers of the telecommunication installation get the energy through the main distributor. Therefore each branch has to have over-current protection, switch off possibility and instrumentation, as needed. The main distributor makes the switch over among the

different feeding inputs possible. This can be done manually (by the intervention of the operating staff), or automatically. Against malfunctioning appropriate protections (locking) is built-in into the main distributor. Usually the quantity of the energy consumed from the public electric network is metered also in the main distributor.

Basically there are two system technical versions of the main distributor known: a design with one bus and with double buses. The more complicated two-bus system is so arranged that each feeding and each branch can be connected to both of the buses, so thus the required variation of connection can be created. This arrangement makes the maintenance and repair of the main distributor, the replacement of the components easier and improves the operational safety. The price of this flexibility of such a two-bus system is that from each switching element, bus, or cable double quantity is needed. Accordingly, the space required by the main distributor and the demanded maintenance, as well as the investment costs of the system significantly increase. Both the one- and two-bus systems are widely used in the practice. These main system technical designs have several versions. For instance, the flexibility of one-bus systems can also be increased significantly using longitudinal bus sectioning.

The size of the main distributor, the number of branches the loadability of the used switching and protecting components always depend on the requirements of the telecommunication installation. In general the main distributor is a unit of individual design and installation. In small installations, which do not need operating staff, the main distributor is a small wall cabinet. In larger installations the powerful distributors, constituting an individual group of equipment, are installed either in separate room or commonly with the stand-by generator (or eventually with the technological power supply). The advanced types of main distributors are of modular-rack design. The individual cabinets have racks for the bus, the cable and the units. An important requirement against the main distributor is that the switching configuration shall always be transparent and the most important parameters can be read on the spot. In case of automatic-operated main distributors, reasonably the possibility of manual switching operations or manual control shall be executable in case of failure of the automatic system. Special attention shall be paid to reliability at the design of the main distributors because we have in vain alternative, stand-by

feeding input, emergency generator, if - due to an unreliably functioning switching element - these units cannot feed the equipment.

B.) Uninterruptible DC power supply system

In a telecommunication installation the main consumer, requiring usually the most energy supplied, is the telephone exchange. For the supplying DC voltage is required, having usually a nominal voltage of $-48 V_{dc}$. The most important requirement for the supply is the continuity, i.e. the powering system must not interrupt even for a second the supplying of the DC voltage. Otherwise the built-up connections would disconnect (in case of the exchanges it would necessitate the re-programming of the exchange, which in the given case could block the provisioning of telecommunication services for hours in a region). Rectifiers fed from the public mains produce the required DC voltage. However, these units can only provide the DC voltage, if the required mains voltage is available. Since the continuity of DC current supplying is to be ensured, and the uninterruptible supply cannot be assured only from the AC current side, the DC current needs to be directly stored. The most suitable for this purpose are the rechargeable and dischargeable chemical energy sources, the batteries. The uninterrupted DC systems are so designed that in case of failure of the mains voltage, the batteries can immediately replace the falling out DC voltage of the rectifiers. The simplest method to implement this is the following: the proper battery set is connected parallel to the rectifier providing the DC voltage, so thus the rectifier - beside the feeding of the consumer - is charging the battery as well (parallel floating charging mode of operation). In case of a mains outage the battery set is taking over immediately (without interruption) the feeding of the consumer. The lead acid batteries can be used for this type of operation. Considering that both in case of DC or AC power supply systems, the key component of uninterruptible operation is the battery, in the followings the batteries applied in the mentioned systems will be discussed in details.

Lead acid batteries can be categorised into the following main *two groups*: *flooded electrolyte batteries* and gel technology *batteries*. In the first type diluted sulphuric acid in liquid state is used as electrolyte. Because of the evaporation of the sulphuric acid these types of batteries need to be accommodated in battery rooms designed specially for this purpose, and beside the charging they require maintenance (e.g. liquid level control), too. In case of gel technology batteries the

sulphuric acid is either in jelly state or in a certain intermediate insulator. This makes it possible to produce these batteries in closed form, i.e. in this case the electrolyte has no contact with the air space. There is a safety valve mounted onto the housing of the battery, which has the task to release the overpressure developed within the accumulator in case of disturbance in operation. The gel technology batteries are more sensitive to the charging voltage and to the ambient temperature. (According to the abbreviation coming from their English denomination, these batteries are called also as VRLA batteries.) The VRLA (Valve Regulated Lead Acid) batteries may be accommodated also in common room with the telecommunications equipment, for e.g. in the frame of it.

Regarding the lead acid batteries the following (cell) voltage levels can be mentioned:

- Nominal voltage: 2V.
- Floating charging voltage: The charged level of the battery can be maintained with floating charging. The value of it is $2,23V \pm 1\%$.
- Boost charging voltage: The discharged battery can be recharged with the help of the boost charging. The value of it, which is limited for e.g. by the developing gas, is usually 2,35-2,4V, but sometimes the manufacturers allow higher values.
- Discharge final voltage: below this voltage the processes going on in the battery become irreversible and the battery deteriorates. The value of this voltage is ca. 1,8V.

We mention that VRLA battery sets require temperature-dependent charging voltage, and the boost charging is usually not allowed in their case. The time, during which the telecommunication system can be powered without the public mains voltage, depends on the capacity of the battery. This time is called as back-up time. In the interest of continuous operation of the telecommunication system the public mains voltage is to be replaced within the back-up time. In case if the voltage tolerance of the consumer requires it a more complicated system shall be applied instead of the parallel floating charging system (e.g. consisting of a 24-cell battery set and of a rectifier operating parallel with it). (Such complex systems can be, for instance, a dropping diode system, or serial converter system, which are used in analogue exchanges with narrow voltage tolerance and in certain types of digital exchanges.)

For the proper operation of the given telecommunications equipment, appropriate power supply is to be ensured. The parameters that are to be met by the power supply, can be specified for every equipment. The most important such parameters are:

- limit values of the output DC voltage of the power supply system;
- power consumption of the supplied equipment;
- the still tolerable maximum value of the noise voltage superimposed onto the output DC voltage (the noise voltage requirements mean one of the quality distinctions between the power supply systems of telecommunications equipment and the power supply systems of other purpose.);
- the maximum value of output voltage changes (transients) caused by the change of load or mode of operation.

The above mentioned are the requirements set by the powered equipment against the power supply. The energetic aspects of power supply (e.g. efficiency, inrush current) are worth to be mentioned and the EMC requirements of the relevant standard specifications shall be met, as well [7.7.4].

C). Uninterruptible AC power supply systems

In telecommunication installations including telephone exchange, the technological equipment have required up to the near past mostly direct current power supply. Nowadays, those, first of all IT type telecommunications equipment, are spreading quickly, which require power supply with 230V alternating current. These systems are also sensitive to the continuity of the power supply. The uninterruptible alternating current systems serve for the satisfaction of these demands.

The demand for the uninterruptible power supply (UPS) requires the intermediate storage with batteries of the energy in this case, as well. At the same time, a unit (inverter), which transforms the stored DC voltage into one- or three-phase alternating voltage, having the frequency and (sinusoid) waveform of the mains current, is also needed. The inverter is the determinant key element of the uninterruptible alternating system. In the case, when the demand for the uninterrupted alternating current is less than the DC output power demand, the (48V) battery of the DC system can be used for the energy storage.

Sensitive consumers are fed from continuously operating inverters (inverter-based operation mode). If mains voltage is available, the inverter is working

synchronised to the mains. (So thus, there is no voltage jump occurring in the feeding voltage in case of a mains outage.) In battery-operated mode the inverter is self-running. In case of failure of the inverter, or if it is switched off, the role of the inverter is taken over by the mains. Even in such cases the switchover must not result in any voltage jump, therefore a high-speed electrical switch (usually a Thyristored solution) controlled by an electrical device is applied (electrical by-pass). The systems have also the possibility of mechanical switchover (mechanical by-pass), which might be necessary for service purposes. This switching device is equipped with appropriate locking. (The output voltage of the inverter must not be interconnected with the mains.)

If the required power is comparable with the output power of the DC system, the application of 48V batteries would not be economical (the capacity of the cells should be increased considerably). Instead of it, the system itself is equipped with an own battery set and charging unit. The battery sets of the alternating current systems are of higher voltage (of 200...400V), which means a higher number of cells (100...200). The higher voltage makes it possible that the same power can be stored with the help of lower capacity cells, which is a more economical solution than using of battery sets having less cells but higher Ah capacity.

D). Stand-by (emergency) generators

Key important consumers are supplied with electrical energy from stand-by (emergency) power generators in case of outage of the public mains over a certain period of time. The stand-by generator itself is basically a small-sized electrical power plant, which consists of an alternating generator driven by an internal-combustion engine. The stand-by generators used widely in the practice do produce 0,4 kV three-phase alternating current and a diesel motor is used in them as power engine. In telecommunication installations there are two different types as to the design of such generators are applied: larger, important installations have built-in – stationary (fixed) – stand-by generators, while to smaller systems movable/transportable – i.e. mobile – stand-by generators can be connected.

The engine part of the stand-by generators of today is a turbo-diesel motor, made of light alloy. Alternatively, gas fuelled engine can also be applied. For the quick start and loadability of the motor, the cylinders of it are preliminarily heated (in order to keep the temperature) with the help of the cooling water. The automatics

provides for the start of the motor, the regulation of the speed (r.p.m.) and the fuel injection, etc. In addition, it has other important function, too: to indicate and forward to the monitoring system the functional problems, signs of malfunctioning. In case of an outage of the mains, the automatics start the stand-by generator (usually with a 1-2 minutes delay-time). The generator is designed with alternating, three-phase voltage.

Stationary, fixed stand-by generators are often co-located with the main distribution unit. This goes along with that the drainage of the exhausted gases, as well as the sound-proofing of the room must be solved. A separate battery set, having its own charger, starts the diesel motor. The construction of the main distributor and that of the stand-by generator must be in line with each other, since the benefits of the automatic-start stand-by generator can only be exploited with an automatic main distributor.

The construction and design of mobile stand-by generators is basically identical with that of the stationary types.

7.7.2. Powering of wire communication networks

In the traditional wire line telecommunication systems the individual customers are connected via metallic conductors (cables) to the nearest telephone exchange. The metallic conductor (e.g. copper pair) is used for telecommunications and for the transmission of signals necessary for the building up of the connections. The required energy is provided by the powering system installed within the exchanges, or the energy is supplied via the metallic network to the equipment to be powered.

In this section a short overview is given for the powering solutions of wire line networks different from the traditional ones.

Similar powering solutions are applied in the optical access networks and in metallic wire digital networks. (These solutions will be described as an example of optical access networks.)

A.) Power supply of optical access networks

In case of optical cables there is no metallic contact between the two endpoints of the cable. The connected equipment includes electrical circuits, which

require electrical energy for their operation. In case of equipment installed in telecommunication systems, the powering is solved: the uninterruptible (48V, direct voltage) power supply systems of the telephone exchanges – beside the powering of other transmission equipment – are feeding the equipment of the optical systems, too.

The uninterruptible powering of equipment installed in outdoor (street) cabinets, in the customer premises or located in the vicinity to the customers, requires individual solutions. The active elements of the optical network can be found in geographically different places, which sometimes are quite far from each other.

In case of remote powering the equipment receive the energy necessary for their operation either from the nearest uninterruptible power supply, or from the power supply system (Power Node, PN) of one other active element of the network. The precondition of remote powering is that the remote power unit (RPU) and the powered equipment shall be interconnected also with a metallic (remote powering) cable.

Accordingly, there are two major versions of remote powering:

- centralised powering, whereas the equipment are supplied with power through the Remote Power Unit, located within the telecommunication installation, and
- cluster powering, whereas Power Nodes (PN) belonging to the equipment (e.g. street cabinets) installed within the network are powering the subscribers, or the network units (ONUs), which do not have own powering system, but require powering.

The remote power voltage is supplied by the Remote Power Units (RPU), the output circuits of which are secondary circuits.

The values of the voltages applied in telecommunication systems can be categorised from safety aspects according to standards [7.7.5 -7.7.6] into the following groups:

- Safety Extra Low Voltage (SELV) circuit: a circuit, where under normal operating conditions the direct current shall not exceed the value of $60V_{dc}$, or the alternating current the $42,4 V_{ac}$ value. Moreover, in the event of a single failure the voltage shall not exceed the highest values given for normal operating voltage, for longer than 0,2 s. Moreover, the limit of $120V_{dc}$ or $71 V_{ac}$ shall not be exceeded.
- TNV1 Telecommunication Network Voltage circuit: a circuit, which complies with the requirements specified for safety extra low voltage circuits, but which is subjected to overvoltage from the telecommunication network.

- TNV2 Telecommunication Network Voltage circuit: a circuit, the normal operating voltage of which exceeds the limit value specified for safety extra low voltage circuits, and which is not subjected to overvoltage from the telecommunication network.
- TNV3 Telecommunication Network Voltage circuit: a circuit, the normal operating voltage of which exceeds the limit value specified for safety extra low voltage circuits, and which is subjected to overvoltage from the telecommunication network.
- Limited current circuit (a circuit limiting the remote feeding current): a circuit, which even in the case of breakdown of the insulation, or defect of any element, complies with the following requirements:
 - For frequencies not exceeding 1kHz, the steady-state current drawn through a resistor of 2000 Ω connected between any two points, shall not exceed the value of 0,7 mA AC or 2 mA DC.
 - For (accessible) parts not exceeding 450V peak AC or DC, the circuit capacitance shall not exceed 0,1 μ F.
 - For (accessible) parts exceeding 450V peak AC or DC, but not exceeding 15000V peak or DC, the (available) stored charge shall not exceed 45 μ C.
 - For (accessible) parts exceeding 450V peak AC or DC, but not exceeding 15000V peak or DC, the available energy shall not exceed 350 mJ.

In case of *centralised powering*, the primary side of the RPN is connected to the 48V power supply system. So thus, the continuity of the remote powering is also assured. Such solution is applied, for instance, at ISDN circuits, or at PCM systems.

In case of *cluster powering* the network unit providing the remote powering shall have its own power supply system. The input energy source of it is the public mains. A continuous (uninterrupted) powering is to be assured also in the event of outage of the public mains; therefore the power supply system shall include battery sets as well. The power supply system, besides the remote powering, has to feed with energy the locally installed equipment, as well; therefore it often includes several consumer outputs of different voltage levels. The battery voltage may be also different from 48V.

In case of *local powering*, the primary energy source of the equipment is the public mains. Since the equipment need to operate also in the event of outage of the mains, an uninterruptible power supply system shall be applied. The construction and the design of the power supply depend on the place of installation of the equipment and on that if it serves one or more subscriber(s).

At the installation of the local powering system, the following issues shall be dealt with:

- the connection to the energy supply network,
- the installation environment of the equipment (street cabinet, etc.),
- the selection and accommodation of the battery set,
- the back-up time of the battery set.

The majority of the equipment of the optical network can be found not in air-conditioned buildings, but these are installed in street cabinets, staircases, etc. Therefore, special care shall be taken for the observation of environmental conditions of the selection and installation of power supply equipment. (For instance, the applicable operating temperature range is very important to avoid overheating problems.)

The selection and installation of battery sets require special attention, too. It is important that only maintenance-free batteries can be built in into the equipment of the optical networks. In customer premises equipment, besides the VRLA-type battery sets Ni-Cd batteries can also be applied. At the same time, for VRLA batteries the recommended operating temperature range (usually it is around 20 °C), shall be taken into account, because at a higher temperature the life-time drastically decreases, or at a lower temperature the full charged quantum cannot be taken out of the battery. The lower temperature range is also limited. Therefore, it is necessary to ensure somehow (e.g. by putting the batteries into a man-hole, or cooling/heating the cabinets) that also the batteries of street cabinets operate under equalized temperature conditions.

While power supply systems of telecommunication installations are capable to bridge over almost without limitation any mains outage, in case of ONUs, which are operating with local powering, the bridge-over time is strictly equal to the back-up time of the built-in batteries (except mobile Diesel operation). So, it is important to choose properly the back-up time of the batteries. It depends on the reliability of the local electrical supply network. When making our choice, the frequency and the average duration of mains outages (failures) occurring in the given area, shall be taken into consideration. In larger cities the electrical network is more reliable, because (in most cases) the supply of energy to the consumers is realized via from the weather protected, buried cables and the distances are smaller (the fault repair

times are shorter). The situation is worst in small, remote settlements and scattered farms, i.e. in places where both the distribution and consumer's networks are made of overhead cables and the consumers are far from the maintenance and repair staff. Therefore, it is reasonable to apply batteries of different back-up times for the equipment, depending on whether they are installed in larger/smaller cities, villages or settlements of scattered farms.

B.) Powering of CATV networks

Cable television (CATV) networks are of hierarchical topology that can be segmented to several individual parts and according to this segmentation also the applied method of powering is different. In general, in CATV networks there are coaxial cables used, but the network may consist of optical fibre cables as well. Beside the passive elements, such networks include line amplifiers and house amplifiers, too. Remote powering usually does the energy supply of line amplifiers. The feeding of house amplifiers can be solved both with local and remote powering. The powering of the CATV head-end stations is to be mentioned, as well, whereas it is always to be constructed and designed according to the local requirements. Head-end stations are always locally powered. The individual equipment may require either 230V AC or 48V DC powering. In case of head-end stations installed in telecommunication systems the uninterruptible DC voltage powering of the station can be solved via the 48V_{dc} power supply system of the installation. If uninterruptible AC voltage supply is required - and if in the installation an uninterruptible alternating current network is not available - the powering can be solved also with the help of individual uninterruptible power supply units (UPS).

Remote powering of CATV amplifiers: Amplifiers, which are applied in the trunk (or main line), or line and distribution network layers of the CATV network, are remotely powered with alternating voltage (maximum 60V), transmitted usually via the coaxial cables. The house amplifiers used in in-house networks are locally powered.

The applicable supply voltage: Because of the risk of corrosion, direct voltage is practically not used in CATV networks for remote powering. Taking into account the 24 V stabilised internal supply voltage applied for the powering of amplifier modules, as well as with consideration to the electrical safety specifications, max. 60V alternating voltage is applied for remote powering. The built-in powering units of

the amplifiers convert this 60V alternating voltage into stable direct voltage. The lower limit of the input alternating voltage is between 27...40V depending on the construction of the amplifier. The remote supply voltage is (usually) produced with the help of ferroresonant voltage stabilisers. At the output of it, a nearly quadratic (trapezoid)-form output voltage appears, which is excellent for the reduction of the output voltage fluctuations, occurring due to the loading changes, or the input voltage fluctuations.

Ferroresonant power units: The alternating voltage stabiliser operating on the principle of ferroresonance, is a special transformer, in which the stabilising effect is achieved by the driving of the iron core into a saturated state. For doing so, beside the usual primary and secondary coils of the transformer, also a third coil is necessary, to which in parallel a capacitor is connected. The third coil along with the capacitor forms a resonant circuit tuned to the network frequency (50 Hz). The stabilising effect is reached by getting the iron core into a saturated state, before the sinusoid input voltage would reach its peak value, so thus, on the output side the voltage practically cannot change. Similarly, even under the effect of changes of the load, the amplitude of the output voltage shall not remarkably change, either. The 'price of it' is that the output voltage is not sinusoid, but it has a trapezoid waveform. The advantage of the ferroresonant stabilisers derives from their relative simplicity and consequently in their reliability and cheapness. Therefore, such power units are greatly applied in CATV networks. The relatively high inrush current (which among others depends on the pre-magnetic status of the iron core, i.e. on the moment of time of the previous switch-off) is a disadvantage of such units. Therefore, the circuit breakers providing for the over-current protection on the input side, shall be selected with due care. The efficiency of the unit reaches a 90% level approximately at half-load.

7.7.3. Power supply interface of telecommunications equipment

One basic condition of the implementation of a power supply system, which is optimal both from technical and economical points of view, is that the parameters of the power supply interfaces of the powered equipment shall be standardised or uniformed. (The power supply interface is the common interface between two

functional units, at which the power unit is connected to the telecommunications equipment.) With the standardisation of the parameters of the power supply interface the compatibility between the powering and the powered equipment can be ensured. At the same time, the conditions necessary for the normal operation of the equipment can be maintained also in the event, when the power supply equipment is feeding several, different telecommunication systems. The standardisation of the parameters makes it possible that telecommunications equipment to be implemented newly can (on a longer term) be connected to already existing power supply systems, without the application of special adapters (e.g. DC-DC converters). Moreover, it will be also possible that power supply units having similar parameters can be applied in all telecommunications equipment. The parameters and characteristics of power supply interfaces are specified in the series of Standards ETSI 300 132 [7.7.2 - 7.7.3]. (The requirements are related to telecommunications equipment operated by 230V alternating current, or by 48V direct current. There are no international specifications available for systems differing from these ones (e.g. for 27 V direct current systems). Similarly, the remote power supply systems are not standardised either.)

Requirements of power supply interface operated by alternating current (AC)

According to Standard ETS 300 132-1, the following major requirements shall apply to power supply interface(s) of equipment powered by UPS of 230V AC nominal voltage:

- The supply voltage range shall be 207-253V (between the neutral and the other conductor); the frequency range shall be 48-52 Hz.
- The equipment shall not suffer any damage (either in its hardware or in its software), if the value of the supply voltage is between 0 - 207V. The frequency range in this case may be between 45 - 55 Hz.
- Following the restoration of the supply to the normal (operating) voltage range, the equipment shall then resume the operation according to its specifications, without requiring any intervention.
- Without the change of its operating parameters, the telecommunications equipment shall be capable to bear voltage fluctuations, occurring within the specified limits due to the regulation of the secondary voltage.
- Among others, the equipment shall also comply with the requirements specified for the inrush current, the harmonic content of the input current, the surge voltage (over-voltage) immunity and the immunity to radio frequency disturbances.

Requirements of power supply interface operated by direct current (DC)

According to Standard ETS 300 132-2, the most important parameters relating to power supply interface in case of equipment requiring direct current power supply, can be summarised as follows:

- The normal service voltage range for the –48 V direct voltage nominal supply at the interface shall be -40,5 to –57 V.
- Telecommunications equipment operated at –48 V nominal direct voltage shall not suffer any damage when subjected to the following - from the nominal value different - voltage ranges: 0 to -40,5 V DC and -57,0 to –60 V. Following the restoration of the normal voltage range, the system shall continue to function within its operational specification without requiring manual intervention.
- The equipment shall comply with the requirements specified in the above standard for transients, voltage drops, as well as for weighted and wideband noise immunity and emission not exceeding 20 kHz. (The requirements for values above 20 kHz are specified in EMC standards.)

List of abbreviations:

Abbreviation:	English equivalent:	Hungarian equivalent:
ONU	Optical Network Unit	optikai hálózati egység
PN	Power Node	tápellátó csomópont
RPU	Remote Power Unit	távtápláló egység
SELV	Safety Extra Low Voltage	biztonsági feszültség
TNV	Telecommunication Network Voltage	távközlési hálózati feszültség
UPS	Uninterruptible Power Supply	Szünetmentes tápellátó rendszer

References

[7.7.1] Janklovics Z. - Gerdai G.: Telecommunications power supply; Magyar Távközlés, 1997. August (in Hungarian)

[7.7.2] ETS 300 132-1 Equipment Engineering; Power supply interface at the input to telecommunications equipment; Part 1: Operated by alternating current (ac) derived from direct current (dc) sources.

[7.7.3] ETS 300 132-2 Equipment Engineering; Power supply interface at the input to telecommunications equipment; Part 2: Operated by direct current (dc).

[7.7.4] ETSI EN 300 386 Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; Electromagnetic Compatibility (EMC) requirements.

[7.7.5] EN 60950 Safety of information technology equipment, including electrical business equipment

[7.7.6] EN 41003 Particular safety requirements for equipment to be connected to telecommunication networks

7.8. Electromagnetic compatibility

Zoltán Janklovics, Ferenc Lénárt, author

György Varjú, reviewer

7.8.1. EMC fundamental definitions, terms and principles

In the interest of proper functioning of equipment in the given environment, i.e. without the degradation of its performance, it is necessary that the different equipment and their operational environment are made electromagnetically compatible. *The electromagnetic compatibility*, or the commonly used abbreviation, EMC (according to the English term), refers to such a professional field, *the object of which is to eliminate or at least to possibly minimise the „mismatch” between the equipment and their operational environment* according to the accepted norms, standards and regulations. In the EMC Chapter of the International Electrotechnical Vocabulary [7.8.1], the term of EMC is defined as follows: „The ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment”.

The electromagnetic interference (EMI) means degradation of the performance of a device, equipment or system caused by an electromagnetic disturbance. Electromagnetic disturbance is any such electromagnetic phenomenon, which degrades the performance of a device, equipment or system, or adversely affects living or inert matter. The EMI phenomenon, the occurring degradation of performance consists of three ingredients, namely:

An emitter, i.e. a source emitting the electromagnetic disturbance;

- A susceptor, i.e. a susceptible (disturbed) device, equipment or system showing degradation of its performance;
- A medium in between, which is called the coupling path.

The definition of the term degradation is as follows: An undesired departure in the operational performance of any device, equipment or system from its intended performance.

It is important that in the definition the adjective „undesired” is used and not the adjective „any”. Therefore, for the tests the kind of undesired departure in the operational performance must be clearly specified (see performance criteria).

In the everyday practice there are usually lots of artificial or natural sources, which are emitting electromagnetic disturbance, creating such electromagnetic environment, in which potential susceptors can be found. Due to the great variety of the possible situations, the electromagnetic environment is very complicated.

EMI has relation to EMC from the two following aspects:

1. The emission determines that condition, under which a given electrical or electronic system is functioning properly, without introducing electromagnetic disturbances, causing degradation of performance in other systems;
2. The immunity determines that condition, under which a given electrical or electronic system is capable to function properly in the given electromagnetic environment, without the risk of degradation of performance.

With some simplification the basic principle of assurance of electromagnetic compatibility can be illustrated as follows. Figure 7.8.1 shows a possible combination of an emission and an immunity level and their associated limits as a function of an independent variable quantity (for e.g. the frequency) in case of single disturbance source (emitter) and a single susceptor.

Limits and levels for a single emitter and susceptor as a function of some independent variable

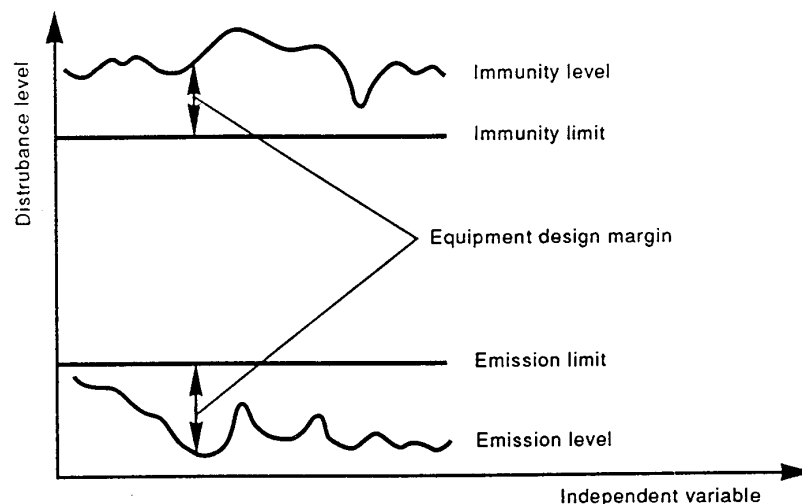


Figure 7.8.1.

According to Figure 7.8.1 the emission level is always lower than its maximum permissible level and the immunity level is always higher than its minimum required level, i.e. the immunity limit. Hence, the emitter and the susceptor comply with the requirements. In the figure there is some margin between the measured level and the limit value. This margin might be called as “equipment design margin”, and is an additional margin in the design to ensure compliance with the limit and it is controlled during the EMC test. The range between the immunity limit and the emission limit is the compatibility range. The compatibility level is within this range.

If the emission level and the immunity level have been designed in a way that they meet the existing electromagnetic phenomenon, then Figure 7.8.1 indicates an electromagnetically compatible situation. The figure shows that the immunity level is higher than the immunity limit and this is higher than the emission limit, which, in turn, is higher than the emission level. [7.8.2].

The two key issues in the problem are the emission and the immunity; the harmonisation of these two criteria is a regulatory task.

7.8.2. Categorisation of EMC according to phenomena

The following table gives an overview of the principal electromagnetic disturbance, which shall be considered accordingly to the list commonly agreed by the IEC and CENELEC [7.8.18].

Note: There is of course no abrupt limit between the low frequency domain and the high frequency domain but a soft transition between 9 kHz and 150 kHz. For formal applications the limit is set at 9 kHz.

The above disturbance phenomena can be classified into the following groups:

According to frequency:

- Low-frequency (less than 9 kHz) disturbances;
- High-frequency (more than 9 kHz) disturbances.

According to mode of propagation (coupling) of the disturbance:

- Conducted disturbances;
- Radiated disturbances.

Conducted low frequency phenomena	Harmonics, interharmonics Signalling voltages Voltage fluctuations Voltage dips and interruptions Voltage unbalance Power frequency variations Induced low frequency voltages d.c. in a.c. networks
Radiated low frequency field phenomena	Magnetic fields ^a Electrical fields
Conducted high frequency phenomena	Directly coupled or induced continuous voltages or currents Unidirectional transients ^b Oscillatory transients ^b
Radiated high frequency field phenomena	Magnetic fields Electrical fields Electromagnetic fields continuous waves transients ^c
Electrostatic discharge phenomena (ESD)	
High altitude electromagnetic pulse (HEMP) ^d	
^a Continuous or transients ^b Single or repetitive (burst) ^c Single or repetitive ^d To be considered under special conditions	

In addition the disturbances can be differentiated also according to their duration in time as:

- Continuous
- Short time (transient) phenomena.

Special phenomena:

- Electrostatic discharge (ESD, combined – conducted and radiated phenomena);
- High Amplitude Electromagnetic Pulse (HEMP), or Nuclear Electromagnetic Pulse (NEMP)
- Lightning Electromagnetic Pulse (LEMP).

The standards are ranking the impacts of electromagnetic pulses of lightning among the conducted and radiated phenomena, while the phenomena are categorised rather according to their physical characteristics, than on the basis of their sources (ESD and HEMP phenomena are exceptions from this point of view).

7.8.3. EMC regulation

In the developed industrial countries the EMC constitutes part of both the technical and legal, statutory regulation. Within the frame of it, the state(s) stipulate(s) mandatory technical requirements for the products and forms of conduct and behaviour, which ensure the observation of these stipulations. Technical regulation is adopted by the state(s) only in cases when a certain defective product is greatly hazardous from the point of view of protection of life, health, environment and property.

The statutes lay down requirements and compliance for manufacturers and distributors. At the same time, there are stipulations given in these statutes also for the ways and means of confirmation and declaration of compliance.

In order to promote unification in the field of EMC regulation in the European Union, the Directive No. 89/336/EEC on Electromagnetic compatibility was issued on 3 May, 1989 (hereunder referred to as: EMC Directive) [7.8.3]. The EMC Directive, which entered into force in the EU in 1996, specifies the scope of its application, as well as those institutional, personal, standardisation, quality certification, statutory, etc. conditions and requirements, the fulfilment of which is required to the conformity with the EMC requirements and in case of products to obtaining the CE mark of conformity. It is worth to mention that an exact interpretation of the EMC Directive is not simple. To help it, the EU has published a guiding document [7.8.4].

The Hungarian EMC Decree is based on the 89/336/EEC Directive and it was issued as 31/1999 (VI.11.) GM-KHVM Common Decree on electromagnetic compatibility and entered into force in 1999 [7.8.5]. (The up-to-date list of endorsed national standards referred to in the Decree is regularly published as Annex to the Hungarian Standardisation Bulletin (Szabványügyi Közlöny). Remarkable that the first list contained 96 standards, which also reflects the complexity of the subject.)

On one part, the importance of the Hungarian EMC Decree consists in that that it stipulates uniformed protection requirements both in respect of emission and immunity in the whole frequency range within the whole scope of EMC, on the other part, that it is in line with the legal harmonisation principle of the European Union and it complies also with the EMC standards of the Community.

Within the scope of this field the Decree specifies the protection requirements and the controlling tasks. It stipulates that „...the equipment shall be so constructed that:

- a) the electromagnetic disturbance it generates does not exceed a level allowing radio and telecommunications equipment and other apparatus to operate as intended;
- b) the apparatus has an adequate level of intrinsic immunity to electromagnetic disturbance to enable it to operate as intended.”

In addition, as one of the most important protection requirements, it stipulates that the equipment should be constructed in such a way that it has an adequate level of electromagnetic immunity in the usual electromagnetic environment where the apparatus is intended to work so as to allow its unhindered operation, taking into account the levels of disturbance generated by apparatus complying with the standards pertaining to the Decree.

The laying down of the adequate system of EMC standards is not the only, but no doubt, one of the most important preconditions of the application of the EMC Directive.

The *system of EMC standards* consists of the following three types of standards [7.8.6]:

a) *Basic standards* give terms and definitions regarding the disturbing phenomena and the description of the phenomena, the detailed testing and measurement methods, the testing devices and measurement configurations of basic tests.

The list of harmonised standards does not contain the basic standards, since from the point of view of declaration of the conformity of products not the basic standards are prevailing.

(For instance the IEC 1000-4-X series contain basic standards, which comply with the above criteria.)

b) *Generic standards* give the EMC requirements (limits), as well as the standardised testing methods that can be applied to equipment operating in a given environment.

c) *Product family standards* give detailed specifications for emission and immunity requirements of equipment in question.

With regard to the complexity of the system of EMC standards, we give a short overview about the present practice of marking of standards.

The IEC (International Electrotechnical Commission) has introduced the marking of IEC 1000-X-Y for the series of EMC standards. According to the second subdivision (X) of these series, the subjects (- following the marking and numbering structure of IEC -) are:

1. General considerations, definitions, terminology
2. Description and classification of the environment, compatibility levels
3. Emission limits, immunity limits (in so far as they are not regulated in a product family standard)
4. Testing and measurement techniques (Basic publication)
5. Installation and mitigation guidelines
6. Generic standards of series numbered as 1000 and 61000
7. Miscellaneous

European Standards with numbering EN 61000-X-Y are those standards, which have entered into force with the adaptation of the relevant IEC 1000-X-Y numbered standards of IEC.

(Recently, IEC is also using the numbering structure of IEC 61000-X-Y, that means that the standards corresponding to each other, issued by the different committees, vary only according to their letter codes.)

EN 60XXX series number have those CENELEC standards that have been adapted from IEC but not belong to the IEC 1000 series. (For instance, hereto belong the EN 60555 series of standards, which deal with disturbances caused in power networks by household appliances and similar equipment.)

The European standards, dealing with radio frequency disturbances, have been taken over from CISPR documents and they have numbering of EN 55XXX series. (Hereto belong for e.g. the emission-related product family standards numbered as EN 55011, EN 55013... EN 55022 (corresponding to CISPR 11, 13, 14, 15 and 22 requirements).

The EMC standards developed by CENELEC are standards numbered as EN 50XXX series. Such general publications are the emission (EN 50081-1, 2) and immunity (EN 50082-1, 2) standards issued on residential, commercial and light industry environment. (These are continuously transferred to general standards of series 61000-6-Y.)

The majority of the telecommunications related standards have been elaborated by ETSI. These are published either as ETSI standards with numbering ETS 300... or as CENELEC standards with numbering EN 300.... The latter ones are, first of all, harmonised standards under the EMC Directive.

7.8.4. Requirements

The majority of *equipment-related requirements* has been produced by ETSI Technical Committee (Electromagnetic Compatibility and Radio Spectrum Matters – ERM). The requirements applicable for the considerable part of telecommunication network equipment are defined in the harmonised standard EN 300 386-2 (Electromagnetic Compatibility and Radio Spectrum Matters; Telecommunication network equipment, EMC requirements; Part 2: Product Family Standard) [7.8.7]. The scope of this standard covers the switching equipment, non-radio transmission equipment (such as multiplexers, SDH, PDH, ATM, DCC systems), power supply equipment and supervisory equipment. (Beside this standard, also other product standards include EMC requirements. For instance, special requirements are applicable for cable television systems.) The requirements according to the standard have been defined in a way so that the equipment has sufficient immunity. There might be cases with low probability, when the level of disturbance is higher than the immunity level specified in this standard. In such cases special mitigation measures shall be made.

According to the installation environment the standard is categorising the equipment into the following two groups:

- Equipment installed in telecommunication centres;
- Equipment installed in locations other than telecommunication centres.

Into the second category belongs, for instance, equipment installed in customer premises and outdoor locations such as street cabinets. In such cases, because of the non-controlled environment, the requirements are more severe.

In the followings – not aiming at the complexity – we introduce what kind of EMC tests are defined in the standard. The individual tests can be given as subsection, according to the ports to be tested:

- Testing of the enclosures (see Table 7.8.1.);

- Testing of ports of outdoor telecommunication signal lines (see Table 7.8.2.);
- Testing of ports of in-house telecommunication signal lines;
- Testing of ports of alternating current power supply;
- Testing of ports of direct current power supply.

Beside immunity and emission, this standard is including also the requirements of „resistibility”. (The resistibility means the ability of telecommunications equipment to withstand the effects of certain electrical, magnetic and electromagnetic phenomena without being damaged.) The following performance criteria serve for the control of compliance with the requirements of immunity and resistibility:

- Criterion „A”: The system shall continue to operate as intended; usually no degradation of performance or loss of function is allowed;
- Criterion „B”: The system shall continue to operate as intended after the test. Usually no degradation of performance or loss of function is allowed. During the test degradation of performance may occur, but no change of actual operating state or stored data is allowed.
- Criterion „C”: Temporary loss of function is allowed, provided that the equipment is self-recoverable.
- Criterion „R”: The equipment shall withstand the test without damage or other disturbances (such as corruption of software) and it shall operate properly according to the specified parameters after the transient electromagnetic phenomenon has ceased. The test may cause the operation of protection or fuses. After having them replaced or reset, the normal operation shall restore.

	Environmental phenomenon	Test levels and characteristics	Reference	Performance criterion	Remarks
Immunity					
1.	Electrostatic discharge	Contact discharge: 4 kV Air discharge: 4 kV	EN 61000-4-2	B	
2	Radio frequency electromagnetic field amplitude modulated	80 – 1000 MHz 3 V/m 80 % AM (1 kHz)	EN 61000-4-3	A	
Emission					
3.	Radiated Electromagnetic field at 10 m	30–230 MHz: 40 dB (μ V/m) 230-1000 MHz: 47 dB (μ V/m)	EN 55022	Not applicable	Large systems should be tested according to ETS 300 127
Resistibility					
4.	Electrostatic discharge	Contact discharge: 8 kV Air discharge: 15 kV	EN 61000-4-2	R	

Table 7.8.1. EMC test of equipment installed in telecommunication centres Enclosure port

Ports for outdoor signal lines

	Environmental phenomenon	Test levels and characteristics	Reference	Performance criterion	Remarks
Immunity					
1.	Fast transients	0,5 kV; 5/50 ns waveform 5 kHz rep. frequency	EN 61000-4-4	B	
2.	Surges	1 kV; 10/700 μ s waveform	EN 61000-4-5	B	
3.	Radio frequency conducted, continuous	0,15 – 80 MHz; 3 V; 80% AM (1 kHz)	EN 61000-4-6	A	
Emission					
Resistibility					
4.	Surges	4 kV; 10/700 μ s waveform	ITU-T Recommendation K.20	R	Applies to cables longer than 500 m with primary protection
5.	Surges	1 kV; 10/700 μ s waveform	ITU-T Recommendation K.20	R	Applies to cables longer than 500 m
6.	Power induction	300 V; 50 Hz; 200 ms	ITU-T Recommendation K.20	R	Applies to cables longer than 500 m

Table 7.8.2. EMC test of equipment installed in telecommunication centres

("Manual" intervention is allowed.)

Criterion „A” is applicable in case of continuous phenomena, criteria „B” and „C” in case of transient phenomena, and criterion „R” in case of resistibility tests.

Health protection and life safety regulations: Since the beginning of its evolution, the biosphere is subjected to the impacts of its environment. Due to the technical development, a wide spectrum artificial radiation with growing intensity is added to that. The natural RF radiation, which, first of all, is coming from the Sun, reaches the Earth with an intensity of less than 0.01 mW/m². Against it, the level of the man-made radio frequency interference (commonly known as “Electro-smog”) is varying in a range from several time ten μ W/m² that can be measured in households to several ten W/m² that can occur in certain workplaces [7.8.8].

In the interest to ensure that electromagnetic fields shall not cause adverse health effects, international and national guidelines, recommendations, regulations and/or standards define the basic restrictions and reference levels for intensity. In

general, these levels are determined with the principle that by evaluating the results of observations and experiments the malfunctioning of the central nervous system is stated and/or the value of the field strength or power density causing undesired overheating on the body surface or in the internal organs, is defined, and than this value is divided by a certain safety factor.

In connection with the above mentioned effects it needs to be mentioned: competent studies dealing with the results of epidemiological investigations emphasise that to date no correct analyses could provide convincing evidence of interrelation of RF exposure and risk of increased incidence of cancer.

In the latest recommendations and specifications - beside or instead of 'field strength' and 'power density' - the term of **SAR (Specific energy Absorption Rate)** averaged over the whole body or over parts of the body, is defined as the rate at which energy is absorbed per unit mass of body tissue and is expressed in watts per kilogram (W/kg).

In Hungary the Standard MSZ 16260-86 issued in the beginning 1987 and modified in 1993, is in force. The limits of the Standard are given in Table 7.8.3.a and Table 7.8.3.b. [7.8.9].

It is worth mentioning that the limits specified in the Hungarian standard are significantly lower than those contained in the EU Recommendation.

For the sake of historical correctness it is worth to mention what happened with the European Prestandard ENV 50166 that has been prepared by CENELEC. In 1994, still as a preliminary standard prENV 50166, it was distributed among CENELEC members with the request to submit their comments. In 1995, it was

Zone	Electric field strength, V/m		
	30 kHz - 3 MHz	3 - 30 MHz	30 - 300 MHz
Non-hazardous	3	3	3
Safety	50	30	20
Work-	120	60	40
Work limited in time	960/t*	480/t*	320/t*
Hazardous	1000	600	400

* Whereas t = duration of time in hours spent within the given zone in one calendar day. The value of t shall not exceed 8 hours.

Table 7.8.3.a - Electric field strength limits according to Standard MSZ16260-86

published in two parts, as European Prestandard:

ENV 50166-1 Human exposure to electromagnetic fields,

Low frequency (0 Hz to 10 kHz)

ENV 50166-2 Human exposure to electromagnetic fields,

High frequency (10 kHz to 300 GHz)

The Prestandard provides detailed information on the indirect and direct effects of low and high frequency electromagnetic fields, the possible sources, the methods for summary of effects of simultaneous exposure from more sources, the calculation and measurement methods, and of course the limits.

Considering that after its prolongation in 1997, it had not been finalised either in 1999, it has lost its effect. Between 1997 and 1999 it has been endorsed and issued also as a Hungarian National Prestandard. The limit values of it can be used even today as good references.

The Council of Health Ministers of the European Union on its meeting in June 1999 in Luxembourg has dealt with the Recommendation on the limitation of exposure of the general public to non-ionising electromagnetic radiation. The Council's work has drawn on the preparatory works of the International Commission on Non-Ionising Radiation Protection (ICNIRP) [7.8.10], and in connection with the adoption of the Recommendation some basic principles have been fixed [7.8.11]. In line with one of these important principles, the Recommendation leaves it to the Member States the classification of the radiation sources and the limitation of their emission. On 12 July 1999, the Recommendation was approved under Ref. no.: 1999/519/EC by the Council of the European Union on its meeting in Brussels [7.8.12]. The limits, basic restrictions in the Recommendation are specified first of all for the general public, the values for workplaces - in the spirit of the Union's Treaty - shall be determined in the Member States by the political decision making mechanisms.

The way of problem handling and the considerations of the Recommendation reflect the approaches of ENV 50166. Two restrictions are differentiated:

Zone	Power density, mW/cm ²	
	Standing radiator	Rotating, or scanning radiator
Non-hazardous	-	-
Safety	0,01	0,1
Work-	0,1	1
Work limited in time	$(0,08 / t^*)^{1/2}$	$(8 / t^*)^{1/2}$
Hazardous	10	100
* Whereas t = duration of time in hours spent within the given zone in one calendar day. The value of t shall not exceed 8 hours.		

Table 7.8.3.b – Power density limits in frequency band 0,3-300 GHz according to Standard MSZ16260-86

The basic restrictions have been calculated so, that 1/50 of the intensity values causing according to the research studies acute (nervous system and/or thermal) effects has been taken into consideration.

The frequency ranges of the basic restrictions are tallying with the following considerations:

- between 0 and 1 Hz basic restrictions are provided for magnetic flux density for static magnetic fields (0 Hz) and current density for time-varying fields up to 1 Hz, in order to prevent effects on the cardiovascular and central nervous system,
- between 1 Hz and 10 MHz the observation of basic restrictions provided for current density makes it possible to ensure normal functions of the nervous system,
- between 100 kHz and 10 GHz basic restrictions on SAR are provided to prevent whole-body heat stress and excessive localised heating of tissues,
- between 10 GHz and 300 GHz basic restrictions on power density are provided to prevent heating in tissue at or near the body surface.

The basic restrictions (limits) are shown in Table 7.8.4.

Reference levels are such, in physical quantities well measurable, limit values, the respect of which ensures that the basic restrictions will not be exceeded, even in the case of closest coupling of the field to the exposed human body. The other important role of the reference levels summarised in Table 7.8.5 and Table 7.8.6 consists in that they give orientation for the determination of the emission limits specified in the different series of standards detailed under section 7.8.2.

It might be of interest to pick out from the wording and make reference on two important statements of the Recommendation:

Frequency	Magnetic flux density, mT	Current density (rms*), mA/m ²	Whole body SAR (average), W/kg	Localised SAR (head, trunk) W/kg	Localised SAR (limbs), W/kg	Power density, (S), W/m ²
0 Hz	40	-	-	-	-	-
0-1 Hz	-	8	-	-	-	-
1-4 Hz	-	8/f**	-	-	-	-
4-1000 Hz	-	2	-	-	-	-
1-100 kHz	-	f/500	-	-	-	-
0.1-10 MHz	-	f/500	0,08	2	4	-
10 MHz-10 GHz	-	-	0,08	2	4	-
10-300 GHz	-	-	-	-	-	10

Table 7.8.4 Basic restrictions for general public according to EU Recommendation

*Averaged over a cross section of 1 cm² perpendicular to the current direction

**f = frequency in Hz

***All SAR values are to be averaged over any six-minute period

- Actions on limiting the exposure of the general public to electromagnetic fields should be balanced with the other health, safety and security benefits that devices emitting electromagnetic fields bring to the quality of life, in such areas as telecommunications, energy, life- and public security.
- Member States, in order to enhance understanding of risks and protection against exposure to electromagnetic fields should provide, in an appropriate format, information to the public on the health impact of electromagnetic fields and the measures taken to address them.

The literatures referred to under [7.8.13] and [7.8.14] provide a great help in the comparison of the national standards regulating this field. The considerations related to mobile handsets and base stations are not discussed here in this study, only a reference is made to the best known source of information on this subject matter [7.8.15]. We only draw the attention to the Hungarian National Standard dealing with the radiation safety requirements of laser products [7.8.16].

7.8.5. Tests

The type approval test carried out under laboratory conditions serves for the certification of EMC. The basic standards of series EN 61000-4-X give provisions for testing and measurement techniques. In the frame of these series there have been

Frequency	E-field strength, V/m	H-field strength, A/m	B-field, μ T	Equivalent plane wave power density, W/m ²
0-1 Hz	-	3.2×10^4	4×10^4	-
1-8 Hz	10 000	$3.2 \times 10^4 / f^2$	$4 \times 10^4 / f^2$	-
8-25 Hz	10 000	$4\ 000 / f$	$5\ 000 / f$	-
0.025-0.8 kHz	$250 / f$	$4 / f$	$5 / f$	-
0.8-3 kHz	$250 / f$	5	6.25	-
3-150 kHz	87	5	6.25	-
0.15-1 MHz	87	$0.73 / f$	$0.92 / f$	-
1-10 MHz	$87 / f^{1/2}$	$0.73 / f$	$0.92 / f$	-
10-400 MHz	28	0.073	0.092	2
0.4-2 GHz	$1.375 f^{1/2}$	$0.0037 f^{1/2}$	$0.0046 f^{1/2}$	$f / 200$
2-300 GHz	61	0.16	0.20	10

Table 7.8.5. Reference levels for general public according to EU Recommendation

*Frequencies are expressed in the relevant measuring unit of the frequency range investigated

issued so far standards dealing with the following issues, and these reflect quite well to the great variety of phenomena to be taken into consideration:

1. Overview of tests;
2. ESD immunity tests;
3. Radiated radio-frequency field immunity test;
4. Electrical fast transient / burst immunity test;
5. Surge immunity test;
6. Conducted radio-frequency immunity test;
7. General guide on harmonics and interharmonics measurements for power supply systems and equipment connected thereto;
8. Power frequency magnetic field immunity test;
9. Pulse magnetic field immunity test;
10. Damped oscillatory magnetic field immunity test;
11. Voltage dips, short interruptions and voltage variations immunity tests;
12. Oscillatory waves immunity tests;
14. Voltage fluctuation immunity tests;

Frequency	Maximum contact current, mA
0 Hz-2.5 kHz	0.5
2.5-100 kHz	$0.2 f^*$
100 kHz-110 MHz	20

*kHz

Table 7.8.6 Contact currents for general public according to EU Recommendation

- 15. Flicker test;
- 16. Conducted common mode disturbance immunity test in the frequency range 0-150 kHz;
- 24. Test methods for protection devices for HEMP conducted disturbance;
- 27. Unbalance, immunity test;
- 29. Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests.

(The list is not complete, because this series of standards is under continuous future development .)

In section 7.8.4.1 the tests of wired telecommunications networks have already been discussed. Regarding wireless systems, some standards, elaborated by ETSI, worth mentioning as well, which specify both limits and measurement techniques:

EN 300 279: Conducted and radiated disturbance signals of Private land Mobile Radio equipment

ETS 300 329: Emission and immunity tests of DECT equipment

ETS 300 339: Measurement methods and limits for radio communications and connected ancillary equipment, regarding which a harmonised EMC standard does not give stipulations

ETS 300 340: Emission and immunity tests of ERMES receivers

EN 300 341: Emission of Land mobile radio communications equipment

ETS 300 342: Emission and immunity tests of GSM and Digital Cellular Systems (DCS)

EN 300 385: EMC measurements and limits for Fixed Radio Links

EN 300 390: Emission of radios with built-in antenna of Land mobile radio communications systems

ETS 300 447: Emission and susceptibility of VHF FM broadcasting transmitters

EN 300 673: EMC measurements for terrestrial VSAT equipment

ETS 300 717: EMC tests for public analogue cellular radio communications equipment. Mobile and portable equipment

ETS 300 826: 2.4 GHz wide-band transmission systems and HYPERLAN

EN 300 827: EMC measurements and limits for TETRA equipment

7.8.6. Guidelines aiming at ensuring electromagnetic compatibility

There are many types of installations and electromagnetic compatibility can be successfully achieved through different approaches. The IEC 61000-5-1 standard [7.8.17] recommends a general approach, by the application of which special mitigation methods might not be necessary when the equipment satisfies applicable emission and immunity requirements.

The process adopted for ensuring electromagnetic compatibility of equipment and installations may take two approaches, depending on how early in the design, and implementation the EMC requirements are taken into consideration.

- At the early stages of major installations, each compatibility level (specific for a given electromagnetic disturbance) can be assigned for the particular environment of the installation or equipment. Through the application of the overall mitigation schemes, the apparatus and its installation practice are then specified with immunity and emission levels corresponding to the predetermined compatibility level.
- At later stages of the design, for the installation of additional apparatus or the initial installation of commercially available apparatus, for which no opportunity exists to modify its EMC characteristics, a mismatch may occur between the overall, *de facto* compatibility level of the site and the capability of the apparatus. In such a case, mitigation methods shall be selected, in order to close the gap between the environment and the apparatus immunity levels to a minimum.

Electromagnetic disturbances are caused by conducted or radiated phenomena. An apparatus can be both the emitter and the susceptor (potential „victim”) at the same time.

With regard to electromagnetic compatibility there are three main areas that can be considered:

- emitters: sources of disturbances, influenced by the design of the apparatus;
- coupling paths: influenced by the installation practices;
- susceptors: influenced by the design of the apparatus.

In order to assure EMC, three types of measures should be applied, as necessary:

- at the emitter: reduction of emission;
- at the coupling: reduction of coupling;

- at the susceptor: increase of immunity.

In the interest to provide a transition from the overall concept by analysis the interrelation between the environment and the apparatus and to come to the application protection method, the ports of the apparatus (which are the interface of the apparatus toward the external electromagnetic environment) shall be investigated. The various EM disturbances enter or exit the apparatus through these ports. By identifying such ports, protective steps can be specifically related to the nature of the EM phenomenon, its coupling path and its impact on the functional elements of the apparatus (immunity) or on the environment (emission).

Figure 7.8.2 introduces the input ports of electromagnetic disturbances.

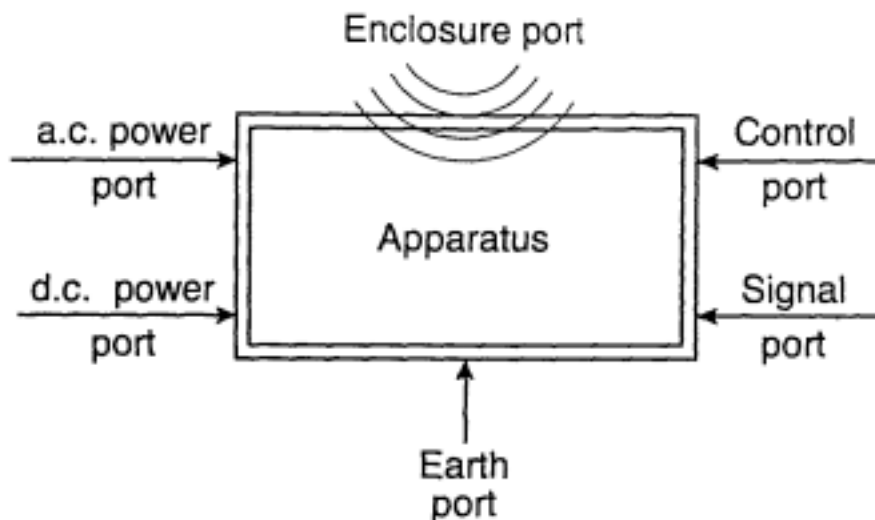


Figure 7.8.2: Representation of equipment ports interfacing with the electromagnetic environment

For the electromagnetic compatibility appropriate mitigation steps should be applied on every port of the apparatus (system, installation).

There are two general approaches to obtain EMC immunity for an installation, either by a global protection (figures 7.8.3. and 7.8.4.) or by a distributed protection (Figure 7.8.5). In certain cases, mitigation methods might not be necessary, for instance, if the equipment has a sufficiently high immunity level, compared with the prevailing disturbance level.

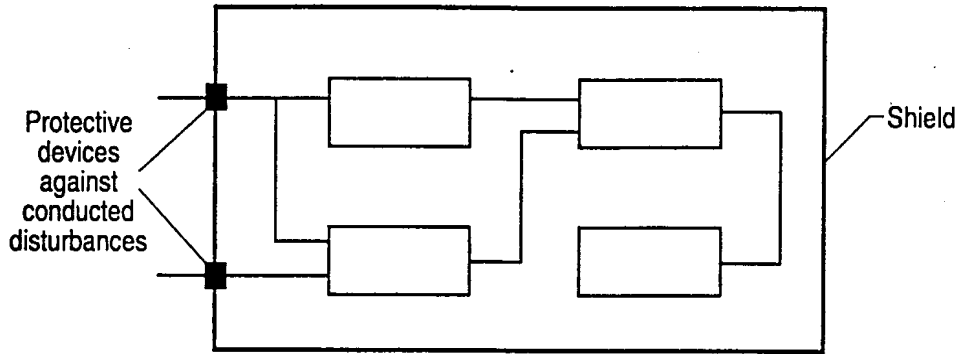


figure 7.8.3: Global protection by single barrier

NOTE: According to the principle of a single barrier, mains filters, surge-protective devices and a shield protect the whole installation. No specific protection is applied to the individual units, except when internally generated disturbances exist.

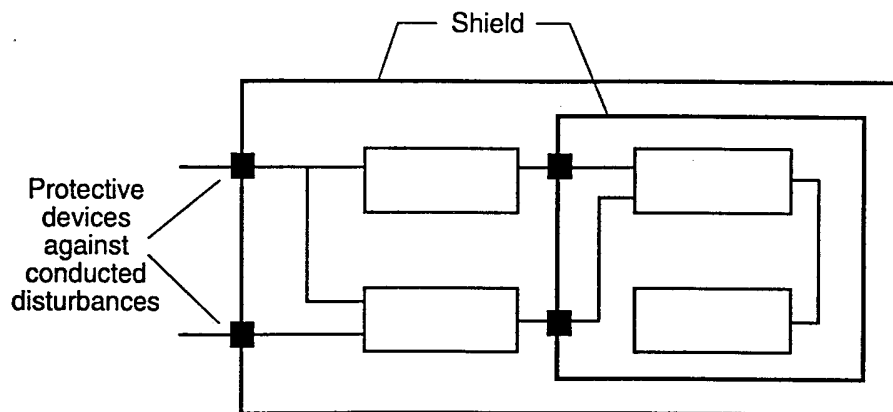


Figure 7.8.4: Global protection by multiple barriers

NOTE: According to the principle of multiple barriers, no specific protection is applied to the individual units, but there is a cascading of multiple electromagnetic barriers according to the susceptibility level(s) of the units.

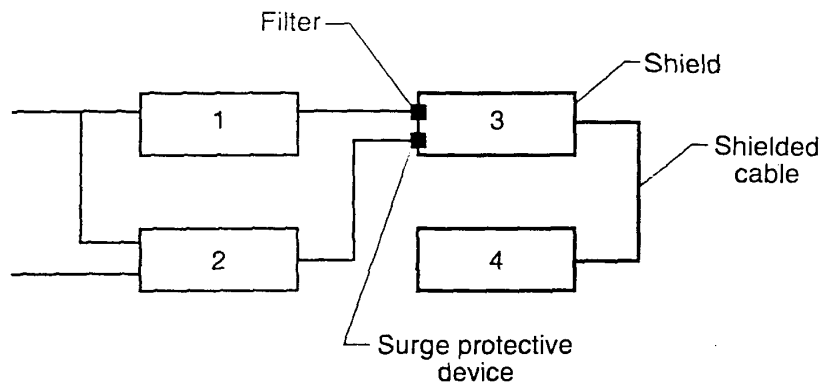


Figure 7.8.5: Principle of distributed protection

NOTE: According to the principle of distributed protection, units 1 and 2 are not protected, only units 3 and 4, which contain sensitive electronics, are protected. For the protection of the latter ones, specific enclosures, filters, or other protective devices and shielded cables are used.

List of abbreviations

CENELEC	European Electrotechnical Standardization Committee
CISPR	International Special Committee on Radio Interference
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ERM	Electromagnetic Compatibility and Radio spectrum Matters (ETSI Technical Committee)
ESD	Electrostatic Discharge
ETSI	European Telecommunications Standards Institute
HEMP	High Amplitude Electromagnetic Pulse
ICNIRP	(International Commission on Non-Ionising Radiation Protection)
IEC	International Electrotechnical Commission
ITU	International Telecommunication Union
LEMP	Lightning Electromagnetic Pulse
NEMP	Nuclear Electromagnetic Impulse
SAR	Specific energy Absorption Rate

Bibliography

- [7.8.1] MSZ IEC 50(161) International Electrotechnical Vocabulary (IEV), Chapter 161: Electromagnetic compatibility (1994)
- [7.8.2] MSZ IEC 1000-1-1: Electromagnetic compatibility (EMC), Part 1: General, Section 1: Application and interpretation of fundamental definitions and terms
- [7.8.3] Directive 89/336/EEC (Electromagnetic compatibility), (1989)
- [7.8.4] Guide to the application of Directive 89/336/EEC, (1997)
- [7.8.5] Joint Decree No. 31/1999. (VI.11.) GM-KHVM on Electromagnetic Compatibility
- [7.8.6] CENELEC Report: R210-001 EMC standardisation for product committees (January, 2000)
- [7.8.7] EN 300 386-2: Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; Electromagnetic Compatibility (EMC) requirements; Part 2: Product family standard (1997-12)
- [7.8.8] WHO: Electromagnetic Fields and Public Health, Fact Sheet N183, <http://www.who.int/inf-fs/en/fact183.html>
- [7.8.9] MSZ 16260-86, Permissible limits of high frequency electromagnetic fields
- [7.8.10] International Commission on Non-Ionising Radiation Protection: Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz), Preprint scheduled to appear in Health Physics April 1998, Volume 74, Number 4, pp. 494-522
- [7.8.11] European Union, Council of Health Ministers: Adoption of a recommendation on the limitation of exposure of general public to electromagnetic fields
http://europa.eu.int/comm/health/ph/news/old/electro_en.htm
- [7.8.12] COUNCIL RECOMMENDATION of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz), (1999/519/EC) Official Journal of the European Communities, 30.7.1999
- [7.8.13] Mátay G., Zombory L.: Physiological impacts of radio frequency radiation and its applications in medicine and biology, University Learning Book Publishing House Budapest Technical University, Budapest, 2000
- [7.8.14] Thuróczy Gy.: Radiation health aspects of mobile communications, 'Magyar Távközlés' July 1998, Volume IX., Number 7, pp. 26-33.
- [7.8.15] International Commission on Non-Ionising Radiation Protection: Health Issues Related to the Use of Hand-Held Radiotelephones and Base Transmitters, Health Physics April 1994, Volume 70, Number 4 pp. 587-593
- [7.8.16] MSZ 16261, Radiation safety requirements of laser products
- [7.8.17] MSZ IEC 61000-5-1: Electromagnetic compatibility (EMC) Part 5: Installation and mitigation guidelines, Section 1: General considerations. Basic EMC publication
- [7.8.18] IEC TS 61000-1-2 : General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena

7.9. Equipment and system selection considerations

Gábor Nagygyörgy dr., author

Kántor Csaba dr., reviewer

7.9.1. Introduction

The purpose of the present chapter is to give a short overview upon the major technical criteria of system selection, but some other considerations, which – in addition to the technical requirements – influence our choice, shall be highlighted as well. Among them, the reliability of the vendor/supplier from market, or financial points of view, or the life-time costs, etc. can be mentioned.

At making a choice of a telecommunication system, the first task of the planner/designer is to determine and specify the main functions of the system, i.e. to decide what is needed. This usually includes a technical analysis based on marketing survey, a system planning. On the basis of the large-scale and later the detailed system plan, the buyer issues a tender invitation. By the assessment and evaluation of the bids received the most appropriate telecommunication system can be chosen on the basis of the analysis of the technical and financial criteria. The system selection means, therefore, such a technical/financial analysing and planning process, in the course of which the buyer – with regard to the market conditions – brings into harmony his needs with the possibilities. In the following chapter we give an overview upon the major steps of this process and the key criteria of (system) selection. Let's clarify first, what is meant by a system.

System (A): a system shall mean the totality of objects being in interrelation with each other, including their interrelations, structure and dynamics.

Telecommunication system (B): a telecommunication system shall mean an organised totality of a certain set of terminal equipment, switching and transmission technical devices for making a service provisioning possible.

7.9.2. Technical aspects of system selection

The planning process described below is for the case of development of an absolutely new system. In the practice, usually new partial, sub-systems are added, adapted to an already existing system, or existing systems are expanded or extended. If it is the case, then certain steps are reasonable omitted from the hereunder described procedures of specification and selection.

7.9.2.1. Large-scale system plan

At system planning the parameters – technical requirements – of the telecommunications system in question are determined with a “from top to bottom” approach. It means that first we are modelling from endpoint to endpoint the whole info-communication connection (in a “high-level model”, “large-scale macro-model”, “large-scale system plan”), on the basis of which – “going downwards” – we determine and allocate the individual system components, elements and the requirements of equipment.

In the large-scale system plan, there shall be specified the signaling, the signal levels, circuit parameters from subscriber to subscriber. In the macro model, all of terminal equipment and network resources constitute a customer-to-customer integral whole, whereas the individual system elements possibly do not have a requirement of their own. The large-scale (high-level) particularities are often prescribed in ITU-T, ETSI or other standardised systems, reference models, but making of our own, non-standardised, individual models is also allowed. Reference network requirements are included also in the fundamental technical plans issued by the national regulatory body (HÍF). The standard reference models sometimes include recommendations for the allocation of parameters of the system elements, as well. The planner has to design the actual system in accordance with the guidelines given by the reference model. The large-scale planning is thoroughly discussed in other chapters of the book. Creation of models is a very time-consuming task, the standardisation bodies are working on their appropriate reference models over years. The planning of non-standardised systems, therefore, requires lot of time and increases the risk of the telecommunication service providers (see later).

The most important aspect of the selection is the implementation of the operation (functions) provided by the system. The planner has to quantify the needs of the customer, transform them into the terms of technical requirements. Such customer needs are the volume of information, the speed of access to the data, the soundness of the data, the usability, reliability of the connection, the expected volume of traffic, the comfort at use, etc. In addition to it, further functional requirements are determined by the financial, economical interests of the telecommunication provider, or by the legislative or authority regulations and stipulations. Here we can mention: the cheap and well manageable operability and maintenance, the billing possibilities, the customer's safety and security, or the noise load on the environment, etc. With due analysis of the functional demands – the logical structure (architecture) of the system can be built up with regard to the different aspects of planning and to the requirements of standards and norms, and in this way the technical requirements for the whole complex system can be specified. In a great number of cases the planner/designer can find a standardised model (reference) system which is suitable for the satisfaction of the functional requirements.

A large-scale system plan is modelling the connection from endpoint to endpoint, the requirements of it describe the technical parameters of the whole connection. The groups of the major requirements of system plans are usually specified in standards. The main categories of the requirements are:

- *Structure of the system, i.e. the logical and functional system architecture.* It includes the system building blocks, the system components as well, along with the location and relations of the sub-systems and equipment. A telecommunication company needs not only the telecommunication functions, but also the support systems which support the servicing of the customers and operation of the network. A state-of-the-art telecommunication system today is planned, designed, constructed and purchased only along with network management, O&M support and billing systems. We have to give the supplier the large-scale system plan (reference model, architecture) for the systems we are intended to purchase, on the basis of which we have specified the requirements for the system and the individual system elements.
- *Quality of the transmitted signals:* signal levels, signal bit rate, signal shape, signal distortion and modulation noise, reflection, attenuation, etc.
- *Continuity of the connection:* susceptibility, drop-out time, time to failures.
- *Message routing, message handling:* signals and protocols, synchronisation.

- *Network management*: traffic routing, monitoring, alarms and security signals, etc.
- *Serveability performance* (number of subscribers, traffic capacity,) and expandability, trafficability and overloadability.
- *General requirements of sub-systems*, like, for instance, the general requirements of NMS, tariffication and billing/accounting systems linked to the telecommunication system.
- *Security system requirements*: control and limitation of access, security system administration, etc.
- *Interface requirements* (integration, adaptation requirements) towards the existing systems, or other platforms, or towards the network management and billing systems,

and in addition any other – above not mentioned – technical requirement, that in general the implemented network and platform shall meet in the interest of establishment and maintenance of a continuous telecommunication connection and proper servicing of customers.

Since the telecommunication systems usually consist of equipment accommodated in different environment and of transmitting media among them, it is possible only rarely to fix requirements also for the installation conditions of the complex system in the large-scale plan. The installation, implementation requirements of the general system plan are applicable for the first implementation and for the deployment. A well-designed telecommunication system can be expanded, extended gradually, in small steps, according to the needs, even by subscriber or by channel. Possible the system shall be so construed that also the first implemented segments can provide full functionality.

7.9.2.2. Detailed system plan: system element-related requirements

The **detailed system plan** can be produced – making due planning considerations – from the general network requirements. In the course of making the detailed planning, the requirements of the sub-systems, system elements, modules can be defined, allocated. Similarly, first the general functional requirements of the system elements and modules are defined in a way, so that they match to the operation of the whole system. The system elements are the elements of the physical network, and at the same time they are telecommunication equipment. Therefore in the course of the detailed system planning, we have to determine expectations,

requirements also for the physical design, outlook, **construction**, as well as for the **installation** of the system elements. The system elements may be hardware and software elements or their combinations.

The system element requirements are defined according to the following categorisation:

- Allocated transmission or signal processing requirements (e.g.: insertion loss, allowed drop-out, noise, etc.),
- Individual operational requirements, (e.g.: signal processing, disturbance/noise emission, etc.)
- Software requirements and
- Equipment-related requirements, as to their:
 - Construction,
 - Accommodation,
 - Operation and Maintenance
- Installation-related design, transportation, mounting and environmental requirements.

With an object oriented approach, it can be stated that the software programs, having their own characteristics, features, are similar, equivalent system elements of a telecommunication system, like the equipment. The software selection and the specification of the software requirements play a very important role from the point of view of the operation and quality of the whole info-communication system. The software elements of the telecommunication system and the requirements of them shall be specified on the basis of the large scale and the detailed system plans as much detailed as it is already usual at the specification of the equipment's construction requirements. Reference [C] gives a quite rich source of literature information and of standards covering this subject matter.

The software programs of telecommunication equipment are very often based on standards (for instance the protocols), in such cases, instead of a detailed system requirement, it is sufficient to refer to the given standard only.

General software requirements are: portability, easy usage, re-usability, accuracy, testing, maintainability, possibility of modification (corrective-, adaptive- and improvement modifications), reliability, efficiency, integrity and finally the deepness, comprehensiveness of documentation.

When making the software specifications, especially the followings shall be taken into consideration:

- The platform on which the software should work.
- Other software systems, with which the software shall interwork, i.e. what are the software interface requirements.
- Remote software monitoring and remote software downloading shall be specified, as a requirement.
- Reasonably the software should be intelligent enough to be able to recognise, identify and possibly prevent the false controlling commands. According to certain statistics, 40% of outages of the modern, sophisticated telecommunication networks is attributable and originated from the issue of false, mistaken commands.
- The software reliability, or the required conditions of reliability assurance.
- Safety of the software
- A special attention shall be given to the software security. The software shall have such a protection system, which recognises the attacks, registers them, or probably can eliminate them. Nowadays, one of the most risky problems in the operation are the malicious attacks against the telecommunication systems. The successful attacks cause harm of reputation of the firm but on a longer time they may lead to that that the subscribers, customers go to another service provider.
- The existence of a software supporting organisation shall be required. This often means a multi-level organisation, which shall render a 365-day, 8760-hour, i.e. continuous (round-o-clock) assistance to the operator of the system.
- Training of the software operators shall be required, as well.

7.9.2.3. Operational requirements

The telecommunication network shall have a *network management sub-system*. The O&M system shall make the “remote alarms”, remote diagnostics, fault detection and fault localisation possible, as well as the re-routing of the traffic from the defective segments to alternative ones. In addition, the fault correction activities shall be supported by fault correction task issuing and feedback, reporting sub-systems (e.g.: workflow programs). There shall be taken into consideration the impact of timescaling of the expansion of network operation and the telecommunication system onto the building up of the management sub-system. For the remote supervision, monitoring of the telecommunication system it is necessary that each and every system element is adapted to the network management sub-system. The type of the management system interface shall be specified. Also the

equipment shall support the remote diagnostics, remote fault detection and regular operational testing (without causing an observable interruption in the operation).

The *availability* of the services is influenced by the reliability of the network. A service network with acceptable availability can be built-up even from less reliable system elements, if the network has hot reserves, alternative routes and paths. Chapter 7.1 of our book discusses in details the interrelations between the reliability of the system elements and that of the network and the relevant planning aspects.

The permitted outage parameter values for the system elements and equipment can be usually calculated, or derived and allocated from the system structure and from the availability requirements of the services. The reliability of the equipment has financial/economical aspects as well, since the more reliable equipment is often more expensive. The reliability allocated to the individual elements is influenced also by the useful life-time costs, or operational considerations: the operation of a more reliable equipment is cheaper, since the probability of outage of such a unit is lower. The system designer has the possibility to optimise the total costs of the whole system with reasonable modification of the system structure, or topology (alternative paths, routes, reserves, etc.).

In case of development of a green-field system, a Billing Sub-System plan shall be made, as well. The details of it – reasonably – are almost the same like the telecommunication system selected according to the above described criteria.

In case of an already existing, known billing system, we prescribe that the new telecommunication system shall have appropriate interfaces towards the tariffication and billing sub-systems.

7.9.3. Design and construction requirements of equipment

7.9.3.1. Construction

The construction of system elements shall be designed with consideration to the criteria of installation. The installation into telecommunication building can be judged first of all on the basis of financial and operational safety considerations. The ease of mounting of the device is one of the important parameters of installation. The modular construction, the easy interchangeability of the components, the

arrangement of and accessibility to the moduls, their stability and protection against tilting over, support and facilitate the operability and maintenance. The possibilities for the accommodation of cables shall be specified both for the telecommunication buildings and for the customer premises. The design and construction of the cooling block, ventilation is important, similarly to its adjustment to the building's air-conditioning system. In addition, the network elements accommodated in the customer's premises shall comply with severe security, safety and esthetical requirements, too.

The investment demand of a telecommunication building installation can be reduced by the reduction of the size of the equipment, by the application of an appropriate form (with proportionate dimensions of the height, width and depth), and low weight- and floor load. At the same time we have to consider that the specific dissipated heat in space of an equipment of smaller size may be higher, which may require more intensive cooling.

The network termination equipment accommodated at the customer's premises shall be as small as possible and protected against environmental impacts.

In telecommunications building installations the equipment are well protected. In outdoor, public places, however, strict protection requirements shall be enforced against the enclosure of the equipment: it shall provide protection against impact, drip, dust, insects, unauthorised access/intrusion, breaking up and line-tapping.

Environmental resistance is standardized in every countries.

Any system element shall operate normally according to its specifications at the place of its installation. The criterion of the selection is that the equipment shall withstand the ambient, environmental operation conditions both indoor in temperature controlled or non-temperature controlled locations and also in outdoor and underground locations in case of stationary or mobile accommodation. The environmental resistance requirements shall be specified for transportation and storage as well. The easiest way to specify the environmental resistance is, making a reference to the relevant standards. The ETS 300 019 multi-part standard series of ETSI, reducing the range of standards specified in the well-known IEC 723 standard series, include a set of environmental requirements applicable for the European climatic conditions. The standards provide recommendations for the requirements of

ambient temperature and air conditions (solar radiation, operation in a heat-trap, etc.), and that of mechanical, climatic, atmospheric, biological, chemical hazards and impacts (like groundwater, gases and impurities, etc.).

Environmental protection criteria is defined in accordance with the possible accommodation

Nowadays it is a very strong expectation from the side of the society that the equipment, facilities of a telecommunication system, if they are accommodated outdoor, shall fit into the landscape. Therefore, such equipment shall be installed in places, where they cannot be seen, or if it is not possible, for e.g. in case of radio equipment, an equipment having a camouflaged enclosure, shall be selected. It is an important criterion of the selection, that quantity of contaminating waste materials during the installation and later the operation shall be minimised. The system elements must not include any radioactive substance (even not in ionizators) and the mounting, installation waste materials shall not be poisoning, either. Similarly, the high frequency signal emission (radiation hazard) might be also an important environmental factor.

Electromagnetic compatibility (EMC) requirements are set forth in standards and legal rules. In Hungary the equipment shall comply with the disturbance emission standards specified in the Decree of the Minister of Economy. In accordance with the standards also the (electromagnetic) susceptibility of the system elements shall be specified, namely according to the requirements of the installation environment. Electromagnetic disturbances may intrude or be emitted through the telecommunication and the energy supply interfaces as well, therefore the EMC requirements shall be enforced against all such interfaces. The key criteria of the selection are: susceptibility (radiated, conducted /low and high frequency), emission (radiated, conducted / low and high frequency, modulated), protection against discharges, fast transients (bursts) and surges.

7.9.3.2. Energy supply and consumption

The energy is becoming more and more expensive, the daily usage time of informatics systems is longer and longer, because of the spreading of on-line services. Due to these, keeping the energy consumption at a low level, is an aspect

at the selection, which is getting more and more important. The energy supply demand of the system element shall be adjusted to the energy supply capabilities of the existing network, in the telecommunication buildings, exchanges, in the access segments (DC power supply, remote feeding), and in the customers' premises, as well (low voltage AC supply). The requirements of the power interface are specified in the knowledge of the existing energy supply system. These requirements shall cover:

Power (feeding) voltage values, operation in normal and abnormal (non-standard) voltage ranges, voltage control, power consumption. In addition, the protection against the mentioned EMC disturbances (noise emission, protection against noise), as well as protection against transient phenomena (e.g.: protection against lightning), possibility of remote diagnostics, protection against electric shock, shall also be specified.

In this respect special attention shall be paid to the uninterruptable power supply of system elements installed at the customer premises (NTU, terminal equipment). The terminal equipment can be powered either from the mains supply network of the public utility company (Electric Works), or locally. In the second case the required uninterruptable energy supply shall be specified on the basis of the customer's needs and in accordance with the prevailing statutory regulations. It shall be considered as well, whether the costs of energy burden the customer, or the telecom service provider.

Grounding is one of the important safety requirements.

The equipment installed in telecommunication buildings shall comply with the requirements of the national grounding standard in force. In the customer premises, living houses of old construction there are often obsolete grounding solutions applied and various grounding systems are in operation in the different regions of the country. It is reasonable, therefore, to require the availability of the equipment operating in the customer premises in a version, which is adaptable to several grounding systems, so that the service provider has not to re-construct, re-build the grounding of the subscriber's building.

Cooling

The energy dissipated by the equipment may lead to such a temperature rise that endangers the normal, standard operation. Therefore, construction of a reliable cooling system is an important criterion, which influences the availability. The energy consumption of the cooling system is considerable, therefore consideration shall be given to the economical construction of the cooling system, too. If the conditions of installation, accommodation are known, it shall be required that the cooling system of the equipment is adapted to the cooling system of the whole building.

7.9.3.3. Safety requirements

The safety characteristics – serving for the protection of life, health and against loss or damage of properties – of system elements installed in telecommunication exchange buildings, or especially in the customer premises or dwelling units, are prescribed generally in mandatorily observable standards. Such ones are:

Electrical safety requirements, e.g.: protection against electric shock

Surface temperature of covers

Shape of covers: it shall not cause a mechanical injury

Requirements in connection with fire protection:

Resistance to fire and

inflammability of the equipment (i.e. its ability to cause fire);

Existence of fire barriers among the components of a large-sized equipment.

Hazard of radiated energy and shielding of the radiation. It is a requirement that the laser shall not go into the eye, but it shall be shielded against other high frequency radiations as well.

7.9.3.4. Transportation and packaging requirements

It shall be required from the manufacturer of the system that the dimensions, the weight, the design of the equipment shall make it as easy as possible the transportation of the unit to the place of destination and putting it into its final place of

installation. The „transportation resistance” as resistivity against damage in transportation we have mentioned already among the environmental resistance criteria. From the packaging it is expected that the packaging material shall not be harmful to the environment and it shall properly protect the equipment, spare part, etc. from the environmental impacts. The packaging of sensitive spare parts or units shall provide protection against electromagnetic disturbances as well. The packaging shall include the identification labels.

7.9.4. Other considerations

Operations and maintenance support

The operation of a system can be effected either by the owner of it, or by the vendor/supplier or other contractor/partner. The vendor/supplier may help this work by rendering professional advisory assistance, shipping of spare parts, supplementary materials, devices or equipment, operating a repair shop, storage facilities, remote supervision or a system support centre. Reasonably from the technically acceptable systems that one should be chosen, the supplier of which provides the most favourable services, possibly for the entire useful life-cycle of the system delivered. The buyer may determine the intended useful life-cycle of operation and fix it in the contract concluded with the vendor.

Training requirements

The operation of the telecommunication, IT systems is becoming more and more difficult and complicated. Attention shall be paid at the selection that the supplier/vendor provides the necessary training for the operating/maintenance staff, even supplying also the customers with adequate informative brochures, descriptions. Mention must be made also of requiring proper documentation on the system elements.

Qualification of the manufacturer, vendor/supplier

According to law, the buyer is responsible for the quality of the system purchased by him. This responsibility cannot be shifted over to the manufacturer, or vendor/supplier. It means that the telecommunication systems are built-up of

equipment, software programs and other system elements, for the quality of which the telecommunication service provider (buyer, owner of the network) is responsible. The quality of the purchased goods is assured by the purchase quality systems, which systems imply also the qualification/certification of goods and the manufacturers as well. This topic is not the subject of the present book, but those who are interested in deeper study of this issue, may refer to the series of ISO 9000 standards and to the rich literature (for instance: D).

7.9.5. Risks of system selection

In the followings, without aiming at complexity, we call the attention only to some important risk elements. In the interest of minimising the risks, the Buyer – after a comprehensive risk analysis – may set forth guidelines or principles and rules for system selection.

If the planner/designer does not have yet matured ideas, since he/she is looking for a very innovative system, for which at the given time a standardised solution is not yet available, then this increases the risk of the selection. It may happen that the technical evolution takes a different turn in the future, and the selected system becomes very soon obsolete or out of date. The operation, expansion, supplement of non-standardised systems cost always more than that of the system based on commonly used standards.

In the most cases, the system selection means the selection of the manufacturer or supplier/vendor, as well, which results in that the buyer is bound for a longer time to the manufacturer and his systems. Therefore, the right selection of the supplying partner implies a high financial risk. The operation, maintenance, repair of the selected system greatly depend on the supply of reserves and spare parts, on the customer service of the supplier. Similarly, the necessity of later technical enhancement, further development or expansion of the system shall be kept in mind, as well. In case of selecting not the right supplier, the manufacturer's technological backwardness, or if the manufacturer's company is wound up, the additional development done by a different company, may lead to huge incremental costs. So thus, whether the manufacturer is a well-qualified, financially strong company, or not, is also an aspect of system selection.

Specification of the requirements not in the right way, bears high risk for the customers. The requirements may be inadequate in different ways: Either we specify insufficient requirements, or to the contrary, we prescribe more parameters than it is necessary; at the selection of the system we enforce less strict, or much more strict than necessary requirements. Especially the appropriate specification/selection of the software elements of the system is important, because more and more portion of operational failures of even sophisticated systems is attributable to system failures. In case of purchasing of an underspecified system, it may happen that we do not buy such functions, features that later become important, or to the contrary, maybe that we purchase unnecessary system intelligence, paying extra price and cost for it, but which we cannot utilise. The specification risk can be minimised with value analysis.

If too much weight is given to the purchasing price among the criteria of the selection, it may happen that we will choose a cheap, but from technical points of view not the best system, which will not fill its function and/or will not fit properly to other, already existing systems.

7.9.6. Tendering

The law sets forth a tendering procedure for the selection of elements of a public telecommunication system and for the establishment of such networks. The infrastructure of a given service shall be selected after due consideration of technical and financial conditions. Within the invitation for tenders the Buyer specifies his financial/economical and above described technical requirements.

Evaluation of tenders

The Act on Public Procurements offers enough flexibility for the constructor of the network, who can make his choice not only and exclusively on the basis of the price of the system. The issuer of the tender invitation is not bound by the law to purchase such systems which are obsolete, or cannot be adapted to his existing systems, even not in the case, when the price of them is the best. There are various applicable methods of evaluation to avoid choosing of a technically unsuitable system. According to the one of the well-known procedures, there are two rounds for bidding organised. In the first round the buyers stipulate their technical/economical/financial criteria in connection with the system. Then the

technically acceptable offers are selected and price offers are asked from the best vendors. In the second round the price offers of these vendors are evaluated.

Life-cycle costs

In the most commonly used procedure, the evaluation of the technical/financial and (budgetary) price offers is taking place in one round. It is very important to establish a reasonable weighting proportion between the price and the technical capabilities of the system. At the consideration of the economical/financial aspects, reasonably not the purchasing prices shall be compared, but the life-time costs which include or take into account the purchasing price and the maintenance, repair costs, expenditures that have to be spent on the system over the whole useful life-cycle. Though the life-time costs to a great extent depend on the organisation, efficiency of the provider (buyer), but it is obvious that the network operator is doing this comparison on the same financial/economical basis. (It is easy to see that in case of a system, which requires less maintenance, also the life-time costs of it will be less.)

References

- [7.9.1] Információrendszer fejlesztés (Information system development) (Raffai Mária, 1999)
- [7.9.2] Távközlő Rendszerek megbízhatósága. Szótár, értelmező szótár (Reliability of telecommunication systems, Explanatory vocabulary.) Híradástechnikai tudományos egyesület 1974
- [7.9.3] Magee, Tripp: Guide to software engineering standards and specifications (Artech House, Boston 1997)
- [7.9.4] Ince, D.: ISO 9001 and Software Quality Assurance, McGraw-Hill, 1994

