3

On Intelligent Network Certification: Performance Issues

Manfred Schneps-Schneppe
R&D Center KOMSET
7 Zeleny prospect, Moscow, 111141 Russia
Fax +7 095 3060104

Abstract

With the rapid deployment of multi-vendor equipment on Russian telecommunication market (in accordance with Russian state and private investment plans) comes the major challenge of preserving network integrity. The more it concerns intelligent networks exploiting the SS7 network - the most sensitive part of telecommunications system. The paper discusses the foreign experience (US, Germany, France, etc.) in service provider certification (qualification), as well as some proposals in development of the standard ITU-T version of the IN concept, the revision of existing ITU-T recommendations and the challenge for memorandum of understanding for implementation of IN CS1.

1 ON THE RUSSIAN TELECOMMUNICATION MARKET

Russian state investment plans have a habit of beginning nationwide projects only to become far more modest when constraints on money and time catch up with planners. Yet, ever since its inception, the 50x50 project has grown and grown. At the outset it was an ambitious plan to connect 50 Russian cities with 50,000 km of fiber optic cable. In the middle of 1994, project was to include at least 100 cities and 100,000 km fiber optic cable. How did it begin? The Russian Federation property committee sold off 30 percent of the former Ministry of Communications (state-owned cables and trunk exchanges and upper level switching nodes) and formed ROSTELECOM in 1993, which is now leading a consortium financed by foreign telecom operators which will undertake a massive construction project called the 50x50 project [1]. Russian officials confirm these ambitions [2]. The most active companies on the Russian telecommunication market are the following: Nokia, Ericsson, Alcatel, AT&T, Italtel, Siemens, etc.

The Ministry of Telecommunications is the regulator exploiting its R&D institutions for certification (qualification) process, e.g., ZNIIS (Moscow) is testing toll exchanges, LONIIS

D. Gaïti (ed.), *Intelligent Networks and Intelligence in Networks*

(St. Petersburg) is with urban and rural switches, NIIR is responsible for radio facilities, KOMSET has experience in billing system certification and network design, etc. Certification procedure contains detailed specifications for hardware and software, factory tests, line tests. Field tests are carried out in the actual Russian public network or in the LONIIS Certification Center (for rural and urban applications) by simulation and protocol-testers as well as through real trunks to existing step-by-step and crossbar switches [3].

In the paper we should like to discuss some difficulties arisen at implementation of intelligent networks on Russian telecommunication market. Intelligent Networks (IN) throughout the world offer the opportunity for telecommunication administrations as well as third-party service companies to provide application development and control of services. These INs are generally composed of systems from many different suppliers, and the services offered may need to function in cooperation with other carriers. In an environment with such distributed and shared responsibilities, it is important to ensure that each part meets expected levels of service integrity, performance, and quality. A certification process for telecommunication administrations, equipment providers, and other service providers may help identify serious vulnerability and network integrity concerns early, so that corrective or compensatory actions can be taken.

We are looking to IN implementation process in Russia as a next step of the now going Russian ISDN pilot project based on the Moscow toll and international network (MMT) having several connections inside Russia and a few international routes. We would like to restrict our discussion on IN certification by the INs built in accordance with ITU-T standards. Considering the standard SS7 as an IN backbone, we have several challenges put by INs:

- IN services lead to a significant increase in the volume and complexity of the SS7 messages exchanged between network nodes. New strategies for overload control must be defined, e.g., different internal overload control strategies for MTP and SCCP levels of the SS7 protocol led to unfair treatment of different message classes in an uncontrolled fashion.
- When telecommunication administrations open their networks to third-party service companies, additional issues of application protection, security, network integrity, network performance and overload must be addressed.

2 IN CERTIFICATION: THE US EXPERIENCE

Nowadays the service evolution is mainly supported by the introduction of the SS7 network. Several well publicized SS7 outages occurred in the US during the last years (in January 1990, the outage of AT&T network had nationwide impact and involved the loss of 65 million calls, the other (in 1991, Washington, DC) involved entire cities and impacted 10 million customers)are of great importance for Russian network designers. After the hearings at the US Congress (in 1989 and 1991) a Network Reliability Council has been formed by FCC [4]. Nevertheless, there is growing dissatisfaction with public network and a crisis is developing.

Why did the recent failures occur? McDonald [4] goes through many driving forces: fiber technology, digital switches, common channel signaling, competition, divestiture of AT&T, customers requirements for faster introduction of new services - all these forces that shaped

network evolution had caused a concentration of network assets and this had increased the customer impact of a given network element failure. Technology to maintain adequate integrity has not been deployed. Forces of technology, regulation, and customer demand have conspired to push the network away from acceptable levels of integrity.

Qualification (certification) procedure as of Bellcore [5] is a three-step process. The first step (so called white box step) is devoted to design review and contains a paper analysis of the supplier's design specifications and focuses on potential vulnerabilities (e.g., overload control algorithms) identified by previous studies and/or network failures. In a design review, internal behavior is examined in detail (internal architecture, functionality, interfaces in reference to generic requirements).

The second, black box step, is devoted to conformance analysis: the independent assurance of stand-alone product conformance to industry standards and telecommunication administrations requirements. A black box's responses to stimuli generated by other simulated network elements are studied. In the case of IN SCPs and switching systems, particular attention is given to testing feature interactions between IN and non-IN features, as well as among various IN features.

The third step is product to product compatibility analysis. As part of the qualification program, Bellcore's laboratory hub concept makes it possible to test IN network elements and systems in an environment that closely resembles an actual network. From a network integrity perspective, real world failure scenarios are introduced in the network (thirty extensive test scenarios until now) and high traffic loads are simulated.

To assure the network integrity, FCC suggested that third parties may provide new services through carriers' IN via mediated access [6]. However, third-party access to INs raises many problems, relating, for example, to incorrect messages, protection from unauthorized users, non-robust products, impacting on others' INs, etc. Third-party IN service providers having their own SCPs can make use of the proposed certification process for suppliers to have their equipment certified. In particular, the certification process should emphasize software integrity, software quality, service introduction and service interaction.

3 WHILE WAITING FOR OPEN EUROPEAN NETWORKING

The European telecommunication market will almost completely be liberalised at the beginning of 1998. The German Telecom announced a "Concept for provision of open access to telephone network functions" [7]. This concept contains a detailed description of how Telecom plans to provide new, non discriminatory accesses to the Telecom telephone network for its competitors (Open Network Provision, ONP). Foreseeing the customer/market needs, the offensive strategy of Telecom in the ONP area is based on Telecom's corporate policy interests: making optimal use of resources, making its services more flexible with regard demand, and stimulating new effective demand while satisfying regulatory requirements.

For provision of different access types, ONP interface protocols have to meet three basic requirements: 1) to be standardised internationally, 2) to provide powerful compatibility mechanisms and 3) to provide functions to protect all interconnected networks.

To discuss the network integrity comprising different aspects, a classification into three areas of risk is applied by Telecom: 1) a disruption of the network (could lead to a complete loss of the signaling network or a complete network outage), 2) disturbances which could cause a degradation of the quality of service, 3) misuse of network functions without the risk of outages or even a degradation of QoS.

At ISS'95, Kung [8] of France Telecom has discussed the third-parties' requirements under question-mark: is an open networking technically possible? His discussion is based on simple model of two players: on the one hand, a network operator who owns a network that provides some "reserved" telecommunication services, and on the other hand, third parties that are able to provide services that are under competition.

The requirements are the following:

1) Independence: Third parties should be able to develop their services independently from other third-party services without rising service-interaction problems.
2) Restricted competition: It is necessary that third parties develop their services jointly or with the network operator.
3) Full life cycle: Rules are to be followed by third parties exist at all stage of the "service life cycle" (from service preparation till service deployment).
4) Guaranteed QOS: It is important to check that all relevant aspect of the calls (busy call, no answer, congested network, call abandoned, etc.) are handled by the service.
5) Hidden basic architecture: Introduction of a new system by the network operator should be unknown to third parties.
6) Standard physical interfaces: Systems should be available from several vendors to be able to shop for the best systems.
7) Global services: It should be possible to provide more global services on several networks. There is the need to take into account all relevant levels (circuit, data bases, OA&M).

4 SIEMENS PROPOSALS FOR THIRD PARTIES

For provision of open network concept, some considerations of SS7 in context of network integrity are needed. The MTP constitutes the signaling network. The network management functions are powerful tools and, if misused, can cause significant problems within a signaling network. To avoid such dangers, the concept for provision of SS7 access products contains as an important requirement that no access is connected directly to the national gateway signaling network. Each network provider has its own signaling network interconnected by the gateway network. This is the essence of proposal by Sevcik and Lueder [9]. They have pointed out some weak points of classical IN scheme:

1) Changes in the service logic by service provider/subscriber are difficult in many practical cases since they might affect and incorrectly interact with other services in the common centralized SCP (e.g. due to common rooting databases, common SS7 SCP-SSP protocol data, etc.)

2) Service providers/subscribers may not be willing to store and manage their proprietary corporate data in a SCP/SMP owned by network operator and shared by other competing service providers.

They proposed a new IN architecture supporting private SCP (PSCP) in addition to the SCP owned by a network operator (NSCP) and using TCP/IP protocol for interworking between PSCP and NSCP. A private SMP exists also. There is clear isolation between IN service logic in the NSCP and the IN services in PSCP (no common data, no common access to the SS7 signaling).The biggest potential for a PSCP owner lies in the opportunity to introduce the sophisticated service features like:

1) Personal screening.
2) The access to customer data base records on a workstation for each call.
3) Individual billing.
4) Voice and fax mailbox controlled by the PSCP.
5) Multimedia server containing product advertisement (video, voice).
6) Private video on demand server.

Leconte with co-authors [10] have offered a way of adding value through the deployment and implementation of innovative Intelligent Peripherals (IP)/Service Node (SN) services. The SN combines: the IP, a service control function, a switching function, a service creation/customization function, all under one physical (or logical) node.

According to the standard IN architecture, intelligent peripherals provide the service resource function for SCP, for example, send information to users participating in a call (prompts, announcements), receive information from users (e.g. authorization codes), modify user information (text to speech synthesis, protocol conversion), provide special connection resources (e.g. audio conference bridge, information distribution bridge).

Whereas an IP's main function is to support an IN SCP, the SN may have its own service logic and may support advanced services such as voice activated dialing, voice/fax messaging and other types of services. The IP/SN may also be directly connected to an SCP via an SS7 Transaction Capability Application Part (TCAP) interface.

5 STANDARD IN CS1 ARCHITECTURE: UNSOLVED PROBLEMS

As a compulsory requirement for certification we propose that the IN facilities follow the standard IN architecture in accordance with ITU-T Recommendations Q.12xx, more precisely in accordance with IN Capability Set 1 defined by Q.121x. Therefore, we would like to discuss the problem in the strong framework of the IN functional model defined by Q.1204 "IN distributed functional plane architecture (DFP)" for CS1 services.

Recall that the DFP architecture:

- provides the support for a large variety of services,
- is vendor/implementation independent,
- accommodate service creation.

For service certification procedure, we are to study relationships between functional entities related to IN service execution. There are as many as 12 types of IN control/management relationships that may be established between functional entities in the DFP (see Figure 2-1 in Q.1204).

The contents of these functions are defined by Q.1204. Each interaction between a communicating pair of functional entities is termed "an information flow".

Let us point out the call control function (CCF) providing call/connection processing and control. An important term here is the trigger mechanism acting in so called detection points of call model to access IN functionality. Triggering tables are located in SSP (Service Switching Point). Whenever a new service is to be introduced, or whenever a user wants to subscribe to a line-based service, it is necessary to update these tables. As SSPs belong to the network operator (otherwise, the third party would be the network operator), the problem is to decide how third parties should access and update triggering tables.

To say a few words about Intelligent Network Application Protocol (INAP). The SS7 INAP for IN CS1 as it was defined by ITU does not support the interconnection of IN network nodes in different networks, the INAP was explicitly developed for the operation within one network. There will be different kinds of INAP interfaces SSF-SCF, SCF-SDF and SCF-SRF. One possibility would be to introduce a new network node type in the IN architecture, the "Inter Network Unit". This unit would separate the links between SCF and SSF. The INAP dialogues would split into two parts. As a consequence, the Inter Network Unit would then have knowledge about the service logic of each SCP connected to it [7].

The next question worth mentioning regards the ISUP-INAP interconnection for correct charging procedures. Q.764 currently recommends that an originating exchange awaits the receipt of an answer message before it through connects its speech path in the forward direction. The procedure is intended to assist in the prevention of fraudulent use of the network, as it is common practice to link the start of charging for call at an originating exchange with the receipt of the answer message. In order to meet the requirements of IN for in-band dialog with the calling party to collect information necessary to complete the call set up to the called party, it is necessary to through connect the speech path at the originating exchange before the called party. This will require a revised protocol that will be included in a future release of ISUP recommendations. It will be necessary for the IN to send an "early" answer message to the originating exchange before the call is established to the called party. Such an early answer message as a procedure in ISUP-INAP interactions recommendation would be specified for the case of calls originating in exchanges that use existing ISUP protocol.

Such revision of ISUP-INAP interaction procedure can be followed by negative features: the operation of some ISDN supplementary services can be seriously jeopardized on calls for which an early answer message is used to ensure through connection at an originating exchange. This is because the change in ISUP procedures associated with the early answer message will prevent the transfer of ISDN supplementary service information from the destination exchange to the originating exchange. An early answer message to ensure through connection at an originating exchange may also cause the exchange to commence charging the call prematurely, or to charge for an unsuccessful call.

The implementation of any new service requires the updating of all triggering tables. How to do this procedure? As mentioned above, the network physical configuration is hidden to the third party, so intermediate management "mediation device" would be needed. Next question. Triggering tables are structured according to call states. Whenever the switch enters a new call state, the switch looks at the relevant part of the triggering tables to check if any triggering condition is met. This particular way of implementing services may raise some service interaction issues. Sometimes, it may happen that several conditions are met and several services may be triggered at the same time. Service interactions problems may arise because parameters in INAP may not exist in ISUP or DSS1 and vice-versa.

It is necessary to provide some management capabilities to third parties. We have already identified the need of filling SSP trigger tables. There are many other data and many other systems than the SSP that need to be updated by third parties: creation of new subscribers, modification of subscriber's service profile, etc. As the exact physical configuration should be hidden to the third party, some single entry point for the management by the third party is needed to manage, e.g., routing tables of switches, triggering tables of SSP, global title data updated in STP.

6 REVISION OF E. 411 AND E. 412 RECOMMENDATIONS

These recommendations are of special interest for IN performance analysis. What about E.411 "International network management operational guidance"? [11], the very meaning of network management is to be changed. Instead of traditional management control status indicators based on 30 second traffic measurement, in case of SS7 and SCP management we are to control the traffic intervals as short as 1 sec and less. SS7 system status provides information that will indicate failure or signalling congestion within the system. It includes such items as: receipt of a transfer prohibited signal; signal link unavailability; signal route unavailability; destination inaccessible. These items form the basis for IN performance management.

Effective intelligent network management requires good communications and cooperation between the various network management elements within an Administration and with similar elements in other Administrations as well as with IN service providers and users. This includes the exchange of real-time information as to the status and performance of circuit groups, exchanges and traffic flow in distant locations.

Such information can be exchanged in variety of ways, depending on the requirements of the Administrations. Voice communications can be established between or among network management centers using dedicated service circuit or the public telephone network. Certain signals may be related to the exchange status (as for the switching congestion indicators) and to the status of the destination as for Hard-To-Reach (HTR) information in particular.

It should be noted that in network management applications, the volume of data to be transferred can be quite large and its frequency of transmission can be as high as every three minutes for traditional voice teletraffic control and much higher (as every 1 sec) for IN services. When this data is transferred over signalling links which also handle user signalling traffic, stringent safeguards much be adopted to minimize the risk of signalling system overloads

during busy periods when both user signalling traffic and network management data transmission are at their highest levels. These safeguards include, besides others, the following:

- limiting the amount of network management information to be transferred on signalling links which also carry user signalling messages;
- developing appropriate flow control priorities for network management information;
- equipping the network management operations system in such a way that it can respond to signalling system flow control messages.

As it is pointed out in the draft of revised E.411 [11], it is important that the network management controls should not become completely unavailable due to the failure or malfunction of the network management operation system or of its communications links with exchanges. Therefore, network management operations systems should be planned with a high degree of reliability, survivability and security.

There are many unsolved problems of intelligent network management. How to introduce IN call gapping for SS7 protection, when a service control function (SCF) communicates with a service switching function (SSF) via an overloaded SS7 line? Traditional congestion control works for an SCF communicated via circuit group. This is the case of SCF implemented in an adjunct, intelligent peripheral or service node that contacts to an SSP via circuit groups with e.g. ISDN interface.

What about new version of E. 412 "Network management controls", two problems are worth to be mentioned:

1) How to control HTR services. To explain the situation. An SCF detects that the destination of a dialled number, which is generally at customer's premises, receives a relatively high volume of ineffective call attempts. The SCF then issues a signalling message to an SSF to request for a call rate control. In return, the SSF activates a call rate control to reduce the rate of services requests that are sent to the SCF. Of special concern is how frequently the HTR information is updated in the receiving exchanges (taken into the mind several IN functions: SST, SCF and others, including service management agent function);
2) What method for IN traffic control should be implemented. With the call rate control method, an upper limit on the rate that calls are allowed to access the network is established (for example 4 calls per second). The leaky bucket counter it seems in here of special interest. Of course, the performance of call percentage control (comparing with call rate control) is to be considered also.

The revision of E.411 and E. 412 from the viewpoint of SS7 overload for IN use is to be carried out under requirements of Q.543 "Digital exchange performance design objectives". An exchange must continue to process a specified load even when offered call exceed its available call processing capacity. Two basic requirements for exchange performance during overload are: to maintain adequate exchange throughput in sustained overload; to react sufficiently quickly to load peaks and the sudden onset of overload.

It is well known that when traffic on real-time processing system rises beyond its capacity, the overall performance of the system degrades. In an ideal case, the throughput rises linearly

as a function of the input load until capacity of the system is reached and then levels off at the system capacity. In the case of actual system the throughput will rise linearly for light and moderate loads, but near the saturation the throughput will not increase as fast as the offered load and beyond saturation the throughput will usually decline. In most cases, if there are not adequate overload controls, this decline in throughput beyond saturation can be precipitous.
The goals of overload control can be stated as follows [12]:

1) Maintain throughput near system capacity, even under periods of extreme overload.
2) Ensure system sanity and perform all critical functions necessary for the system and network to work properly regardless of overload level.
3) The system should protect itself from becoming deadlocked.
4) The system should be able to protect itself if network congestion or flow controls do not work.
5) The system should be able to recognize and shed excessive network management work without violation goal 2.

Recommendation Q.542 "Digital exchange design objectives" contains the description of statistical indicators for HTR service detection. For IN management the HTR process should be modified in many aspects:

- HTR administration (codes of IN services, thresholds for detection of overload and load reduction conditions, procedure of HTR control list review) and
- methodology for HTR service determination, e.g. by SIB QUEUE mechanism.

7 NEW E.7INX SERIES

ITU-T Study group 2 is in a very starting point with drafts for this series. For our reason of IN certification the most useful should be E.7IN4 "Traffic and congestion control requirements for SS7 and IN-structured networks"[12]. The authors of E.7IN4 draft have stated four main purposes:

- to choose the performance characteristics implementable in different types of network;
- to avoid fault and congestion propagation, network instability;
- to provide the interconnecting networks for various vendor products;
- to provide high level requirements for traffic and congestion control.

IN control includes SS7 control as an element MTP traffic management procedures (according to Q.704) contain the transfer-prohibited, transfer-restricted and transfer-allowed procedures. Congestion control of a signalling route in under transfer-controlled procedure and traffic flow control actions. These MTP control procedures as an important part of SS7 are developed now in detail. SCCP management procedure for signalling point and subsystem status changes including broadcasting about subsystem prohibited conditions are less developed.

What about IN, only preliminary congestion control requirements are named. Part of them would be included in IN certification procedures. The question is - what part? A list of recommended high level requirements includes the following aspects:

- Share load. Load should be balanced over the possible serving element so that delay may be minimized. Thus congestion controls should automatically balance loading across more than two network elements, across elements of unequal capacity, across elements with distributed logic or data.
- Harmonize across levels and layers. The IN congestion and overload controls should be a harmonized set of functions providing overload control within each element to maintain sanity and call processing should higher level controls not work, as well as congestion control appropriate to the scope of data available and to the span of the control or network management system.
- Control effectively. The control process (the way a congestion is activated and modified) should be capable of taking the appropriate control action to handle traffic surges and peaks that cause congestion across network providers, across network boundaries (including Global Title Translation), across networks implementing different SS7/IN procedures.
- Control properly. A proper IN flow control is essentially a feedback control system. It should operate in stable, controlled manner, avoiding wide swings in the control parameters and actions. The controls should respond quickly to changing user traffic levels. Flow control is based on parameters such as: dialled number, originating switch, class of service of caller, IN-service requested.
- Overload triggers. Overload is usually caused by insufficient real-time in a processor to handle the workload, and it is usually recognized by certain buffer occupancies exceeding a threshold. Overload triggers should be set so that adequate time is available for the controls to take effect before the system performance degrades significantly. Unsolved problem here is how to set thresholds.
- Network robustness is concerned with the ability of a network to withstand both traffic overloads and failures of network elements. In the case of IN-structured networks, in addition to controls in the IN function layer, some control activation may be appropriate in the signalling and bearer portions of the network, such as call admission controls in the circuit-switched network.
- Requirements for screening messages. One of the potential dangers in interconnecting signalling network is that one network might send another message the receiving network considers invalid. One way to protect against this potential failure mechanism is to have a screening capability where the traffic enters the system (e.g., at the receive side of signalling link) and check messages to ensure all parts of the message meet the requirements for that network.

These are basic requirements be considered as topics of IN certification methodology.

8 SUMMARY

With the rapid deployment of intelligent networks comes the problem of presenting network integrity. The IN certification process is a systematic activity associated with a multi-supplier, multi-carrier environment, with new network systems, new operating systems, new

interfaces, additional signalling traffic, and the emergence of third party service companies. Russian telecommunication system is in the very start point of this process. Therefore we are looking for the knowledge and existing experience.

The paper proves the emergency of standardised IN certification methodology. The main features of methodology might be the following:

- three-step approach (as of Bellcore);
- standardised subset of IN architectures (e.g. containing private SCP, enhanced SN);
- fixed ISUP-INAP interaction procedure for fixed subset of CS1 services (e.g. freephone, credit card, VPN);
- revised E. 412 (leaky bucket for HTR service control);
- developed E.7 IN4, contained minimised high level requirements, fixed overload triggers, developed concept of robustness (as for Q.543 defined overload control scheme based e.g. on SIB QUEUE mechanism);
- minimum subset of QoS parameters for IN throughput analysis.

Following the Memorandum of Understanding (MOU) for the implementation of an European ISDN service by 1992, the similar kind of document MOU IN'96 could be created.

9 REFERENCES

[1] Lyudi, D. (1994) Supplement Telecommunications, June , 3-8.
[2] Krupnov A. J., Elektrosvjaz, 1994, #8, 2-3.
[3] B. S.Goldstein, IEEE Journal on SAC, vol. 12, #7, Sept 1994, 1186-1191.
[4] J. C. McDonald, IEEE Journal on SAC, vol. 12, #1, 1994, 5-12.
[5] R.J.Baseil, and B.Hoang, ISS'95, Berlin, vol. 1, paper P.g5.
[6] FCC, Notice of proposed rulemaking, CC Docket #91-346, Aug 1993.
[7] R. Kickartz, and H. Gottschalk, ISS'95, Berlin, vol. 2, paper B5.4.
[8] R. Kung, ISS'95, Berlin, vol. 2, paper B5.3
[9] M. Sevcik, and R. Lueder, ISS'95, Berlin, vol. 2, paper P.y6.
[10] A. Leconte et al, ISS'95, Berlin, vol. 1, paper P.g3.
[11] Draft E.411. ITU-T COM 2-R 28E, 1995.
[12] Draft E.7IN4 ITU-T COM 2-R 32E, 1995.

10 BIOGRAPHY

Manfred Schneps-Schneppe has published numerous papers on economics, stochastic processes, and teletraffic engineering, and written several books on the same subjects. He has had the chair in Telecommunication at Latvia technical University in Riga and been visiting professor to The Technical University of Denmark. Now he is working with future telecommunication services and training at R&D Center KOMSET in Moscow (editors note).