

## Introduction and Overview

### 1.1 On the Interest in SS 7 Network Security and Reliability

Our modern industrial society requires high-performance communication systems which may be adapted very quickly and at low cost to individual customer's needs. With this objective network operators are introducing modern communication systems. These are open systems that need their own internal communication system to realize their different distributed tasks. This internal communication system for the interconnection of digital exchanges in public telecommunication networks is called Signalling System No. 7 (SS 7), the functions of which are based on the SS 7 network. According to the Open Systems Interconnection (OSI) model the term "*network*" refers to the Layer 3 *network service*, which is offered by the Message Transfer Part (MTP) and Signalling Connection Control Part (SCCP) to higher layers. An SS 7 network outage results in a breakdown of signalling between the individual nodes of the network, so that telecommunication network services are no longer available to customers. Apart from the tremendous financial damage to the network operator, the social consequences of such a network breakdown cannot be underestimated.

Since the MTP is the central part of the SS 7 network, it is of crucial importance for network security and reliability. The MTP is published in different versions within the "*Yellow Book*", the "*Red Book*", the "*Blue Book*" and the "*White Book*". This means that the MTP has been developed and specified for about 16 years and should now be what we call "*stable*". Is it really stable? Does it work properly in real networks? Does it fit new requirements so that no further changes within the MTP are needed?

Various different implementations have existed for a long time and are used in national as well as the international network. Due to this, an objective is not to perform any further changes within the MTP in order to avoid compatibility problems with existing and running systems. Experience shows that compatibility problems are *always* related to further development of the MTP. As a consequence, the overall opinion is that changes within the MTP should only be considered if problems oc-

cur which cannot be solved within other layers. Are there problems such that further changes within the MTP are really necessary?

This question has been studied intensively during the White Book study period and detailed discussions are going on now. In particular, the following items were raised:

- There are some indications that existing MTP procedures do not work properly during normal operation. What are the reasons?
- New applications like mobile or intelligent network (IN) applications, the realization of high-speed links by using the MTP-3 over the Internet protocol (IP) or the use of the MTP-3 above the signalling ATM adaptation layer (SAAL) in a broadband ISDN (B-ISDN) environment could cause a change or an adaptation of the MTP to new requirements.
- Several SS 7 network outages have occurred. Are modifications of the MTP procedures necessary in order to assure SS 7 network security and reliability?
- The sending of preventive transfer prohibited messages (TFP) via routes with highest priority and other items for further study are still not clarified.

After 20 years of development, specification, and implementation, we should now expect the MTP procedures to work well. However, serious SS 7 network outages have occurred in real networks. The great interest in the question of SS 7 network outages is shown by the fact that, during the study period 1992–1996, an SS 7 network reliability group was established within the ITU-T with the objective to investigate whether those SS 7 network outages were caused by faulty specified MTP procedures and, if so, to remove those problems. However, due to the complexity of the problems, the results of these studies were not very satisfactory.

First of all, the question of SS 7 network outages might be rather curious because, in the case of local outages of single signalling links and/or exchanges, and thus signalling routes, the specified changeover and rerouting procedures within the MTP specification cater for a proper diversion of the signalling traffic towards alternative links and routes. In addition, the SS 7 flow control caters for a reduction of the signalling traffic in the case of a congestion situation as long as it exists. How do SS 7 network outages actually occur?

In fact, especially with respect to further development of the SS 7 network to meet new requirements, there are many more problems and questions at least some of which we will summarize in the following:

- Does the level of signalling traffic influence network security?
- Are faulty implementations responsible for SS 7 network outages?
- Are the MTP procedures working correctly, or are there faulty MTP procedures which could cause SS 7 network outages?
- Are the MTP procedures based on fundamental assumptions and have they to be taken into consideration in network planning?
- Could problems result from network management activities?
- Is compatibility between different color book versions necessary and assured?

- Is the function of the MTP procedures influenced by network planning or affected by failure situations within the network?
- Does the network size influence SS 7 network security?
- Could awkward network planning cause SS 7 network outages?
- Is a transfer of problems from foreign networks to the home network via gateway nodes possible?
- Is bidirectionality within the SS 7 network important and, if so, how can it be assured also in the case of outages?
- How can routing loops be avoided, also in the case of failure situations?
- Can bidirectionality, loop-freeness, and node-disjoint routes between *any* two nodes in the network be realized?
- Is the chosen network structure important with respect to SS 7 network security and which structures are suitable?
- How can continuous network development be performed without causing problems?
- Could different applications (B-ISDN, IN, mobile communications, TMN, etc.) have an influence on network security?
- Are there problems with PSTN and IP network convergence?
- Are there problems arising from fixed and mobile network integration?
- Is it possible to achieve network security and reliability, and how can this be performed?

For a network operator, it is important to be aware of the problems and to know how they may be avoided. It would be wrong to change any MTP procedure in order to solve a specific problem without detailed investigations, since solving one problem might cause other and more serious problems. Thus, the objective of the presented investigations is to provide a clear understanding of how SS 7 network outages can occur, and it is discussed how network reliability and security of an SS 7 network can be reached and maintained while the network is further developed with respect to the introduction of new services and applications.

First of all, the fundamental development and conception of SS 7 is considered in the second chapter, so far as it is relevant to network reliability and security. In the third chapter, the development of the MTP procedures is discussed in describing the problems that were identified during the specification of the MTP procedures and how they were solved. Especially, it is shown that the fundamental philosophy has been changed over the years.

## 1.2 Basic Developments in Telecommunications

Recently the public telecommunication networks and the Internet have developed and grown nearly independently and now offer worldwide communication services. In parallel to the ITU specification work, the Internet Engineering Task Force (IETF) has been developing the *distributed IP telephony model* which provides the framework for the convergence of the *voice world* of the public switched telephone net-

works (PSTN) and the *data world* of the Internet. What is the reason for these efforts and why is there interest in this network convergence?

The first services offered by the public switched telephone networks (PSTN) were the telephone, telefax, and data transfer services which were extended during the realization of the integrated services digital network (ISDN) concept by the various ISDN services as well as the new intelligent network (IN) services. Due to the emerging demand for broadband services, the need to integrate both interactive and distributed services, and the need for high-speed transmission and switching technologies the broadband ISDN (B-ISDN) concept has been foreseen to integrate the various data, voice, audio, video, and multimedia services within the same network. The public land mobile networks (PLMN) offer a mobility service which allows a roaming subscriber to be reached by a calling party, who need not know where the mobile subscriber is actually located. Besides the ISDN and telefax services, there is a short message service (SMS) offered via mobile phones, which is used extensively. The interconnection of PSTN and PLMN is improved within the framework of fixed-mobile network integration. To summarize, in telecommunication, convergence of the various services and the integration of circuit and packet transfer modes into one universal network has been foreseen for a long time.

The Internet was optimized for data exchange between computer systems. Today, nearly any information is available via the Internet without major time delays and worldwide. We can do our banking activities or shopping via the Internet and can use the email service, one of the most popular services offered by the Internet. Also video and multimedia services are foreseen to be offered via the Internet. Are two different networks which offer similar services really needed?

In fact, we are now at the stage that both networks are growing together. This is due to the following reasons. First, since Internet services are currently accessed via the subscriber lines of the PSTNs, the growing Internet traffic requires an improvement of the network transition. Furthermore, the services offered via both networks are increasingly mixing:

- It is possible to send an email message to a called party which is, for example, converted to a short message and transferred to a mobile subscriber or transferred as a voice message to a mail box system, and vice versa.
- Considering that fixed network and mobile phones are increasingly becoming multi functional terminals, shouldn't it be possible to access special Internet web sites via mobile phones?
- Shouldn't it be possible to enhance a PC with a telecommunication system that supports a wide range of data, voice, audio, video, and multimedia applications?
- Could IN services, available in telecommunication networks, be used for the realization of Internet services?

The increasing Intelligent Network Application Part (INAP) traffic to service control points (SCPs) and Mobile Application Part (MAP) traffic to home location registers (HLRs) can cause congestion problems and problems with the flow control. In order to avoid these problems it is recommendable to use high-speed links be-

tween SCPs/HLRs and the intermediate transfer nodes. Those high-speed links can be realized as IP links. Finally, considering that the MTP Level 2 protocol

- Has been based on and adapted to unreliable transmission systems,
- Has been based on ancient processor technology,
- Was specified in order to save “expensive” memory and
- That it is optimized for 64 kbit/s transfer rate and, thus, limited to a low bandwidth,

there is a need for a new and cost effective transport protocol for switched circuit network (SCN) messages. Due to the cost benefits of the Internet protocol (IP) some network operators would like to migrate completely to an IP-based network, where every type of information is just viewed as packets of information, called datagrams, with IP being the predominantly preferred packet technology. The realization of these ideas necessarily leads to the convergence of both networks. However, how can this network convergence be performed?

In order to realize the above objectives, the IETF signalling transport (SIGTRAN) group is currently defining SS 7 over IP to enable SS 7 message exchange between IP network elements and with PSTN signalling points. In this respect the following fundamental questions arise:

- Is there a need for MTP-2 and MTP-3 functionality within the overall signalling system?
- Do we need MTP-3 network management functions within the overall signalling system?
- How can SS 7 signalling messages be transported over IP?
- How can the signalling performance requirements for voice and data services over IP be realized?
- How can PSTN and IP network convergence be performed?
- What is the detailed protocol structure for IP links or voice over IP (VoIP)?
- Is there a transfer of problems from one network to the other via signalling gateway nodes and how can they be avoided?

SS 7 over IP is designed to provide the signalling system for the interconnection of PSTN and IP networks. However, basic SS 7 knowledge and a discussion of SS 7 network security and reliability is not covered. Thus, regarding the SS 7 over IP developments, this book intends to provide more detailed background knowledge and, in this way, complement the IETF specifications.

In the fourth chapter we first describe how the SS 7 and IP network convergence can be realized, i.e., we describe the overall distributed IP telephony model, the basic signalling requirements, and the framework architecture for signalling transport. In the fifth chapter we summarize the different signalling transport protocol architectures based on the various adaptation modules. The SCTP as the underlying common transport protocol cannot by itself provide the availability and performance of MTP-3. Thus, redundant signalling network architectures are needed and are discussed in the sixth chapter. In the seventh chapter we describe in more detail the underlying protocols.

### 1.3 MTP Procedures, Network Structure, and SS 7 Network Outages

Behind the isolation and outage of wide network areas or an outage of the whole network, there exist a lot of more or less likely reasons. In the presented investigations, however, only protocol relevant network outages and those caused by network planning are considered. The cause of an SS 7 network outage is not faulty MTP procedures, but the causes may be searched for within implementations, the network structure, and network planning as well as the application of the MTP, especially in large SS 7 networks. With this objective we describe in Chap. 11 real SS 7 networks and discuss routing and topology aspects as well as network interconnection.

In order to judge the risk of a real SS 7 network outage, we describe in Chap. 8 how SS 7 network outages occur where we distinguish between correlated and uncorrelated network outages. In the twelfth chapter we summarize potential problems related to the application of the MTP in real networks. In particular, we describe the occurrence and consequences of a loss of bidirectionality within the network. Because of the fact that the SS 7 flow control plays the central part with respect to SS 7 network outages, we describe in some detail the function of the SS 7 flow control in Chap. 9 as well as potential problems with the flow control in real networks. Given that an unprotected node may be the source of correlated and uncorrelated network outages a functioning restart procedure is of crucial importance. Thus, we describe in Chap. 10 problems with the restart procedure and their solutions that eventually led to the White Book restart procedure.

Unfortunately, the described problems, especially in the case of a growing signalling network, cannot be solved after all. However, the problems can be avoided by going back to the original philosophy of SS 7. This may be done by using the MTP in the original sense and by assuring bidirectionality and loop-freeness of the routing data within the network as well as the function of the flow control, or by the introduction of new high-performance transmission and switching technologies, as would become possible in ATM- or IP-based networks. In particular, we show in Chap. 13 how SS 7 network security and reliability can be increased by changing the network structure, by the introduction of IP-based high-speed links as well as the separation of different traffic streams in the new SS 7 over IP environment, and how problems with the network convergence can be avoided. Finally, we end with a short discussion of the migration to an IP-based network in Chap. 14.

<http://www.springer.com/978-3-540-74985-1>

Developments in Telecommunications  
With a Focus on SS7 Network Reliability

Rufa, G.

2008, XVIII, 278 p. 108 illus., Hardcover

ISBN: 978-3-540-74985-1