Achieving the Safeguarding Performance of the V5.2 LE

Igor Radujkov, Saša Marjanović, and Vojin Šenk

Abstract— **The Local Exchange (LE), supporting the V5.2 interface, is modularized for the safeguarding performance. Although solutions for modularizing the Switching Exchange, known as Tandem Exchange, that could be easily modified and used for the LE modules, already exist but none of them supports the V5.2 access. Hereby, we have described the basic principles of a tandeming protocol, a specific upgrade of the V5.2 interface, used for achieving the safeguarding performance of the V5.2 LE system.**

Keywords— **Telecommunication network, Local exchange, V5 interface, Safeguarding performance**

I. Introduction

The ITU-T Recommendations [1] and [2] specify the electrical, physical, procedural and protocol requirements for the V5.2 interface for the connection of an Access Network (AN) and the Local Exchange (LE) for the support of the following access types:

- analogue telephone access (PSTN);
- ISDN basic access (BA) with an NT1 separated from the AN, or integrated in the AN, based on [3] and [4];
- ISDN primary rate access (PRA) with an NT1 separated from the AN, or integrated in the AN, based on [5] and [6];
- other analogue or digital accesses for semi-permanent connections without associated outband signalling information.

The AN and the LE are connected through the V5.2 interface with flexible information channel (bearer channel) allocation on a call by call basis which provides concentration capability within the AN. Such connection is provided by use of a bearer channel connection (BCC) protocol which allocates and deallocates bearer connection required on demand, identified by the signalling information, under the control of the LE.

The signalling from the PSTN user port is converted into a stimulus protocol with a functional part for the signalling path using layer 3 multiplexing for the information from the different user ports. The signalling from the ISDN D channels is frame relayed in the AN and delivered unmodified to LE.

The individual user port status information exchange and control function required for the coordination with the call control procedures in the LE, are provided by a control (CTRL) protocol. As [1] may use up to 16 2048 kbits/s (E1) links on one V5.2 interface, it defines a link control (LINKC) protocol for the multi-link management to control link identification, link blocking and link failure conditions.

A protection (PROT) protocol, operated on two separate data links for security reasons, manages the protection switching of communication channels (C-channels) in case of link failures.

Igor Radujkov, Saša Marjanovi; and Vojin Šenk are with the Faculty of Engineering, University of Novi Sad, Trg Dositeja Obradovića 6, 21000 Novi Sad, Yugoslavia

II. Basic Terms

The *C-channel* is a 64 kbit/s time slot on a V5.2 interface provisioned to carry communication paths (C-paths).

The *C-path* is either the layer 2 data link carrying one of the housekeeping protocols (BCC, CTRL, LINKC, PROT), or layer 2 data link carrying the PSTN signalling data, or frame relayed ISDN D channel data.

The *logical C-channel* is a group of one or more C-paths, all of different types, but excluding the C-path for the PROT protocol.

The *physical C-channel* is a 64 kbit/s time slot on a V5.2 interface which has been assigned for carrying logical C-channels. A physical C-channel may not be used for carrying bearer channels.

The *primary link* is the E1 link in a multi-link V5.2 interface whose physical C-channel in time slot 16 carries C-paths for the housekeeping protocols.

The *secondary link* is the E1 link in a multi-link V5.2 interface whose time slot 16 carries a C-path for the PROT protocol and, on V5.2 initialization, acts as the standby C-channel for the other housekeeping protocols.

Protection group 1 consists of time slot 16 of the primary and time slot 16 of the secondary link. *Protection group* 2 contains all provisioned C-channels which are not included into protection group 1.

III. V5.2 LE Functional Model

Housekeeping protocols together with the PSTN protocol form the layer 3 of the V5.2 interface. Layer 3 messages have the same structure as these used for ISDN, specified in Q.931, with protocol discriminator value 72. For each of these protocols one layer 2 data link connection is established, except for the PROT protocol which requires two such connections. Layer 2 in the V5.2 interface (known as LAPV5) consists of two main parts: the LAPV5-DL, based on Q.921 (LAPD) over which each protocol establishes its own connection identified with LAPV5-DL address, and the LAPV5-EF which encapsulates the LAPV5-DL or LAPD messages by prefixing them with the envelope function address (EFaddr) needed for distiguishing the ISDN D channel data from the V5 layer 3 protocol data.

Besides OSI protocol structure, the V5.2 interface has

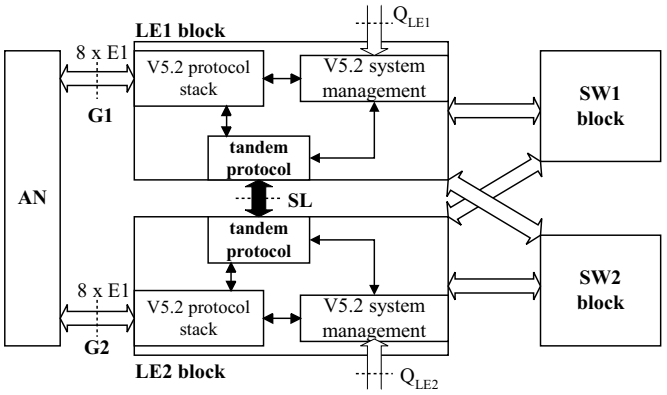

Fig. 1. Modularized V5.2 LE system for the safeguarding performance.

management functions for starting up the interface, reprovisioning, link, variant and interface identification, BCC resource management as well as the link management and the protection management functions. Additionaly, [1] specifies finite state machines (FSMs) required for each user port and for the E1 interfaces, which are maintained by the service management in the LE or the access management in the AN. Figures 3 and 6 in [1] show the functional model of the V5.2 interface.

IV. Safeguarding Performance in the LE

If an LE is modularized for the purpose of safeguarding performance then physical C-channels should be provisioned in such a way that performance could be safeguarded through protection switching. It is very suitable to connect the primary link to one LE module and secondary link to another LE module. Our solution, Fig. 1, consists of two LE modules (LE1, LE2) connected to one AN module, each of which manages one half of the whole V5.2 interface capacity.

LE modules should have the same provisioning data with the following exceptions:

- each module should be aware of the group of E1 links that it manages (G1 or G2);
- both modules operate in different modes (master, slave, non-operational);
- the master LE module maintains the complete signalling information exchanged through the V5.2 interface;
- in the slave LE module, the PROT protocol, link control FSMs, user port status FSMs, BCC resource manager and management functions are performed only;
- the slave LE module should react only on protection switch-over requested for the protection group 1.

LE modules are connected internaly with a tandeming protocol over the safeguarding link (SL on Fig. 1). As the tandeming protocol is layer 3 protocol, the SL link has to provide layer 1 and layer 2 functions and requirements. Here, we do not restrict the use of any kind of layer 1 and layer 2, since the multiplexing of different types of data is fully performed within the layer 3, instead of the V5.2 protocol stack which multiplexes data within both layer 2 and layer 3.

When several internal links are used for safeguarding, it is the matter of provisioning how to organize tandem connections over them since there is no protection mechanism defined for safeguarding links.

Both modules are responsible for detecting all the failures that may appear at the V5 interface, at the internal link or at the neighbour module, and for the adequate reactions on such failure occurences.

A. Activities in the Master LE Module

The primary E1 link is connected to the master LE module. Let the LE1, in Fig. 1, be the master LE module. The V5.2 protocol stack with its maintainence and management functional blocks is completely executed on this module. Management of the signalling information is the responsibility of the master LE module. A logical C-channel of the protection group 1 has to be carried over the G1 group of E1 links maintained by the master LE module. Such requirement does not allow sharing the call control responsibility. In case of call control function residing in both LE modules, pending the incoming signalling path requires greater internal link (SL) capacity and multiplexing within both layer 2 and layer 3, since it is possible for the path to be established over other module which maintains the active logical C-channels. The incoming ISDN signalling path could be resolved with less effort then the incoming PSTN signalling path.

The status information of each user port and of the E1 links is sent over the tandeming protocol to the slave LE module which updates its relevant status information.

The following information is transmitted through the SL link using the tandeming protocol:

- the status information of each user port and of the E1 links;
- the information about allocated, deallocated and unavailable resources on the V5.2 interface;
- the information about active logical C-channels.

B. Activities in the Slave LE Module

The secondary E1 link is connected to the slave LE module which is responsible for collecting the information sent from the master module over the SL link.

V. Tandem Management

The tandem management is responsible for adequate reaction on failures that may appear in the V5.2 system, and could be one of the following:

- the slave LE module failure;
- the internal link failure;
- the master LE module failure;
- the primary link failure;
- the secondary link failure;
- the AN failure;
- the link failure (neither primary nor secondary).

The V5.2 system management should be informed about all the actions being performed by the tandem management.

A. Activities on the Slave Module Failure Occurence

When the master LE module receives no response from the slave LE module over the SL link within TSG2 seconds (TSG2 is about 500msec), the link management immediately blocks all E1 links maintained by the slave LE module (G2 links) and informs the system management about the action.

The same action is performed in the master module when the internal link failure has been occured. In such case, the slave LE module will wait for the protection switching initiation from the AN side and as it will not receive such request it enters the non-operational mode.

B. Activities on the Master Module Failure Occurence

When the slave LE module receives no response from the master LE module over the SL link within TSG2 seconds, it enters the state of waiting for protection switching request from the AN side and starts the TSG3 (about 2sec). The master module failure will cause the data link failure of protection group 1 to be detected by the AN side. After detection of such failure, the AN issues the protection switch-over request for the protection group 1 which will be delivered to the slave LE module over the secondary link. When such request is received during TSG3 seconds, the slave module enters the master mode, issues the protection switch-over requests for all active logical C-channels within the G1 group onto stand-by C-channels within the G2 group and blocks all E1 links from G1 group.

If no request is received form the AN within TSG3 seconds, then the slave LE module is aware of internal link failure and enters the non-operational state.

C. Activities on the Primary Link Failure Occurence

After detection of the primary link failure, the master LE module (LE1) informs the slave LE module (LE2) over the SL link about the failure and enters the slave mode. The slave module (LE2) issues the protection switch-over request for the protection group 1 and enters the master mode. Then, it issues the protection switch-over request for all active logical C-channels within the G1 group onto stand-by C-channels within the G2 group and blocks all E1 links from G1 group.

D. Activities on the Secondary Link Failure Occurence

After detection of the secondary link failure, the slave LE module informs the master LE module over the SL link about the failure and enters the non-operational mode. The master module should block all E1 links within the G2 group.

In the event of protection switching being required for logical C-channels belonging to the G1 group of E1 links, the protection management initiates the switch-over within the same group of E1 links. All the changes in the logical C-channel evidence should be sent over SL to the slave LE module for the purpose of eventual protection switching managed by the slave LE module.

TABLE I

TANDEM MANAGEMENT ACTIVITIES IN BOTH LE MODULES.

Event	LE1 activities	LE2 activities
Primary link failure (note 1)	enter slave mode	enter master mode, switch G1 onto G2
Internal link failure (note 2)	deallocate G2, block G2	enter non-operational mode
LE1 module failure (notes 1, 2)	/	enter master mode, switch G1 onto G2, deallocate G1, block G1
LE2 module failure (note 2)	deallocate G2, block G2	/

Note 1: AN initiated protection switch-over for protection group 1.
Note 2: No response over internal link (SL).

VI. SAFEGUARDING PROVIDED BY V5.2 PROTOCOLS

Safeguarding protocol should be responsible for updating the evidence in both LE modules about:

- the status information of each user port, which will be sent or confirmed whenever the relevant user port status FSM changes its state;
- the status information of each E1 link, which will be sent or confirmed whenever the relevant link layer 1 FSM changes its state;
- the information about allocated, deallocated and unavailable resources on the V5.2 interface, which will be sent or confirmed whenever the BCC finishes its processes successfully;
- the information about the active logical C-channels, which will be sent or confirmed whenever the protection switching of the logical C-channel(s) within protection group 2 is successfully completed.

These requirements will be fulfilled by a slight modification of the V5.2 layer 3 protocols described in the sequel.

A. Tandem Protocol Management

The tandem protocol specifies the inactivity timer TSG1 (about 100msec) which is restarted after appearence of any event in the tandem protocol entity. When TSG1 expires, the tandem entity sends Ready Request (RR) to the another module, starts TSG2 and waits for Ready Confirm (RC). If RC is received within TSG2 seconds, then the tandem entity stops the TSG2 and restarts the TSG1. If no response is received during TSG2 time, the tandem management enters the state of waiting the switch-over request from the AN and runs TSG3.

Handling of different situations in tandem management are already described in chapters IV and V.

B. Port Control Protocol

The port blocking and unblocking is only allowed for the V5.2 system management residing in the master LE module (LE1). When the port blocking is initiated, [2], the MPH-BI primitive is sent to both relevant port status FSM (either ISDN-BA, ISDN-PRA or PSTN) and tandeming protocol entity which will send Block Command over SL

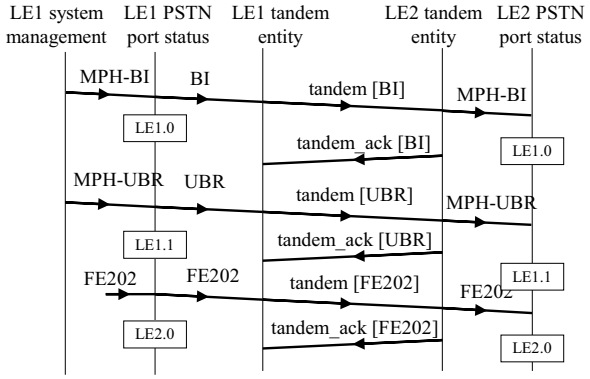

Fig. 2. Port control protocol safeguarding.

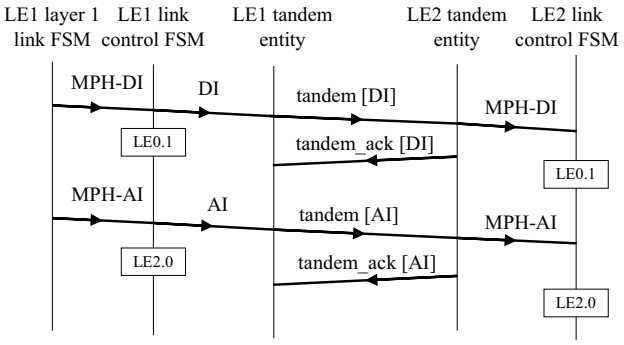

Fig. 3. Link control protocol safeguarding.

link, Fig. 2. In the slave LE module, tandeming entity issues the MPH-BI primitive to the relevant port status FSM.

When the port unblocking is initiated, [2], the MPH-UBR primitive is sent to both relevant port status FSM and tandeming protocol entity which will send Unblock Request over SL link, Fig. 2. In the slave LE module, tandeming entity issues the MPH-UBR primitive to the relevant port status FSM. After reception of Unblock acknowledgement (FE202) via V5 interface, the port status FSM in the master LE module issues the same functional element to the tandeming entity which will propagate it to the slave module over SL link. All other situations of port blocking and unblocking are similar to these.

C. Link Control Protocol

The E1 link blocking and unblocking is also allowed only for the V5.2 system management residing in the master LE module (LE1). The link blocking and unblocking procedured are similar to those used for port blocking and unblocking, respectively.

In the event of expiry of persistence check timer, the V5.2 interface layer 1 link FSM issues the MPH-DI primitive to the link control FSM, [1], which propagates it over the SL link to the slave module, Fig. 3. When the internal failure disappeares, the MPH-AI is issued and sent over the safeguarding link to the slave module changing the state in the relevant link control FSM.

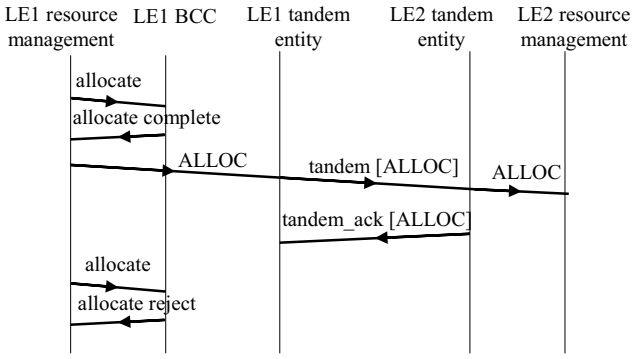

Fig. 4. BCC protocol safeguarding.

D. Resource Management

When allocation and deallocation processes are completed successfully, it is responsibility of the resource management to inform the safeguarding module about the action, Fig. 4. The audit and AN fault processes results are not transmitted over the SL link.

E. Protection Management

After successful switch-over completion, the protection management informs the safeguarding module about the switching having been performed in order to back-up the evidence of the active logical C-channels within the G1 group. The tandem protocol procedures for protection management are similar to those used for BCC safeguarding mechanism. When protection switching is requested for protection group 1, the slave LE module will be informed over the SL link about the result of switching.

VII. Conclusion

The V5.2 tandeming protocol prevents the eventual V5.2 system data loss by handling different types of failures that may occure in the LE equipement. Failures not covered with [1] are detected using the safeguarding timers (TSG 1-3), whose values define the delay of the safeguard switching initiation. The V5.2 tandeming protocol, together with the tandeming of the LE manager functions (call control functions), not specified in this paper, achieve the safeguarding performance in the complete LE system keeping the service information in the case of safeguard switching and providing the persistence of service delivery.

References

[1] ITU-T Recommendation G.965, *V-interfaces at the digital Local Exchange (LE) - V5.2 interface (based on 2048 kbit/s) for the support of Access Network (AN).*
[2] ITU-T Recommendation G.964, *V-interfaces at the digital Local Exchange (LE) - V5.1 interface (based on 2048 kbit/s) for the support of Access Network (AN).*
[3] ITU-T Recommendation G.960, *Access digital section for ISDN basic rate access.*
[4] ITU-T Recommendation I.430, *Basic user-network interface - Layer 1 specification.*
[5] ITU-T Recommendation G.962, *Access digital section for ISDN primary rate at 2048 kbit/s.*
[6] ITU-T Recommendation I.431, *Primary rate user-network interface - Layer 1 specification.*