THE BELL SYSTEM TECHNICAL JOURNAL
Vol. 57, No. 2, February 1978
Printed in U.S.A.

Common Channel Interoffice Signaling:

No. 4 ESS Application

By L. M. CROXALL and R. E. STONE

(Manuscript received May 7, 1977)

Common channel interoffice signaling (CCIS) is provided as an integral part of No. 4 ESS. The unique hardware required for CCIS consists of a common systems CCIS terminal and associated access circuit, continuity check transceivers, and unitized terminal equipment for CCIS trunks. The control of the CCIS hardware and the logic required for CCIS administrative functions is provided by programs resident in the 1A Processor. This paper discusses the system design requirements, the signaling hardware, and the software design for CCIS in the No. 4 Electronic Switching System.

I. INTRODUCTION

No. 4 ESS, a large-capacity toll switching machine, was originally designed to handle two basic address signaling systems, Dial Pulse (DP) and Multifrequency (MF). With the introduction of common channel signaling into the domestic toll network, No. 4 ESS included as part of its initial offering the Common Channel Interoffice Signaling (CCIS) capability. Other papers discuss the basic system architecture,[1] hardware,[2] and call-handling software[3] of the No. 4 ESS with emphasis on the DP and MF signaling systems. This paper deals with the specific hardware and software design associated with CCIS. Section II describes the overall CCIS design constraints, system architecture and hardware as it applies to No. 4 ESS. Section III describes the CCIS software organization and functional implementation.

II. SYSTEM DESIGN

The major components that compose the basic system architecture for No. 4 ESS are illustrated in Fig. 1. The 1A Processor controls all ac-

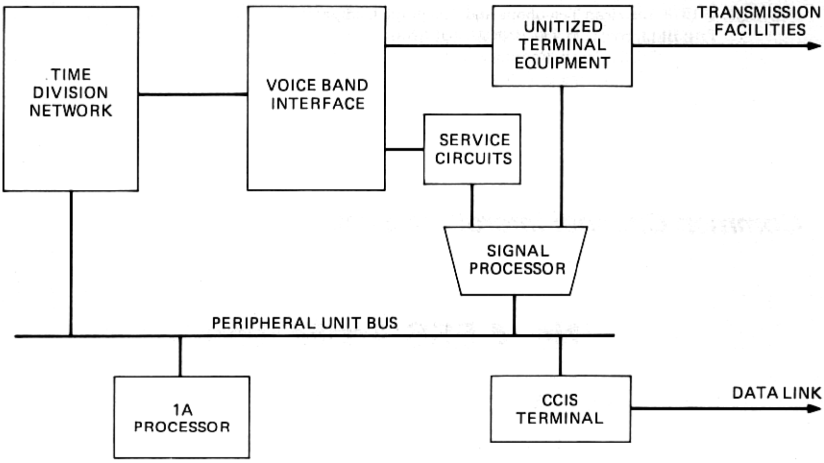

Fig. 1—No. 4 ESS system architecture.

tions of the No. 4 ESS by executing programs residing in core memory. The digital time division network, under control of the processor, establishes connections between all trunks and service circuits. Trunks for all signaling types are housed in unitized terminal equipment frames. Since all switching is done in digital format, any analog signals must be converted to digital format by voiceband interface units.

The Signal Processor (SP) is an autonomous unit which performs the supervisory scanning and distribution functions for E and M trunks. It also performs scan and distribution functions for service circuits, power control, and office alarms. The CCIS signaling terminal interfaces a CCIS data link which carries supervision and address information for CCIS trunks. Both of these signaling units, as well as the time division network, are controlled by the 1A Processor over a peripheral unit bus.

2.1 CCIS hardware

The major hardware modules required for common channel signaling in No. 4 ESS are CCIS terminals, CCIS continuity check circuits, and trunk terminal equipment. The CCIS terminal used in No. 4 ESS is the common systems design[4] used in 4A/STP, 4A/CCIS and No. 1 ESS toll. Up to 16 CCIS terminals are housed in a terminal grouping frame (TGR) and there can be up to 16 TGRs in a No. 4 ESS office. Data transmission between the 1A Processor and the CCIS terminals takes place over the peripheral unit bus via a Terminal Access Controller (TAC). The TAC is duplicated and is a part of the terminal grouping frame. The CCIS terminals are stored program controlled units and are initialized by the 1A Processor. Once initialized they perform all required CCIS data link operations asynchronously from the 1A Processor. The terminals notify the 1A

Processor via a "signal present" scan point when they have received data.

The CCIS Continuity Check Transceiver (CCT) is configured and housed similiar to other No. 4 ESS service circuits (e.g., MF transmitters and MF receivers). The CCTs are packaged and powered in modules of six and are mounted on a miscellaneous frame. Each CCT is assigned a unique termination on the time division network and has control access from the signal processor. Four distribution points are provided for each CCT to allow the 1A Processor to set the operating mode (2 wire or 4 wire) and to sensitize the receiver to the expected round trip via net loss of the trunk. Each CCT uses one scan point for reporting the completion of a successful continuity test.

CCIS voice trunks are similar to those equipped for E and M supervisory signaling except that the Single Frequency (SF) to E and M conversion is not provided. Echo suppressor control, if required, is provided via a signal distribution point in the signal processor. There are no other connections for supervisory or address purposes. Up to 96 CCIS trunks without echo suppressors (48 with echo suppressors) are housed in a CCIS unitized terminal equipment frame.

2.2 CCIS data link

Load-shared CCIS data links are provided between No. 4 ESS switching offices and CCIS Signal Transfer Points (STPs).[5] A pair of data links, one to each STP, is engineered for up to 3000 CCIS trunks. Each CCIS data link consists of a CCIS terminal at the No. 4 ESS, a voice frequency link (VFL), and a CCIS terminal at the STP. For reliability, each data link has both an active and standby VFL. As shown in Fig. 2, the two VFLs and the CCIS terminal are terminated on the time division network. Under program control a connection between a VFL and the terminal is made through the time division network to establish the CCIS data link. This configuration allows switchable access to both the VFLs and the CCIS terminal for automatic or routine maintenance actions.

2.3 CCIS software

As with the hardware, the No. 4 ESS software architecture is modular and for the most part independent of signaling type. Several major program modules are provided for CCIS functions: a call-handling module, a CCIS link security module, and various initialization and hardware maintenance modules. Each of these modules was designed to use as much as possible the same major data and timing structures provided for E and M signaling call types (MF and DP).

Every trunk in No. 4 ESS is assigned a 2-word trunk register (TR) to record the call and maintenance state of the trunk and to provide link-

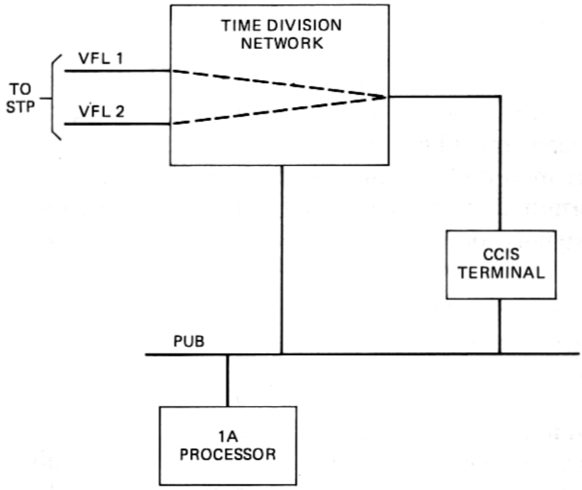

Fig. 2—CCIS data link configuration.

ages to other software structures. An item in the TR indicates whether the trunk is equipped for a CCIS call. This substate allows CCIS call states to be consistent with the call states defined for the other signaling types. All call programs in No. 4 ESS use a common set of TR data layouts, timing lists, and queueing strategies.

The basic structure used to maintain call information during the call setup stage is the 64-word call register (CR). Information in the CR records the state of the call, the incoming and outgoing trunk states, the received digits, connected service circuit information, and routing and outpulsing data. CCIS programs use the general layout of the CR for the CCIS call function. Some new states and data items (e.g., terminal label of trunk) are unique to CCIS.

The trunk structures and trunk translation data organization within the No. 4 ESS is based on the trunk signaling appearance (TSN) on the signal processor. This organization allows SP reports associated with E and M trunks to be handled efficiently. As a CCIS trunk does not require a signal processor for signaling purposes, a pseudo assignment of a TSN is made for each CCIS trunk to maintain commonality of the translation data and call structures. The SP to which the CCIS trunk TSN is assigned does not have to be physically equipped. This allows the CCIS trunk structure and translation data structures to be common, but does not require actual equipment expenditure. To maintain this commonality requires a translation from this internal identification (TSN) to an external identification (terminal and label) when call-related CCIS messages are transmitted. When receiving CCIS messages, the reverse translation must be made.

The design and implementation of the CCIS call-handling module in the No. 4 ESS was based on a "reasonableness table" developed to indicate the domestic CCIS call flow. This reasonableness table which identified the call actions required of every CCIS message in every call state was also used to specify the design for the 4A/CCIS and No. 1 ESS toll machines.

The call-handling functions performed for incoming CCIS calls are independent from those performed for outgoing CCIS calls. This design allows a convenient interface with the non-CCIS (E&M) call-handling programs. The interfaces between the various call-handling programs are simplified because the same data structures are used. Communication between the modules is by direct transfer to perform a defined function.

The CCIS link security module is responsible for maintaining a viable CCIS signaling configuration. As the link security function is not common to other types of signaling programs, it requires independent programs and data structures to perform the CCIS signaling link security functions. The link security module uses three data structures to perform signaling security functions. A 2-word data structure is used for quick reference by call processing to determine the general status of a CCIS link and to determine the backup CCIS link if required. An 8-word register is used to keep detailed status, perform timing functions, and queue multiple CCIS terminal action requests. The third structure keeps signaling status on the bands associated with a signaling link.

CCIS initialization and maintenance functions, including trunk maintenance, CCIS terminal fault recognition, and diagnostics, do not require any major unique data structures. These functions are provided by appropriate additions and modifications to programs responsible for E&M trunks and signaling equipment. A special initialization routine is used to load and initialize the program that is resident in the CCIS terminals.

III. SOFTWARE ORGANIZATION

This section describes the software modules that provide the CCIS functions in No. 4 ESS. The largest module is the call-handling module which performs the actions directly associated with the switching of CCIS calls. It is divided into two programs, the CCIS task dispenser and the CCIS call task routines. As shown in Fig. 3, the CCIS task dispenser interfaces directly with the CCIS terminals. CCIS call messages are distributed by the task dispenser to the appropriate call task routines. These routines perform the actions necessary to respond to the call stimuli and advance the call state. These actions include the sending of CCIS messages, calling special purpose service routines and interfacing with E&M signaling programs.

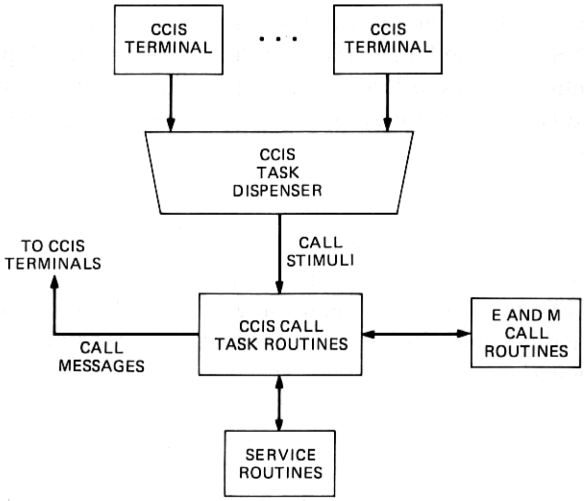

Fig. 3—CCIS call-handling module.

The CCIS link security module is primarily responsible for maintaining a viable configuration of CCIS signaling links. It performs actions in response to error conditions on CCIS data links and in response to manual requests from the maintenance personnel. Figure 7, which is described in Section 3.2, shows the major interfaces with the link security module.

The CCIS fault recognition module responds directly to maintenance interrupts from the TGR. Its main function is to configure components of the signaling hardware (terminal access controllers and terminals) in response to hardware failure indications and schedule appropriate diagnostic routines.

CCIS diagnostic programs, resident in the file store, are paged into core and executed upon demand of fault recognition programs or maintenance personnel. Separate diagnostic programs are provided for the TAC and CCIS terminal.

CCIS trunk maintenance routines respond to manual and automatic test activities associated with CCIS trunks. These programs also respond to CCIS trunk problems (ineffective attempts) as they are detected by the call-handling module.

A CCIS terminal initialization module is used to load and initialize the program which is resident in the CCIS terminal. This module is called whenever a terminal is brought back into service after diagnosis or during system initialization.

There are several other software modules in No. 4 ESS which provide administrative functions for CCIS. These include the recent change and verify capability for CCIS related translation structures, traffic and plant measurement counters for CCIS calls and signaling equipment, network management routines to handle CCIS dynamic overload control (DOC) signals, and a special trunk query routine scheduled by the audit system.

The remainder of this section describes in detail the operation of the call-handling and link security modules. The description of the call-handling module includes the actions associated with a switched CCIS-to-CCIS call.

3.1 CCIS call-handling

The CCIS call-handling programs in No. 4 ESS are organized to provide a convenient interface with the CCIS signaling hardware and to provide efficient interfaces with other signaling and administrative programs. The two major programs are the CCIS task dispenser and the CCIS task routines.

3.1.1 CCIS task dispenser

The CCIS task dispenser provides the major operational interface with the CCIS terminals. Two separate task dispenser routines are provided, one for each of the two priorities of received CCIS messages. The terminal's high priority buffer is unloaded by a CCIS task dispenser routine which is scheduled every 10 ms by the interject level executive control program. The low priority buffer of the terminal is unloaded by a CCIS task dispenser routine which is scheduled once per base level by the executive control program. Each of the two dispenser routines first scan the signal present points for all TGRs to identify which ones have terminals with messages waiting to be unloaded. Those TGRs with terminals containing messages are then polled to determine which of the associated 16 terminals have messages. A separate set of signal present points is provided for each priority and they are duplicated. A software masking arrangement is used to filter out signal present indications from terminals that are in a maintenance state. Once a terminal is selected, its receive buffer is unloaded until it is empty. Each call message is decoded by the task dispenser and sent to the appropriate task routine which handles that type of message. Once the task routine completes action on that message it returns control to the task dispenser which unloads the next call message. Messages are unloaded until all terminals are empty or a predetermined threshold (set by the overload program) is reached.

3.1.2 CCIS task routines

The CCIS call task routines perform the actions necessary to advance the call state in response to CCIS call stimuli: the CCIS call functions performed are sufficiently different from other No. 4 ESS signaling types to require separate programs. However, these programs use the common structure, data translators, and E&M call processing routines as much as possible. Whenever the call action to be performed is common to all signaling types or is special purpose (e.g., translations), an interface is made to a common service routine. Actions unique to other signaling types, (e.g., E&M supervisory actions) are performed in general by those signaling programs. In those cases any appropriate data is passed along with the call control.

There are several major interfaces between the CCIS call-handling programs and other operational feature programs in No. 4 ESS. *Translations*—CCIS translation and office data is retrieved from the data base using translation subroutines. These routing and trunk hunt routines are common for all signaling types. *Overload*—The overload control program monitors the occupancy of the CCIS queues and transceivers and places governors on the amount of work to be performed by the CCIS call-handling programs. *Network*—All actions required of the time division network (path hunts, network connections) are performed by a special-purpose network program. *Traffic*—General CCIS call data is passed to the traffic and plant measurements programs for the pegging of various event counters. These counters are subsequently summarized on machine status reports. *Network Management*—Interfaces exist with the network management program for placing routing controls (e.g., route skip, code block) on CCIS calls. *Initialization*—Initialization programs are called to initialize CCIS call-handling structures during system abnormalities. A special interface is required to govern the number of CCIS messages transmitted to prevent terminal buffer overflow. *Audits*—All the CCIS programs provide defensive checks (e.g., address range check) as part of the logic. Should a check fail, program control and any relevant data is passed to an audit routine for analysis.

3.1.3 CCIS-CCIS call

The CCIS-CCIS call is composed of the following three functions: supervision (seizure, answer, disconnect, abandon), addressing, and continuity checking. How these functions are implemented in the No. 4 ESS is described in the following text and associated pictorial representation of the hardware and software relationships.

A CCIS incoming call is initiated upon receipt of an Initial Address Message (IAM) for an idle trunk over the CCIS data link. The CCIS call-handling program translates the label in the IAM into a network appearance and busies the CCIS trunk in memory to outgoing seizures. The CCIS call-handling program then performs the following incoming

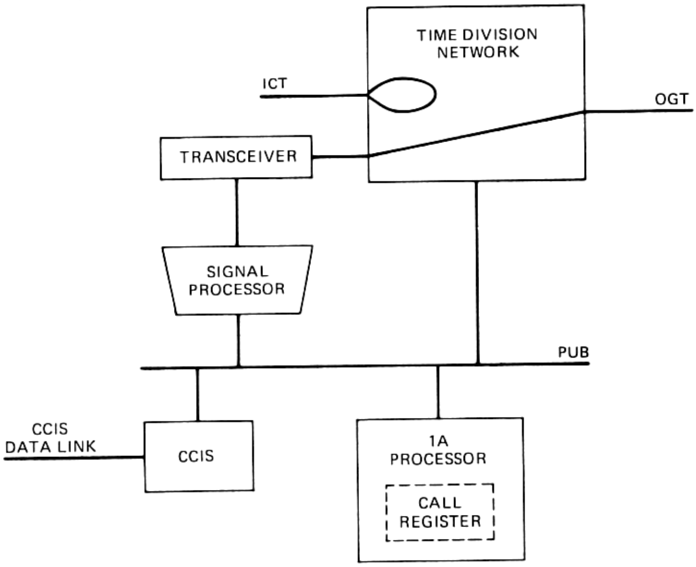

Fig. 4—Incoming and outgoing continuity checking.

functions; seizes and initializes a Call Register (CR), places the trunk information and the address information in the CR, and directs the network program to send orders to the time-division network to connect (loop) the incoming trunk's (ICT) transmit and receive sides for the incoming continuity check. Next the CCIS call-handling program requests the digit analysis and routing program to translate the address digits to obtain an outgoing route. The trunk subgroups in this route are hunted using the trunk hunt routine to obtain an Outgoing Trunk (OGT). If a non-CCIS trunk is selected, non-CCIS call-handling routines are given control of the call. If a CCIS trunk is selected, the outgoing portion of the CCIS call-handling program busies in memory the outgoing trunk to other outgoing calls, it then initiates the outgoing continuity check by hunting a transceiver, causing it to be connected through the time-division network to the outgoing trunk, and initializing the transceiver via an SP distribute point. When these actions are complete an IAM is formulated and sent for the selected outgoing trunk over the CCIS data link.

Figure 4 illustrates the system configuration at this point in the call. The incoming trunk is being tested for continuity by the preceding switching office. A transceiver connected to the outgoing trunk through the network is performing the continuity check on the outgoing trunk. A call register has been seized in memory and is linked via the trunk register to the call. One of two call stimuli are expected at this time; (*i*) a continuity (COT) message for the incoming trunk indicating a successful continuity test of the ICT or (*ii*) an outgoing continuity report via the

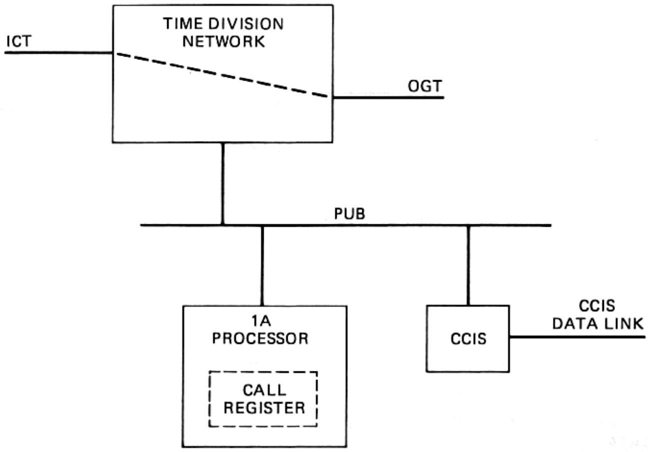

Fig. 5—Waiting for address complete.

signal processor indicating that the transceiver has successfully completed the continuity test of the OGT. If a COT message for the incoming trunk is received first, the CCIS call-handling program will abandon the loop on the ICT and wait for the outgoing continuity report. If the outgoing continuity report is received first, the transceiver is disconnected from the outgoing trunk and made idle. The call then waits for a continuity message for the ICT. When both the ICT continuity message and outgoing continuity reports have been received, a path is reserved in the time division network between the incoming trunk and the outgoing trunk and a COT message is sent for the outgoing trunk. The call is placed in the state "waiting-for-address-complete" as illustrated in Fig. 5. The CR is still linked to the call which allows retrial and announcement treatment in the event of outgoing call irregularities.

The next call setup signal expected is the address complete (ADC) message for the OGT. This message indicates the call has been successfully routed over the last CCIS trunk in the built-up network connection. The CCIS call-handling program requests connection of the incoming and outgoing trunks through the time-division network using the path previously reserved. At this point the CR is released (all transient data is erased) and the call is put in the waiting-for-answer state. No reattempt or call failure messages can be acted on once the call has reached this state since the CR data has been erased.

If a backward failure message (e.g., vacant national number, confusion) is received for the outgoing trunk rather than an ADC, processing of the call is discontinued and the outgoing trunk is made idle by the sending of a CLF. Depending on the type of failure, the call-handling program may retry the incoming call or terminate it by passing the same failure

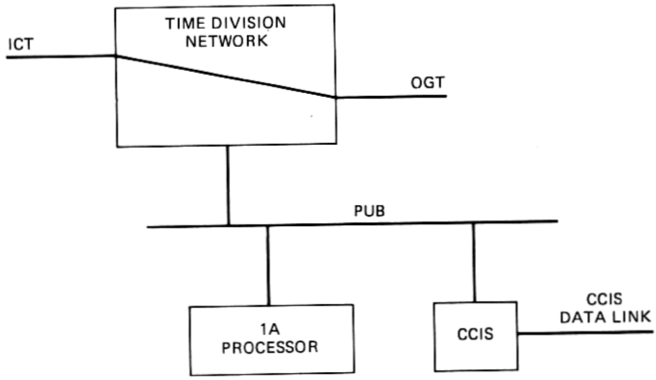

Fig. 6—Waiting for answer or talking.

message for the incoming trunk. In the latter case the program will place the incoming trunk into a call state which waits for an acknowledging CLF from the previous office to idle the ICT.

If an answer message (ANC) is received for the outgoing trunk, the call-handling program will send an answer signal for the ICT and place the call into the talking state. Error conditions on the signaling channel can cause an answer signal to arrive before the ADC. In this case, the call-handling program will advance the call directly to the talk state by performing the actions described above. In the talking state, clear back (CB) and reanswer (RA) messages will be passed (OGT to ICT) as they are received. Figure 6 shows the configuration of the system in the waiting-for-answer and talking states.

The CCIS call-handling program will abandon calls in any state when it receives a clear forward (CLF) message for the incoming trunk. A release guard (RLG) message is sent for the incoming trunk to acknowledge the idling of the trunk. If there is an outgoing CCIS trunk associated with the call, a CLF will be sent for the outgoing CCIS trunk. The OGT then goes to a state where it is waiting for a RLG. If a network connection is up, it will be taken down.

3.1.4 E&M-CCIS call

On hybrid E&M to CCIS calls, the outgoing CCIS functions are performed as if the ICT had been CCIS. Since continuity is assumed to be inherent on an incoming E&M trunk, the COT message can be sent for the outgoing CCIS trunk when the outgoing continuity check is completed and the incoming and outgoing trunk network path is reserved. The receipt of ADC for the outgoing trunk causes the ICT to OGT connection to be made and the call to enter the wait-for-answer state. The receipt of ANC for the outgoing trunk will cause the CCIS call-handling program to send an off-hook on the E&M trunk. The clearing sequences are also similiar. An on-hook condition on the E&M trunk causes the call to be terminated and both the ICT and OGT are made idle. The E&M ICT is made idle by releasing the M relay (on hook). A CLF will be sent for the CCIS outgoing trunk. If a backward failure message is received for the CCIS outgoing trunk, the call is either retried or terminated. If the call is terminated the incoming E&M trunk is connected to an announcement.

A special case of an E&M to CCIS call is one where the ICT requires call recording for Centralized Automatic Message Accounting (CAMA). Both the calling and called numbers are received by the CAMA program before an outgoing trunk is hunted. If a CCIS trunk is selected, the call progresses as previously described for E&M to CCIS calls up to the waiting-for-answer state. If an answer signal is received for the CCIS OGT, the charge administration routine in the CAMA program is called to record the answer time. The same routine is called when the ICT goes on-hook to record the disconnect time.

3.1.5 CCIS-E&M calls

An incoming CCIS call may be switched to an outgoing E&M trunk. On this hybrid call, the regular E&M trunk seizure and outpulsing routines are entered to perform the outgoing functions. The last digit is withheld from the outpulsing routines until a COT message is received for the CCIS incoming trunk. This prevents the possibility of the call being set up all the way to the called party before the continuity of the ICT talking path is verified. The CCIS call-handling program will send an ADC for the incoming trunk when the COT is received for the ICT, providing an E&M trunk has been successfully hunted and seized. Failures detected prior to the sending of address complete (e.g., all trunks busy) will cause the appropriate CCIS failure message to be sent for the incoming trunk. After outpulsing is completed, an off-hook on the outcoming E&M trunk causes an ANC message to be sent for the incoming trunk. Upon receipt of a CLF for the CCIS ICT the CCIS call-handling program will send a RLG for the ICT and place the OGT on-hook by releasing the M relay.

3.1.6 CCIS trunk maintenance

The trunk maintenance features for CCIS trunks are very similar to those provided for E&M trunks. Normal trunk maintenance functions such as routine signaling and transmission tests and manually requested calls to far end test lines are the same for CCIS and non-CCIS trunks. The continuity retest and the translation integrity check are incorporated as additional maintenance tests that can be run on any CCIS trunk. There are special routines to administer blocking and unblocking signals for CCIS trunks. The trunk maintenance features for collecting, analyzing, and outputting data associated with call irregularities is also applicable to CCIS trunks. The CCIS call-handling programs are used as much as possible to handle the signaling sequences associated with test calls. This approach simplified the trunk maintenance design and provided clean software interfaces.

The voice frequency links are treated essentially as normal voice trunks by the trunk maintenance program. They can be switched to a manual test position for all normal manual testing activity. An interface with the link security module is provided to inhibit trunk maintenance activity for a VFL that is being used as part of a CCIS data link.

3.1.7 Initialization procedures

During system initialization special procedures are required to idle CCIS trunks. Because there is no access to the trunk circuit to place it on hook (as is the case for E and M trunks) the CCIS data link is used to notify the far end of trunk idling actions. In the lower level initialization phase of No. 4 ESS (phases 1, 2, and 3) individual Reset Trunk (RST) messages are sent for all trunks that are in a transient state (not waiting for answer or talking). In the highest level phase (phase 4), Reset Band (RSB) messages are sent to idle all CCIS trunks. The CCIS data link must be resynchronized in a phase 4 because the connection between the terminal and the VFL has been removed during the network initialization.

3.2 Link security

CCIS link security is another major software module in No. 4 ESS. Its functions include monitoring the error performance of CCIS data links, responding and reconfiguring CCIS data link components (CCIS terminals, VFLs) to maintain a viable signaling channel, responding to band status messages from STPs, and providing an interface for the maintenance personnel to perform test activity on the CCIS data links. The No. 4 ESS link security system is designed to work in a load-sharing configuration as described in Section I. Each CCIS terminal is dedicated to a data link.

Figure 7 shows the major interfaces with the CCIS link security module. Stimuli to link security can be received from any of the following sources: internal data in the CCIS terminal, fault recognition programs, maintenance personnel, or the STP (via the CCIS terminal receive buffers).

Permanent translation data is provided for each pair of CCIS data links which includes the identities of the CCIS terminals, the associated VFLs and time division network assignments. This translation status along

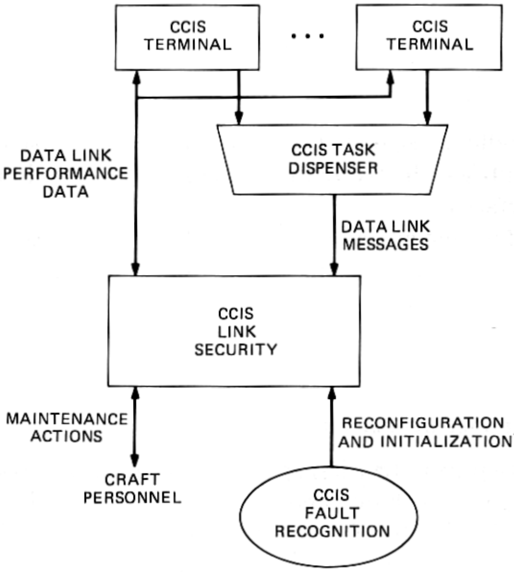

Fig. 7—CCIS link security module.

with three status tables are used by the link security module to perform its actions. The operational link status table provides a summary of the operational status of the data links for all the bands assigned to the data link. Detailed data link status information for each band, such as "restricted" or "prohibited" conditions, is maintained in a band status table. The CCIS call-handling programs interface with both of these tables to determine the operational status of a CCIS signaling link and band. These tables are updated by status messages received from the STP. The link security terminal register is a software data block reserved for each CCIS terminal and contains the specific state, condition indicators and event timers for the terminal and associated signaling link. The link security program responds to data link stimuli by consulting this register to determine the state of the signaling link. This register is also used to queue multiple requests for a signaling link waiting action by the link security program.

3.2.1 Link security actions

The link security program receives its inputs from the CCIS terminals via messages received over the data link (through the CCIS task dispenser) or by direct scanning of the CCIS terminals. In the later case the CCIS terminal will report data link status changes via a scan point assigned on the signal processor. This scan point is driven by the software in the CCIS terminal. The terminal is interrogated directly by link security to determine the particular condition the terminal is reporting (e.g., synchronization achieved, buffer overflow).

One condition reported in this manner is a synchronization report indicating that the signaling link has become operational. In this case the link security program will request an update of the band status information from the STP. When the update is completed, the status of the data link is updated in the operational link status table and the state of the link is changed in the terminal register. The data link is then available for carrying CCIS signaling information.

Another condition reported from the terminal is a high error rate on the signaling channel. In this case the data link has become inoperable and changeover procedures are invoked. Any messages waiting transmission that are stored in the CCIS terminal serving the failing data link are transferred to the transmission buffer of the CCIS terminal serving the load sharing (mate) data link, providing it is operational. The terminal status is updated in the operational link status table to direct call-handling actions toward the in-service CCIS terminal. Standard recovery procedures are started to resynchronize the failing data link. The resynchronizion is attempted using both VFLs. The CCIS terminal is switched between the two VFLs every three seconds. If the data link does not resynchronize within three minutes, the CCIS terminal is taken out of service and diagnosed. If the data link resynchronizes on either VFL, the data link is put in service and signaling is restored as described previously. Bad VFLs are reported to trunk maintenance programs for further maintenance actions.

Hardware faults within a CCIS terminal or TAC are detectable through an all-seems-well mechanism over the PUB. These failure conditions are handled by the peripheral bus fault recovery program on a maintenance interrupt level. This program isolates the failure to the CCIS equipment and calls in the CCIS fault recovery program to establish a viable CCIS configuration. If a CCIS terminal is removed from service, the CCIS fault recognition program interfaces with link security to update the status of the CCIS terminal to an out-of-service state. CCIS messages are not removed from a faulty terminal since access may be restricted. The CCIS fault recognition program will request a diagnostic for the faulty terminal. When the CCIS terminal passes diagnostics, a report is made to link security and normal recovery procedures are invoked by link security.

The interface between the craftsperson and the link security module is primarily for maintenance of the CCIS data links and is handled by teletypewriter (TTY) input and output messages. A craftsperson can manually remove a data link from service by inputting an appropriate TTY message. The link security module will check the input message for validity, insure that the load sharing data link is in service, and then request concurrence of the STP by sending a manual changeover message. The STP will respond with a manual changeover acknowledgement which will cause link security to remove signaling information from the data link and force new signaling information to the load-shared data link. A manual restoral to service input message will return signaling traffic to the data link. Manual configurations of CCIS terminals and VFLs are similiarly requested and handled by link security with proper acknowledgment (via the data link) of the STP. A request for the operational status of any CCIS data link may be made at any time via TTY messages.

The link security program also responds to data link configuration requests from the STP (via CCIS messages). These messages may, for example, request a test of the inactive VFL on a data link. In this case the link security program will loop the VFL so that it may be tested by the STP. The STP will notify the No. 4 ESS via a CCIS message whether the test passed or failed. If a VFL fails this test it is reported to trunk maintenance.

Other data link messages processed by link security include those which contain band status information. These messages are sent by the STP to reflect the partial or total loss of signaling capability in the CCIS signaling network. In response to these messages, link security updates its band status tables as appropriate and removes or restores affected trunks from service.

A unique feature of the CCIS terminal is a timer which insures the sanity of the main processor. In No. 4 ESS, should the 1A Processor fail to access the CCIS terminal within a specified time, the CCIS terminal will automatically transmit processor outage signals on the data link. Processor outage signals can also be received over the data link from the CCIS terminal at the STP. The link security program will respond to these signals from the STP by evoking special congestion procedures which throttle the signals transmitted on the CCIS data link. Similar procedures are evoked by link security if a buffer overflow condition is detected from the CCIS terminal.

IV. SUMMARY

This paper describes the major hardware and software subsystems necessary to provide CCIS in the No. 4 ESS. The authors would like to acknowledge other major contributors to the software development for CCIS, L. D. Bethel, T. J. Cieslak, R. L. Else, A. M. Frantzen, S. F. Heath, M. T. Smith, and M. Sundararaman as well as the hardware designers, E. Grueser, R. Metz, W. H. Schurter, and R. E. Wallace. This team combined to provide a successful introduction of CCIS into the No. 4 ESS.

REFERENCES

1. A. E. Ritchie, A. E. Spencer, and L. S. Tuomenoksa, "No. 4 ESS: System Objectives and Organization," B.S.T.J., *56,* No. 7 (September 1977), pp. 1017–1028.
2. J. H. Huttenhoff, J. Janik, Jr, G. D. Johnson, W. R. Schleicher, M. F. Slana, and F. H. Tendick, "No. 4 ESS: Peripheral Hardware," B.S.T.J., *56,* No. 7 (September 1977), pp. 1029–1056.
3. T. J. Cieslak, L. M. Croxall, J. B. Roberts, M. W. Saad, and J. M. Scanlon, "No. 4 ESS: Software Organization and Basic Call Handling," B.S.T.J. *56,* No. 7 (September 1977), pp. 1113–1138.
4. B. Kaskey, J. S. Colson, R. F. Mills, F. H. Myers, J. T. Raleigh, A. F. Schweizer, and R. A. Tauson, "Technology and Hardware," B.S.T.J., this issue.
5. P. R. Miller and R. E. Wallace,"Signaling Network," B.S.T.J., this issue.