SHORE TELECOMMUNICATION EQUIPMENT

CONTENTS

SHORE TELECOMMUNICATION EQUIPMENT

INTRODUCTION

1 Although the Shore Telecommunication System is complex and widespread, recently attempts have been made to rationalise the equipment supporting it. In particular a Common Receiver has been introduced, the CHM, which is replacing a number of obsolescent receivers. New transmitters (both UHF and HF), VF equipment and EDC equipment have been introduced. In addition several new sub-systems are on course of installation.

2 New equipment will be introduced into BR 333(4) (Summaries of Telecommunication Equipment (Ashore)), and most of it will be the subject of PJT courses, (Booking - HMS COLLINGWOOD Ext 202) and so will not be reviewed here.

3 This Chapter will briefly review the main sub-systems, designed to meet the requirements of NSRs. In order to facilitate insertion and removal of sub-systems, they have been arranged as ANNEXES to this chapter.

THE NAVAL SHORE TELECOMMUNICATION NETWORK

INTRODUCTION

1 The Naval Shore Telecommunication Network (NSTN) carries all Naval operational and administrative signal traffic within the UK and Gibraltar and provides broadcast and ship/shore terminal facilities to and from the Fleet at communication centres (COMMCENs) ashore. It comprises a number of major relay stations which interface with other communication networks and with the Fleet, together with connected tributaries (military stations which transmit and receive signal traffic). It includes the bearer network connecting relay centres and tributaries.

NETWORK DETAILS (Fig 5A.1)

2 The NSTN consists of eight switching centres (nodes) in UK and Gibraltar. These are located at Northwood, Pitreavie, Plymouth, Whitehall, Fort Southwick, EDCC, Faslane and Gibraltar.

3 When Whitehall is fitted with its new equipment, all nodes will be fully equipped with TANDEM non-stop computer systems.

4 The numbers and types of processors fitted at NSTN sites varies. Processor types include Non-Stop II (NSII) and TXP, differing only in the amount of processor onboard memory (NSII - 8 Mbytes/processor, TXP - 16 Mbytes/processor) and VLX with 16 Mbytes/processor.

5 NSII and TXP processors are interchangeable in a system while VLX is not. The numbers of processors fitted per site vary up to a maximum of 16 per system, although systems may be interconnected to increase capacity provided such interconnected systems are within 1 km for NSII/TXP or 4 km for VLX and TANDEM's fibre-optic system FOX II is used.

6 With the exception of Fort Southwick and Northwood which have VLX processors fitted, NSTN nodes are equipped with NSII or TXP processors.

THE TANDEM COMPUTER SYSTEM (Fig 5A.2)

7 The TANDEM computer system uses multiple processors allowing simultaneous running of multiple processes. Each process is loaded in at least two processors so that, should the primary processor fail, the back-up machine, having sensed the failure, will automatically continue to run the process from the point of failure.

8 In addition, each input/output (I/O) device is connected to two processors via an I/O controller to ensure that a single processor failure will not cause the total loss of any service.

9 I/O controllers, although connected to two processors, can only be controlled by one processor at any time.

10 TANDEM processors have independent power supplies together with a back-up battery that will retain the internal memory in the event of a power failure.

NB: The back-up battery does not allow operation of the processor.

11 I/O controllers are fed from two independent I/O power supply systems to increase flexibility.

12 Disc drives are connected to, and may be controlled by, two disc drive controllers each of which is connected to two processors giving four possible information paths to ensure continuous availability. In addition, discs are run as mirrored pairs (primary and mirror) ie information is read to both discs in a pair so that, in the event of the primary disc failing, the mirror contains all the information and may be brought into service.

13 TANDEM Non-Stop computer systems are configured to suit the node with I/O devices connected in such a way as to balance the load on the available processors.

14 The optimum size of a TANDEM installation is such that, with all processors carrying an equal share of the load, an activity level of less than 70% of the available time is a good starting point to allow for expansion and operational peaks. The first effect of overloading the system is a slowing down of processes that have hitherto appeared instantaneous. Should this occur in an otherwise correct installation, then consideration should be given to the application program to see if the workload can be reduced. In addition, non-stop operation will be prevented under fault conditions, ie processor failure, due to there being no migration space for the activity.

15 The TANDEM computer can accept and process a large range of input information, both asynchronous (telegraph) and synchronous (data), at speeds ranging from 50 Baud to kilostream rates. It can be programmed to deal with both full and half-duplex communication channels.

16 The computer carries out the automatic routeing of signal traffic as in earlier TARE's together with the distribution of signal traffic to action and information addressees. This second function is similar to that carried out by AMRAD.

17 Fig 5A.3 shows the typical signal flow within the node, including synchronous and asynchronous inputs/outputs, core network and ship communications.

18 Each node is connected to other nodes as required, to tributaries in the geographical area of the node and to operators message handling facilities locally.

Packet Switch Network (Core Network)

19 The nodes are interconnected by a network utilising the principles of X25 (1980) across bearers carrying medium speed data at 9.6 kbps (limited in speed by available lines).

20 The packet switches in the network are the core multiplexers fitted at each node. These act as statistical multiplexers passing data packets between TANDEM aggregate input ports.

21 When secure and survivable bearer systems become available they will be used by the NSTN. Such systems are expected to be developed as part of the Naval Fixed Telecommunication System (NFTS), and eventually the Defence FTS (DFTS).

Cryptographic Equipments

22 It is planned that all communication links between nodes and tributaries will be protected by cryptographic equipments. On asynchronous circuits, all common telegraph crypto equipments can be used, but older equipments limit the speed. On synchronous circuits, current modern equipment is capable of data rates up to 9.6 kbps.

23 On data circuits, timing is taken from the line modem (currently BT Type 4961). This allows data rates of 4.8 kbps or 9.6 kbps. Under normal circumstances the landline standard prevents use of higher data rates.

Concentrator Sites

24 To save on-line costs and computer ports, and to simplify survivability arrangements, a number of line concentrator sites are arranged. Each site serves a specific geographical area and is one of two general types.

25 Synchronous lines only. A single high speed data line from the TANDEM carries traffic for each addressee served by the concentrator. At the concentrator site the decrypted data stream is fed to a multiswitch acting as a statistical multiplexer. Each remote site is then fed as though it were a signal terminal site (Fig 5A.4).

26 Synchronous and Asynchronous lines. At the TANDEM site, the asynchronous and synchronous lines are fed to separate channels of an Omnimux. The aggregate data channel is passed to the concentrator site where a second Omnimux recreates the asynchronous and synchronous lines. The asynchronous line is fed directly to its terminal equipment, the synchronous line is fed to a multiswitch (statistical multiplexer) to be demultiplexed and passed to remote sites (Fig 5A.5).

Single Terminal Sites

27 The simplest situation is the station fed with synchronous data by high speed line. (Fig 5A.6). Used for stations which do not necessarily fall into geographical area of a concentrator site.

28 For sites which are activated at irregular intervals, a low speed covered telegraph circuit is provided, terminating on a TGN. The TANDEM provides a "user-friendly" facility for these sites (Fig 5A.7).

NSTN INTERFACES

29 The NSTN provides interoperability with the following communication networks:

(1) NATO NICS TARE.

(2) RAF UNITER.

(3) Defence Communication Network including RAF TARES.

(4) DCS Croughton (AUTODIN).

Ship/Shore/Ship Communications

30 The software package for each TANDEM is common and provides a number of ship/shore/ship communication facilities.

31 Broadcast. Each node can control up to four Broadcasts which may be LF, HF or SHF as required. Each broadcast may be continuous or scheduled. Nodes will be allocated control of broadcasts as a back-up to MEP at Whitehall. Local broadcasts will be controlled by the nearest node, eg B41T uses Fort Southwick.

32 Satellite Ship/Shore. Each node will have the capability of controlling up to six satellite ship/shore channels with one CARB channel.

33 Maritime Rear Link. Each node will be equipped to operate two MRLs.

34 Local Area Communications. Software will be provided to control local area communications, eg Harbour RATT, but only selected nodes will be required to use the facility.

35 Secure Net Alongside Communication (SNAC). Each node will have software to control SNAC, but not necessarily the hardware. SNAC fitted nodes will provide three crypto covered channels which may be connected to up to 18 external lines. Ships wishing to use SNAC will be automatically allocated access on a "first come, first served" basis.

36 MEP/MAP Interface. Normally MEP controls all ship communications using Whitehall TARE as the interface into the DCN. TANDEMs at Fort Southwick and Plymouth have facilities to interface with MEP using 2 × 600 Baud asynchronous channels.

37 HF Ship/Shore. All nodes have the software to control 10 channels of HF ship/shore, but will not necessarily have the associated hardware.

SECURITY

38 To prevent unauthorised access to data in the system, the NSTN uses a number of techniques incorporating physical, documentary, personnel and computer security.

39 Physical security methods include the normal access control for buildings and areas within buildings, on-line encryption on all external lines and the normal electronic security countermeasures including extensive use of fibre-optic techniques.

40 The normal rules for documentary and personnel apply.

41 Computer security is a multi level system with strict control being exercised over access to information held, such access being on a "need to know" basis. Users are individually named in the system, being uniquely identified by a magnetically coded card and password (changed at 6-monthly intervals). Users are given access only to that material necessary for them to be able to carry out their assigned duties, and are only able to access the system at predetermined terminals.

42 Users are held strictly accountable for all their actions including being responsible for data generated by them. All actions taken on the system are logged, the resulting secure logs being available for inspection by the Node Security Officer as required. To allow for genuine errors, each user is allocated thresholds for illegal accesses, ie attempts to access anything outwith that allowed by their registration. Should a user reach such a predetermined threshold, he is not warned, but his access is barred by the system. Further access may only be obtained after the Security Officer has investigated and cleared the record/reset the threshold.

SURVIVABILITY

43 The NSTN is configured in such a way that each tributary is connected to one node with the nodes being interconnected. A number of connections exist from previous systems, but these are not sufficient to ensure complete secondary connectivity.

44 For DCN sites, the provisions of DCNP 6 (DCN Network Operating Orders) apply with other nodes taking over services normally operated by the failed node.

45 Survivability of NSTN nodes is enhanced by use of uninterruptible power supplies for computer and crypto equipment, non-stop computer systems and provision of installed spare equipment.

46 Should a TANDEM fitted node fail, the following is the normal situation:

(1) The core network will continue to function whether or not the packet switch exchange concerned remains operational. (Automatic re-routeing of packets by X25 protocol.)

(2) Directly connected tributaries go down with their TANDEM host and must be covered by a 'guard station'.

(3) Concentrator sites and their tributaries are provided with a secondary host node (Fig 5A.8) and must physically reconnect to, and access the secondary node.

47 In some instances, high priority tributaries connected via a concentrator are given standby connections to bypass the concentrator site in the event of bearer or concentrator site failure.

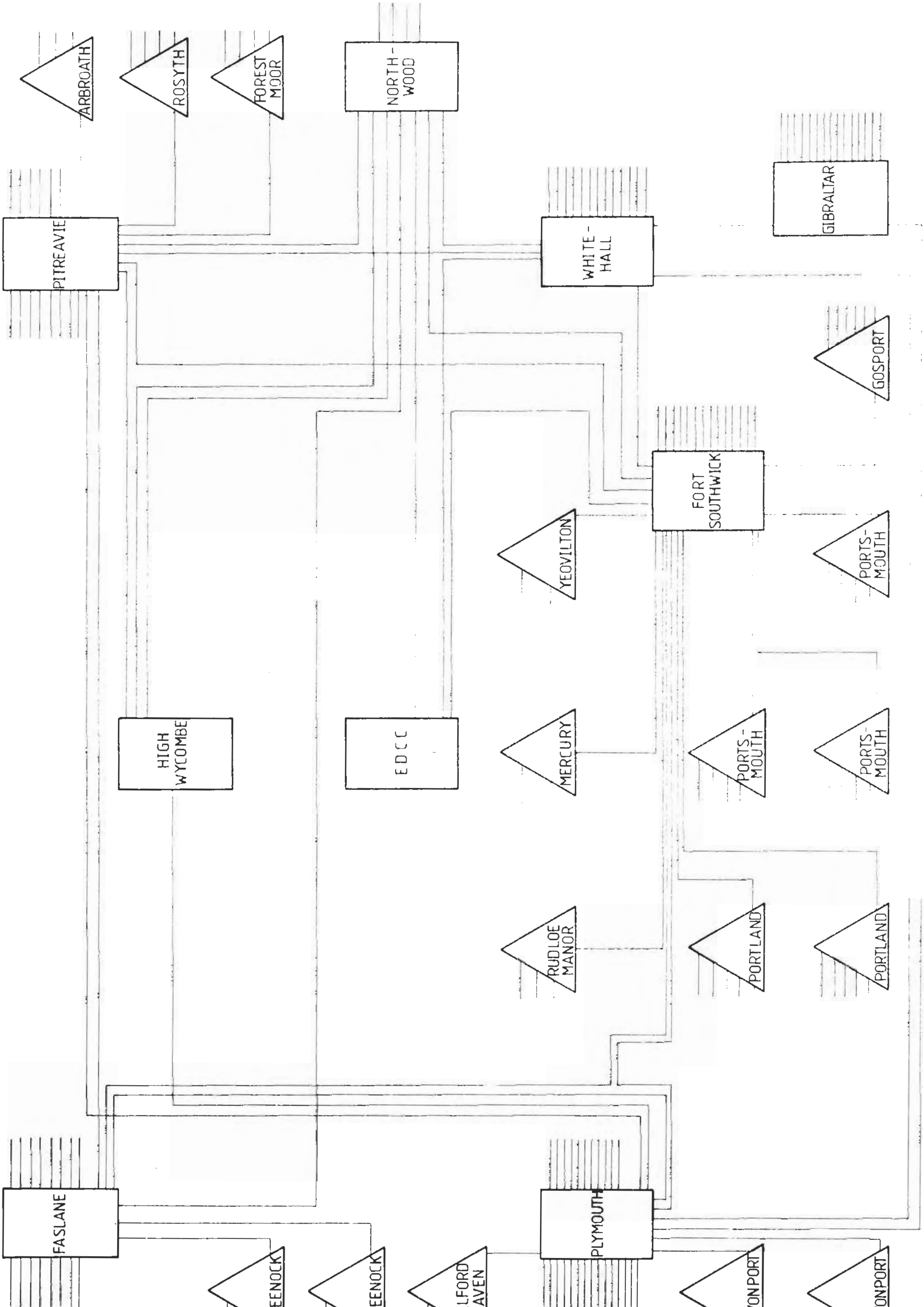

FIG 5A.1 NAVAL SHORE TELECOMMUNICATION NETWORK

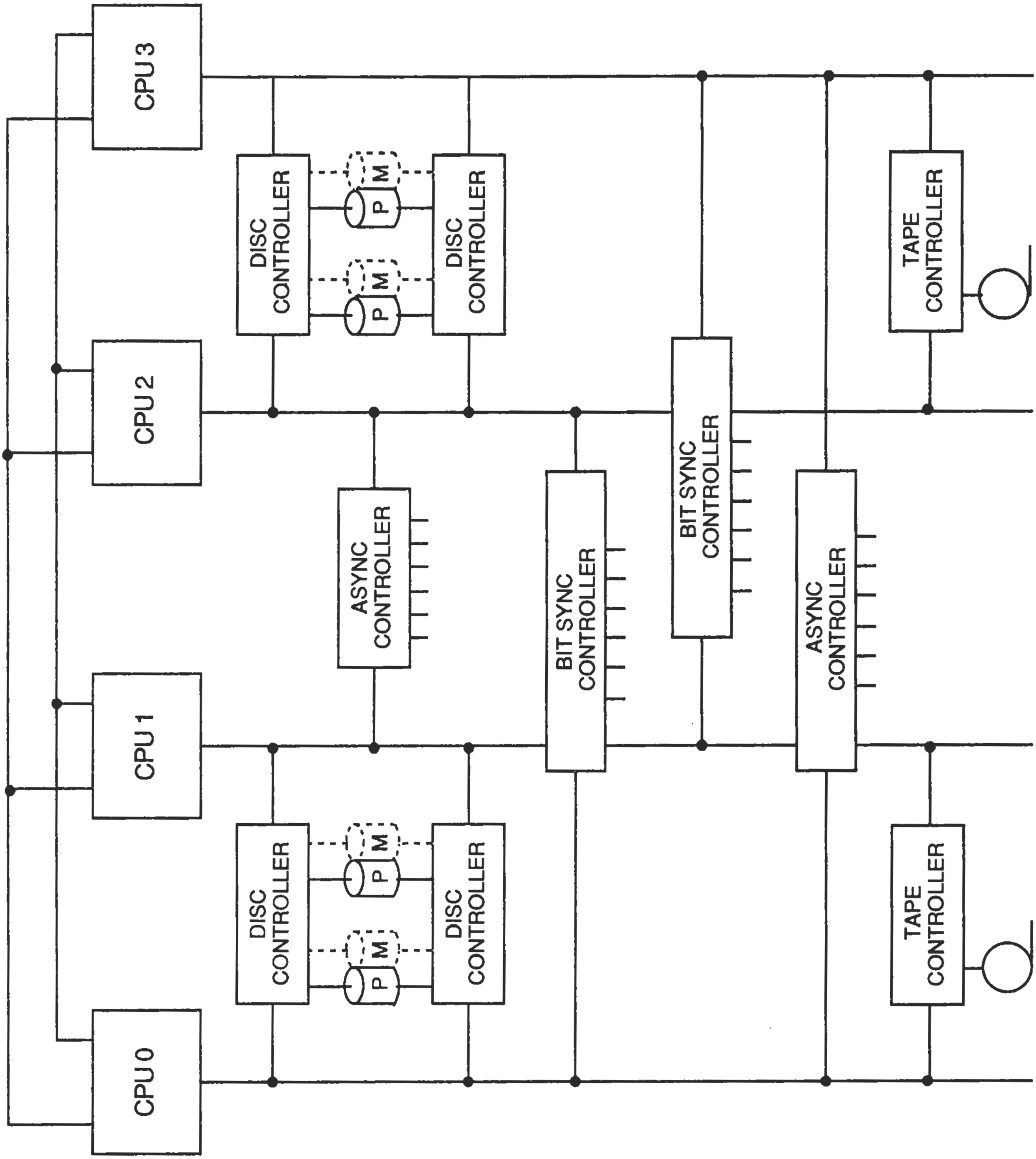

FIG 5A.2 TANDEM SYSTEM CONFIGURATION

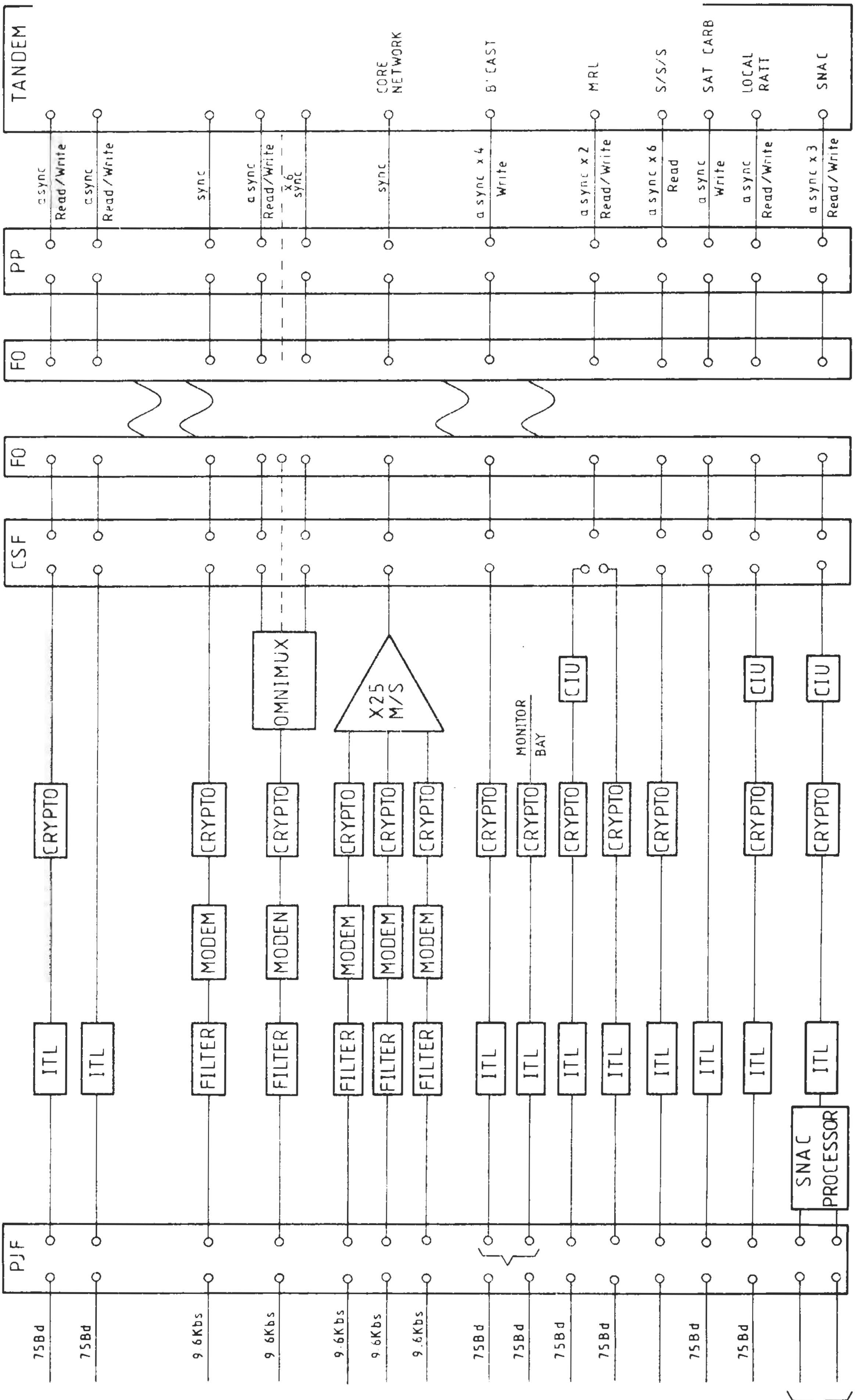

FIG 5A.3 NSTN NODE

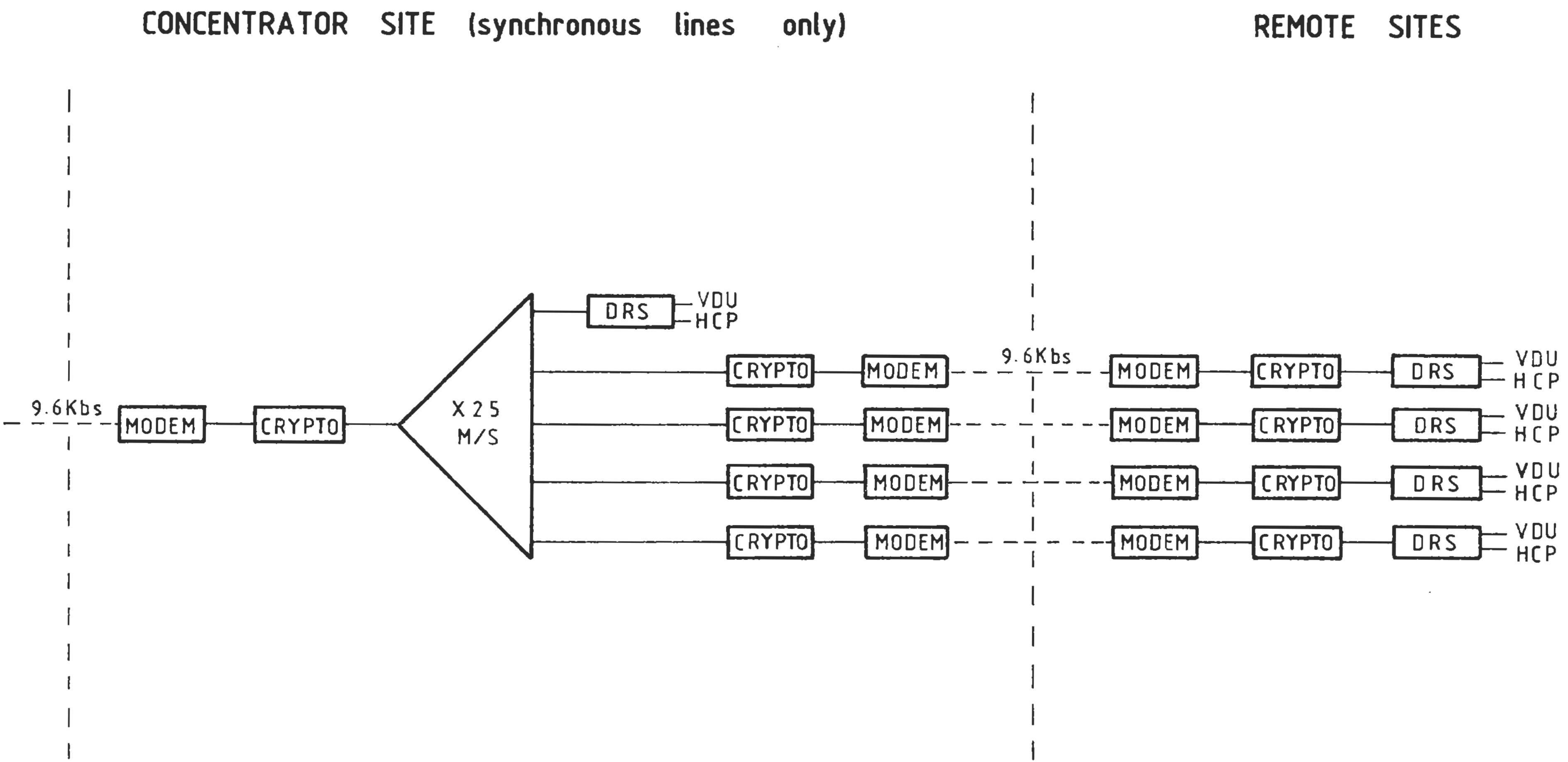
CONCENTRATOR SITE (synchronous lines only)
REMOTE SITES
9.6Kbs
MODEM
CRYPTO
X 25
M/S
DRS
VDU
HCP
CRYPTO
MODEM
9.6Kbs
MODEM
CRYPTO
DRS
VDU
HCP

FIG 5A.4

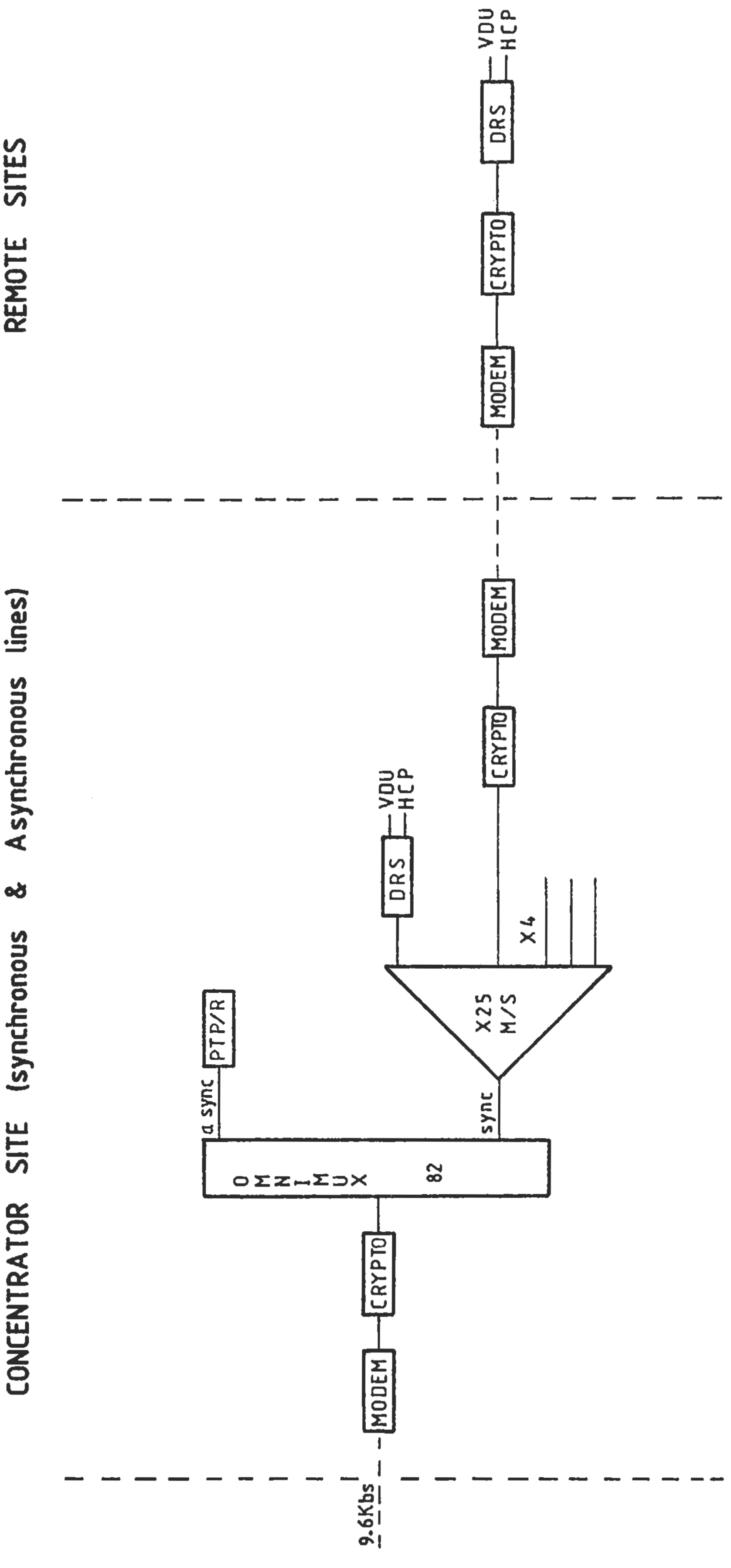
CONCENTRATOR SITE (synchronous & Asynchronous lines)
REMOTE SITES
VDU
HCP
DRS
CRYPTO
MODEM
MODEM
CRYPTO
VDU
HCP
DRS
X4
X25
M/S
PTP/R
a sync
sync
OMNIMUX
82
CRYPTO
MODEM
9.6Kbs

FIG 5A.5

FIG 5A.6 SINGLE TERMINAL SITE (SYNCHRONOUS)

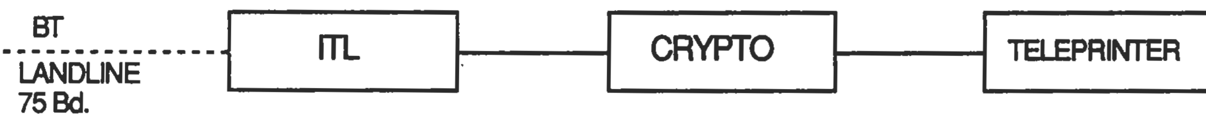

FIG 5A.7 SINGLE TERMINAL SITE (ASYNCHRONOUS)

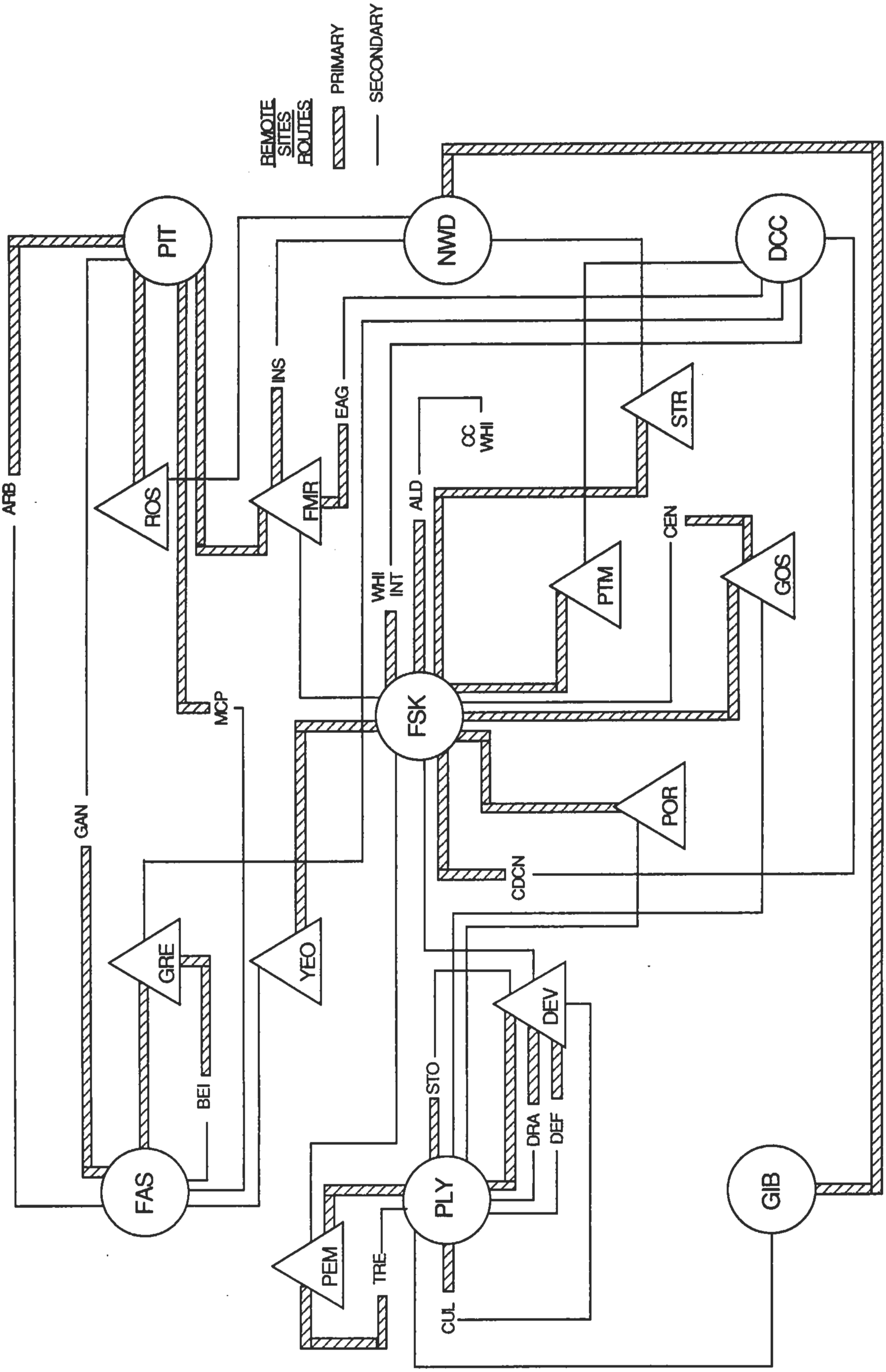

FIG 5A.8 REMOTE SITE SURVIVABILITY OVERVIEW