PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G08B 25/01

A1

(11) International Publication Number: **WO 98/24078**

(43) International Publication Date: 4 June 1998 (04.06.98)

(21) International Application Number: PCT/GB97/03180

(22) International Filing Date: 19 November 1997 (19.11.97)

(30) Priority Data:
96308546.9 26 November 1996 (26.11.96) EP
(34) Countries for which the regional or international application was filed: GB et al.

(71) Applicant *(for all designated States except US)*: BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventors; and

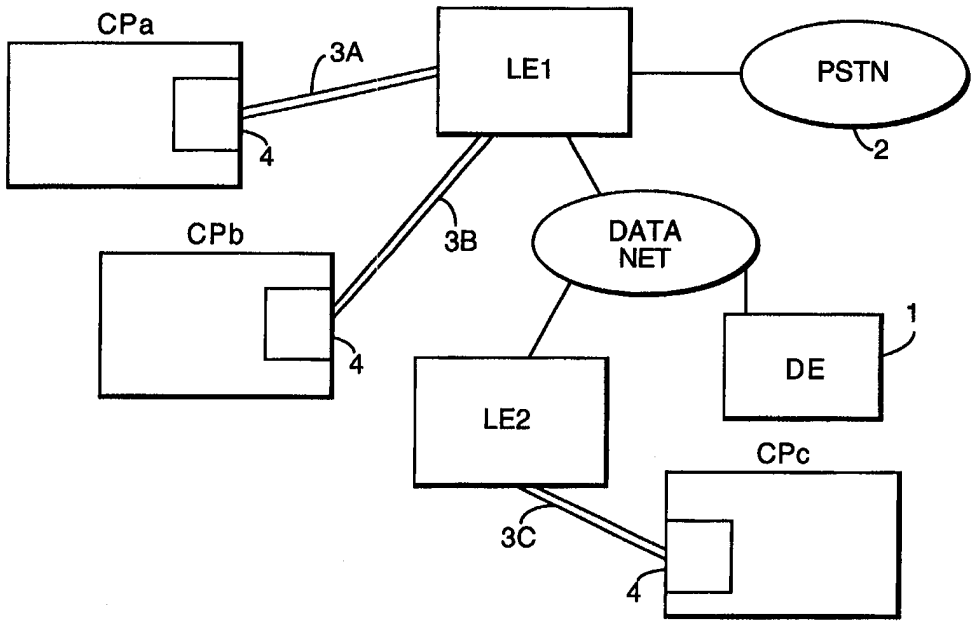
(75) Inventors/Applicants *(for US only)*: KNIGHT, Richard, Robert [GB/GB]; Bramcote, The Street, Ashfield, Stowmarket, Suffolk IP14 6LY (GB). PARKINSON, David, William [GB/GB]; 36 Henley Road, Ipswich, Suffolk IP1 3SA (GB). TUCK, Robert, Ernest [GB/GB]; 14 The Greenway, Daventry, Northants NN11 4EE (GB).

(74) Agent: WELLS, David; BT Group Legal Services, Intellectual Property Dept., Holborn Centre, 8th floor, 120 Holborn, London EC1N 2TE (GB).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: COMMUNICATIONS SYSTEM



(57) Abstract

A communications system includes a telecommunications link (3) between a remote terminal (CPa–c) (such as a burglar alarm control panel) and a control station (1). Polling requests are transmitted on a digital messaging channel which is carried by the telecommunications link. The remote terminal (CPa–c) generates a poll response message which is partially encrypted and is returned on the digital messaging channel to the control station where it is decoded.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

COMMUNICATIONS SYSTEM

The present invention relates to a system for monitoring remote terminal equipment, such as a security alarm, over a telecommunications link.

There are a number of situations in which it is necessary to monitor at a central site the status of terminals at remote locations. One example is provided by burglar alarm systems of the type which send an alert to a monitoring service. Conventionally, a telephone line has been used to provide the connection between the alarm equipment at the customer premises and the monitoring station. An analogue tone is transmitted on the line to the local exchange and is used for signalling between the alarm and the monitoring station, including the transmission of alarm signals. Such an arrangement provides only a limited degree of protection against attacks intended to defeat a security system. If the tone is interrupted by the line being cut, then this is detected at the monitoring station. The signals transmitted on the analogue link may be encrypted, although in practice any such encryption may be detected and broken over relatively short time scales. Once the code has been broken, then an attack may be made by cutting into the line and substituting a dummy terminal which masquerades as the real terminal. This makes it possible to disable the security system at the customer premises without the monitoring service being alerted.

According to a first aspect of the present invention there is provided a method of operating a communications system including a telecommunications link between a remote terminal and a control station, the method comprising:

a) transmitting polling requests on a digital messaging channel carried on the telecommunications link ;

b) generating at the remote station a poll response message and encrypting part only of the said poll response message;

c) returning a response signal from the remote terminal to the control station on the digital messaging channel; and

d) at the control station decrypting the poll response message.

The present invention provides a monitoring system which offers improved security and greater flexibility in operation combined with low transmission

overheads. This is achieved by establishing a digital messaging channel between the remote site and the central station, polling the site on the digital messaging channel, and then partially encrypting the polled response. The use of digital messaging makes possible the application of more powerful encryption techniques, and the encryption of part only of the polled response message allows authentication of the poll response at the central station while only adding marginally to the bandwidth required for signalling between the remote station and the central station.

Preferably the digital messaging channel is the D channel of an ISDN circuit.

A further advantage of the present invention is that it is suitable for implementation using standard ISDN technology for the telephone link. In particular, the messaging channel may be integrated with the existing D channel of an ISDN line. The monitoring function can then operate transparently, without interfering with the operation of the ISDN line. The ISDN line is therefore available for simultaneous use, for example, for voice telephony.

Preferably the remote terminal transmits the poll response in a plurality of segments and the central station returns to the remote station an acknowledgement of each segment received and a further acknowledgement for the message assembled from the segments.

This preferred aspect of the invention divides the poll response message into a number of parts each of which is transmitted separately. A handshake is carried out with the central station both for the individual segments, and also for the message as a whole formed by assembling the segments.

Preferably each polling request from the central station includes a different identifying code, and the encrypted part of the poll response includes the identifying code of the respective poll request.

The security of the system is further enhanced by including in each poll from the central station an identifying code or "challenge" which is specific to that particular poll. The remote terminal is then required to include the appropriate "challenge" in the response to the poll. Including the challenge in the encrypted part of the poll response then provides a double layer of security. Encryption with the key belonging to the particular remote terminal serves to authenticate the

source of the polled response while the inclusion of the challenge identifying code indicates that the response has been freshly generated in answer to the respective poll. This provides a safeguard against attacks on the security of the system in which genuine poll responses from the remote terminal are intercepted and stored for later forwarding to the central station.

Preferably the telecommunications link includes a local access network which links the remote station to a local exchange. Alternatively, or in addition, some of the polling requests and responses may be transmitted over a wireless communications link which may be, for example, a GSM link.

The present invention is not limited in applicability to systems in which the remote terminal is a burglar alarm, although the high degree of security offered by the invention is particularly advantageous in this context. Other uses for the invention include remote monitoring of meters, for example electricity, gas or water meters, or remote monitoring of the status of an automatic vending machine.

According to a second aspect of the present invention, there is provided a communications system comprising:

a control station including a polling request generator and a decoder for decoding poll response messages;

a remote terminal including a polling response generator for generating a polling response message;

an encoder arranged to encode part only of the polling response message;

a telecommunications circuit including a digital messaging channel which, in use, carries polling requests from the control station to the remote terminal and carries partially encoded response messages from remote terminal to the control station.

According to another aspect of the present invention, there is provided a control station comprising:

a) a digital messaging channel interface which is arranged to transmit and receive messages to and from a remote station on a digital messaging channel;

b) a polling request generator which is arranged to generate a polling request for transmission on the digital messaging channel;

c) a decoder arranged to decode a partially encrypted poll response message which is received on the digital messaging channel; and

d) a controller which is arranged to interpret the poll response messages.

The invention encompasses control stations and remote terminals (such a, e.g., a burglar alarm control panel) for use in methods in accordance with the first aspect of the invention.

Systems embodying the present invention will now be described in further detail, by way of example only, with the reference to the accompanying drawings, in which:

Figures 1a and 1b are schematics of systems embodying the present invention;

Figure 2 is a schematic showing the functional interfaces in the systems of Figure 1;

Figure 3 is a detailed schematic of equipment for implementing the control station of the system of Figure 1

Figures 4a and 4b show alternative protocol stacks used in systems embodying the invention;

Figures 5a and 5b are state transition diagrams

Figure 6 is a message flow diagram illustrating the operation of the system when an alarm state arises;

Figure 7 is a diagram showing the format of a poll request message;

Figure 8 is a diagram showing the format of an alarm;

Figure 9 is a diagram showing the basic format of a poll response message;

Figure 10 is a diagram showing in detail the format of an alarm poll request;

Figure 11 is a diagram showing the format of a telemetry poll response;

Figure 12 is a diagram showing the format of a non-secure poll response;

Figure 13 is a diagram showing the format of acknowledgement messages;

Figure 14 shows the message sequence used to establish session keys;

Figure 15 shows the format of an initial message sent to an alarm unit;

Figure 16 shows the message returned in response to the message of Figure 15;

Figure 17 is a diagram showing the format of a response from the central site;

Figure 18 is a diagram showing the alarm site response;

Figure 19 is a diagram showing the architecture of the software used to implement the customer premises equipment in the system of Figure 2;

Figures 20a to 20d are SDL diagrams for the Alarm Handler process of Figure 19;

Figures 21a to 21 g are SDL diagrams for the Protocol & Security process of Figure 19.

A communications system includes a control station 1 which incorporates a data engine DE. Data is received at the data engine via local exchanges LE1, LE2 of a telecommunications network 2. The local exchanges are linked by ISDN lines 3a, 3b, 3c to remote terminals, 4, at different customer premises CPa, CPb, CPc. A number of different local exchanges are linked via a data access network to the control station 1. Although for the purposes of illustration only three customer premises are shown, in practice, many more terminals may be linked to a particular control station. The present example can accommodate 1024 individually addressable units at each of the customer premises. In this example the remote terminals 4 are the control panels of security alarm systems arranged to communicate with an alarm monitoring centre via the control station 1. The terminals 4 are also referred to herein as "customer premises equipment" (CPE).

The ISDN connections between the customer premises and the local exchange use the ISDN D channel for traffic relating to the alarm system. The alarm data communication operates transparently to the user, so that the ISDN channels remain available for voice telephony and/or other data transmissions.

In Figure 1B, in addition to using ISDN connections via a fixed network, the system includes a back-up connection between the remote terminal 4 and the control station 1 which uses a GSM mobile telephony network. Specifically, the connection is formed using the GSM short messaging service (SMS) to provide the required digital messaging channel.

It will be understood that the present invention can be applied to a variety of different network topologies, and the two networks illustrated are chosen by way of example only. One further alternative is the application of the invention in a network in which access to/from the customer premises is entirely based on a mobile telephony system, such as GSM.

Figure 2 shows in further detail the components making up the system of Figure 1. An ISDN line 21 terminates at the local exchange in an ISDN termination 22, and terminates at the customer premises in an NT-1 (Network Termination 1) device 23. In this example, the ISDN line is a BRI (Basic Rate Interface) line comprising two 64 kbps bearer (B) channels for voice or data, and one 16kbps data (D) channel. The NT-1 converts the two-wire interface of the ISDN line to a 4 wire S/T interface. An S/T bus 24 connects the NT-1 to the CPE, and may also connect other devices such as an ISDN modem (not shown). In the CPE, terminal adapter 25 provides a duplex connection to the S/T bus. A control processor 26 located in an alarm panel receives data from a number of alarm detectors 27 a-c. The alarm detectors may include, for example, motion sensors to detect intruders, and smoke detectors to detect fire. The alarm panel and alarm detectors, other than in their manner of communication with the control station, are entirely conventional in construction and operation and so will not be described further here.

From the local exchange, signals to or from the ISDN termination 22 are communicated via a data access network to the data engine 28. The data engine 28, which operates in accordance with the protocol described in further detail below, may, as in the example illustrated in Figure 3, run on a platform comprising a number of UNIX workstations, such as those available commercially as Sun UltraServers II. The connection from the ISDN termination to the data engine 28 may be way of an X25 (packet switching) network 229 or alternatively by way of a dedicated D channel access network 230. In layer 2 of the D-Channel protocol, the service access point identifier is set to a value which indicates the use of a packet access service.

In the example shown in Figure 3, the data engine is incorporated in a platform which also handles alarm signals from conventional analogue systems. Incoming signals on Kilostream channels are received at front-end processors 310

and pass on a 10BaseT network to the data engine core servers 37, 38. An access server 39 allows communication with platforms at other sites using, in this example, TCP/IP protocols. Signals may also be communicated via this TCP/IP interface with other networks, such as a mobile telephony network. Signals from the data engine pass via a terminal server 36, which in this example is a DEC Alpha ARS, and a multiplexer 37 onto a kilostream link. The kilostream link connects the data engine to a respective one of a number of alarm receiver centres (ARC). In this example, the ARC 35 includes both analogue alarm receiving equipment 31 and a digital user system 32. It is this latter digital user system 32 which handles alarm calls generated by the data engine.

When an alarm signal generated by CPE (customer premises equipment) is received at the data engine, this is passed on via an X.25 network 31 to the appropriate one of a number of alarm receiver centres 32a, 32b. In use, the data engine 28 generates polling request signals at regular intervals. These are transmitted via the ISDN line to the CPE. The CPE responds with a call response message which indicates either that there has been no change in the status of the alarms, or that there has been a change and the nature of the change. As further described below, the poll response message generated by the CPE includes an encrypted signature generated using a hash function. Included in the encrypted signature is the challenge sent by the data engine in the relevant poll request.

Figure 4a shows one example of a protocol stack for the system illustrated in the preceding figures. As discussed above, one option is that data should be transferred from the ISDN line across a X.25 network. The other option is to connect the data engine directly from the "D" channel access network. This option however then does not provide such functions as segmentation and reassembly of information blocks which are too large to fit into one message. Where this option is adopted, then as shown in Figure 4b, an X.25 layer 3 may not be present since the access network only terminates layer 2. The data engine then implements a simplified X.25 network side (layers 2 and 3) as an option to cater for the direct connection to the access network. Two typical protocol stacks are shown in Figure 4, demonstrating the flexibility of the alarm protocol in functioning with different protocol stacks in different environments.

The following description sets out the protocol for the functional interfaces A and B illustrated in Figure 2 taking into account the services that the X.25 layer 2/3 provides.

The protocol used for the interfaces to the data engine is designed to be robust, secure and efficient. The data engine is required to be able to determine if the CPE is still operating effectively, and to determine that it has not been interfered with. This is achieved through a polling mechanism, such that the data engine (DE) connects to the CPE and interchanges a simple status message. The polling rate in this example is every 8 seconds (T_{711}). To support this, a permanent X.25 connection must be made. Failure to gain an acceptable response from the CPE is reported only after a configurable number of polls (N_{711}) at intervals of T_{711} and after a further single period of T_{711}. This delay is such that the report is generated in 40-90 seconds. A total of 5 unsuccessful poll attempts would result in a report to the alarm receiver centre (ARC) between 40-48 seconds after a customer line has been cut. The CPE is not considered to be sending reliable (and therefore reportable) information until it has correctly responded to a predetermined number (N_{712}) polls. In this example N_{712} has the value of 2.

The DE differentiates between a number of different types of failures including network congestion; invalid response; and failure to connect. These different types of failure require different degrees of urgency at the ARCs and this is reflected in the protocol at interface B. The DE classifies the CPE as being in one of three states: decommissioned (alarms are disabled); active (the normal state); and CommsFailed (when the CPE has failed to respond to N_{711} poll attempts).

The protocol is message based and reports on individual alarms only when a change of state occurs. The protocol is able to identify uniquely 1024 different alarms from each individual (addressable) CPE. Each alarm may be in one of four states: normal (inactive); alarm (alarm channel activated); outstanding (registered at ARC); and reset (alarm channel deactivated). The alarm and reset states are used to indicate that the change of status has been registered at the DE but not yet confirmed at the ARC. The progression of alarms between these states is controlled by the ARC the DE and the CPE. The protocol is responsible for carrying the information and for the orderly progression through these states.

To allow some remote fault diagnosis, a simplified (non-secure) message and acknowledge is implemented for decommissioned CPEs.

All interactions between the DE and the CPE are acknowledged as are all interactions between the DE and the ARC. The DE re-sends information to the ARC after timer T_{702} has expired, normally after 60 seconds. There is no limit to the number of times it will be reported to the ARC if an acknowledgement is not received.

When the CPE has been unreachable and classified at the DE as "CommsFail" it is not treated by the DE as being reliable unless two consecutive polls have been successful. Figures 5a and 5b are state transition diagrams illustrating the state transitions discussed above.

The system embodying the present invention minimises message lengths by exchanging details of alarms only when a change of state occurs. Under static conditions, the CPE reports only the number of alarms currently in each state. However, when an alarm changes state, this is reported to the DE (as part of the regular poll) identifying the alarm channel and its new state. The DE then acknowledges the alarm and subsequent polls only report the number of alarms in each state. Figures 6 shows an example of information flows illustrating this process.

An important feature of the system described above is its ability to provide a high level of security. In particular it address the risks arising from the fact that the system uses part of the PSTN access network which is vulnerable to interception.

Five specific threats to the security of the system have been identified:

T1 - the communications line is cut to isolate the alarmed system from the central site.

This is the simplest form of attack where the wires connected the alarm system to the central monitoring site are cut.

T2 - the communications between the alarm system and the central site are intercepted and the messages modified in transit.

For example the "normal" and "alarm" fields are adjusted to their quiescent values, thus disguising the operation of an alarm circuit.

T3 - the line is intercepted and a unit inserted to masquerade as the alarm system.

This is a variant of T2 but the inserted unit acts as the alarm system, continually reporting a "no change".

T4 - the line is intercepted and a unit inserted to masquerade as the central site.

In this case the attack is to issue commands that would disable (or decommission) the alarm system. It may also try to cycle rapidly an alarm system from an alarm state back to the normal state by replaying earlier "poll" and "acknowledge" messages.

T5 - the line is monitored that so than an attacker can determine when the alarm system is decommissioned. This is the only threat which relates directly to the ability of an attacker to read communications on the link between the remote site and the DE. An attacker may take advantage of knowing when an alarm system was switched off.

The threats enumerated above are dealt with in the present system by the following counter measures:

C1- polling the alarm system at frequency intervals.

By polling the CPE equipment on a regular basis the system can detect if the communications circuit is broken (or the CPE unit disabled).

C2 - using a cryptographic integrity check on all acknowledgement messages.

If the poll response is cryptographically signed, then any attempted modification of the message, (e.g. to conceal an alarm entering the "alarm" state), will be detected. This applies to all acknowledgement message that change the state of the alarm systems.

C3 - cryptographic binding of a poll response to the specific poll request.

If the poll response message is bound to the request message (e.g. using a sequence number or "challenge"), then a successful attack cannot be made by replaying earlier messages in an attempt to conceal a change in state of the alarm system.

C4 - encryption of sensitive commands.

If messages such as "decommission" are encrypted, then an eavesdropper is unable to determined the exact state of the alarm equipment. It is important that the behaviour of the equipment and the size of the command message does not leak this information. For this reason the CPE is arranged still to respond to polls when decommissioned, and the command message size is the same for all command messages.

C5 - mutual authentication.

Whenever a security critical command is being carried out, e.g. decommissioning an alarm unit or downloading a new session key, then the alarm equipment confirms the identify of the central site before acting on the command.

In combination, these counter measures protect the system from the threats listed above. Table 1 below shows the relationship between the enumerated threats and counter measures. The effectiveness of the counter measures relies upon the secrecy of the encryption keys. For good security, the keys are changed on a regular basis. To facilitate this a master key, session key hierarchy may be used. Here the master key is used infrequently (reducing its exposure), while the session key is used for the bulk of the work. New session keys are distributed on-line, protected by the master key, and changed on a regular basis with minimum administrative overhead. It is important then that the session keys are changed regularly, for example on a monthly basis and that all keys for different CPEs should be unique.

Encryption is effected using, in this example, the MD5 hash algorithm specified in RFC1321, "The MD5 Message-Digest Algorithm", MIT and RSA Data Security, Inc. The system uses a master key size of 12 octets (96 bytes) and a session key size of 8 octets (56 bytes). The MD5 hash algorithms specified in the RFC is unkeyed. In order to use it in a keyed fashion some additional processing is necessary. In this example this is carried out using the HMAC function defined:

$HMAC_{sk}(x) = F(sk,pad_1,F(sk,pad_2, x))$

Where: F( ) is the MD5 algorithm

sk is the Session Key

pad_1 is the byte 0x36.

pad_2 is the byte 0x5C.

x is the message over which the hash is calculated.

MDF works on 512 bit blocks (64 octets). In each instance of F() above the session key sk is padded to 512-bytes by replicating the specified pad nbit as many times as is necessary. The 64 byte sequence (sk, pad_2) is prepended to the message x. The total message is then hashed using MD5. Finally the 64 byte sequence (sk, pad_1) is prepended to the 16 byte output of the previous hash and the resultant 80 bit block MD5 is hashed to produce the 16 byte hash value to be appended to the message x. A saving in computational time can be achieved by precomputing f(sk, pad_1) and f(sk, pad_2) and saving them along with the session key.

When an encryption function is required, the data is encrypted by "exclusive-OR"ing it with a sequence of bytes generated by a single operation of the hash function. The MD5 hash function operates on a 512 bit (64 byte) input block. The input block is built by concatenating: the master key (12 bytes); an initialisation vector (8 or 16 bytes); and a replicated pad character (0x5C).

Random numbers are required for session keys, for the random challenges included in poll requests, and for initialisation vectors. The system maintains a circular buffer 512 bytes in size at the central site, and buffers 16 bytes in size at the alarm sites. A random "RND()" function supplies the next n bytes from this buffer every time it is called, with the pointer wrapping around to the start whenever the end of the buffer is reached. Conveniently, the random buffer is updated using the same MD5 algorithm which is used for hash generation. The MD5 function is modified to include a pointer into the random buffer. Following the completion of round 3 of the MD5 hash process, the first 13 bytes of the internal 16 byte buffer are XOR'd into the random buffer commencing at the point indicated by the internal pointer. The pointer is updated to point at the next point to be modified. Table 2 is a code listing for the random function.

Figure 7 shows the format of the PollRequest message which is transmitted from the data engine to the CPE. The PollRequest includes a challenge that the CPE is required to include in the response. If the challenge were to be predictable, then the system would be vulnerable to a "man in middle" attack. This might be guarded against by integrity checking the PollRequest packet, although this adds significantly to the packet size and processing overhead. The present implementation therefore uses a random challenge rather than a

predictable challenge. The size of the challenge depends on the frequency of key changes and it must not repeat within the lifetime of a session key. It is also necessary to ensure that an attacker cannot accumulate a reasonable full set of responses within a practical time scale through direct polling of the alarm system. In the present embodiment, using a polling frequency of one a second, a 16-bit challenge would be exhausted after 18 hours. By contrast, a 32-bit challenge would be exhausted after 136 years. Accordingly a binary field of 4 octets (32 bits) is used for the challenge.

The CPE generates three types of PollRequest. The alarm poll request has the format shown in Figure 8 and is sent to the CPE to initiate an update on the status of alarm interfaces within the alarm unit. This message is not encrypted or otherwise protected, other that in the poll identification number of "challenge" is a random number.

A second PollRequest type is the telemetry PollRequest (TPoll). This is sent by the data engine to request data from a telemetry application interface within the CPE. The message is not encrypted, but a hash field is provided to protect the integrity of the message, preventing interception and alteration. A random challenge is included, and the message also includes fields for additional information for use with the telemetry application.

A third type of PollRequest is the non-security PollRequest (SPoll). This is sent by the data engine to request data from an application interfaced within the CPE but does not carry sensitive information. For example, this might be used in an application monitoring the status of a vending machine.

Figure 9 shows the basic format of a poll response message. The integrity of the poll response packet is checked to guard against modification. This is done by appending a keyed cryptographic hash of the message to the end of the message. The message body includes the challenge sent in the PollRequest and includes an octet identifying the hash function used. The hash function produces, in this example, a 128-bit output (16 bytes) although a subset of the output may be used to reduce the transmission overhead although there is then some loss of relative security.

When a decommissioned alarm system responds to a PollRequest the status of the alarm system "commissioned or decommissioned" is also signalled in

the response. As this is sensitive information it is embedded in the hash - either in its generation (through using the inverse of the session key) or by selecting a different set of output bytes, should less than 16 bytes be appended to the message. For security it is necessary that the decommissioned alarm system should signal its state to the central site - either by not replying to a PollRequest message, or by using a modified hash.

Figure 10 shows in further detail the format of the alarm PollRequest.

Figure 11 shows the format of the telemetry poll response sent in response to a telemetry poll request message.

Figure 12 shows the format of the non-secure poll response message. This is sent to the data engine from applications at the CPE which do not carry information requiring protection. Unlike the previous poll responses, this type does not require a hash function to protect message security.

Figure 13 shows the format of acknowledgement messages. These are used to cycle the state of the alarm equipment following changes signalled in the data fields of poll response messages. The integrity of these acknowledgement messages is protected by the inclusion of the hash function.

Figure 14 shows the message exchange system which is used for the passing of session keys. The sequence is designed so that an alarm system only accepts such session keys from the central site. Similarly, any command that causes a security-relevant change of state (such as decommissioning) is only accepted if it originates from the central site. The message exchange system is designed to verify the identity of each end of the communications link. In the message sequence shown in the figure, Id is an octet identifying the message type. Challenge X is a random number used as a challenge. IV is an random initialisation vector. The session key is an 8 octet session key to be used for subsequent communications between the alarm system and the central site. Data is up to 15 octets of data which is specific to the alarm unit. [x_k implies encryption of the field x using the encryption key k.]

Figure 15 shows in further detail the initial message sent by the central site to the alarm unit. Cmd is a single octet identifying the command, C-6 are 7 octets of a challenge and IV0.....7 are 8 octets of random data sent in clear. The [CMD] [C0....6] fields are encrypted using the master key and the IV field.

Figure 16 shows the alarm unit challenge returned in response to the command challenge. 'Type' identifies the alarm unit challenge, C0-6 are the 7 octets of response, A0-6 are 7 octets of challenge from the alarm unit and R is a random octet for padding. The 16 octets from 'Type' to R are encrypted as described above using the master key and previous message (16 octets) as an initialisation vector (IV).

Figure 17 shows the central site response. K0-7 are 8 octets of the new session key (or random data if this is not a session key update).

Figure 18 shows the alarm site response. Type is an octet identifying the alarm site final response data are up to 15 octets data specific to the alarm unit. These 16 octets are encrypted using the session key and the previous encrypted message as an initialisation vector.

Figure 6 shows one example of information flows between the CPE, data engine (DE) and ARCi n the case where a new alarm is reported by the alarm detectors connected to the CPE. Message a is a first PollRequest sent from the DE to the CPE. Message b is the response from the CPE to the first poll. At this point there has been no change in status, and so the response simply records the number of alarms in the different respective states. After message b, the alarm message is received by the CPE from the alarm detector. Message c is the first PollRequest sent to the CPE following the alarm. This time the response, message d, includes in addition to the usual status data, data which identifies the identity of the new alarm, the alarm state, and any additional information returned by the alarm equipment in the CPE. In response, the DE returns an alarm acknowledgement, message e. Message f is an alarm report transmitted from DE to ARC, the ARC returns a report acknowledgement message, message g. The DE then transmits message f notifying the CPE that the alarm condition has been acknowledged by the ARC. This changes the status of the alarm to "outstanding". Message i is sent in acknowledgement. Message j is the next of the periodic PollRequests. Message k is the response to the PollRequest returning the status of the alarms at the CPE.

Table 3 below lists the timer and counter values used in the protocol described above.

Figures 19 to 21 document, using the ITU SDL (Specification and Description Language) formalism, software for use in implementing the system described above. Figure 19 shows the main process components in the CPE. These comprise the Alarm Handler Process (AlrmHndlr), the Protocol and Security Process (ProtH) and the Segmentation Handler (SegmH). The last of these is a transport protocol which is generally conventional in nature, and which may be substituted by other transport protocols. In the Figure, interface R9 is an output to a GSM backup link, which may be used to communicate with the central station in the event that the telephone line is cut. Interfaces R3, R4 are connected to the alarm hardware. R10 is the route for the security violation signal. R5,R6 are the normal interactions between the alarm handler and ProtH components, and R7,R8 are the normal interactions between SegmH and ProtH. R1,R2 are the connections to/from the ISDN D channel and R11,R12 are connections to an alternative communications channel, for example to the GSM network.

Figure 20 shows the Alarm Handler Process, and corresponds to the state diagram of Figure 5B. Figure 20a shows the transitions from *start-up*. Figure 20b shows the transitions from *Alarm* to *outstanding*. Figure 20c shows transitions from *outstanding* to *reset-raised*, from *reset-raised* to *reset*, and from *reset* to *normal*. Figure 20 d shows transitions from *alarm-raised* to *alarm*.

Figure 21 shows the Protocol and Security Process and corresponds to the state diagram of Figure 5A. Figure 21A shows the transitions from *idle* to *commissioning*. Figure 21D shows *commissioning* to *active*, 21C *decommissioning* and security changes in the *Active* state, 21D *normal* and *outstanding* messages from the data engine, and acknowledgements, in the *Active* state. Figure 21E shows polling in the Active state, 21F acknowledgement of *Alarms* and *Clears* in the *Active* state, and 21G shows additional features of the transitions of Figure 21C.

TABLE 1

	T 1	T 2	T 3	T 4	T 5
C1 - Polling	√				
C2 - Integrity Check		√			
C3 - Binding to request			√		
C4 - Encryption					√
C5 - Mutual Authentication			√	√	

TABLE 2

```
MD5(...)
{
   static int ip;
   .....
   for( round=1; round<5; ++round)
   {
      ....
      if( round == 3 )
         for( x=0; x<13; ++x )
         {
            rand[ip] = MD5buffer[x];
            ip = (ip+1) & 511;
         }
      ....
   }
}
```

TABLE 3

Timer or Counter	Value	Description
N701	1	Number of Transfer Segment Re-transmissions
N721	154	Maximum Message Size
T720	30 secs	Security Time Interval for Challenge Responses
T_{721}	6 secs	Time interval for CPE retransmissions

CLAIMS

1. A method of operating a communications system including a telecommunications link between a remote terminal and a control station, the method comprising:

a) transmitting polling requests on a digital messaging channel carried on the telecommunications link;

b) generating at the remote station a poll response message and encrypting part only of the said poll response message;

c) returning a response signal from the remote terminal to the control station on the digital messaging channel; and

d) at the control station decrypting the poll response message.

2. A method according to claim 1, in which the digital messaging channel is the D channel of an ISDN circuit.

3. A method according to claim 1 or 2, in which the remote terminal is a security alarm and in which the poll response includes data indicating the alarm status.

4. A method according to any one of the preceding claims. in which the remote terminal transmits the poll response in a plurality of segments and in which the central station returns to the remote station an acknowledgement of each message received and a further acknowledgement for a message assembled from the segments.

5. A method according to any one of the preceding claims, in which the telecommunications link includes a local access network which links the remote station to a local exchange.

6. A method according to any one of the preceding claims, in which each polling request from the central station includes a different identifying code, and the encrypted part of the poll response includes the identifying code of the respective poll request.

7. A method according to any one of the preceding claims, in which some of the polling requests are transmitted over a wireless communications link.

8. A communications system comprising:

a) a control station including

a polling request generator; and

a decoder for decoding poll response messages;

b) a remote terminal including

a polling response generator for generating a polling response message;

an encoder arranged to encode part only of the polling response message; and

c) a telecommunications circuit including

a digital messaging channel which, in use, carries polling requests from the control station to the remote terminal and carries partially encoded response messages from remote terminal to the control station.

9. A system according to claim 8, in which the telecommunications circuit is an ISDN circuit, and the messaging channel is carried in the D channel of the ISDN circuit.

10. A control station for use in a method according to any one of claims 1 to 7, the control station comprising:

a) a digital messaging channel interface which is arranged to transmit and receive messages to and from a remote station on a digital messaging channel;

b) a polling request generator which is arranged to generate a polling request for transmission on the digital messaging channel;

c) a decoder arranged to decode a partially encrypted poll response message which is received on the digital messaging channel; and

d) a controller which is arranged to interpret the poll response messages.

11. A remote terminal for use in a method according to any one of claims 1 to 7 and including:

a) a polling response generator for generating a polling response message;

b) an encoder connected to the polling response generator and arranged to encode part only of the polling response message; and

c) a digital signalling interface for connection to a digital messaging channel and arranged to output a partially encoded poll response message generated by the polling response generator and the encoder .

Fig.1A.

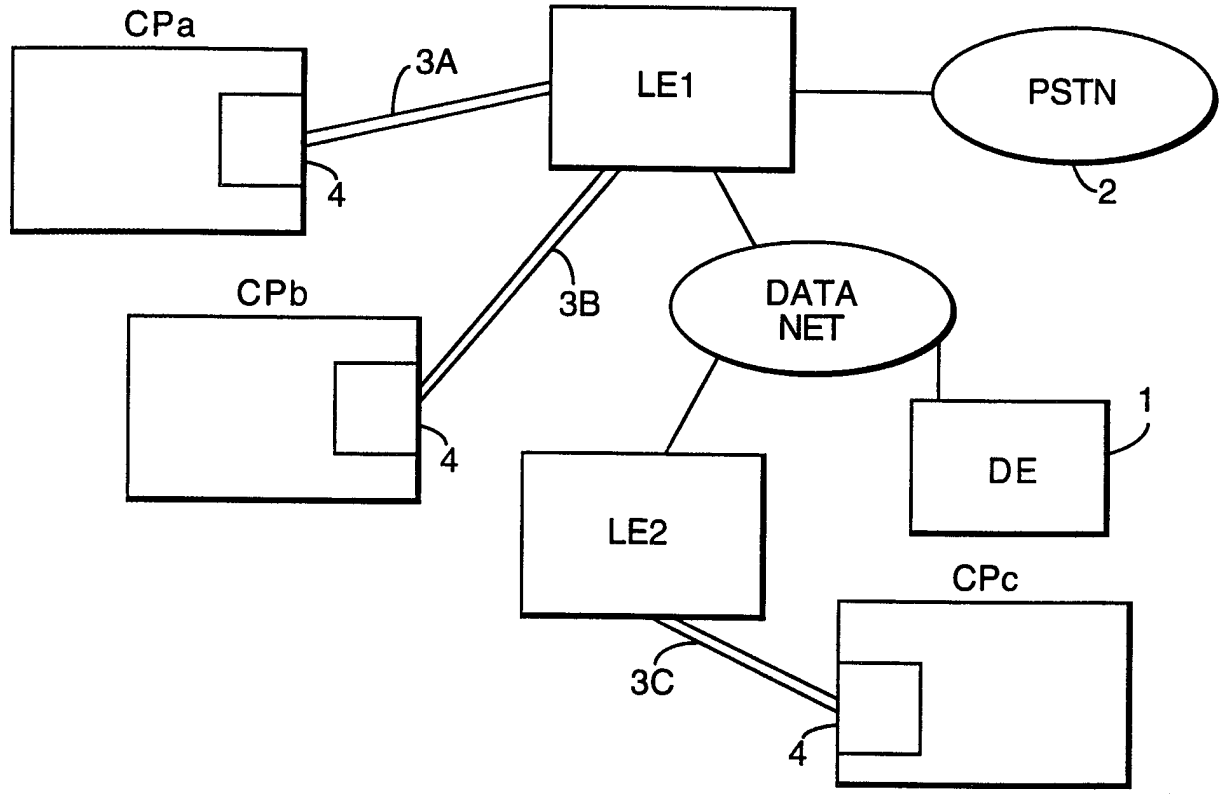
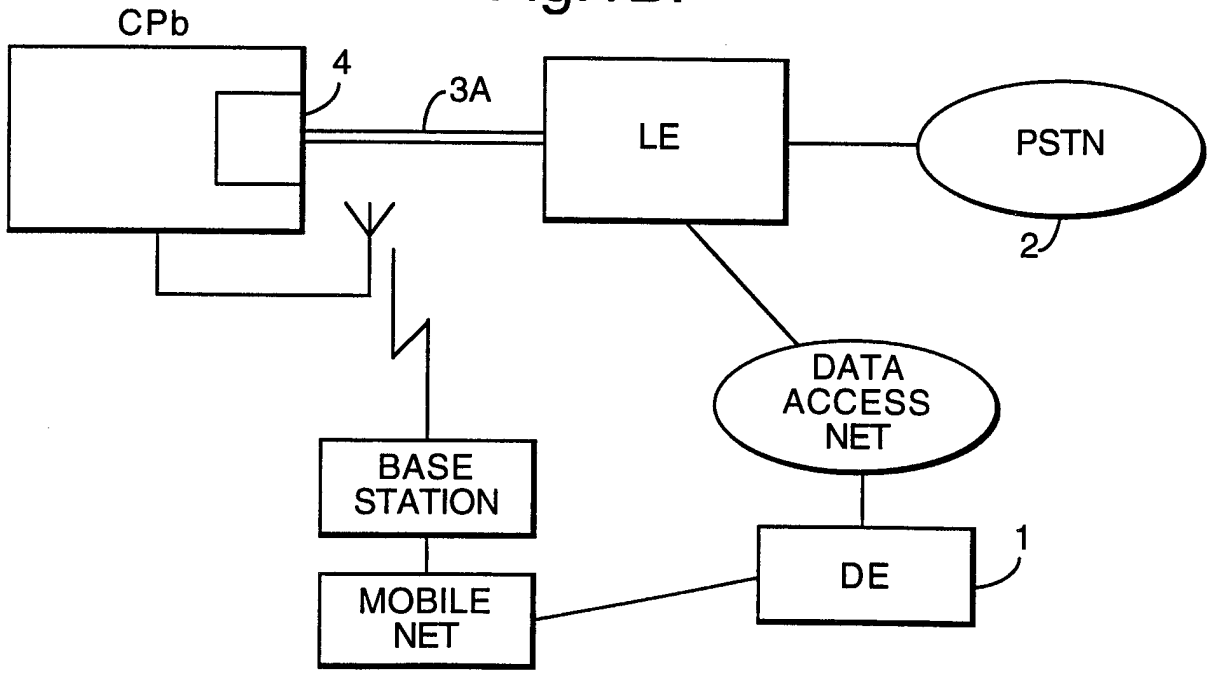

CPa
3A
LE1
PSTN
4
2
CPb
3B
DATA NET
4
1
DE
LE2
CPc
3C
4

Fig.1B.


CPb
4
3A
LE
PSTN
2
DATA ACCESS NET
BASE STATION
1
DE
MOBILE NET

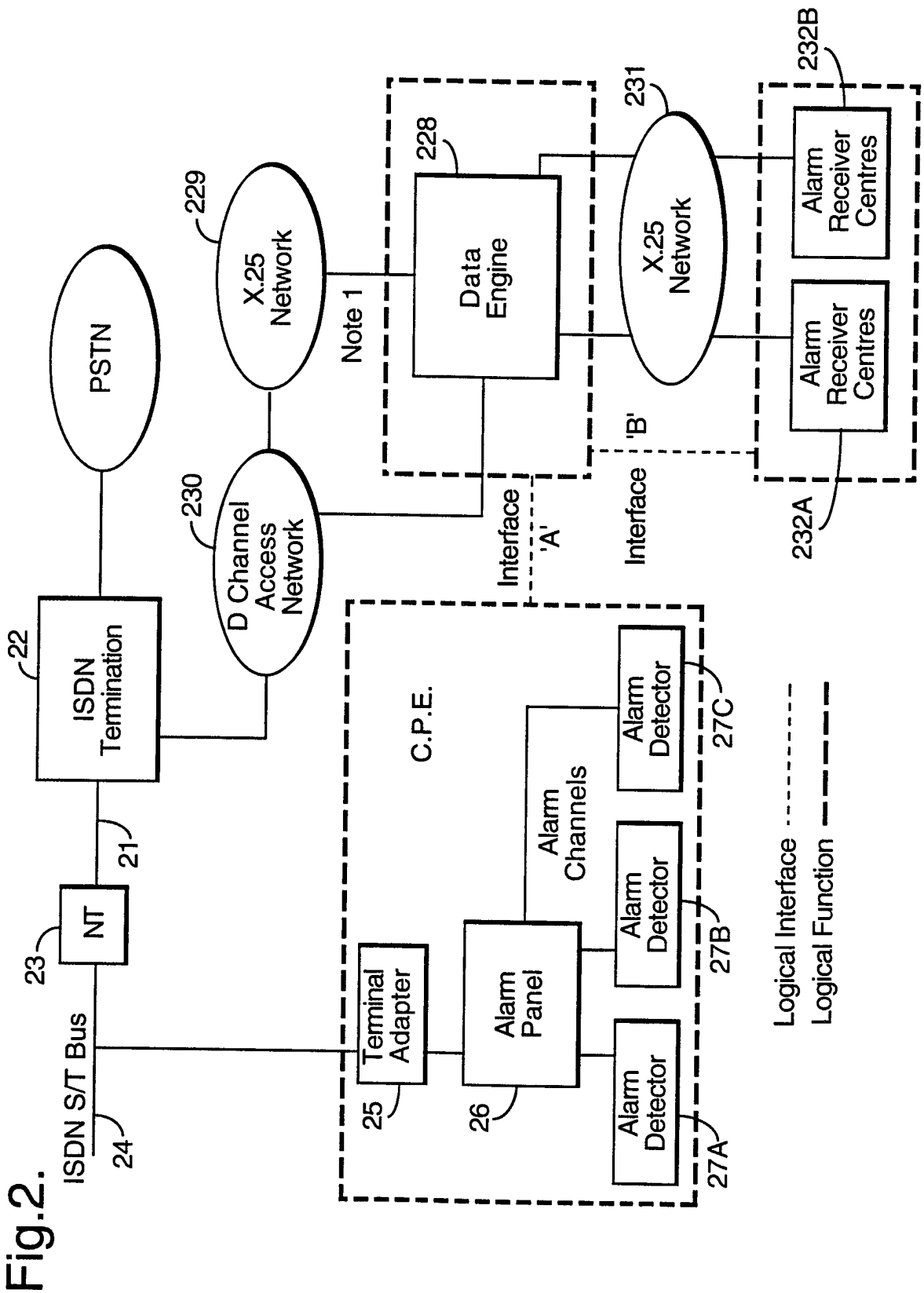
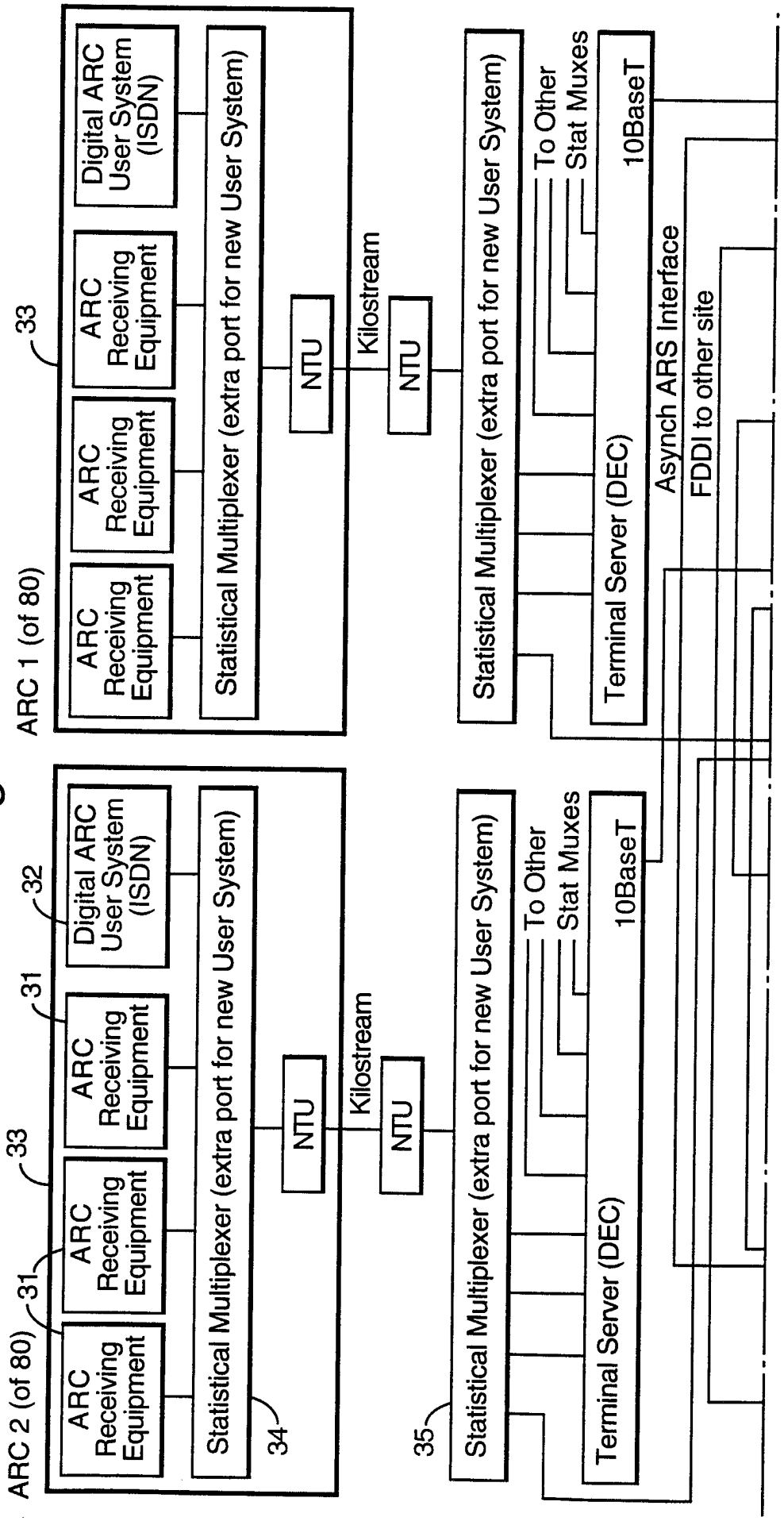

PSTN
X.25 Network
229
Note 1
Data Engine
228
X.25 Network
231
Alarm Receiver Centres
232B
Alarm Receiver Centres
232A
D Channel Access Network
230
Interface 'A'
Interface 'B'
ISDN Termination
22
C.P.E.
Alarm Channels
Alarm Detector
27C
Alarm Detector
27B
Alarm Detector
27A
Terminal Adapter
25
Alarm Panel
26
NT
23
21
ISDN S/T Bus
24
Logical Interface
Logical Function

Fig.2.

Fig.3.


ARC 1 (of 80)
33
ARC Receiving Equipment
ARC Receiving Equipment
ARC Receiving Equipment
Digital ARC User System (ISDN)
Statistical Multiplexer (extra port for new User System)
NTU
Kilostream
NTU
Statistical Multiplexer (extra port for new User System)
To Other Stat Muxes
Terminal Server (DEC)
10BaseT
Asynch ARS Interface
FDDI to other site
ARC 2 (of 80)
31
33
ARC Receiving Equipment
ARC Receiving Equipment
Digital ARC User System (ISDN)
32
31
Statistical Multiplexer (extra port for new User System)
34
NTU
Kilostream
NTU
35
Statistical Multiplexer (extra port for new User System)
To Other Stat Muxes
Terminal Server (DEC)
10BaseT

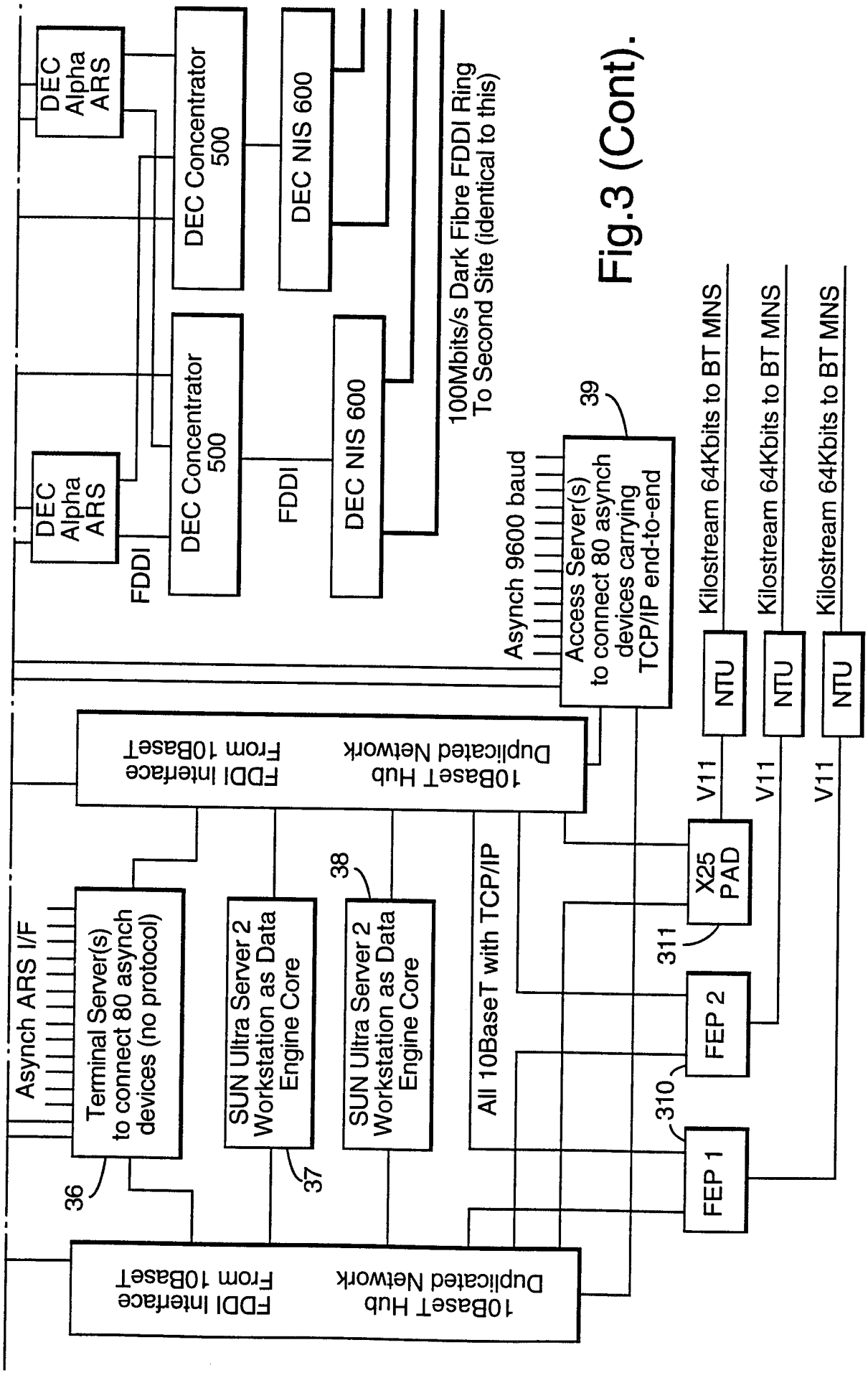

DEC Alpha ARS
DEC Concentrator 500
DEC NIS 600
100Mbits/s Dark Fibre FDDI Ring To Second Site (identical to this)
DEC Alpha ARS
FDDI
DEC Concentrator 500
FDDI
DEC NIS 600
Asynch 9600 baud
39
Access Server(s) to connect 80 asynch devices carrying TCP/IP end-to-end
Kilostream 64Kbits to BT MNS
Kilostream 64Kbits to BT MNS
Kilostream 64Kbits to BT MNS
NTU
NTU
NTU
V11
V11
V11
10BaseT Hub Duplicated Network
FDDI Interface From 10BaseT
X25 PAD
311
FEP 2
310
FEP 1
All 10BaseT with TCP/IP
38
SUN Ultra Server 2 Workstation as Data Engine Core
SUN Ultra Server 2 Workstation as Data Engine Core
37
Asynch ARS I/F
Terminal Server(s) to connect 80 asynch devices (no protocol)
36
10BaseT Hub Duplicated Network
FDDI Interface From 10BaseT

Fig.3 (Cont).

Fig.4A.

Application Layer	Alarms Protocol
Network Layer	X.25 Layer 3
Link Layer	X.25 Layer 2
Physical Layer	ISDN 'D' Channel

Fig.4B.

Application Layer	Alarms Protocol
Link Layer	X.25 Layer 2
Physical Layer	ISDN 'D' Channel

Fig.5A.

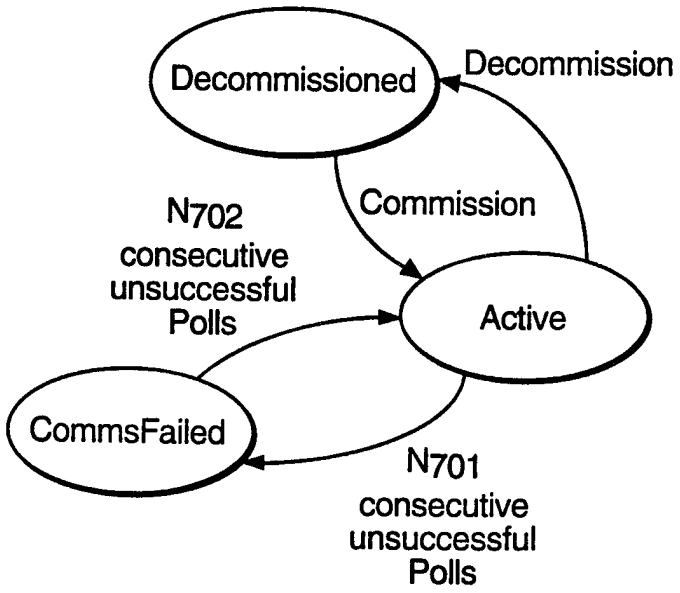


Fig.5B.

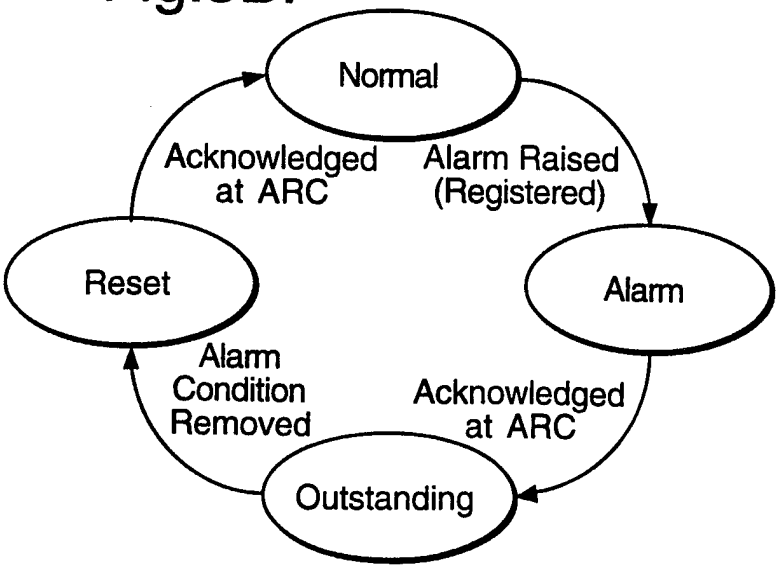
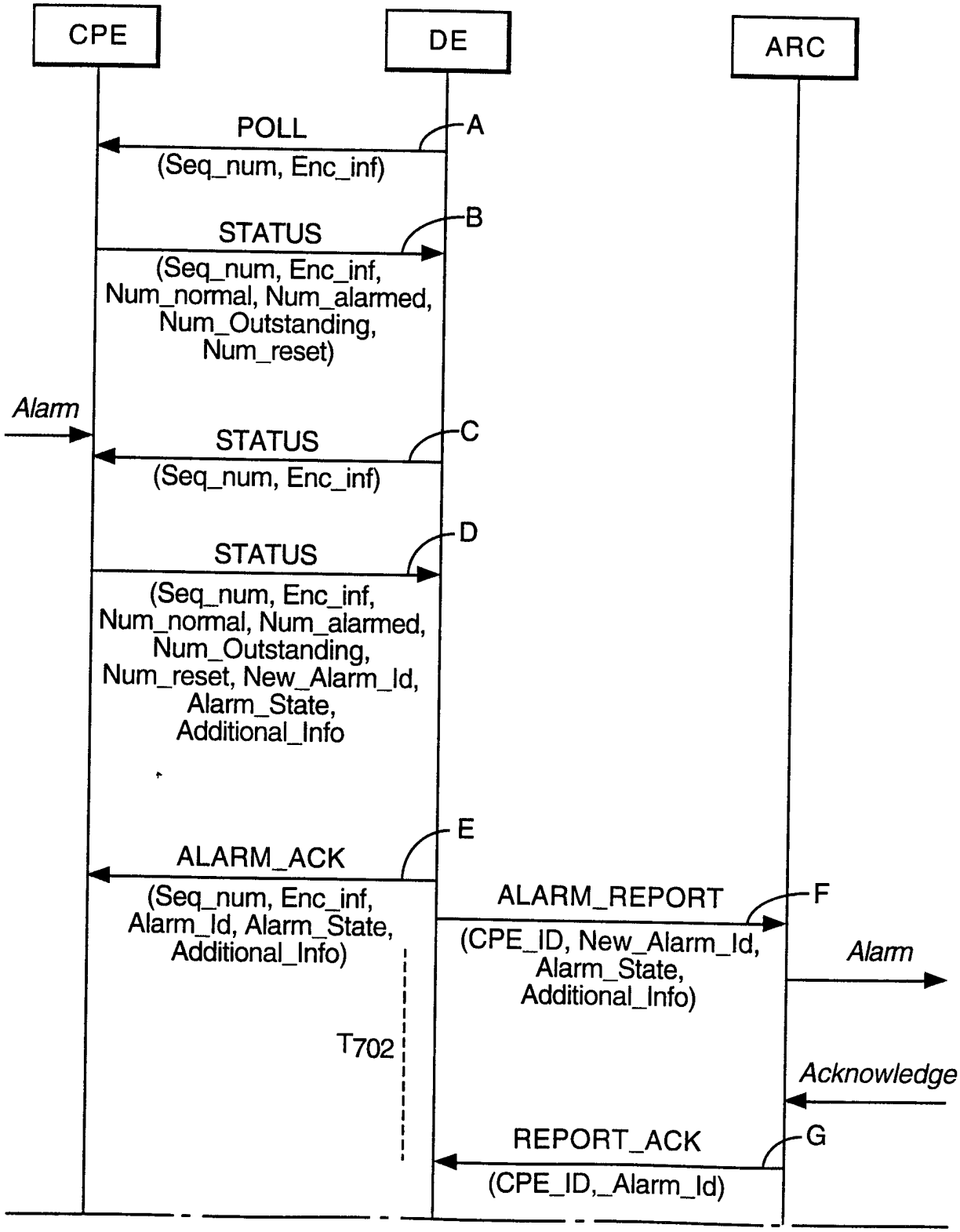


Fig.6.


CPE
DE
ARC
POLL
(Seq_num, Enc_inf)
A
STATUS
(Seq_num, Enc_inf, Num_normal, Num_alarmed, Num_Outstanding, Num_reset)
B
Alarm
STATUS
(Seq_num, Enc_inf)
C
STATUS
(Seq_num, Enc_inf, Num_normal, Num_alarmed, Num_Outstanding, Num_reset, New_Alarm_Id, Alarm_State, Additional_Info
D
ALARM_ACK
(Seq_num, Enc_inf, Alarm_Id, Alarm_State, Additional_Info)
E
ALARM_REPORT
(CPE_ID, New_Alarm_Id, Alarm_State, Additional_Info)
F
Alarm
T702
Acknowledge
REPORT_ACK
(CPE_ID,_Alarm_Id)
G

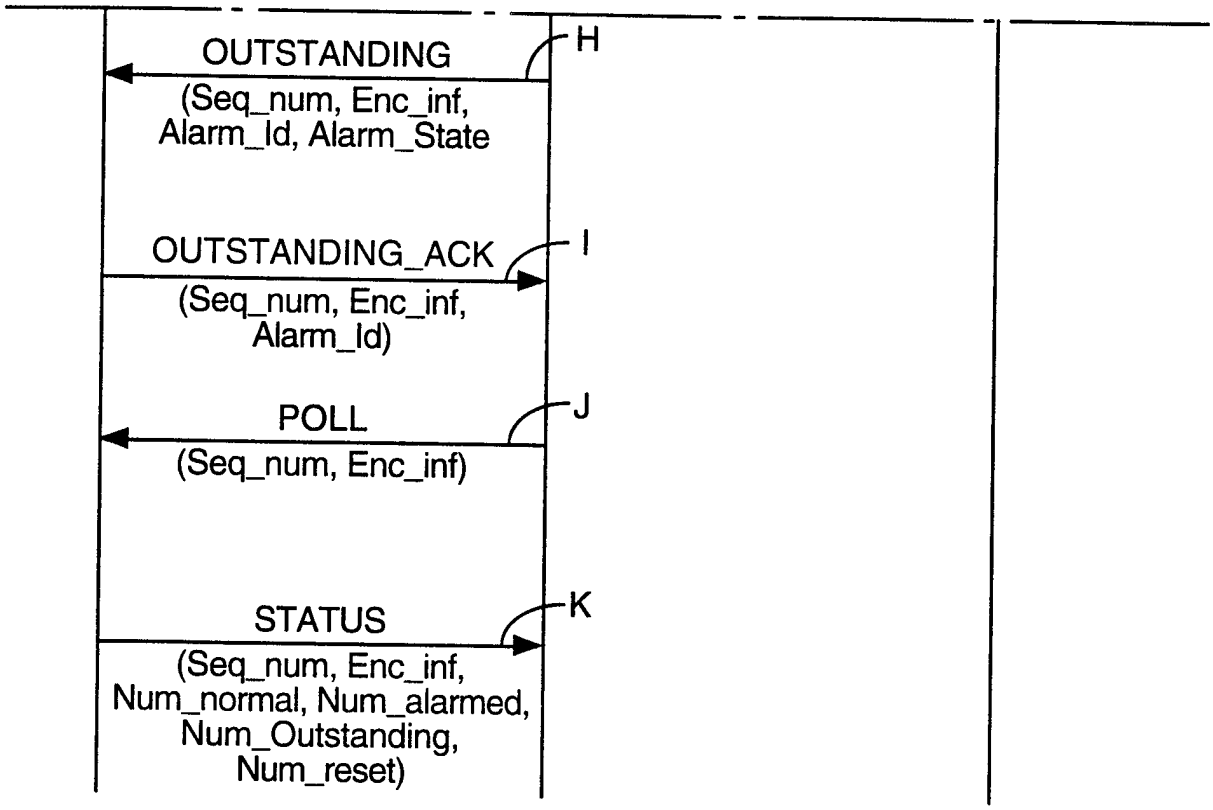

OUTSTANDING
H
(Seq_num, Enc_inf,
Alarm_Id, Alarm_State
OUTSTANDING_ACK
I
(Seq_num, Enc_inf,
Alarm_Id)
POLL
J
(Seq_num, Enc_inf)
STATUS
K
(Seq_num, Enc_inf,
Num_normal, Num_alarmed,
Num_Outstanding,
Num_reset)

Fig.6 (Cont).

Fig.7.

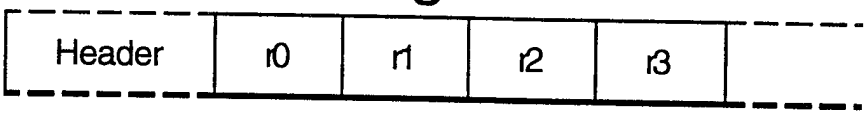


Fig.8.

	MSB							LSB
	Protocol Message Type (Poll Response)							
	0	0	0	0	0	0	1	0
2	CPE Identification Number *(Binary Random Number, 4 octets long)*							
	b	b	b	b	b	b	b	b
3	b	b	b	b	b	b	b	b
4	b	b	b	b	b	b	b	b
5	b	b	b	b	b	b	b	b

Fig.9.

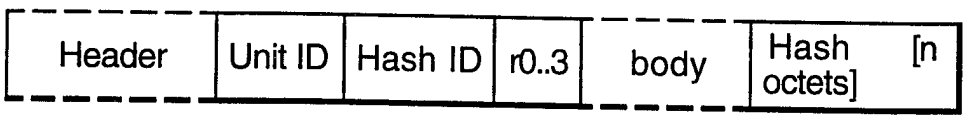


Fig.10.

	MSB							LSB
	Protocol Message Type (Poll Response)							
1	0	0	0	0	0	0	1	1
2	CPE Identification Number *(Binary Number, 4 octets long)*							
	b	b	b	b	b	b	b	b
3	b	b	b	b	b	b	b	b
4	b	b	b	b	b	b	b	b
5	b	b	b	b	b	b	b	b
6	Hash Identification (one Octet)							
	b	b	b	b	b	b	b	b
7	Poll Identification Number *(Binary Random Number, 4 octets long)*							
	b	b	b	b	b	b	b	b
8	b	b	b	b	b	b	b	b
9	b	b	b	b	b	b	b	b
10	b	b	b	b	b	b	b	b
11	N_NORMAL field, 2 Octets (binary number, 0 to 1023 inclusive)							
	b	b	b	b	b	b	b	b (lsb)
	Null						N_NORMAL	
12	0	0	0	0	0	0	b (msb)	b
13	N_ALARM field, 2 Octets (binary number, 0 to 1023 inclusive)							
	b	b	b	b	b	b	b	b (lsb)
	Null						N_ALARM	
14	0	0	0	0	0	0	b (msb)	b
15	N_OUTSTAND field, 2 Octets (binary number, 0 to 1023 inclusive)							
	b	b	b	b	b	b	b	b (lsb)
	Null						N_OUTSTAND	
16	0	0	0	0	0	0	b (msb)	b
17	N_RESET field, 2 Octets (binary number, 0 to 1023 inclusive)							
	b	b	b	b	b	b	b	b (lsb)
	Null						N_RESET	
18	0	0	0	0	0	0	b (msb)	b

Fig.10 (Cont).

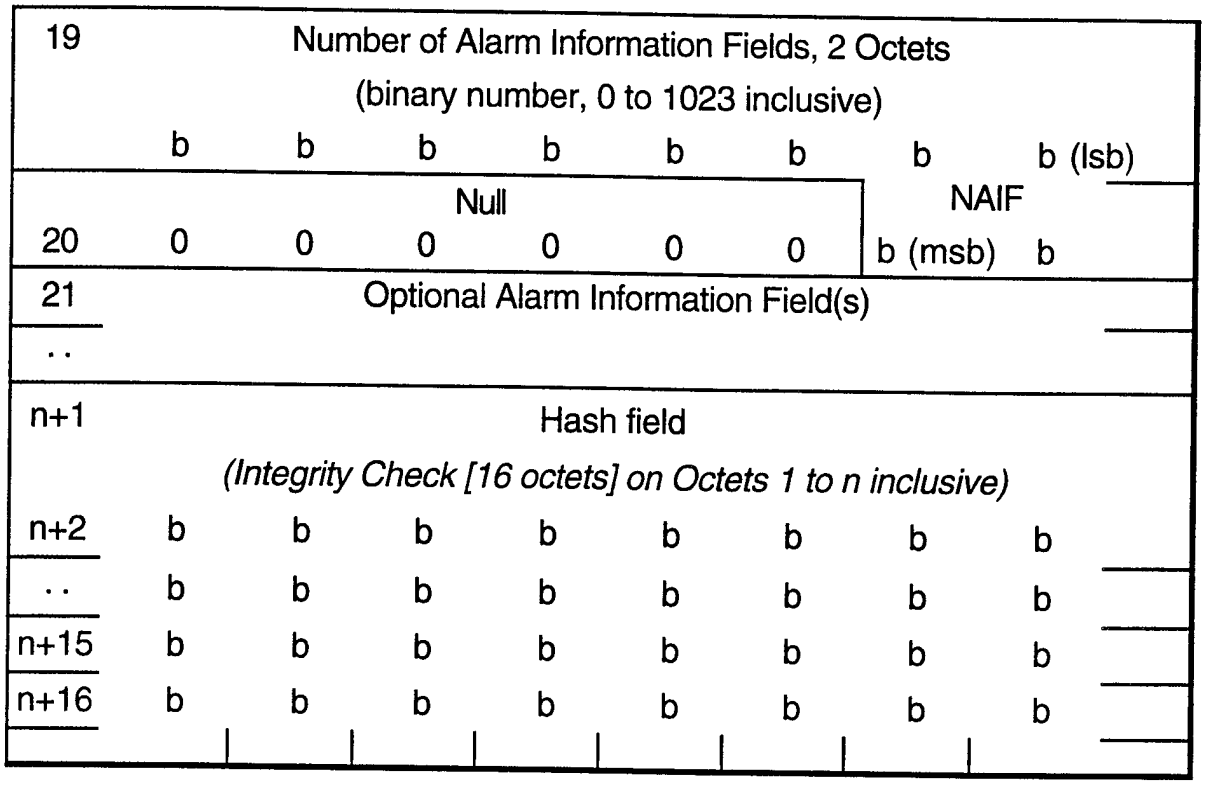

19
Number of Alarm Information Fields, 2 Octets
(binary number, 0 to 1023 inclusive)
b b b b b b b b (lsb)
Null
NAIF
20 0 0 0 0 0 0 b (msb) b
21
Optional Alarm Information Field(s)
..
n+1
Hash field
(Integrity Check [16 octets] on Octets 1 to n inclusive)
n+2 b b b b b b b b
.. b b b b b b b b
n+15 b b b b b b b b
n+16 b b b b b b b b

Fig.11.

	MSB							LSB
	Protocol Message Type (Telemetry Poll Request)							
	0	0	0	0	0	1	0	0
2	CPE Identification Number *(Binary Number, 4 octets long)*							
	b	b	b	b	b	b	b	b
3	b	b	b	b	b	b	b	b
4	b	b	b	b	b	b	b	b
5	b	b	b	b	b	b	b	b
6	Poll Identification Number *(Binary Random Number, 4 octets long)*							
	b	b	b	b	b	b	b	b
7	b	b	b	b	b	b	b	b
8	b	b	b	b	b	b	b	b
9	b	b	b	b	b	b	b	b
10	Hash Identification (one Octet)							
	b	b	b	b	b	b	b	b
	Length of Addition Information (binary value, range 1 to 127 including this Octet)							
11	0	b	b	b	b	b	b	b
	Additional Information *(Optional, maximum of 126 octets)*							
12	i	i	i	i	i	i	i	i
..	i	i	i	i	i	i	i	i
137	i	i	i	i	i	i	i	i
138	i	i	i	i	i	i	i	i
n+1	Hash field *(Integrity Check [16 octets] on Octets 1 to n inclusive)*							
n+2	b	b	b	b	b	b	b	b
..	b	b	b	b	b	b	b	b
n+15	b	b	b	b	b	b	b	b
n+16	b	b	b	b	b	b	b	b

Fig.12.

	MSB							LSB
Protocol Message Type (Non-Secure Poll Response)								
1	0	0	0	0	0	1	1	1
2	Poll Identification Number *(Binary Random Number, 2 octets long)*							
	b	b	b	b	b	b	b	b
3	b	b	b	b	b	b	b	b
Length of Addition Information (binary value, range 1 to 127 including this Octet)								
4	0	b	b	b	b	b	b	b
Additional Information *(Optional, maximum of 126 octets)*								
5	i	i	i	i	i	i	i	i
..	i	i	i	i	i	i	i	i
130	i	i	i	i	i	i	i	i
131	i	i	i	i	i	i	i	i

Fig.13.

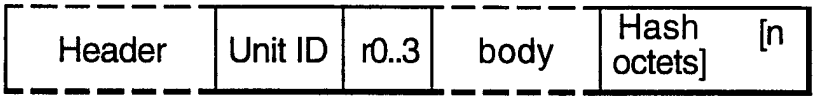


Fig.14.

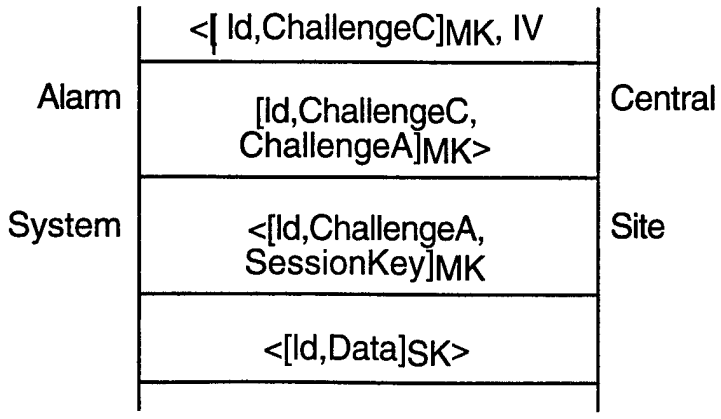


Fig.15.

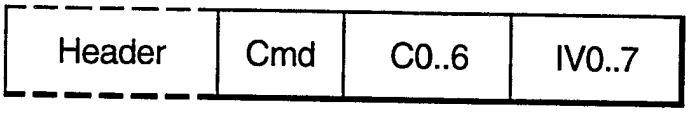


Fig.16.

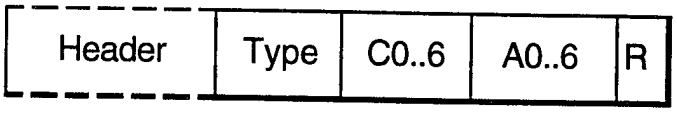


Fig.17.

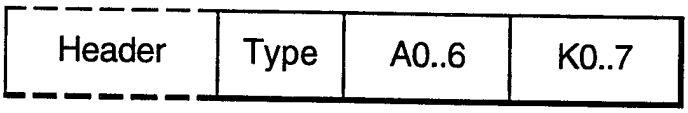


Fig.18.

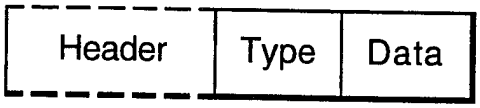


Fig.19.

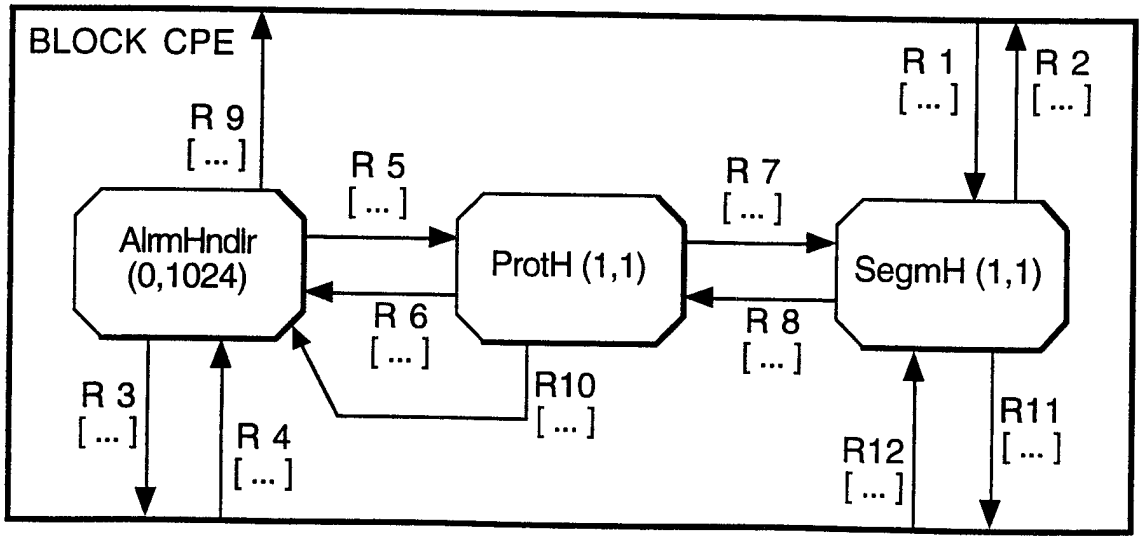


Fig.20A.

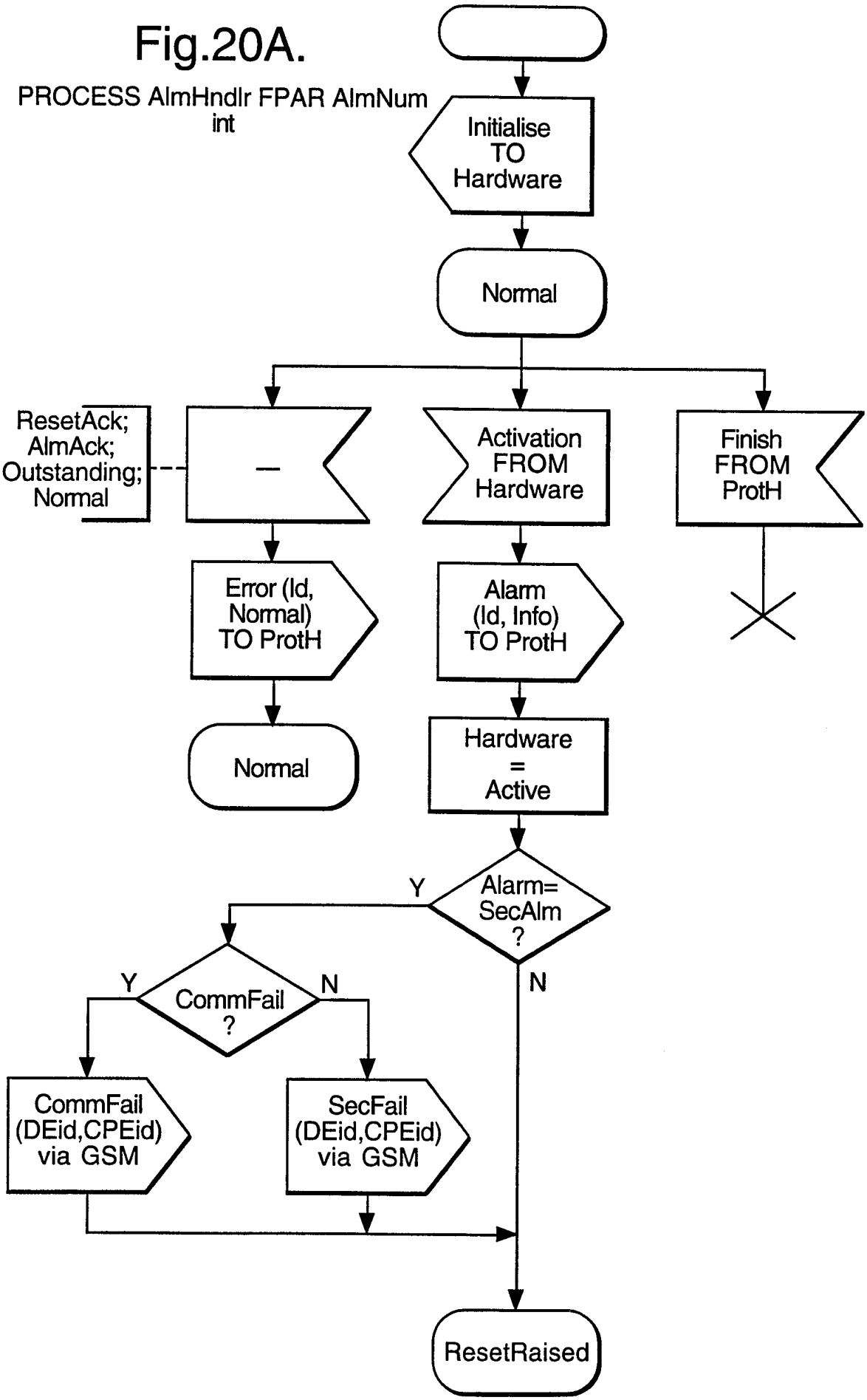

PROCESS AlmHndlr FPAR AlmNum int
Initialise TO Hardware
Normal
ResetAck; AlmAck; Outstanding; Normal
—
Activation FROM Hardware
Finish FROM ProtH
Error (Id, Normal) TO ProtH
Alarm (Id, Info) TO ProtH
Normal
Hardware = Active
Y
Alarm= SecAlm ?
N
Y
CommFail ?
N
CommFail (DEid,CPEid) via GSM
SecFail (DEid,CPEid) via GSM
ResetRaised

Fig.20B.

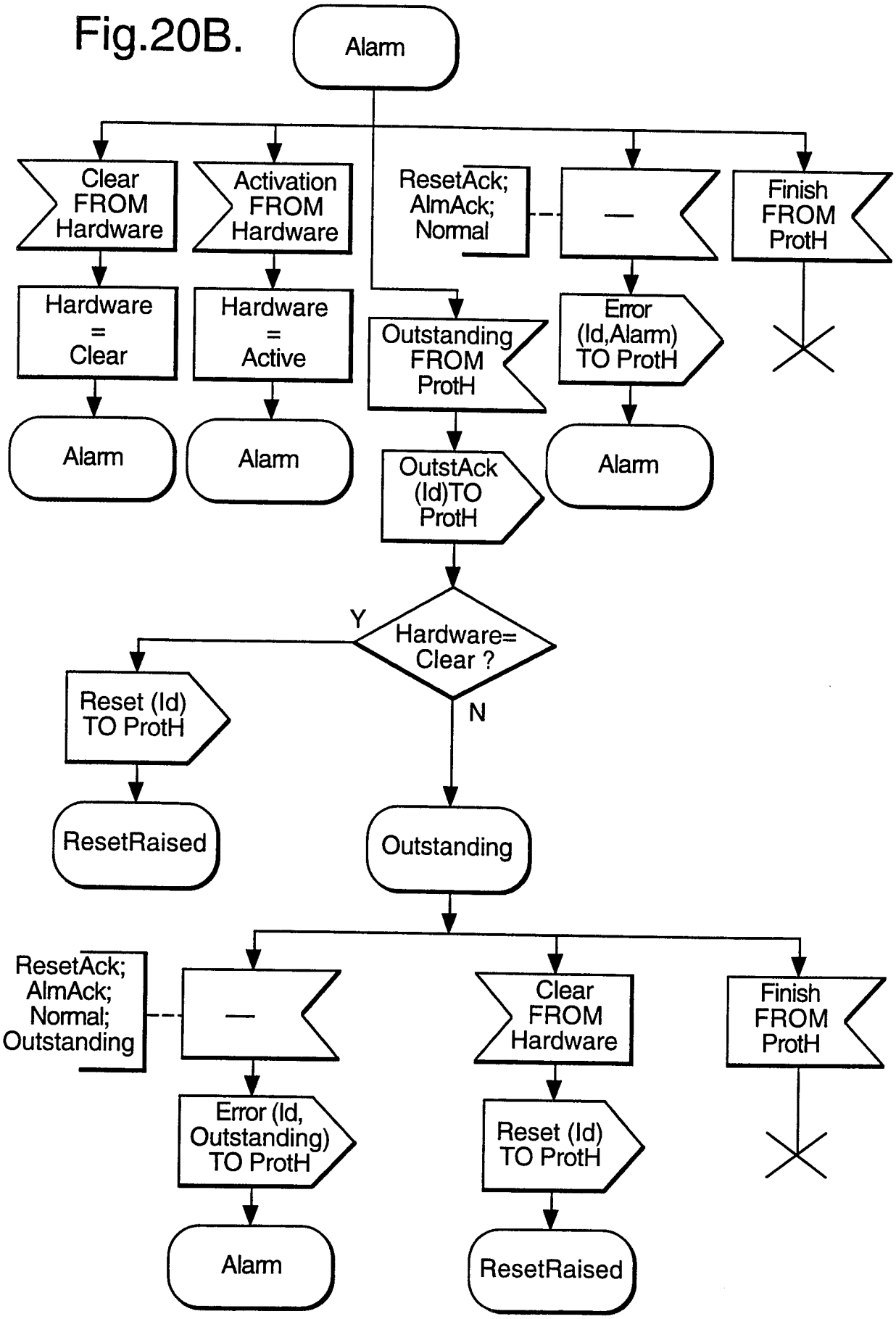

Alarm
Clear FROM Hardware
Activation FROM Hardware
ResetAck; AlmAck; Normal
—
Finish FROM ProtH
Hardware = Clear
Hardware = Active
Outstanding FROM ProtH
Error (Id,Alarm) TO ProtH
Alarm
Alarm
Alarm
Alarm
OutstAck (Id)TO ProtH
Y
Hardware= Clear ?
N
Reset (Id) TO ProtH
ResetRaised
Outstanding
ResetAck; AlmAck; Normal; Outstanding
—
Clear FROM Hardware
Finish FROM ProtH
Error (Id, Outstanding) TO ProtH
Reset (Id) TO ProtH
Alarm
ResetRaised

Fig.20C.

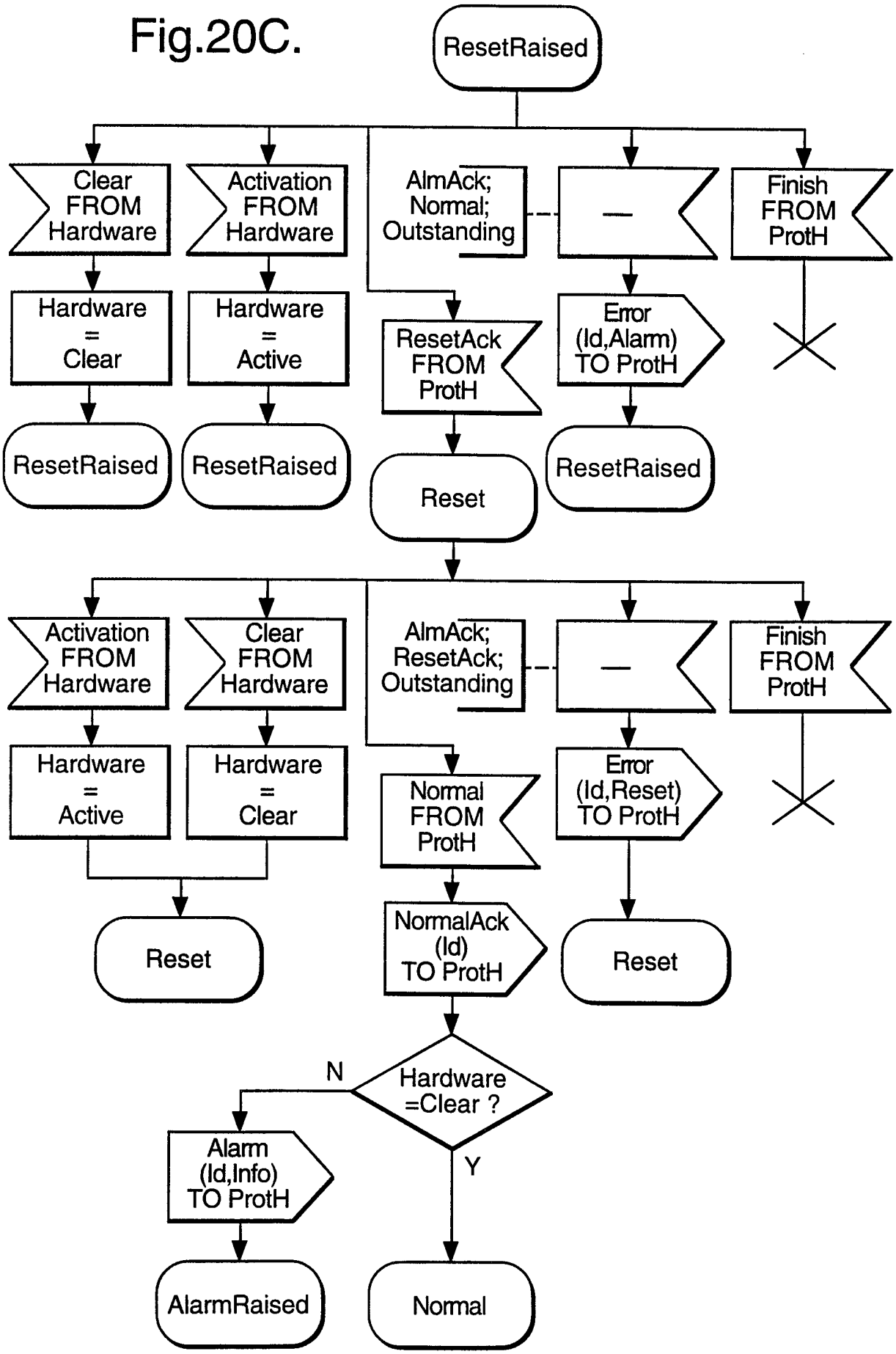

ResetRaised
Clear FROM Hardware
Activation FROM Hardware
AlmAck; Normal; Outstanding
—
Finish FROM ProtH
Hardware = Clear
Hardware = Active
ResetAck FROM ProtH
Error (Id,Alarm) TO ProtH
ResetRaised
ResetRaised
Reset
ResetRaised
Activation FROM Hardware
Clear FROM Hardware
AlmAck; ResetAck; Outstanding
—
Finish FROM ProtH
Hardware = Active
Hardware = Clear
Normal FROM ProtH
Error (Id,Reset) TO ProtH
Reset
NormalAck (Id) TO ProtH
Reset
N
Hardware =Clear ?
Y
Alarm (Id,Info) TO ProtH
AlarmRaised
Normal

Fig.20D.

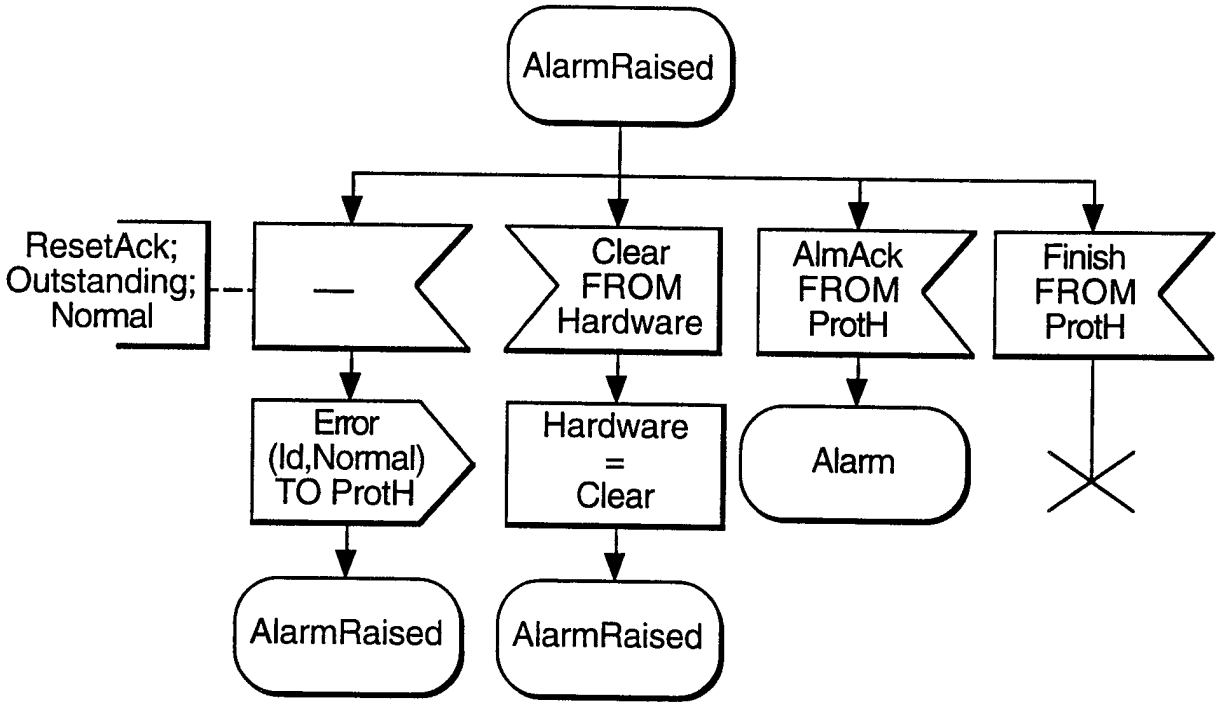

AlarmRaised
ResetAck;
Outstanding;
Normal
—
Clear
FROM
Hardware
AlmAck
FROM
ProtH
Finish
FROM
ProtH
Error
(Id,Normal)
TO ProtH
Hardware
=
Clear
Alarm
AlarmRaised
AlarmRaised

Fig.21A.

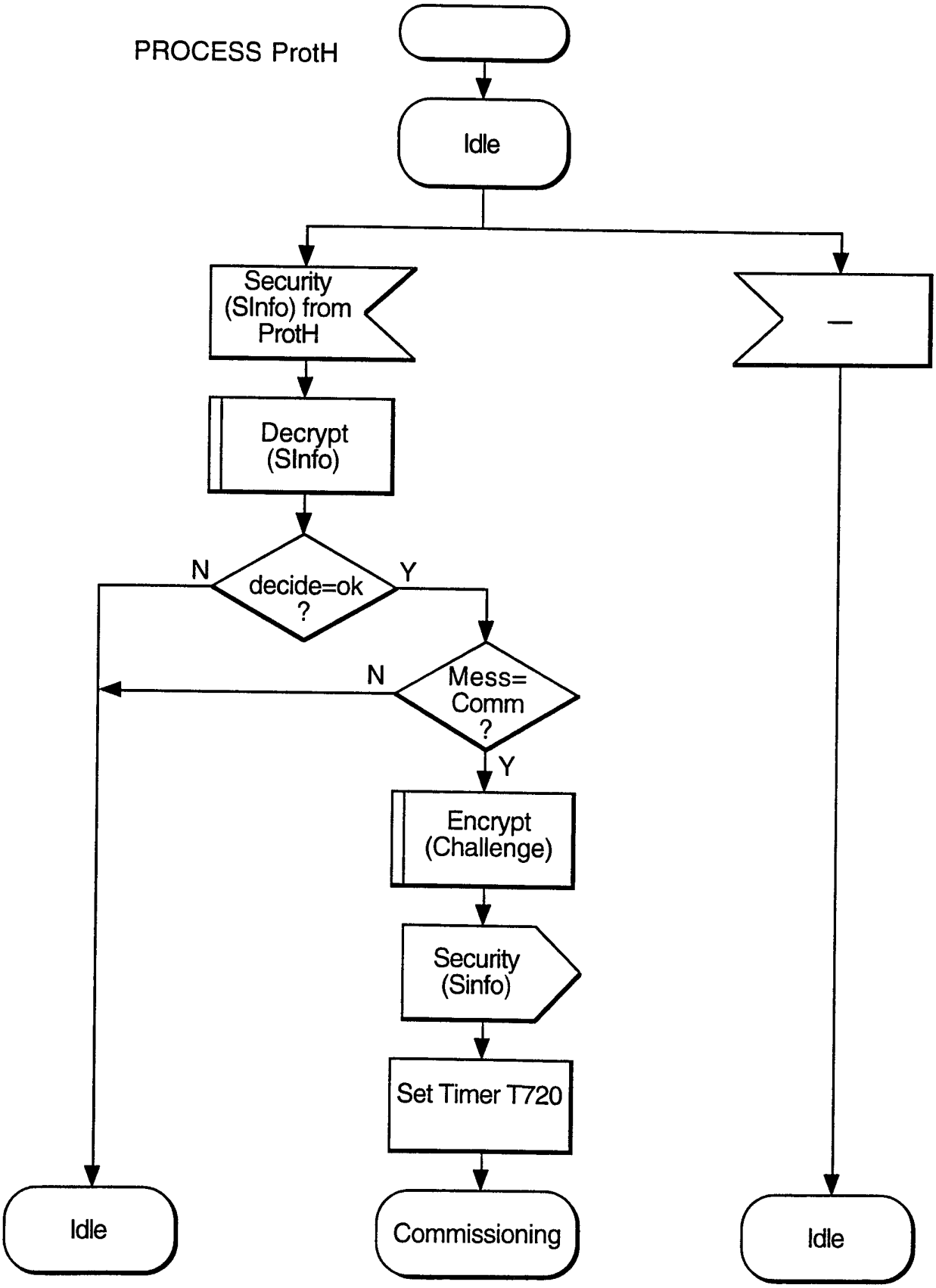

PROCESS ProtH
Idle
Security (SInfo) from ProtH
—
Decrypt (SInfo)
N
decide=ok ?
Y
N
Mess= Comm ?
Y
Encrypt (Challenge)
Security (Sinfo)
Set Timer T720
Idle
Commissioning
Idle

Fig.21B.

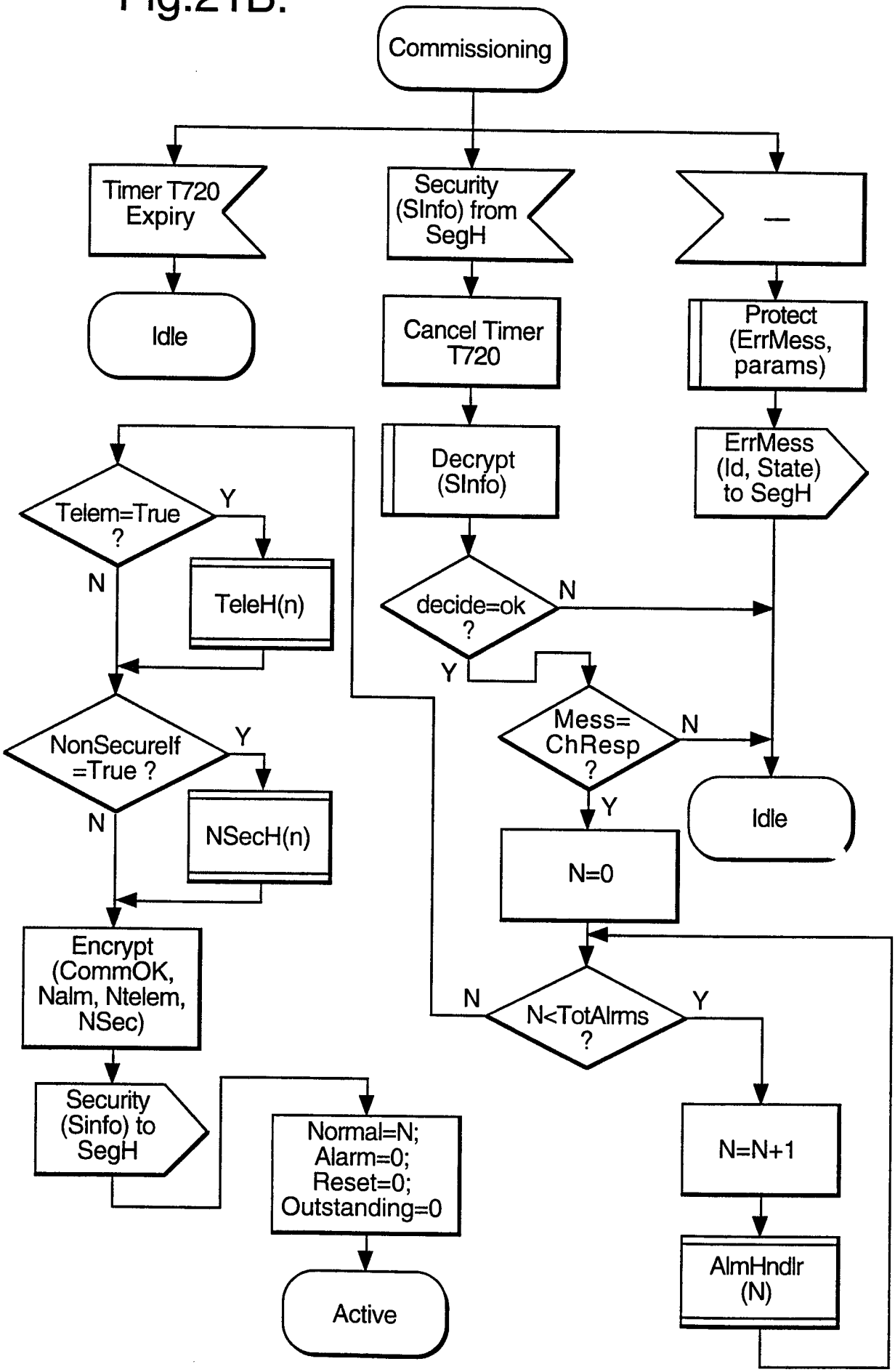

Commissioning
Timer T720 Expiry
Security (SInfo) from SegH
—
Idle
Cancel Timer T720
Protect (ErrMess, params)
Decrypt (SInfo)
ErrMess (Id, State) to SegH
Telem=True ?
Y
N
TeleH(n)
decide=ok ?
N
Y
Mess= ChResp ?
N
Y
Idle
NonSecureIf =True ?
Y
N
NSecH(n)
N=0
Encrypt (CommOK, Nalm, Ntelem, NSec)
N
N<TotAlrms ?
Y
Security (Sinfo) to SegH
Normal=N; Alarm=0; Reset=0; Outstanding=0
N=N+1
AlmHndlr (N)
Active

Fig.21C.

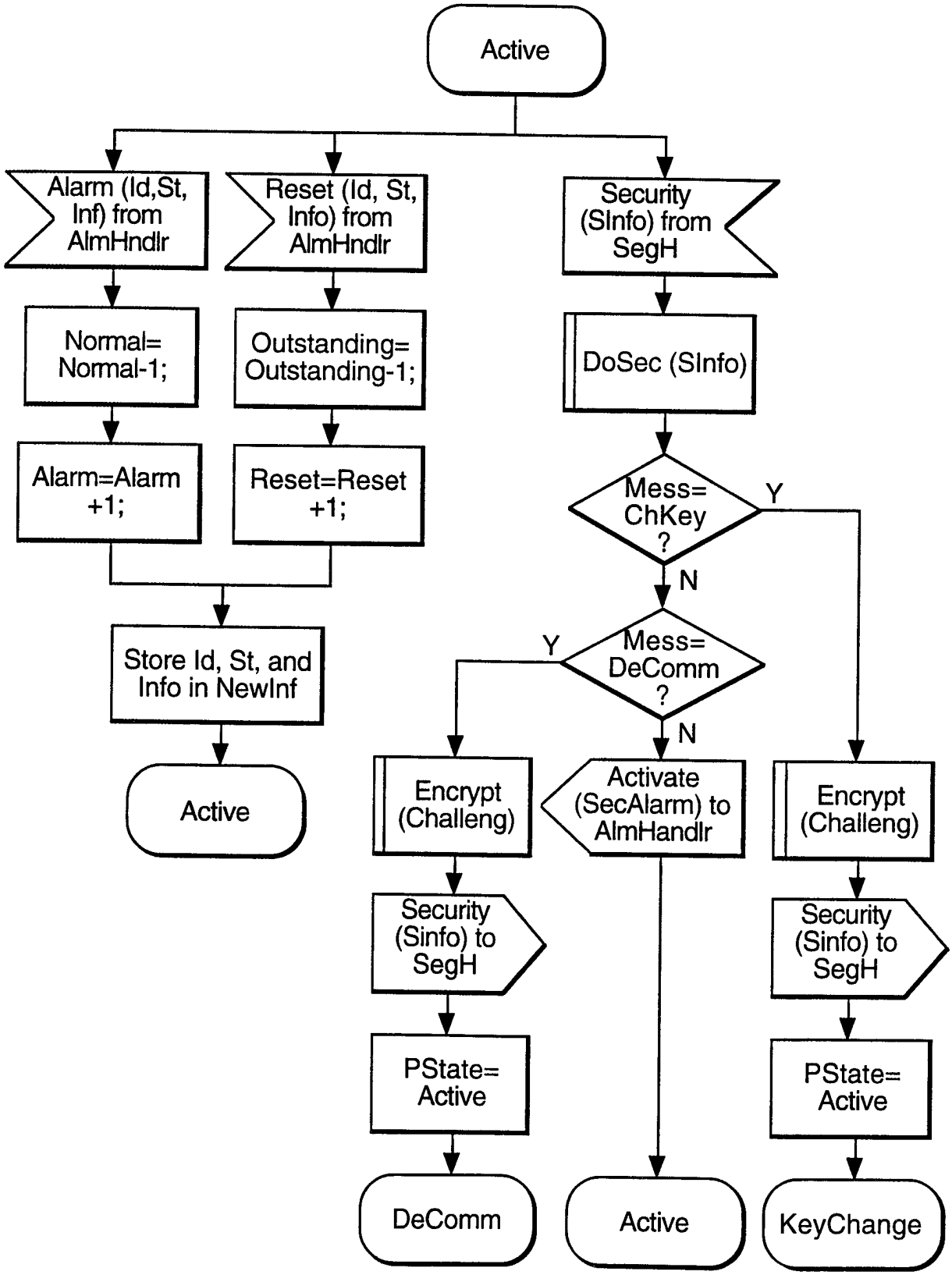
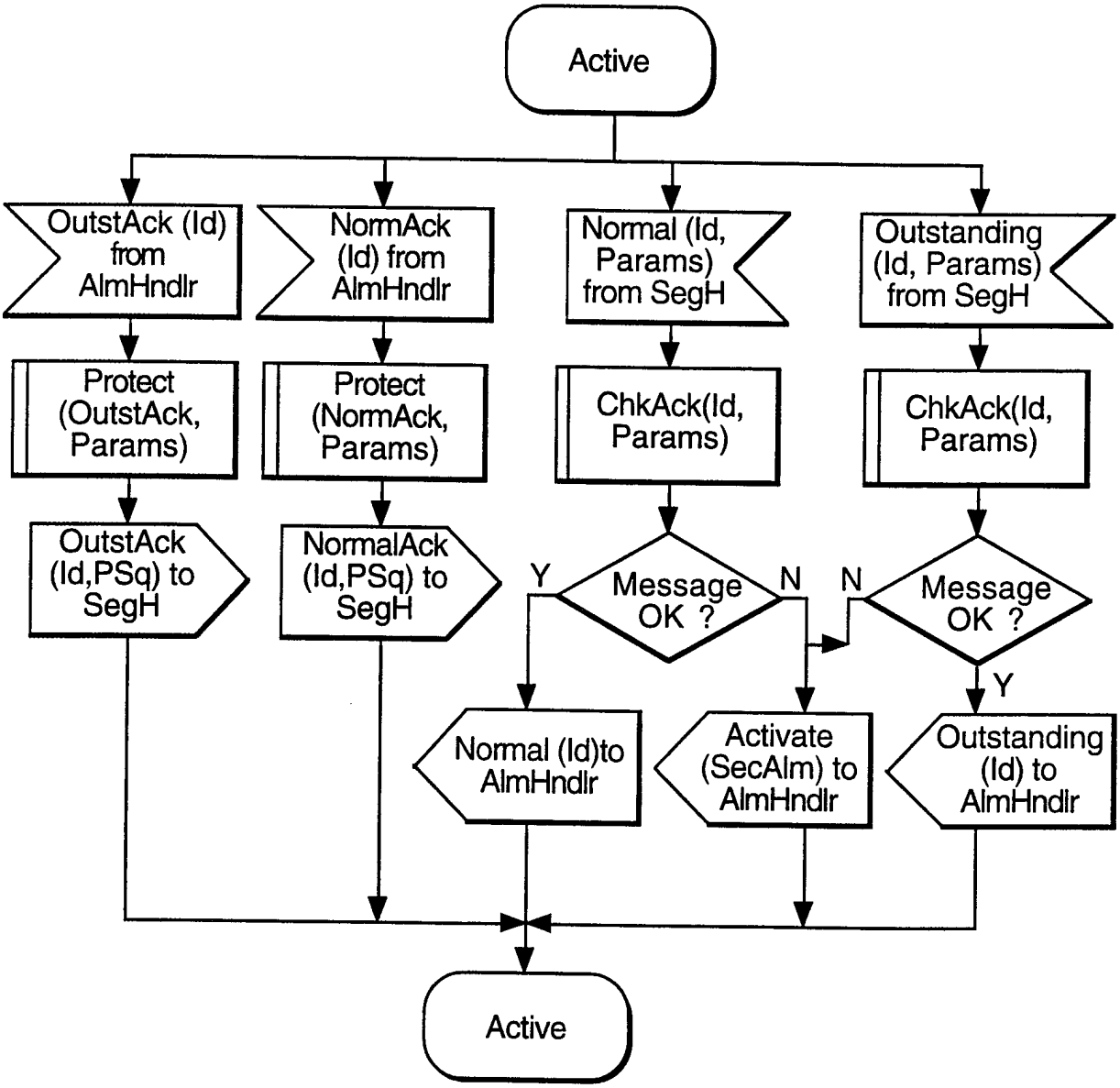

Active
Alarm (Id,St, Inf) from AlmHndlr
Reset (Id, St, Info) from AlmHndlr
Security (SInfo) from SegH
Normal= Normal-1;
Outstanding= Outstanding-1;
DoSec (SInfo)
Alarm=Alarm +1;
Reset=Reset +1;
Mess= ChKey ?
Y
N
Store Id, St, and Info in NewInf
Mess= DeComm ?
Y
N
Active
Encrypt (Challeng)
Activate (SecAlarm) to AlmHandlr
Encrypt (Challeng)
Security (Sinfo) to SegH
Security (Sinfo) to SegH
PState= Active
PState= Active
DeComm
Active
KeyChange

Fig.21D.


Active
OutstAck (Id) from AlmHndlr
NormAck (Id) from AlmHndlr
Normal (Id, Params) from SegH
Outstanding (Id, Params) from SegH
Protect (OutstAck, Params)
Protect (NormAck, Params)
ChkAck(Id, Params)
ChkAck(Id, Params)
OutstAck (Id,PSq) to SegH
NormalAck (Id,PSq) to SegH
Y
Message OK ?
N
N
Message OK ?
Y
Normal (Id)to AlmHndlr
Activate (SecAlm) to AlmHndlr
Outstanding (Id) to AlmHndlr
Active

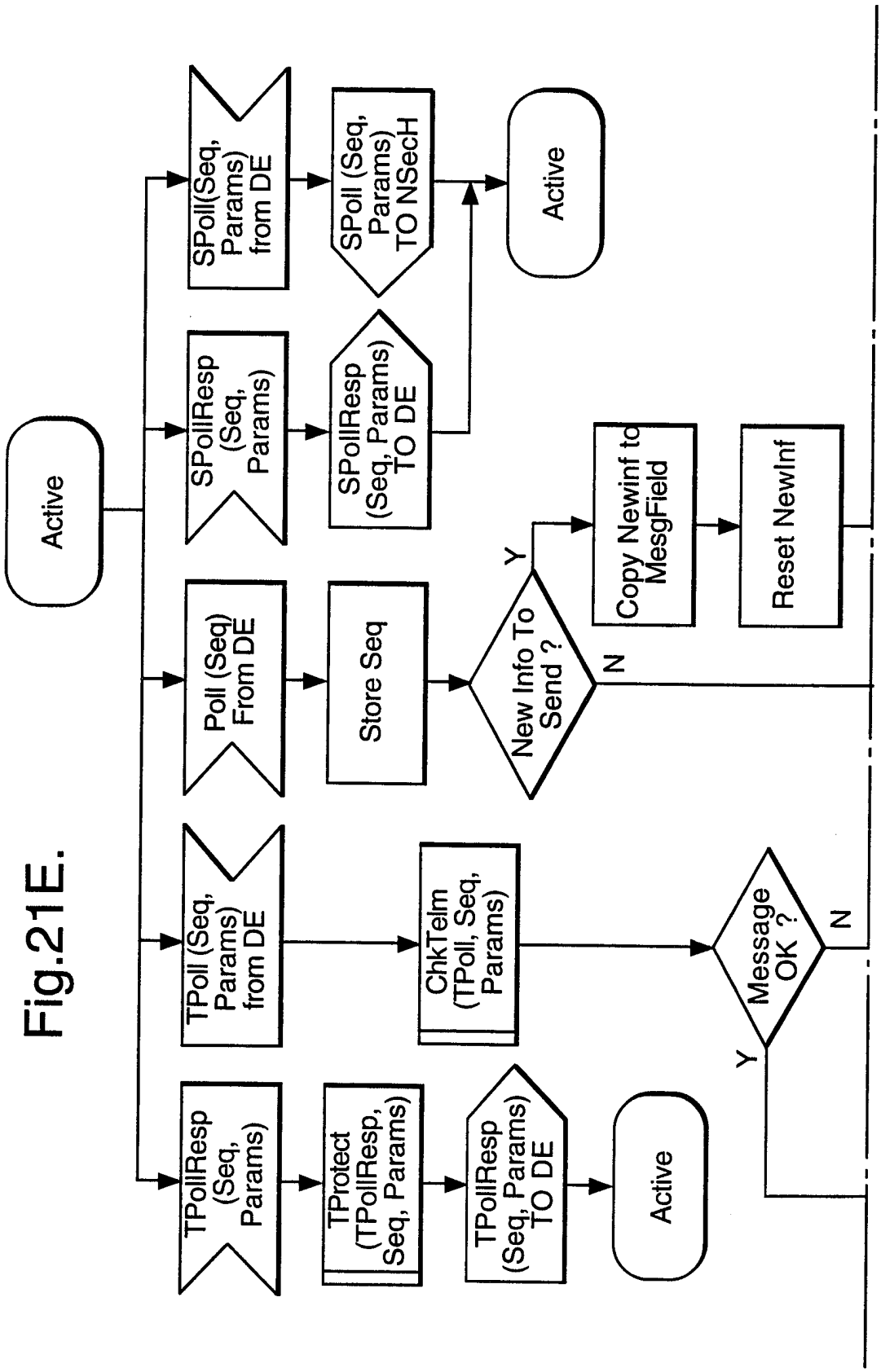

Active
SPoll(Seq, Params) from DE
SPoll (Seq, Params) TO NSecH
Active
SPollResp (Seq, Params)
SPollResp (Seq, Params) TO DE
Poll (Seq) From DE
Store Seq
New Info To Send ?
Y
N
Copy Newinf to MesgField
Reset NewInf
TPoll (Seq, Params) from DE
ChkTelm (TPoll, Seq, Params)
Message OK ?
Y
N
TPollResp (Seq, Params)
TProtect (TPollResp, Seq, Params)
TPollResp (Seq, Params) TO DE
Active

Fig.21E.

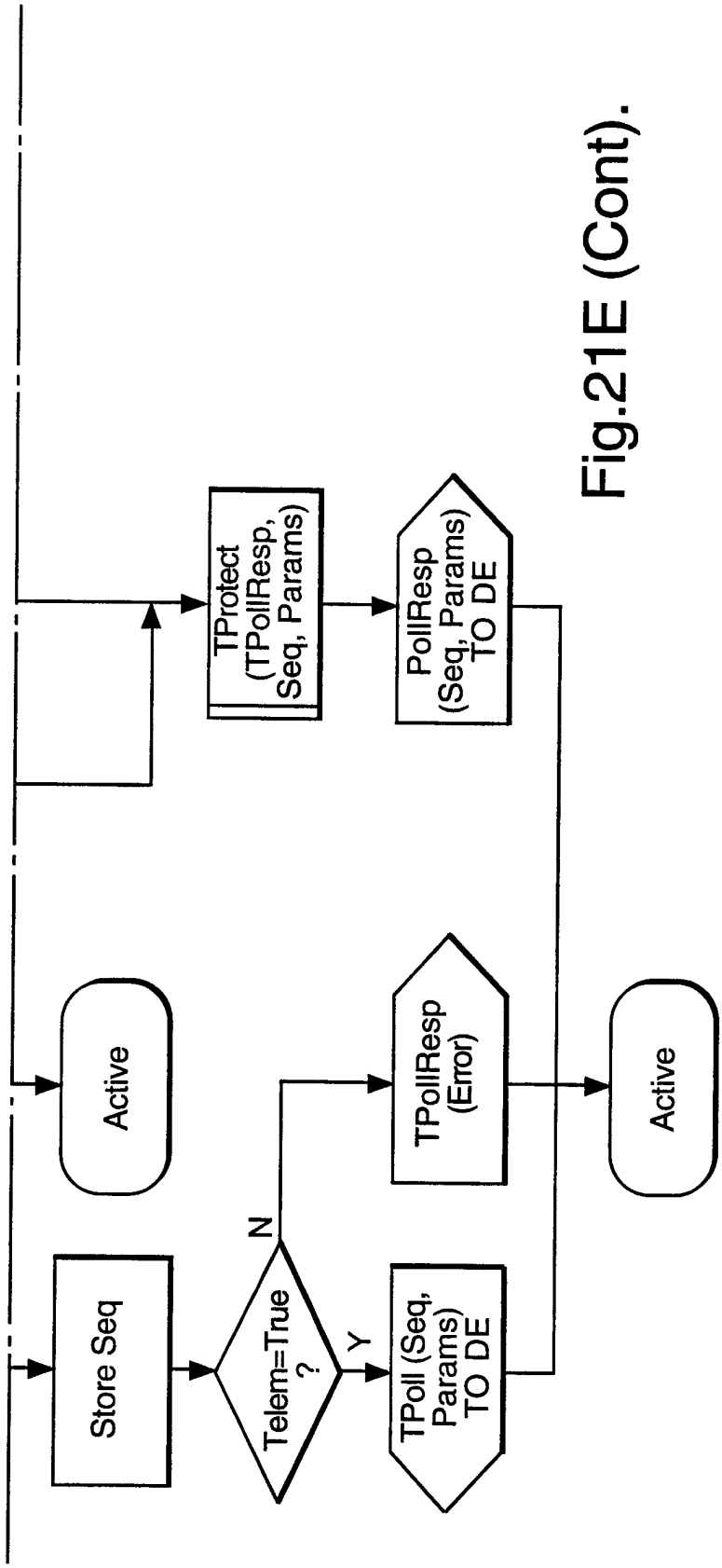

Store Seq
Telem=True ?
N
Y
Active
TProtect (TPollResp, Seq, Params)
PollResp (Seq, Params) TO DE
TPoll (Seq, Params) TO DE
TPollResp (Error)
Active

Fig.21E (Cont).

Fig.21F.

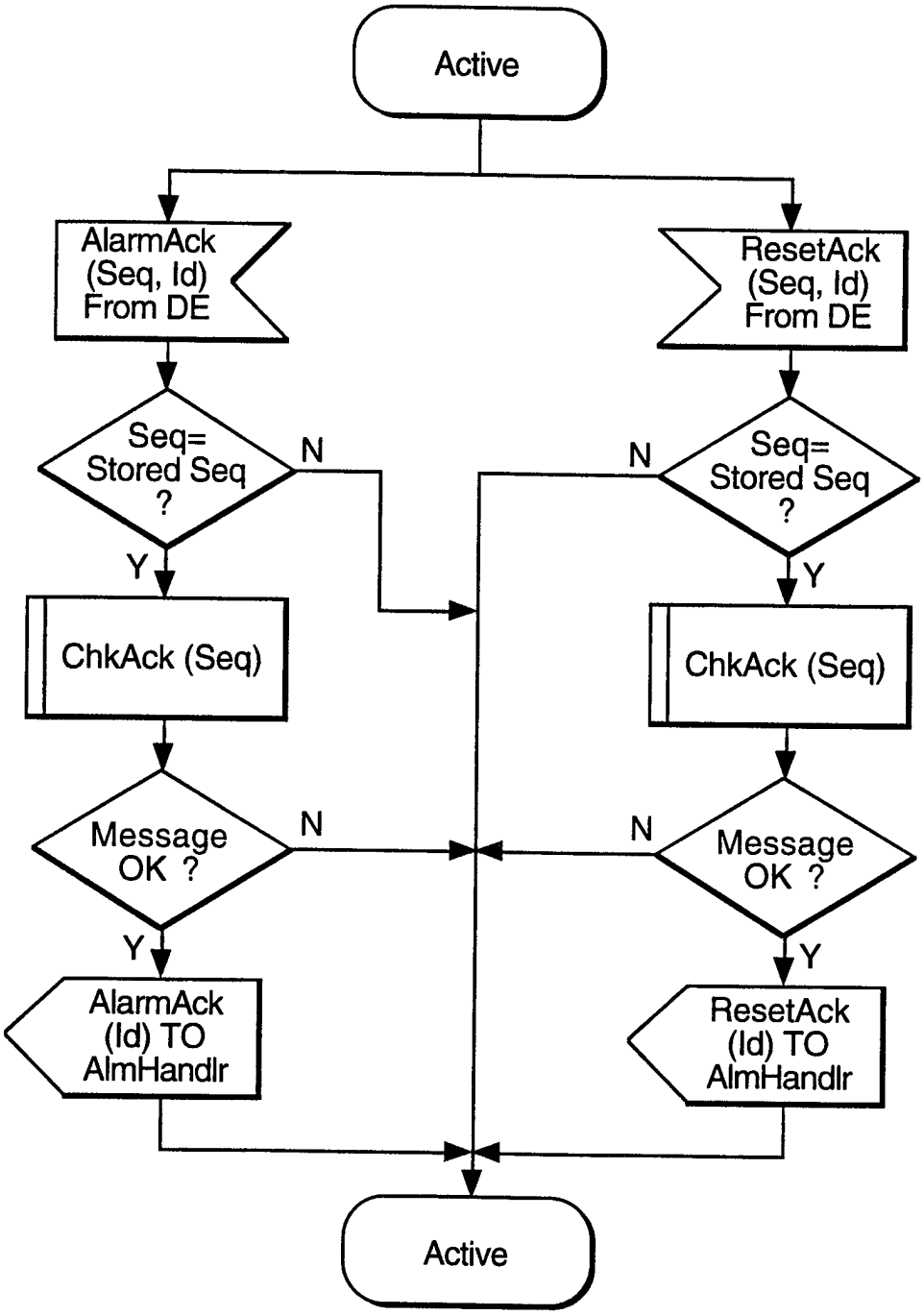
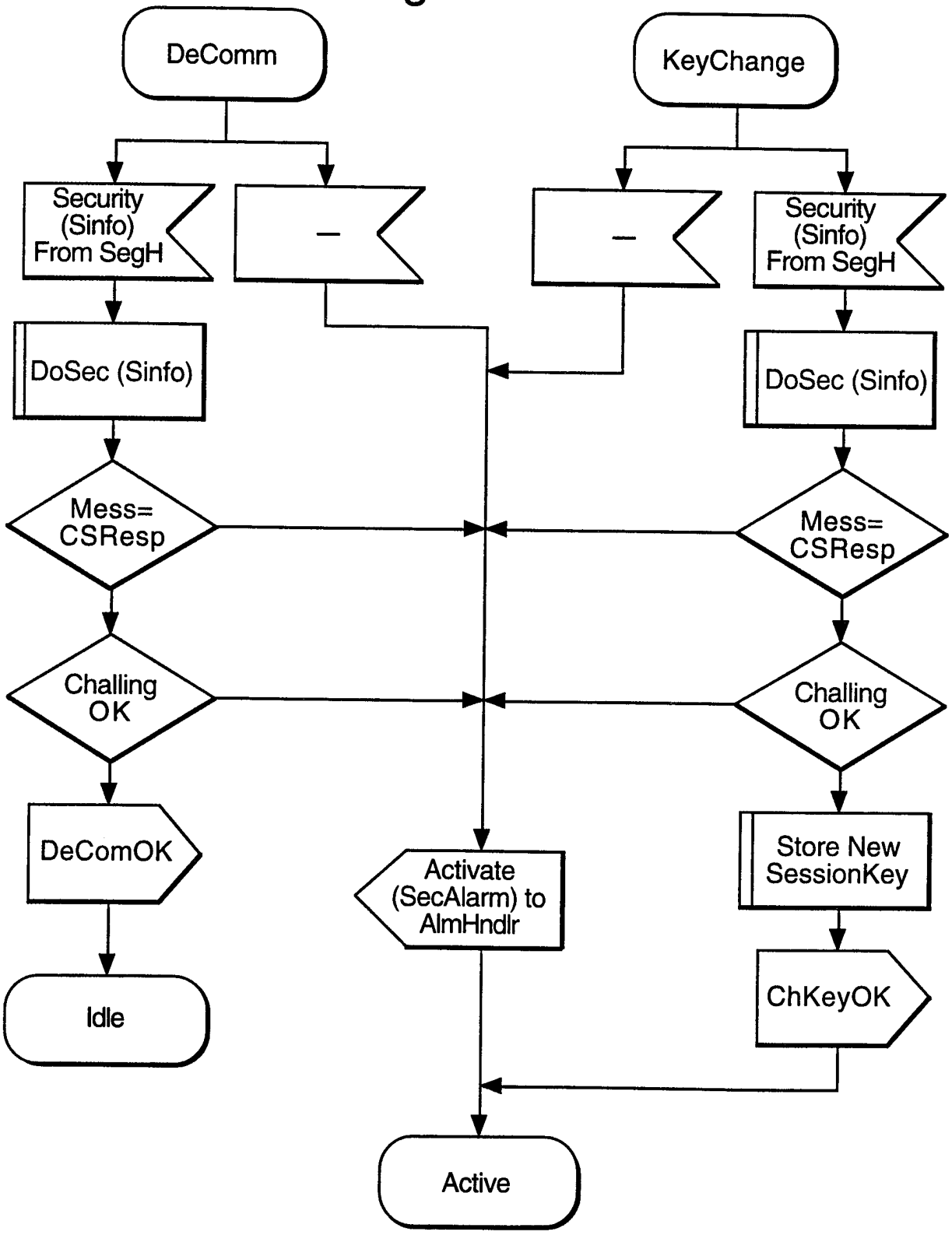

Active
AlarmAck (Seq, Id) From DE
ResetAck (Seq, Id) From DE
Seq= Stored Seq ?
N
Y
ChkAck (Seq)
Message OK ?
AlarmAck (Id) TO AlmHandlr
ResetAck (Id) TO AlmHandlr
Active

Fig.21G.


DeComm
KeyChange
Security (Sinfo) From SegH
—
—
Security (Sinfo) From SegH
DoSec (Sinfo)
DoSec (Sinfo)
Mess= CSResp
Mess= CSResp
Challing OK
Challing OK
DeComOK
Activate (SecAlarm) to AlmHndlr
Store New SessionKey
Idle
ChKeyOK
Active

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/GB 97/03180

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G08B25/01

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G08B H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 466 001 A (MOORE ET AL.) 14 August 1984 see abstract; figures 1-4A see column 3, line 26 - line 51	1
A	*Idem*	4,10

Y	PATENT ABSTRACTS OF JAPAN vol. 15, no. 147 (E-1055), 12 April 1991 & JP 03 022697 A (NEC CORP.), 31 January 1991, see abstract	1

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
10 February 1998	25. 03. 98
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Danielidis, S

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/GB 97/03180

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SUBBARAO ET AL.: "Development of a security network (SECNET) based on ISDN." ANNUAL REVIEW OF COMMUNICATIONS, vol. 48, 1994 - 1995, CHICAGO,IL.,U.S, pages 599-602, XP000543209 see the whole document	1
A	WO 81 01933 A (RACAL-MILGO,INC.) 9 July 1981 see abstract; figures 3-5,14 see page 17, line 28 - line 33 see page 18, line 6 - line 10	1,4
A	US 3 713 142 A (GETCHELL) 23 January 1973 see abstract; figures 1,2 see column 5, line 19 - line 37	6
A	DE 28 15 183 A (STADELMAYR) 11 October 1979 see claim 1; figure 1 see page 20, line 11 - line 15	7
A	PATENT ABSTRACTS OF JAPAN vol. 16, no. 499 (E-1280), 15 October 1992 & JP 04 185042 A (TOSHIBA CORP.), 1 July 1992, see abstract	2,9

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna l Application No
PCT/GB 97/03180

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4466001 A	14-08-84	NONE	
WO 8101933 A	09-07-81	US 4322576 A	30-03-82
		BE 886898 A	16-04-81
		CH 656761 A,B	
		FR 2472890 A	03-07-81
		GB 2078063 A,B	23-12-81
		NL 8020502 T	02-11-81
		SE 427402 B	28-03-83
		SE 8105098 A	28-08-81
US 3713142 A	23-01-73	NONE	
DE 2815183 A	11-10-79	WO 7900902 A	15-11-79
		EP 0014714 A	03-09-80
		JP 55500742 T	09-10-80