ADatP-16(E)

STANDARD OPERATING PROCEDURES

FOR NATO LINK 16

VOLUME 2

FEBRUARY 2006

NORTH ATLANTIC TREATY ORGANISATION

NATO STANDARDISATION AGENCY (NSA)

NATO LETTER OF PROMULGATION

February 2006

1. ADAtP-16(E) Volume 2 - STANDARD OPERATING PROCEDURES FOR NATO LINK 16 is a NATO UNCLASSIFIED publication.

2. ADatP-16(E) Volume 2 is effective upon receipt. It supersedes ADatP-16(D) Volume 2 which shall be destroyed in accordance with the local procedure for the destruction of documents.

J MAJ
Brigadier General, POL(A)
Director, NSA

This page is reserved for
National Letter of Promulgation

CHAPTER	RECORD OF RESERVATIONS BY NATIONS
1	NONE
2	NONE
3	NONE
4	NONE
5	NONE

NATION	RESERVATION

RECORD OF CHANGES

CHANGE NO.	DATE ENTERED	EFFECTIVE DATE	BY WHOM ENTERED

Allied Data Processing Publication 16(E)

The Standard Operating Procedures for NATO LINK 16

(Short Title: ADatP-16(E))

Volume 2

Reference: STANAG 5516

FOREWORD

1. These standard operating procedures are produced by the Information Systems Sub-Committee (ISSC) - Data Link Working Group (DLWG).

2. Proposed changes to this document should be addressed to:

NATO HEADQUARTERS
NHQC3S/ISEB (DLSS)
B-1110 BRUSSELS
BELGIUM

ADATP-16 STRUCTURE

VOLUME 1:

VOLUME 2:

Table of Contents enclosed.

VOLUME 3:

National Supplement 4	Denmark
National Supplement 5	France
National Supplement 6	Germany
National Supplement 7	Greece
National Supplement 8	Hungary
National Supplement 9	Iceland
National Supplement 10	Italy
National Supplement 11	Luxembourg
National Supplement 12	NATO
National Supplement 13	Netherlands
National Supplement 14	Norway
National Supplement 15	Poland
National Supplement 16	Portugal
National Supplement 17	Spain
National Supplement 18	Turkey
National Supplement 19	United Kingdom
National Supplement 20	United States and Possessions

VOLUME 2
CONTENTS

Chapter Page

Chapter Page

LIST OF FIGURES

LIST OF TABLES

ANNEXES

CHAPTER 1

INTRODUCTION

1.1 GENERAL

Volume 2 of ADatP-16 contains specific guidelines and procedures for personnel responsible for the following Link 16 network management activities:

a. Network Design.

b. Pre-mission Planning and Network Initiation.

c. Network Operation.

d. Cryptonet Management.

A Summary of Contents for Volume 2 is provided at Table 1.1.

1.1.1 Network Design

Network Design is the process of specifying the communications requirements for a given scenario, translating them into sets of terminal initialisation data and distributing completed network designs to all intended network participants. While each nation takes responsibility for network design support for their national assets, the actual network design is done for all forces, both national and visiting, by the network design facility responsible to the respective operational commander. For NATO command forces, network design is accomplished at the Strategic Command (SC) level. The NATO Network Design Facility (NDF) is responsible for Allied operations, exercises and training. Guidelines and procedures for Network Design are to be found in Chapter 2 of this Volume.

1.1.2 Pre-mission Planning and Network Initiation

1.1.2.1 Pre-mission Planning is the process of determining data link connectivity requirements, selecting the appropriate network design(s), identifying crypto requirements and assigning network duties to meet a specific operational task. Responsibility for network selection for regional use lies at the Regional Command (RC) level. Responsibility for day-to-day coordination of network use may be delegated to the Tactical Commander. In NATO, day-to-day operations are conducted by the Combined Air Operations Centres (CAOC).

1.1.2.2 Network Initiation is the process of preparing JU crypto and initialisation data, initialising the terminal and commencing network operations. The Tactical Commander is responsible for ensuring that all participating JUs receive the data necessary to enable them to achieve network entry and participate fully in network operations.

1.1.2.3 Guidelines and procedures for Pre-mission Planning and Network Initiation are found in Chapter 3 of this Volume.

1.1.3 Network Operation

Network Operation encompasses the monitoring and modifying of Link 16 network operations. Responsibility for this function should be delegated to a suitably equipped unit to act as Network Manager Station (NMS) for the operation of the chosen Link 16 network. The Network Manager should be active on the Link 16 interface and as such, the extent of his responsibility should be confined to a single network. Sub network managers may be assigned to manage portions of a Link 16 network, where the OPNET Management workload is expected to be heavy. In such cases the division of responsibility for management of the network should be hierarchically organised and defined in the OPTASK LINK. Guidelines and procedures for Network Operation are to be found in Chapter 4 of this Volume.

1.1.4 Cryptonet Management

Guidelines and procedures for Cryptonet Management are to be found in Chapter 5 of this Volume.

1.1.5 Synchronised Link 16 and IJMS Operations

1.1.5.1 Until the end of the transition from IJMS to Link 16, some networks will be required to accommodate both Link 16 and IJMS participants.

1.1.5.2 Operating procedures must be adapted to permit the differing capabilities of these two JTIDS user types to operate in a single synchronised network and to provide some mutual support. All procedures for such operations are contained in Volume 1, Chapter 7.

CHAPTER NUMBER	TITLE	SUMMARY OF CONTENTS
Chapter 1	Introduction.	
Chapter 2	Guidelines and Procedures for Network Design.	Covers all aspects of the Network Design function from the definition of requirements and design aims to the distribution of approved network designs. Step by step procedures are defined for the design process.
Chapter 3	Guidelines and Procedures for Pre-mission Planning and Network Initiation.	Details the Pre-Mission Planning activities required to select and tailor a network design and Network Initiation procedures for the preparation and loading of network data into participating platforms.
Chapter 4	Guidelines and Procedures for Network Operation.	Covers all aspects of Network Monitoring and Modifying from commencement of link operations to termination. Procedures are defined to coordinate the entry and exit of JUs and to manage network resources in response to changing operational situations.
Chapter 5	Guidelines and Procedures for Cryptonet Management.	Details guidelines and procedures for the distribution, loading and management of cryptovariables including procedures for Over the Air Rekeying (OTAR).

Table 1.1 ADatP-16 Summary of Contents for Volume 2

CHAPTER 2

GUIDELINES AND PROCEDURES FOR NETWORK DESIGN

2.1 DEFINITION OF LINK 16 NETWORK REQUIREMENTS

2.1.1 Operational Plans

NATO Operational Commanders are responsible for the production of operational plans to meet the expected threat for a range of anticipated scenarios. These planning activities enable requirements for Link 16 networks to be defined well in advance, thus permitting the design of appropriate networks.

2.1.2 Generation of Link 16 Network Design Requirements

2.1.2.1 MSCs are responsible for defining Link 16 network requirements to support NATO operational plans. When coordinating the operational requirements for individual Link 16 network designs, MSC staffs should consider the following:

a. Military Objective.

b. Geographical Area of Operations.

c. Force Structure:

   (1) Type of force: e.g. Link 16 only, Link 16/Link 11 etc.

   (2) List of participating platforms, including their data link capabilities; e.g. Link 16 only, Link 16/Link 11 etc.

   (3) Disposition of Forces.

d. Data Exchange Requirements:

   (1) Platform Connectivity requirements per PG.

   (2) Relay requirements per PG.

   (3) IER priorities/trade-offs; Surveillance, EW, Command and Control, Fighter-to-Fighter, Voice.

e. Multi-link Considerations:

   (1) Data forwarding requirements.

   (2) Management of concurrent operations

(3) Multi-link information management.

f. Communication Requirements:

(1) Peacetime frequency restrictions.

(2) Cryptonet requirements.

(3) Required anti-jam margin.

2.1.2.2 It is the responsibility of network designers, in conjunction with operational commands, to take these operational plans and from them to extract specific requirements for each Link 16 network to be developed. Each PG will normally be considered separately, subject only to the constraints of the time slot requirements of other PGs.

2.1.3 Network Operating Environments

The range of network designs should accommodate the following range of operational environments:

a. Peacetime - Network designs must conform to agreed peacetime operating restrictions according to the area of Link 16 operations, as detailed in Volume 3. Full Interference Protection Features (IPF) are applied (override off).

b. Peacetime Exercise - IPF may be “Exercise Overridden” to remove a number of restrictions but only with prior permission of the appropriate civil authority.

c. Wartime - IPF is “Combat Overridden” to remove all peacetime restrictions.

Network designs should facilitate the transition between different network operating environments.

2.1.4 Network Design Aims

2.1.4.1 It is the responsibility of the Network Design function to produce libraries of Link 16 network designs that are robust, workable and effective in meeting the defined range of anticipated operational scenarios. A number of design aims are identified:

a. Networks should be designed such that their operation does not rely heavily on particular planned participants to maintain essential connectivity. If such participants exist, they act as nodes which offer vulnerable points of attack to an enemy attempting to disrupt the flow of vital tactical information on the network by either jamming or weapon strikes.

b. Networks should be capable of sustaining operations through high levels of ECM. Flexible operation of relay and optimum use of MIDS ECM-resistant features, (through employment of lower packing levels and normal range mode), should be incorporated into network designs wherever possible.

c. Networks should be designed to be tolerant of minor changes in operational requirements and capable of continued operation in support of such changes. Such flexibility of design will reduce the number of occasions when a change of Link 16 network will be required, thus precluding complete network reinitialisation for all participants in every case and minimising disruption to network operations.

d. Network designers should aim to balance the following, often conflicting, factors:

(1) Communications requirements for planned participants.

(2) Communications requirements for network management and system maintenance.

(3) Network capacity limitations.

(4) MIDS terminal/host limitations.

(5) Operating restrictions in force.

(6) Cryptonet size limitations.

e. Network designers must consider both of the following:

(1) Operational requirements of the given scenario.

(2) Variations in Link 16 implementations and concepts of operation which may exist among the types of platforms of the different nations and/or Services that are required to participate in NATO Link 16 operations.

Details of national/Service implementations and technical differences required to be considered by designers of NATO networks are contained in Annex A to this Volume. Specific platform implementation details down to message and action value level are contained in National Supplements in Volume 3.

2.1.4.2 The guidelines presented above are not always mutually compatible. Dependency on certain nodes for continued network operation creates points of vulnerability within the network design. Therefore robust networks should be virtually “nodeless” to eliminate these vulnerable points. However, networks capable of flexibility of operation essentially require provision for dynamic network management and therefore rely on intervention by the Network Manager to ensure continued operation. Individual requirements considered together may often exceed the capacity available for allocation, particularly when ECM-resistance must be optimised. Consequently network designers may not be able to satisfy all of the communication requirements for JUs.

2.1.4.3 Network Design should involve consideration and analysis of all conflicting requirements. It will be necessary to accept some concessions to develop network designs which are effective in meeting overall requirements. Network designers should establish with Operational Command the priorities for each requirement in each given scenario.

2.1.5 Link 16 Network Library Sizes

Network Designers should aim to produce the minimum number of network designs necessary to meet defined operational requirements and Force structures. As requirements change to meet a developing threat, network designs should be updated accordingly.

2.1.6 Network Naming Convention

Each network design produced should be allocated a name in accordance with a set convention that conveys a certain amount of information to the user. Network names consist of five elements: Owner (Network Configuration Manager); Originating Network Design Facility (NDF); Network Use/Environment; Series Identifier and Version Identifier. The NATO network naming convention complies with the nine alphanumeric-character limit of the OPTASK LINK message and comprises these five elements plus a field for National use, as shown in Figure 2-1 below.

Owner	Originating NDF	Network Use/ Environment	National Use	Series Identifier	Version Identifier
(2 characters)	(1 character)	(1 character)	(2 characters)	(2 characters)	(1 character)

Figure 2-1 Network Naming Convention

2.1.6.1 Owner

Ownership of a network design is indicated with two alpha characters. A list of designators for owning Nations/Services is shown in Table 2.1.

AA=UNITED STATES/ARMY	IN=ITALY/NAVY
AC=UNITED STATES/COMBINED	NA=NATO
AF=UNITED STATES/AIR FORCE	NF=NORWAY/AIR FORCE
AJ=UNITED STATES/JOINT	NH=NORWAY/ARMY
AM=UNITED STATES/MARINE CORPS	NJ=NORWAY JOINT
AN=UNITED STATES/NAVY	NN=NORWAY NAVY
CA=CANADA ARMY	SA=SPAIN/ARMY
CF=CANADA AIR FORCE	SF=SPAIN/AIR FORCE
CN=CANADA NAVY	SJ=SPAIN/JOINT
FA=FRANCE/ARMY	SN=SPAIN/NAVY
FF=FRANCE/AIR FORCE	TJ=TURKEY/JOINT
FJ=FRANCE/JOINT	TA=TURKEY/ARMY
FN=FRANCE/NAVY	TN=TURKEY/NAVY
GA=GREEK/ARMY	TF=TURKEY/AIR FORCE
GF=GREEK/AIR FORCE	UF=UNITED KINGDOM/ROYAL AIR FORCE
GJ=GREEK/JOINT	UJ=UNITED KINGDOM/JOINT
GN=GREEK/NAVY	UN=UNITED KINGDOM/ROYAL NAVY
HA=NETHERLANDS/ARMY	WF=SWISS/AIR FORCE
HF=NETHERLANDS/AIRFORCE	YA=GERMANY/ARMY
HN=NETHERLANDS/NAVY	YF=GERMANY/AIR FORCE
IA=ITALY/ARMY	YJ=GERMANY/JOINT
IC=ITALY/COMBINED	YN=GERMANY/NAVY
IF=ITALY/AIR FORCE	
IJ=ITALY/JOINT	All other codes = unspecified

Table 2.1 Owner Designators - Owning Nation/Service

2.1.6.2 Originating Network Design Facility

Design responsibility is vested in the originating NDF which is indicated with a single alpha character. A list of designators for Originating NDF is shown in Table 2.2.

A=US ARMY	L=FRANCE NAVY
B=US AIR FORCE	N=NATO MIDS NETWORK DESIGN FACILITY
C=US MARINE CORPS	O=CANADA JOINT
D=US NAVY	S=SPAIN
E=US JOINT	T-TURKEY
F=FRANCE JOINT	U=UNITED KINGDOM
G=GREECE (HELLAS)	W=SWISS
H=HOLLAND (NETHERLANDS)	X=NORWAY NDF
I=ITALY	Y=GERMANY
J=FRANCE ARMY	
K=FRANCE AIR FORCE	All other codes = unspecified

Table 2.2 Originating Network Design Facility Designators

2.1.6.3 Network Use/Environment

Network Use/Environment is indicated with a single alpha character. A list of designators for Network Use/Environment is shown in Table 2.3.

D=WARTIME/CRISIS MANAGEMENT	U=TRAINING
E=EXERCISE	X=EXPERIMENTAL
O=OPERATIONAL	Z=OTHER
P=PEACETIME	
T=TEST	All other codes = unspecified

Table 2.3 Network Use/Environment Designators

2.1.6.4 National Use

Reserved for National use. The default setting is zero.

2.1.6.5 Series Identifier

The Series Identifier is a two character alphanumeric designator. It is used by network designers as a unique identifier within that design activity. When considered along with the Originating NDF designator, it forms a unique identifier across all design activities.

2.1.6.6 Version Identifier

The version identifier is a single alpha character. It is assigned by network designers to identify updates to a network design.

2.2 NETWORK DESIGN PROCEDURES

2.2.1 General

Network Design is a specialised activity performed in advance of network operations. The purpose of this function is to produce network designs which specify all initialisation parameters, including the allocation of time slot assignment parameters to all planned participants, to satisfy the requirements of defined operational scenarios. Technical support should be provided in the form of computerised design aids for the design of complex networks involving many different participants. However, the same basic network design procedures should be followed, irrespective of the complexity of the network to be produced or the facilities available.

2.2.2 Establishment of Connectivity

2.2.2.1 Establish Participation Groups

2.2.2.1.1 After establishing the numbers and types of JUs to be concurrently supported in the worst case scenario, the first step in the design process is to determine those JUs which must communicate with each other and on which subjects, i.e., establish PGs. A terminal organises and executes the transmission of messages as a function of PGs, which are defined by a PG Index Number. PGs can be further defined by the allocation of cryptovariables (see paragraph 2.2.2.2.3). If any of the planned participants are to operate beyond line-of-sight (LOS) of one another, the network designer must make provision for relay (see paragraph 2.2.2.3).

2.2.2.1.2 The type of PG employed is determined according to the basis for categorising communities of interest (COIs) among participating units:

a. Network PGs (NPGs) - these PGs are functionally orientated and based on the message exchange categories required. They are defined by PG index numbers between 0 and 31.

b. Needline PGs - these PGs are destination orientated and defined according to intended network recipients. Within a Needline PG any message can be exchanged. They are defined by PG index numbers between 32 and 511. (Needline PGs are not considered further in this document as they will not be widely implemented within NATO).

2.2.2.1.3 A number of NPGs have been defined to support Link 16 information exchange as follows:

NPG 1	- Initial Entry
NPG 2	- RTT-A
NPG 3	- RTT-B
NPG 4	- Network Management
NPG 5	- PPLI and Status Group A
NPG 6	- PPLI and Status Group B
NPG 7	- Surveillance
NPG 8	- Mission Management/Weapons Coordination and Management
NPG 9	- Control
NPG 10	- Electronic Warfare
NPG 12	- Voice Group A
NPG 13	- Voice group B
NPG 19	- NonC^2 JU-to-NonC^2 JU A
NPG 20	- NonC^2 JU-to-NonC^2 JU B
NPG 21	- Engagement Coordination
NPG 22	- Composite A
NPG 23	- Composite B
NPG 27	- Joint Net PPLI
NPG 28	- Distributed Network Management
NPG 29	- Residual Messages
NPG 30	- IJMS Position and Status
NPG 31	- Other IJMS Messages

NPGs 1 through 6 must be implemented by all planned participants to ensure effective network operation. NPG numbers not listed above are currently undefined but may be specified for use in tactical communications plan(s) to meet specific operational requirements.

2.2.2.1.4 Composite NPGs are implemented by some JUs and may be employed in order to reduce network capacity requirements when available network capacity is limited (e.g. when operating under peacetime restrictions and required to operate on a single net). When Composite NPGs are utilised, Link 16 messages, with the exception of RTT and terminal-generated PPLIs, are selected for transmission in one of two NPGs, Composite A or Composite B, instead of the Standard Link 16 NPGs, as follows:

a. Composite A - covers the following Standard NPGs: Network Management; PPLI & Status A and B; Mission Management/Weapons Coordination & Management; Control; NonC^2 JU to NonC^2 JU; Spoke.

b. Composite B - covers the following Standard NPGs: Surveillance; Electronic Warfare.

Link 16 networks may be designed to utilise both Composite NPGs and Standard NPGs, providing no JU is allocated time slot capacity for a Composite NPG and the corresponding Standard NPGs simultaneously. Network designs may incorporate Composite A and/or Composite B NPGs; however, Composite A and B cannot be used with stacked nets.

2.2.2.1.5 For the guidance of network designers and the Network Manager, a standard NPG and other applicable NPGs are identified for each Link 16 message (excluding national messages) in Table 2.4. Not all JUs will be able to exchange the complete list of messages shown, and some JUs may exchange messages in an NPG other than as shown in Table 2.4. Nevertheless, the guidance provided by Table 2.4 should provide a firm basis upon which the Network Manager can determine allocations of transmission capacity, relay capabilities or cryptographic assignments in the selected functional area(s). The Network Manager should also note that, in the absence of different instructions from the host TDS, some terminals will transmit in accordance with the message to standard NPG applicability given in Table 2.4.

Message No	Standard NPG	Other Applicable NPGs
J0.0, J0.2	1	-
J0.3, J0.4, J0.6	4	Composite A
J0.5	As required	All except 2, 3, 12, 13
J0.7	As required	All except 2, 3, 12, 13
J1.1	4	6, Composite A
J2.0	7	Composite B
J2.2, J2.3, J2.4, J2.5, J2.6	6	5, 27, 4, 7
J3.0, J3.1, J3.2, J3.3, J3.4, J3.5, J3.6, J3.7	7	Composite B
J5.4	7	29, Composite B
J6.0	7	Composite B
J7.0, J7.2, J7.3, J7.4, J7.5, J7.6, J7.7	7	Composite B
J7.1	7	Composite A
J8.1	7	Composite B
J9.0, J9.2	8	Composite A
J9.1	21	-
J10.2	8	21, Composite A
J10.3, J10.5, J10.6	8	Composite A
J12.0	9	19, 20, Composite A
J12.1, J12.2, J12.3, J12.4, J12.5	9	Composite A
J12.6, J12.7	9	19, 20, Composite A
J13.0, J13.2, J13.3, J13.5	6	5, 27, 8, 9, 10, Composite A
J14.0, J14.2	10	Composite B
J15.0	7	8, Composite B
J28.2(0)	As required	All except 2, 3, 12, 13
J31.0, J31.1	4	Composite A
J31.7	As required	All except 2, 3, 12, 13
MIDS Free Text (Voice)	12/13	-
MIDS Free Text (Non-Voice)	As required	All except 2, 3, 12, 13
RTT-A	2	5, 6, 27, 30
RTT-B	3	-
IJMS P1,P2,P3,N7-1	30	-
Other IJMS	31	-

Table 2.4 Message to NPG Applicability Table

2.2.2.1.6 In determining communication requirements to be supported by PGs, network designers should consider:

a. Message types to be exchanged within the functional areas to be supported.

b. Sources and destinations associated with each message type.

c. Limitations imposed by platform implementation levels.

d. Security requirements.

e. Operating restrictions which may be imposed.

2.2.2.2 Multinetting

2.2.2.2.1 Multinetting can be employed where two or more sub-communities of JUs can be identified, which have mutually exclusive communication requirements for particular functions. Each sub-community may utilise the same time slot blocks but on different nets. Each net is defined by a frequency hopping pattern which is determined by net number and cryptovariable. Multinets should not be used for PGs in which data exchange must take place freely throughout the network, e.g. PPLI PGs or RTT-A PG. The following guidelines apply:

a. Networks must be operated in Communications Mode 1 to allow multinetting.

b. A JU may be initialised to switch between PGs on different nets on a time slot by time slot basis but cannot be required to participate simultaneously on more than one net in any one time slot.

c. PG capacity allocations should be planned to allow JUs to communicate on a net when required without communication conflicts on other nets.

2.2.2.2.2 A specialised form of multinetting, known as Stacked Nets, may be used where the operator requires a degree of control over the channel number used. This form of multinetting applies specifically to the Voice and Control PGs, enabling the operator to switch between any channel numbers (0 to 126 inclusive) as operational requirements dictate. The RTT-B PG, although not strictly a stacked net PG, does use all assigned time slots for the PG in nets 0-15 inclusive; the terminal selects the net number automatically. To create a stacked net configuration, the allocation of time slots must be coordinated and is considered in paragraph 2.2.4.3.

2.2.2.2.3 Cryptonets should be established according to defined connectivity and security requirements. All planned participants required to communicate with each other must hold common cryptovariables, thus establishing a cryptonet. If a particular exchange of information should be restricted to a certain number of planned participants, then the network designer should assign a different MSEC cryptovariable for that exchange (providing the network is to be operated in Partitioned Variable Mode). Different cryptovariables can be assigned on a time slot basis, depending on the crypto mode to be used:

a. In the Common Variable Mode (CVM) a single cryptovariable is used to accomplish all necessary crypto-processing for a time slot.

b. In the Partitioned Variable Mode (PVM) crypto-processing for a time slot is performed by two different cryptovariables:

(1) TRANSEC cryptovariable for transmission processing, and

(2) MSEC cryptovariable for message processing.

Further guidelines on the definition of cryptonets are produced in Chapter 5.

2.2.2.2.4 Network designers should additionally consider the following factors when determining the number and distribution of cryptovariables:

a. Sensitivity of information to be exchanged.

b. Need-to-know access for participating JUs.

c. Cryptonet size limitations.

d. Terminal cryptovariable storage limitations.

2.2.2.2.5 Cryptovariable usage within a network design is identified by means of Cryptovariable Logical Labels (CVLLs), denoted by a number from 1 to 127. Network designers should produce tables detailing the association of CVLLs and Crypto Period Designators (CPDs) to Secure Data Unit (SDU) loading locations for each platform type. An example is given in Table 2.5, although it should be noted that it is not essential for each CVLL to be assigned two CPDs as shown here. The CPD defines which of the two cryptovariables, which may be allocated for each CVLL, applies to the current cryptoperiod. As a standard, CPD 0 should always be associated with SDU locations 0,2,4 and 6 and CPD 1 with SDU locations 1,3,5 and 7, as indicated in the Table. Note that if OTAR is to be used, SDU locations 4 and 5 must be reserved for that purpose. JUs can use SDU locations 4 and 5 for other key requirements when OTAR is not specified to be used in the network in which they intend to operate.

2.2.2.2.6 The CVLL/SDU loading plans should be distributed to crypto-custodians at relevant participating operational units. The cross reference between cryptovariables (by short title) and CVLLs is made during Pre-Mission Planning by the designated Cryptonet Manager and is promulgated to all units via the OPTASK LINK.

PLATFORM TYPE..		
CRYPTOVARIABLE LOGICAL LABEL	CRYPTOPERIOD DESIGNATOR (CPD)	SDU MEMORY LOCATION
CVLL 1	0 1	0 1
CVLL 2	0 1	2 3
CVLL 3	0 1	4 * 5 *
CVLL 4	0 1	6 7

* Reserved for OTAR, if implemented.

Table 2.5 Example of CVLL Loading Instructions

2.2.2.3 Establish Relay Requirements

2.2.2.3.1 Because MIDS operates at LOS frequencies, many operational scenarios will require the employment of relay to maintain the required connectivity among JUs. Network designers should anticipate the need for relay and make the necessary provisions within each network design.

2.2.2.3.2 Two relay methods are available for use in Link 16 networks as follows:

a. Paired Slot Relay.

b. Repromulgation Relay.

Of these, Paired Slot Relay is the primary method providing JUs with a relatively fixed, dedicated access relay capability as determined within the network design. Repromulgation Relay provides a secondary relay capability particularly suitable for multihop relay. In order to function as a relay unit for a net, a JU must be assigned the TRANSEC cryptovariable for that net. PVM can be used with paired slot relay to do "blind relay" where the relaying terminal does not have the MSEC cryptovariable and therefore cannot interpret the relayed information. PVM can also be used with Repromulgation Relay, but the relaying terminal must have the MSEC cryptovariable in order to interpret the repromulgation counter. Network Designers are cautioned that this combination of PVM and Repromulgation Relay would defeat the purpose of "blind relay".

2.2.2.3.2.1 Paired Slot Relay

a. Paired Slot Relay requires the assignment of relay capacity within the network design in the form of paired time slot blocks, one in which to receive information and one in which to retransmit. Each paired slot must be labelled according to the chosen relay function assigned to it. The relay function options available are:

(1) Main Net Relay - data are received in time slots allocated to PGs on the main net and retransmitted in the associated relay time slots also on the main net.

(2) Voice Relay - voice transmissions are received in time slots allocated to Voice Groups A or B on a specified net and are retransmitted in the associated relay time slots on the same net.

(3) Control Relay - control data are received in time slots allocated to the Control PG on a particular net and are retransmitted in the associated relay time slots on the same net.

(4) Zoom Relay - data are received in time slots allocated to PGs on the main net and are retransmitted in the associated relay time slots but on a different specified net.

(5) PG Relay - paired slot blocks must be annotated with the number of the PG in which the relay transmissions are to be made. Data are received in time slots allocated to the named PG on a designated net and retransmitted in the associated relay time slots within the same PG on the same or any other designated net.

(6) Directed Relay - performs in much the same way as PG Relay above but is not confined to a single PG.

The Main Net and Zoom relay functions utilise the same time slots and so will not be operated simultaneously.

b. Relay functions may be controlled using the following relay modes:

(1) Conditional - the relay function automatically becomes active only when that JU provides the best LOS coverage. The terminal utilises altitude and positional information contained in received PPLI messages to determine its relay potential relative to surrounding JUs. Conditional relay mode is applicable to Main Net, Voice and Control relay functions only.

(2) Unconditional - all valid messages are automatically retransmitted.

(3) Suspended - the relay function is temporarily suspended but the JU retains its relay time slot assignments.

c. The time slot blocks to be used for retransmission of relay data must be of the same size as the corresponding receive assignment and are defined by a fixed time offset, known as the relay delay.

d. Network designers must pre-plan probable relay requirements for a given scenario and allocate network capacity to suitable platform types. Factors which should be considered in determining platform types for relay are:

(1) Anticipated deployment, especially altitude.

(2) Mobility and permanence in any location.

(3) Nature and extent of network participation.

(4) Physical security requirements or vulnerability to compromise.

e. Network designers should always assess the requirement for paired slot relay to improve LOS connectivity between planned participants against:

(1) Overall demand for network capacity, and

(2) Anticipated ECM operating levels.

Paired slot relay quickly becomes expensive in terms of capacity as the number of relay hops increases. The requirement for relay should not be allowed to impact adversely upon the provision of capacity in essential functional areas. However, where high levels of ECM are anticipated, the provision of relay may greatly improve the quality of data exchange under these operating conditions.

2.2.2.3.2.2 Repromulgation Relay

a. Repromulgation relay provides a secondary relay capability which may be implemented where there is a requirement for multihop relay, or when paired slot relay is not available due to demand for network capacity. Repromulgation relay has the following operating characteristics:

(1) Conserves network capacity in a multihop relay environment.

(2) Requires no specific assignment of network capacity. Time slots for the retransmission of messages are "donated" by the originating JU.

(3) Requires no centralised control for normal operation.

(4) Requires no knowledge of connectivity or externally-supplied routing information, as messages cannot be relayed along a defined path.

(5) Incorporates a degree of overhead as each message designated for relay must be preceded by the Repromulgation Relay (J0.5) message. This message specifies the number of times the message is to be relayed and, by defining the delay between message receipt and retransmission, identifies the time slot donated for retransmission.

b. If there is a requirement to implement Repromulgation Relay, network designers should consider the need to donate time slots when determining time slot allocations. The network design should also specify appropriate settings for each planned participant for:

(1) Repromulgation Control parameter, set at either:

- Relay and Originate, or

- Relay only.

(2) Repromulgation Counter, to indicate number of repromulgation hops desired and set between 0 and 15.

Platforms can only participate in repromulgation relay if they have been initialised to do so.

2.2.3 Network Capacity Allocation

2.2.3.1 The second step in the design process is to identify the number of time slots, the net and cryptovariable that will be used for each exchange of information, taking into account the requirement for relay and receipt/compliance.

2.2.3.2 Network capacity is first allocated on a PG basis. The Initial Entry PG is a fixed assignment shared by all terminals. In addition to this, a terminal is capable of accepting transmit time slot block assignments (up to a maximum of 64 blocks) for up to 31 different PG index numbers in the range 2 - 511.

2.2.3.3 Network designers should initially allocate capacity to those PGs which must be implemented by all JUs (as identified in Table 2.4). The capacity requirements for these PGs should be fairly static. Remaining capacity is then allocated among those PGs where capacity requirements will vary depending on the tactical operations to be supported. Capacity allocations made at this stage for each PG should be based on worst case aggregates for all JUs.

2.2.3.4 PG capacity requirements should be calculated as a function of:

a. Transmission requirements of individual platforms requiring PG participation, to meet data throughput and message response time requirements.

b. Requirement for relay within the PG.

c. Chosen access mode (see paragraph 2.2.3.5 below).

d. Requirement for receipt/compliance.

e. Upper limit defined for message packing.

f. Additional considerations for Voice PGs are:

(1) Voice rate.

(2) Requirement for error coding.

2.2.3.5 Use of Access Modes

The access mode chosen for each PG will be a significant factor in determining the total number of time slots required for that PG. The access modes available provide different benefits but each has its own disadvantage, as discussed below.

2.2.3.5.1 Dedicated Access Mode

Dedicated Access mode is used when it is essential that transmissions from one JU do not conflict with those from another JU. This requirement may arise because the messages in that PG are likely to be operationally critical and they must be given the best probability of successful reception. The transmission requirements of the JU should be reasonably constant over time. This access mode is the most expensive mode in terms of numbers of time slots required. National peacetime operating restrictions (see Volume 3) will in most cases require time slot assignments to be operated in Dedicated Access mode.

2.2.3.5.2 Dedicated Reuse

Dedicated Reuse is a special use of the Dedicated Access mode in which the same time slots are assigned to more than one JU. Dedicated Reuse relies on the MIDS ability to “capture” the transmission from the closest terminal if more than one terminal transmits in the same time slot. When allocating network capacity for Dedicated Reuse, the network designer should consider the assignments as a pool. Dedicated Reuse is the normal method of assigning Voice capacity. It should also be used:

a. When only the closest transmitting JU is of interest to the receiving JU. This will normally occur when geographical separation with other JUs in the Dedicated Reuse “pool” is such that JUs do not directly communicate with one another or with a common third JU using these assignments (used in non-LOS, geographically stable situations). The size of the time slot allocation for the Dedicated Reuse “pool” (other than for MIDS voice) will depend on the number of transmission time slots required by the JU with the largest transmission requirement.

b. When the requirement to transmit in Dedicated Access assignments will be infrequent and therefore contention is unlikely. This use of Dedicated Access may result in all or some JUs having more time slots available for transmission than would be strictly necessary to accommodate the message traffic originated by those JUs in that PG. If there are few messages to transmit, the terminal would automatically reduce the packing structure. This would lead to the inefficient packing of messages in time slots, with the consequence that the terminal would transmit in more time slots than necessary. Thus contention could be high. In determining the size of the time slot allocation for the Dedicated Reuse “pool” (other than for MIDS voice), the network designer should consider the following factors:

   (1) The number of JUs needing to transmit.

   (2) Each JU’s transmission requirements (remembering that the JU will be authorised to transmit in every time slot).

   (3) The proximity of each receiving JU to the transmitting JU or JUs which are of interest.

2.2.3.5.3 Contention Access Mode

Contention Access mode is a special form of time slot reuse and is particularly useful when a JU has a need to communicate at a high rate with nearby JUs but can tolerate a slower rate with more distant units. As in Dedicated Reuse, more than one JU is assigned to operate in a pool of time slots. However, in Contention Access mode each JU is assigned a specific number of transmission “opportunities” per time period, defined by access rate, and selects time slots for transmission at random from the pool. This results in a greater probability, when compared with Dedicated Reuse, that messages from more distant JUs will be received because the closer JUs will not be transmitting in some time slots. Contention Access mode should be used only when it is acceptable that the probability of message reception in perfect connectivity conditions is less than 100 per cent.

2.2.3.5.4 Time Slot Reallocation (TSR)

TSR is an access method which allows JUs to share a predefined pool of timeslots. JUs are allocated capacity dynamically, according to their current demands. TSR is designed to avoid time-slot reuse. TSR allows a variable number of JUs to share the TSR pool and entry to and exit from the TSR community is automatic. TSR should be used when either the number of JUs in a PG community may vary (e.g. the Control PG) or when the demands of the JUs within a PG community will vary (e.g. the Surveillance PG) or both. Although TSR will ensure a 100 per cent probability of message reception in conditions of perfect connectivity and no overload, it must be accepted that this probability may be reduced in unfavourable conditions.

2.2.4 Terminal Assignment

2.2.4.1 The third step of the design process involves assigning the time slot allocations from step two to specific terminals. These terminals will be assigned to transmit, receive or relay in these time slots by terminal initialisation parameters. A terminal will automatically receive messages in time slots not assigned for transmission or relay on the default net and cryptovariable (as defined by initialisation data). If message reception is required on another net or using a different cryptovariable, specific receive assignments must be made. At the completion of this step, initialisation parameters will have been developed for every terminal required to operate in the network.

2.2.4.2 A total of 98,304 time slots are available per epoch, divided into three sets (A, B and C). Each set contains 32,768 time slots per epoch and is interleaved with the other sets so as to be evenly distributed throughout the epoch. Time slots are uniquely identified by set and time slot index number, beginning with A-0, B-0, C-0, A-1...... through to A-32,767, B-32,767, C-32,767. Network designers must assign time slots to planned participants in time slot blocks, which are sized by an integer power of 2. A time slot block assignment is made by identifying the first time slot in the block by set and time slot index number, and by defining the recurrence rate number (RRN), where the RRN represents log2 of the number of time slots in the time slot block. Therefore an assignment of A-0-6 represents 64 time slots per epoch; one slot per 12 seconds. This particular assignment is always reserved for Initial Entry. Individual time slot requirements can be met by assigning multiple blocks. For example, a requirement for 20 time slots per 12 seconds may be satisfied by the assignment of a block of 16 plus a block of 4. A frame is defined as 1/64th of an epoch or 12 seconds. There are 1536 time slots per frame. Because the frame includes the message response time for most messages, the frame is normally used as the time interval in which to schedule time slot assignments. That is, time slots are calculated in terms of time slots/frame up to a maximum of 1536 time slots for a network.

2.2.4.3 Where a stacked net configuration is to be incorporated into the network design, time slot blocks will be allocated with the same set, time slot index number and recurrence rate number. This allows net utilisation to be under operator control through channel selection.

2.2.4.4 Time slot block assignments should be produced for each platform or platform type as required. Each assignment should be defined by the time slot assignment parameters listed at Table 2.6 and identified by a form of notional reference. This facilitates the allocation of time slot assignment sets to specific platforms during Pre-Mission Planning. Network designers should consider the viability of developing a standard set of time slot block assignments within a network design for those platforms which have similar requirements. Such a practice would considerably simplify both the design and the initialisation processes.

Parameter	Range of Allowable Values
Participation Group Index No.	2 - 511 (1 = Initial Entry which is a fixed assignment for all terminals.)
Time Slot Block Definition	
Set	A, B or C
Time Slot Index No.	0 – 32767
Recurrence Rate	0 – 15
Net No.	0 - 127 (127 = No Statement - only valid for stacked Nets)
Time Slot Block Usage	
Relay/Time Slot Indicator	Time Slot
Time Slot Type	Transmit or Receive
Access Mode	Dedicated, Contention or TSR
Access Rate	0 -15 (only for Contention Access)
Crypto Mode	Common or Partitioned
TRANSEC Cryptovariable	CVLL No.
MSEC Cryptovariable	CVLL No.
Relay Delay Switch	Offset Delay
Relay Delay	6 – 31
Relay net, receive	0 – 127
Original transmit net	0 – 127
Relay Time Slot Block Usage	
Relay/Time Slot Indicator	Relay Slot
Relay Function	Main Net , Voice, Control, Zoom, PG or Directed
Relay Control	Conditional, Unconditional or Suspended
Relay Delay	6 - 31
Net Number, transmit	0 – 127
Crypto net relay	Yes or No
Crypto Mode	Common or Partitioned
Decrypt Indicator	Decrypt or Do Not Decrypt
Original transmit net	0 – 127
End-to-End relay delay	6 – 31
TRANSEC cryptovariable	CVLL No.

Table 2.6 Time Slot Block Assignment Parameters

2.2.4.5 General Time Slot Assignment Rules

Detailed rules on the technical validity of time slot block assignments are not included in this document. However, there are a number of general rules which network designers should observe when developing time slot block assignments for each JU planned to participate in a network. These general rules are:

a. The time slot assignments must be capable of passing the terminal validity checks.

b. No terminal can operate on more than one net per time slot.

c. Time slot assignments for the Voice and Control PGs should be in the form of stacked nets whenever possible.

d. Individual allocations should consist of the minimum number of time slot blocks. Time slot requirements should be based upon message transmission requirements per frame. (When dynamic re-assignment of time slots would be facilitated by a network design in which individual allocations consisted of more time slot blocks than the minimum, the network designer should attempt to achieve a satisfactory balance between the two requirements).

e. The use of different access modes and the desired time slot packing structure will impact the size of time slot assignments and must be considered.

f. Time slots are assigned in blocks sized to the power 2 and defined by set, time slot index number and RRN. Multiple time slot blocks may be assigned to meet individual platform requirements.

2.2.4.6 Use of the Initial Entry Message

2.2.4.6.1 Network designers should consider the operational requirement for new JUs which have no explicit time slot assignments to be able to join the network and participate immediately in the following PGs:

a. PPLI PGs.

b. RTT-B PG.

c. Control PG.

d. Voice PGs.

2.2.4.6.2 Network designers should note that, while it is desirable, it is not necessary to tailor the time slot assignments for all these PGs to conform with their definition in the Initial Entry Message; each PG should be considered individually. The use of the Initial Entry Message for this purpose will reduce the reliance on the Network Manager for dynamic time slot management.

2.2.5 Network Parameter Assignment

The fourth step involves making assignments and choosing values for network level system parameters which must be given the same or compatible values for every terminal in the network. These parameters define the operating characteristics of the network. For example, all terminals must choose the same range mode and only one terminal in the network may be initialised as NTR. The choice of these parameter values, therefore, is a system-level design decision and should be dealt with at that level rather than addressing, for example, the choice of range mode on a terminal by terminal basis.

2.2.6 Individual Terminal Parameter Assignment

In the final step, the network designer transfers network parameter choices to initialisation parameter values for each individual terminal and then completes the selection of values for each terminal for those parameters which affect individual terminals only, not the entire network.

2.2.7 Network Design Validation

Completed designs are subject to validation. Networks should be validated to the highest possible level which can be achieved with the available validation environment, however the lowest acceptable level of validation prior to operational use is level 2. Each network design has to indicate the validation status as listed in Table 2.7.

Level 1	Machine Validation: If the design tool produced it, it must work because the tool has been validated.
Level 2	Designer Validation: The designer reviewed the tool output and is satisfied that it will work as designed.
Level 3	Load Validation: The individual terminal load files, after designer validation, were checked by loading into a terminal to ensure that the terminal would accept them.
Level 4	Simulation Validation: After load validation, the network design was validated in a “scenario” simulation by a computer simulator and/or a multi-terminal ground test rig.
Level 5	Operational Use Validation: The network has been used and has been found to meet originally stated requirements.

Table 2.7 Approval Levels*

*Approval levels are to be used as a general guide between NDF’s to indicate network validation. Each NDF should still perform its own validation checks and tests.

2.3 DISTRIBUTION AND MAINTENANCE OF NATO NETWORK DESIGNS

2.3.1 Configuration Control of Link 16 Network Designs

NDFs are responsible for the configuration control of all network designs originated by that NDF. Configuration control of Link 16 network designs encompasses the following procedures:

a. The NDF must maintain a library of all network designs produced by that NDF.

b. The network library should contain, as a minimum, master and back-up copies of each network design under separate storage arrangements.

c. The NDF must maintain a record of the version status of each network design produced and should record details of any updates made.

d. The NDF must maintain a distribution record for each network design and is responsible for ensuring that every unit holding a particular network design receives all subsequent updates to that design.

2.3.2 Network Design Libraries

Libraries of NATO Link 16 network designs should be maintained as follows:

a. The NATO NDF will maintain a master library of all completed NATO network designs.

b. MSCs will maintain regional network libraries, containing all networks designed to meet regional network requirements.

c. Sub-libraries will be maintained at all units supporting Link 16-equipped platforms.

2.3.3 Network Description Summaries

2.3.3.1 A Network Description Summary (NDS), which is a description of the operational and essential technical characteristics of the network, will be issued by the originating NDF with each network design, to facilitate selection and modification of networks during the Pre-Mission Planning process. An example NDS is given in paragraph 2.3.3.3. This format may be modified to meet the full requirements of individual nations and situations. However, it should contain, as a minimum, the following:

a. Network Name. The network name provides a unique network design identifier in accordance with the network naming convention as described in paragraph 2.1.6.

b. Executive Summary. The executive summary provides sufficient information to give a full description of the primary operational and technical characteristics of the network.

c. Connectivity Matrix. A connectivity matrix provides a clear overview of all network connectivity parameters per time slot group. It reflects the connectivity provided to fulfil the Information Exchange Requirements (IERs) and should, as a minimum, include the following parameters: TSEC, MSEC, net number, Access Mode, packing limit, NPG, time slots per frame per unit and total slots per frame. The connectivity matrix should specify per JU and slot group whether it transmits, receives or relays.

d. Network Time-Line. The network time-line illustrates the proportion of time slots allocated to each NPG per net within a frame. The time-line should also specifiy any time slots not used.

e. Crypto Load Map. The crypto load map assigns CVLLs to SDU locations for each JU in the network. SDU LOCATIONS MAY BE PAIRED TO ALLOW ROLLOVER.

f. Time Slot Duty Factor (TSDF). The TSDF calculations represent the assessed network TSDF and individual platform TSDFs. The standardised method of calculation of the Platform TSDF is described in the paragraph 2.3.4.

g. The Validation Level in accordance with Para. 2.2.7 to which the Network has been validated.

2.3.3.2 NDSs should be compiled in the form of library catalogues for the use of network designers and users, as follows:

a. A comprehensive catalogue of NDSs for all network designs produced should be maintained and controlled by the NDF and distributed to the relevant formations.

b. A master catalogue of NDSs for all completed NATO network designs should be held at each MNC.

2.3.3.3 Example of a Network Description Summary

1. Network Name: UFUP0007B

2. Executive Summary:

2.1 Introduction. Network UFUP0007B is intended to support UK JTIDS platforms detached to Denmark. The network supports IJMS assignments and a modified version of the Link 16 portion of the Net 3 assignments of the NATO-wide network NANP01AV0. UK participants should note that this network operates in Exercise IPF Override in order to utilise the higher packing levels allowed under the Danis Frequency Clearance Agreement.

2.2 Participants. The network supports the following participants:

- 8 x Tornado F3.
- One E-3D.
- One NATO C^2.
- One E-3 IJMS H/O.
- 4 x NADGE IJMS DLBs.
- 8 x NATO Fighters (the assignments contained in the NATO network are reserved for any type of JTIDS equipped fighter that may operate in ACE).

2.3 Description. The network incorporates NPGs for Network Management (NM), PPLI-A and -B, Surveillance (SURV), Mission Management (MM), Control (CTR), Residual, 2.4 and 16 Kb/s Voice and IJMS. The network default net is Net 3. This NATO network does not support an RTT NPG so to achieve synchronisation, the terminal will transmit RTT messages in lieu of PPLI messages in NPGs 5 and 6 when required. To achieve synchronisation between a mixture of Class 1 and Class 2 units, a Class 2 unit acting as NTR transmits the Link 16 Initial Entry Message and an IJMS N7-! Net Entry Aid in alternate frames in time slot A-0-6 on Net 0. Therefore, NADGE units must initialise their terminals to receive this time slot block. A Class 1 unit acting as Master transmits the N7-1 message in time slot A-0-6 also but on its Main Net, in this instance Net 3, not the Link 16 default net (Net 0).

2.4 Relay Platforms. There are no relay platforms.

2.5 Surveillance Capacity. The overall Surveillance time slot pool support approximately 125 track reports. The allocated IJMS track capacity supports approximately 225 tracks. The Link 16 Surveillance pool is divided between the E-3D and NATO C^2. The IJMS Track pool may be allocated wholly or partially to the E-3A (IJMS) and/or the E-3D.

2.6 Voice. Both 16 Kb and 2.4 Kb Voice are included.

2.7 Crypto. The network design incorporates Common Variable Mode for all platforms.

2.8 Range Mode. The Range Mode is Normal.

2.9 IPF Override. The IPF Override is Exercise.

3. Connectivity Matrix

			Slot Gp	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
			TSEC	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
			MSEC	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
			Net No	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
			NPG	NM	PPLI A	PPLI A	PPLI B	SUR V	MM	CTR	CTR	CTR	VA	VB	RES	RES	P	Th	Th	Th	Th
			NPG No	4	5	5	6	7	8	9	9	9	12	13	29	29	30	31	31	31	31
			Packing	P2SP	P2SP	P2SP	P2SP	P4	P2SP	P2SP	P2SP	P2SP	STD	P2SP	P2SP	P2SP	STD	STD	STD	STD	STD
			Access	D	D	D	D	D	D	D	D	D	DSR	DSR	D	D	D	D	D	D	D
			S/F/U	2	8	4	1	32	8	8	8	4	64	224	8	4	1	160	64	32	8
		No.	S/F	4	64	32	2	64	16	16	64	32	64	224	8	4	54	160	128	64	8
Row	Functional Groups	Units	Pool	4	64	32	2	64	16	16	64	32	64	224	8	4	54	160	128	64	8
1	Tornado F3	8		R	T						T		T	T			T/R		R	R	
2	E-3D	1		T			T	T	T	T			T	T	T		T/R	T	R	R	R
3	NATO Ftrs	8		R	R	T/R	R	R	R	R	R	T/R	T	T			T/R				
4	NATO C^2	1		T			T	T	T	T			T	T		T	T/R		R	R	R
5	E-3 IJMS H/O	1											T				T/R	R			
6	NADGE DLBs	2											T				T/R	R	T		
7	NADGE DLBs	2											T				T/R	R		T	
8																					

T = Transmit
R = Explicit Receive
T/R = Transmit and Explicit Receive
Y = Relay
Relay Prefix Identifiers
C = Control
M = Main Net
P = Participation group
V = Voice
Relay Suffix Identifiers
U = Unconditional
C = Conditional
S = Suspended

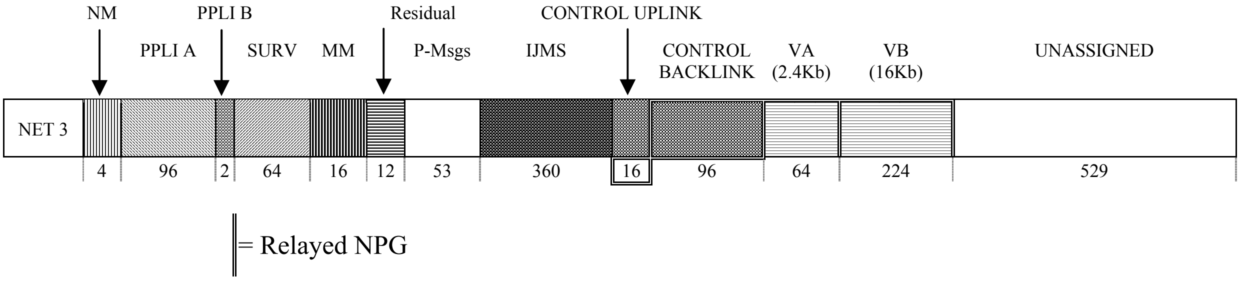
Packing:
STD = Standard
P2SP = Pack 2 Single Pulse
P2DP = Pack 2 Double Pulse
P4 = Pack 4 Single Pulse
Access:
D = Dedicated
DR = Dedicated Sol Reuse

S/F/U = Slots per frame per unit
S/F = Slots per frame

Notes:

1. N/a.
2. GE and AEW P-messages is a reuse pool on different nets for all operating within the area of ACE.
3. This can be any type of JTIDS equipped fighter that may operate in the Ace area.
4. Surveillance Pool is divided between the E-3D and NATO C^2.
5. Surveillance Pool caters for between 125 – 180 tracks.

4. Network Time-Line



5. Crypto Loading Map

Participant/Unit	SDU Cryptovariable Locations			
	0/1	2/3	4/5	6/7
Tornado F3 E-3D NATO C^2 E-3 IJMS H/O NADGE IJMS DLBs	CVLL 1 CVLL 1 CVLL 1 CVLL 1 CVLL 1			

6. Time Slot Duty Factor

6.1 The table below shows the TSDF for each platform within the network. This is calculated as the sum of all transmit time slot block assignments per platform, taking into account the packing level for each NPG, including relay assignments but excluding any voice assignments. To calculate the total TSDF per platform, the additional TSDF loading for Voice A and/or Voice B must be included as appropriate. The TSDF loading for a platform initialised to relay voice will be increased by the appropriate additional Voice TSDF when relaying another platform's Voice transmissions.

Participant	TSDF % (Without Voice)	Remarks
Tornado F3	1.11%	
Sentry E-3D	15.82%	
NATO Ftrs	0.59%	
NATO C^2	5.15%	
E-3 IJMS H/O	0.59%	No Voice B
NADGE DLBs	4.23%	No Voice B
NADGE DLBs	2.15%	No Voice B

Additional TSDF for Voice A (%)	4.17
Additional TSDF for Voice B (%)	14.58

Example:

Tornado F3 transmitting Voice B = 1.11% + 14.58% = A Total TSDF of 15.69%.
Sentry E-3D transmitting Voice B = 15.82% + 14.58% = A Total TSDF of 30.40%.
NADGE DLBs transmitting Voice A = 4.23% + 4.17% = A total TSDF of 8.40%.

6.2 The assessed Network TSDF is 66.67/34.57

7. Network Validation Level: 2

2.3.4 <u>Standardised Method of Platform TSDF Calculation</u>

2.3.4.1 Introduction

This paragraph proposes a standardised method for the calculation of Time Slot Duty Factor (TSDF) for individual platforms. Because nations have different frequency restrictions, it is incumbent on the planner, when calculating geographic area TSDF, to refer to the national annexes for specific variations, if any, from the method presented below.

100 percent TSDF is defined as a maximum of 396,288 pulses transmitted over a 12-second frame of 1536 time slots. This procedure steps through the process of calculating a platform's TSDF. The calculation method that follows is an agreed standard among the Network Design Facilities. The purpose of this calculation method is to facilitate the sharing of network design information, such that the NDF receiving the network will understand how the designed value for TSDF was derived. This procedure steps through the process of

calculating a platform's TSDF via the use of examples. These examples will illustrate the methods used for all access modes (such as dedicated, contention), and functions (relay, NTR, NETE), that the platform/terminal is operating in for each slot group. Throughout this procedure the connectivity matrix in Table 2.8 will be used as an example network.

2.3.4.2 Definitions

2.3.4.2.1 Total Pulse Density

a. To calculate the platform TSDF all transmitted pulses are added together:

b. (Total dedicated, T_d) + (Total contention, T_c) + (Total relay, T_r) + (T_{NETE}) + (Total Options, T_O) + (Total Voice, T_v) = (T_{dcrnov})
i.e., (T_d) + (T_c) + (T_r) + (T_{NETE}) + (T_O) + (T_v) = (T_{dcrnov})

2.3.4.2.1 Packing Limits

For the remainder of this procedure, the packing limits are defined as follows:

Packing Limit	Pulses per Time Slot
STD or P2SP	258 pulses
P2DP or P4	444 pulses
RTT-A and RTT-B (NPG 2 and 3)	72 pulses

Slot Group				1	2	3	4	5	6	7	8	9	10
NPG Name				RTT-A	RTT-B	PPLI-A	PPLI-B	PPLI-B	PPLI-B	RELAY	SURV	RELAY	SURV
NPG Number				2	3	5	6	6	6	TY	7	TY	7
Net Number				0	0	0	0	0	0	0	0	0	0
TSEC Variable				1	1	1	1	1	1	1	1	1	1
MSEC Variable													
Access Mode				D	4	D	D	8	D		D		D
Packing Limit						P2SP	P2SP	STD	P2SP		P2DP		P2DP
Per Unit Slots/Frame				1		4	2		1				32
Total Slots/Frame				10	8	40	20	96	24	24	112	112	64
Participant ID	NETE	Default Net	User Seq Number	Connectivity									
1. SHIP(1)/6	Y	0	1-6	R	T		R	R	T/R	Y	O	Y	R
2. E2C(1)/2	Y	0	1-2	R	T		R	R	T/R	Y	O	Y	R
3. E3(1)	Y	0	None	R	T		R	R	T/R	Y	R	Y	T/R
4. PAT_ICC(1)/2	Y	0	None	R	T		R	R	T/R	R	R	R	R
5. THAAD(1)/2	Y	0	None	R	T		R	R	T/R	R	R	R	R
6. F14D(1)/4	Y	0	1-4	R	T	T/R	T/R	R	R	R	R	R	R
7. FA18(1)	Y	0	None	R	T	R	R	R	R	R	R	R	R
8. F15(1.1.1)	Y	0	None	R	T	R	R	T	R	R	R	R	R
9. TAOM/2	Y	0	None	R	T		R	R	T/R	R	R	R	R
10. ADCP/2	Y	0	None	R	T		R	R	T/R	R	R	R	R
11. NATO_E3(1)	Y	0	None	R	T		R	R	T/R	Y	R	R	T/R
11. F3(1)/6	Y	0	None	T/R	R	T/R	T/R	R	R	R	R	R	R
12. GE-PAT(1)	Y	0	None	T/R	R		R	R	T/R	R	R	R	R
13. DDG_CASSARD(1)	Y	0	1	T/R	R		R	R	T/R	R	O	R	R
14. PA CDG(1)	Y	0	1	T/R	R		R	R	T/R	Y	O	Y	R

Table 2.8 Connectivity Matrix

LEGEND:

T= Transmit
D= Dedicated Access
S/F/Unit = Slots Per Frame Per Unit
Y= Relay Transmission
Y (NETE Column) = Yes

R= Receive
R (in Access Mode row) =DSR= Dedicated Access With Slot Reuse
S/F Total = Slots Per Frame Total For NPG
O= Design File Options Contain Transmit Assignments

Slot Group				11	12	13	14	15	16	17	18	19	20
NPG Name				SURV	M-M	A/C-U	A/C-B	A/C-B	F/F	F/F	F/F	VOICE-A	RELAY
NPG Number				7	8	9	9	9	19	19	20	12	TY
Net Number				0	0	127	127	127	0	0	0	127	127
TSEC Variable				1	1	1	1	1	1	1	1	1	1
MSEC Variable													
Access Mode				D	D	R	9	D	D	14	14	R	
Packing Limit				P2DP	P2DP	P2SP	STD	P2SP	P2SP	P2SP	P2SP	P4	
Per Unit Slots/Frame				16	8								
Total Slots/Frame				96	128	16	96	64	64	160	96	112	112
Participant ID	NETE	Default Net	User Seq Number	Connectivity									
1. SHIP(1)/6	Y	0	1-6	R	T/R	T	R	R		R		T	VY
2. E2C(1)/2	Y	0	1-2	R	T/R	T	R	R		R		T	VY
3. E3(1)	Y	0	None	T/R	T/R	T	R	R				T	VY
4. PAT_ICC(1)/2	Y	0	None	T/R	T/R								
5. THAAD(1)/2	Y	0	None	R	R								
6. F14D(1)/4	Y	0	1-4	R	R	R		O	O	R		T	VY
7. FA18(1)	Y	0	None	R	R	R	T		R	T	T	T	VY
8. F15(1.1.1)	Y	0	None	R	R	R	T		R	T	T	T	R
9. TAOM/2	Y	0	None	T/R	T/R	T	R	R				T	VY
10. ADCP/2	Y	0	None	R	R							T	R
11. NATO_E3(1)	Y	0	None	T/R	T/R	T	R	R				T	VY
11. F3(1)/6	Y	0	None	R	R	R	T		R			T	VY
12. GE-PAT(1)	Y	0	None	R	R								
13. DDG_CASSARD(1)	Y	0	1	R	T/R	T	R	R				T	VY
14. PA CDG(1)	Y	0	1	R	T/R	T	R	R				T	VY

Table 2.8 Connectivity Matrix (continued)

LEGEND:

T= Transmit
D= Dedicated Access
S/F/Unit = Slots Per Frame Per Unit
Y= Relay Transmission
Y (NETE Column) = Yes

R= Receive
R (in Access Mode row) =DSR= Dedicated Access With Slot Reuse
S/F Total = Slots Per Frame Total For NPG
O= Design File Options Contain Transmit Assignments

2.3.4.3 Pulse Count Calculation per Slot Group and Access Mode

2.3.4.3.1 Dedicated Access

The TSDF calculation for an individual platform assigned time slots using dedicated access is the product of the number of time slots assigned for transmission (TS) and the number of pulses associated with the packing limit assigned to the slot group (SG).

(T_d)= (TS) x (72 or 258 or 444 pulses) = Pulses in Dedicated Access.

Example:

Ship (1) TSDF for Slot Group 6, 12, and 13
Ship (1) = (1 ts) x (258 pulses) = 258 pulses for (SG 6)

These steps are repeated for every SG in which the platform is assigned transmission time slots. The results are added together to obtain the total number of pulses transmitted in dedicated access by this platform.

Platform (n) = (SGn) + (SG $_{(n + 1)}$) + …+ (SG$_{(n\ )}$) = (T_d)

Ship (1) = (1 ts) x (258 pulses) = 258 pulses for (SG 6)
= (8 ts) x (444 pulses) = 3552 pulses for (SG 12)
= (16 ts) x (258 pulses) = 4128 pulses for (SG 13)
Total Dedicated:
Ship (1) = (258 pulses) + (3552 pulses) + (4128 pulses)= (T_d) = 7938 pulses

Surveillance options will be discussed later within this document.

2.3.4.3.2 Relays

When relays are assigned they are handled as dedicated access transmission time slots, irrespective of the relay mode (unconditional, conditional, suspended) that is being performed. The calculation of TSDF for repromulgation relay assignments has not yet been agreed amongst the NDFs. Accordingly, reference should be made to the specific national annexes.

For relay TSDF, use the number of Total Slots/Frame assigned for relayed transmission (TS), for each active platform assigned the relay function, multiplied by the number of pulses associated with the packing limit assigned to the relayed slot group, (258 or 444 pulses). In connectivity matrix notations where there is a Per Unit Slots/Frame requirement, then the number of time slots/frame assigned for the relayed transmission (TS) should be equal to the number of transmitters in the original transmit slot group or relay receive slot group multiplied by the Per Unit Slots/Frame requirement. For example, in slot group 6, while 24 time slots are assigned, there are only 21 units that could use the time slots, at one slot per frame per unit. Therefore, only 21 slots will be relayed in slot group 7.

Platform (n) (T_r) = (TS) x (258 or 444 pulses) = Pulses for assigned relay time slots.

Example:

Ship (1) TSDF for Slot Groups 7 and 9 (voice relay will be discussed later).
Ship (1) = (21 ts) x (258 pulses) = 5418 pulses for (SG 7)

These steps are repeated for every SG in which the platform is assigned relay transmission time slots. The results are added together to obtain the total number of pulses transmitted in relay by this platform.

Platform (n) = (SGn) + (SG $_{(n+1)}$) + …+ (SG$_{(n)}$) = (T$_r$)
Ship (1) = (21 ts) x (258 pulses) = 5418 pulses for (SG 7)
= (112 ts) x (444 pulses) = 49728 pulses for (SG 9)
Total Relay:
Ship (1) (T$_r$) = (5418 pulses) + (49728 pulses) = 55146 pulses

2.3.4.3.3 Contention Access

For the remainder of this procedure Table 2.9 is used. This table presents access codes, rates, and equivalent slots/frame values for use when using contention access.

Contention Access Codes		
Value	**Access Rate**	**Equivalent Slots/Frame**
0	1 per 48 sec	1
1	2 per 48 sec	1
2	3 per 48 sec	1
3	2 per 24 sec	1
4	3 per 24 sec	2
5	2 per 12 sec	2
6	3 per 12 sec	3
7	4 per 12 sec	4
8	6 per 12 sec	6
9	8 per 12 sec	8
10	12 per 12 sec	12
11	16 per 12 sec	16
12	20 per 12 sec	20
13	26 per 12 sec	26
14	32 per 12 sec	32
15	64 per 12 sec	64

Table 2.9 Contention Access Codes

TSDF for an individual platform assigned time slots using contention access shall be calculated by determining the number of equivalent transmission time slots per frame that corresponds to the access code (AC). The access code is the numerical value entered in the 'Access Mode' row of the connectivity matrix. Multiply the number of timeslots associated with the given AC by the number of pulses associated with the packing limit assigned to the slot group (72, 258 or 444).

Platform (n) (T$_c$)** = (TS) x (72, 258 or 444) = Pulses for assigned time slots.

** There are some special considerations in the calculation of contention access for F-18s, and they are described after the following example.

FA18(1) = (access code (9) = 8 Equivalent slots/Frame) x (258) =
(8ts) x (258 pulses) = 2064 pulses for (SG 14)

These steps are repeated for every SG in which the platform is assigned contention access transmission time slots. The results are added together to obtain the total number of contention pulses transmitted by the platform.

Platform (n) (T_c) = (SGn) + (SG (n + 1)) + …+ (SG(n))

FA18(1) = (access code (9) = 8 Equivalent slots/Frame) x (258) =
(8ts) x (258 pulses) = 2064 pulses for (SG 14)

FA18(1) = (access code (14) = 32 Equivalent slots/Frame) x (258) =
(32ts) x (258 pulses) = 8256 pulses for (SG 17)

FA18(1) = (access code (14) = 32 Equivalent slots/Frame) x (258) =
(32ts) x (258 pulses) = 8256 pulses for (SG 18)

Total Contention:
FA18(1) = (2064) + (8256) + (8256) = 18576 pulses

2.3.4.4 Special Considerations

2.3.4.4.1 RTT-A and RTT-B

For both NPG 2 (RTT-A) and NPG 3 (RTT-B), the worst case scenario is used, i.e., the total number of time slots that are possible for transmission by the platform is assumed, even though as an NTR or NETE, all assigned time slots may not be used. At the design level, the network designer does not know which platform will be assigned duties as the NTR. Before reception of the OPTASK LINK, all units are considered as potential NTR, NETE, and main net relays. Therefore, the designer picks the worst case for RTT-A computation, that is, the packing limit of 72 multiplied by the number of active participants or the total number of TS per frame, which ever is greater. For RTT-B, the calculation is the packing limit of 72 times the number of time slots in the contention pool, regardless of access code. At the operational level, a network manager will have knowledge of the platform assigned as the NTR. Thus, the network manager can use the more definitive operational level computation of RTT-A and RTT-B as described in Appendix A.

2.3.4.4.2 Time Slot Reallocation (TSR)

When calculating pulse density for platforms transmitting in a TSR pool, the total number of time slots assigned to the pool is multiplied by the packing limit, and is then multiplied by either 22% or 60%. The demand limit default value is 22%, and if the Demand Limit Override bit is set in the network design, the demand limit is set at 60%. So for an assigned pool of 96 timeslots at a standard packing limit, with the demand limit override bit set to zero (default - 22%), the calculation is:

$T_{C[tsr]}$ = (96ts) * (258 pulses) * 0.22 = 5449 pulses

2.3.4.4.3 Platform Specific

For national platform specific variations, refer to the appropriate National Annexes.

2.3.4.4.4 Net Entry Transmit Enable (NETE)

NETE is a special case. A platform participating as an NETE is indicated with a 'Y' for ‘Yes' in the NETE column of the connectivity matrix. The NTR transmits the net entry message every 12 seconds in a standard double pulse time slot structure. Platforms assigned as NETEs or Main Net Relays will transmit the net entry message at an average rate of once every 24-second in a contention mode. A platform assigned to be an NTR shall add 258 pulses to their total pulse count, (T_{NTR}). All platforms assigned to be an NETE or operating as a Main Net Relay shall add 258 pulses to their Total pulse count, (T_{NETE}). This issue affects the total network pulse density more than an individual platform pulse density.

Platform (n) = (258) = (T_{NETE}) (where n = User Sequence Number)

Ship(2) = 258 pulses = (T_{NETE})

2.3.4.4.4 5 Options

Surveillance, Control (Air Control Backlink), and NC2 to NC2 option pools are handled using the procedures that follow. When dealing with options, separate matrices for SURV, Control, and NC2 to NC2 are created presenting assigned time slots for all combinations of options and Seq. No. Examples are presented in Tables 2.10, 2.11 and 2.12. The pulse density for the option pool matrix will be calculated using the dedicated access procedures discussed earlier.

	Seq No. 1	Seq No 2	Seq No 3	Seq No ……….
OPTION 1	64	16	16	4
OPTION 2	80	16	8	4

Table 2.10 Surveillance (NPG 7) Options pool time slot assignments

	Seq No. 1	Seq No 2	Seq No 3	Seq No 4
OPTION 1	32	32		
OPTION 2	16	16	16	16

Table 2.11 Control (NPG 9) Options pool time slot assignments

	Seq No. 1	Seq No 2	Seq No 3	Seq No 4
OPTION 1	32	32		
OPTION 2	16	16	16	16

Table 2.12 NC2 to NC2 (NPG 19) Options pool time slot assignments

When calculating total pulses for a platform, the Options/Sequence Number combination that has the highest value is used. For example, when calculating pulses for a unit participating in the surveillance NPG, Table 2.10 shows that 80 time slots is the highest value for any of the participants, thus 80 time slots is used for all participants.

To calculate total option TSDF, all options in which a platform transmits are summed up and added into platform TSDF.

Therefore, Total Surveillance Option, (TS_O) + Total Control Option, (T_{CO}) + Total NC2 to NC2 (Fighter) Option, (T_{FO}) = Total Options, (T_O)

In this example the highest surveillance time slot assignment is Sequence 1 of Option 2, or 80 time slots. This is used as the worst case for all platforms transmitting in the surveillance option pools, i.e. Ship (1-6), E-2C (1-2), DDG Cassard (1), and PACDG (1).

Ship(1.1) using SURV Option #2 seq. No. 1 = 80 time slots = (T_{SO}) = (T_O)
Ship(1.1) = (80 ts) x (444 pulses)= 35520 pulses = (T_O)

F14D(1.1.1) participating in Control Option pool and NC2 to NC2 Option pool. Inspection of both tables indicates that 32 (the highest value) timeslots will be assigned to all platforms for calculation purposes.

F14D(1.1.1) = T_{CO} +TFO = TO (SGs 15 and 16)
F14D(1.1.1) = (32 ts) x (258 pulses) + (32 ts) x (258) = 16512 pulses = (T_O)

2.3.4.4.6 Voice

When calculating TSDF for an individual platform assigned Voice, a separate matrix is created presenting all data rates and packing limits. The pulse density for the matrix is calculated using the dedicated access procedures mentioned earlier.

VOICE Time Slots Per Unit/12 sec				
Voice Data Rate	STD DP	P2SP	P2DP	P4SP
2.4 kbs W/O EDAC	64	not used	not used	not used
2.4 kbs W EDAC	128	64	64	not used
16 kbs W/O EDAC	448	224	224	112

Table 2.13 Voice Time slots per Unit/12 second Frame

Example:

E-3(1) = (112 ts) x (444 pulses) = 49728 pulses for (SG 19) + (112 ts) x (444 pulses) = 49728 pulses (relayed) for (SG 20)

Total Voice:
E-3(1) = 49728 + 49728 pulses = (T_v) = 99456 pulses

2.3.4.5 Total Platform TSDF

To calculate a platform's total TSDF the equation is as follows:

Platform TSDF = [(T_{dcrnov}) / (396288)] x 100

Some examples follow:

Examples:

a. Ship (1.1) calculation

$(T_d) + (T_c) + (T_r) + (T_{NETE}) +(T_O) + (T_v) = (T_{dcrnov})$
(T_c) = (8 ts) x (72 pulses) = 576 pulses (SG 2)
(T_{d6}) = (1 ts) x (258 pulses) = 258 pulses (SG 6)
(T_{d12}) = (8 ts) x (444 pulses) = 3552 pulses (SG12)
(T_{d13}) = (16 ts) x (258 pulses) = 4128 pulses (SG13)
(T_{r7}) = (21 ts) x (258 pulses) = 5418 pulses (SG 7)
(T_{r9}) = (112 ts) x (444 pulses) = 49728 pulses (SG 9)
(T_O) = (80 ts) x (444 pulses) = 35520 pulses (SG 8)
(Tv) = (112 ts) x (444 pulses) = 49728 pulses (SG 19)
(T_{vr}) = (112 ts) x (444 pulses) = 49728 pulses (relayed) (SG 20)
(T_{NETE}) = (1 ts) x (258 pulses) = 258 pulses (NETE)
so, if $(T_d) + (T_c) + (T_r) + (T_{NETE}) +(T_O) + (T_v) = (T_{dcrnov})$
Ship(1.1) = [258 + 3552 + 4128] + [5418 + 49728]+[576] + [258] + [35520] + [2 x 49728] = (T_{dcrnov})
Ship(1.1) = [198894 / 396288] x 100 =
Ship(1.1) = 50.19 % pulse density

b. F14D(1.1.1) calculation

$(T_d) + (T_c) + (T_r) + (T_{NETE}) + (T_O) + (T_v) = (T_{dcrnov})$
(T_c) = (8 ts) x (72 pulses) = 576 pulses (SG 2)
(T_{d1}) = (4 ts) x (258 pulses) = 1032 pulses (SG 3)
(T_{d2}) = (2 ts) x (258 pulses) = 516 pulses (SG 4)
(T_{CO}) = (32 ts) x (258 pulses) = 8256 pulses (SG 15)
(T_{FFO}) = (32 ts) x (258 pulses) = 8256 pulses (SG 16)
(Tv) = (112 ts) x (444 pulses) = 49728 pulses (SG 19)
(T_{vr}) = (112 ts) x (444 pulses) = 49728 pulses (relayed) (SG 20)
(T_{NETE}) = (1 ts) x (258 pulses) = 258 pulses (NETE)
F14D(1.1.1) = [1032 + 516] + [576] + [0] + [258] + [8256 + 8256] + [2 x 49728] =118350 pulses = (T_{dcrov})
F14D(1.1.1) = [118350 / 396288] x100 =
F14D(1.1.1) = 29.86 % pulse density

c. E3(1.1) calculation

$(T_d) + (T_c) + (T_r) + (T_{NETE}) + (T_o) + (T_v) = (T_{dcrnov})$
(T_c) = (8 ts) x (72 pulses) = 576 pulses (SG 2)
(T_{d1}) = (1 ts) x (258 pulses) = 258 pulses (SG 6)
(T_{r1}) = (21 ts) x (258 pulses) = 5418 pulses (SG 7)
(T_{r2}) = (112 ts) x (444 pulses) = 49728 pulses (SG 9)
(T_{d2}) = (32 ts) x (444 pulses) = 14208 pulses (SG 10)
(T_{d3}) = (16 ts) x (444 pulses) = 7104 pulses (SG 11)
(T_{d4}) = (8 ts) x (444 pulses) = 3552 pulses (SG 12)
(T_{d5}) = (16 ts) x (258 pulses) = 4128 pulses (SG 13)

(Tv) = (112 ts) x (444 pulses) = 49728 pulses (SG 19)

(T_{vr}) = (112 ts) x (444 pulses) = 49728 pulses (relayed) (SG 20)

(T_{NETE}) = (1 ts) x (258 pulses) = 258 pulses (NETE)

(T_{dcrnov}) = [258 + 14208 + 7104 + 3552 + 4128] + [576] + [5418 + 49728} + [258] + [0] + [2 x 49728]

(T_{dcrnov}) = 184686 pulses

E3(1.1) = [184646 / 396288] x 100 =

E3(1.1) = 46.60 % pulse density

d. <u>F15(1.1.1) calculation</u>

$(T_d) + (T_c) + (T_r) + (T_{NETE}) + (T_O) + (T_v) = (T_{dcrov})$

(T_{c1}) = (8 ts) x (72 pulses) = 576 pulses (SG 2)

(T_{c2}) = (6 ts) x (258 pulses) = 1548 pulses (SG 5)

(T_{c3}) = (8ts) x (258 pulses) = 2064 pulses (SG14)

(T_{c4}) = .5 (32 ts) x (258 pulses) = 4128 pulses (SG 17)

(T_{c5}) = .5 (32 ts) x (258 pulses) = 4128 pulses (SG 18)

(Tv) = (112 ts) x (444 pulses) = 49728 pulses (SG 19)

(T_{NETE}) = (1 ts) x (258 pulses) = 258 pulses (NETE)

(T_{dcrnov}) = [0] + [576 + 1548 + 2064 + 4128 + 4128] + [258] + [49728] = 61998 pulses

F15(1.1.1) = [62430/ 396288] x 100 =

F15(1.1.1) = 15.75% pulse density

F15(1.1.1) without voice = [0] + [576 +1548 + 2064 + 4128 + 4128] +[258] = 12702 pulses

F15(1.1.1) without voice = [12702/ 396288] x 100 =

F15(1.1.1) without voice = 3.2% pulse density

e. <u>GE-PAT(1) calculation</u>

$(T_d) + (T_c) + (T_r) + (T_{NETE}) + (T_O) + (T_v) = (T_{dcrnov})$

(T_{d1}) = (10 ts) x (72 pulses) = 720 pulses (SG 1)

(T_{d2}) = (1 ts) x (258 pulses) = 258 pulses (SG 6)

(T_{NETE}) = (1 ts) x (258 pulses) = 258 pulses (NETE)

(T_{dcrnov}) = [720 + 258] + [0] + [0] + [258] + [0] + [0] = 1236 pulses = (T_{dcrov})

GE-PAT(1) = [1236 / 396288] x 100 =

GE-PAT(1) = 0.31 % pulse density

2.3.5 Distribution of Network Design Data Between NDFs

2.3.5.1 Where appropriate, the originating NDF should dispatch to any supporting (national) NDF(s) the completed network design to allow initialisation loads to be generated in the appropriate media for that nation's platforms.

2.3.5.2 The standard medium and format for the exchange of NATO network design data between NDFs is specified in NETMAN T/1.

APPENDIX A TO CHAPTER 2

RTT-A AND RTT-B TSDF CALCULATIONS IN OPERATIONAL SCENARIOS

A.1 INTRODUCTION

There are many variables used in the calculation of pulses using RTT-A and RTT-B. The following are just a few variables used in determining actual transmission of RTT-I and RTT-R messages: geographic positioning (connectivity), network roles, equipment operational status, Time Quality (Q_t), and length of time established in the network.

The following connectivity matrix is used as an example to calculate pulses for a single platform.

Slot Group:			1	2
NPG Name:			RTT-A	RTT-B
NPG No:			2	3
Net Number:			0	0
TSEC Variable:			1	1
MSEC Variable:				
Access Mode:			D	4
Packing Limit:				
S/F Unit:			1	
S/F Total:			16	16
Participants	User Seq No.	IEJU	Connectivity	
SHIP (1)	1	Y	T/R	T
E-2C (1)	1	Y	T/R	T
F-14D (1)/8	1-8	Y	T/R	T
E-3 (1)		Y	T/R	T
CRC (1.1)		Y	T/R	T
F15 (1.1.1)		Y	T/R	T

A.2 RTT-A

a. The first variable is determining which unit is interrogated (addressed) by the platform transmitting the interrogation message (RTT-I). The second variable is determining how many other platforms could interrogate that same addressed unit. The RTT-Is and RTT-Rs are transmitted using 72 pulses each. For this example SHIP (1) will be assigned the NTR role, and the E-2C is a non-NTR. This assignment indicates that the SHIP (1) will not transmit an RTT-I, however, it can and will transmit RTT-Rs. Picking the worst case scenario, only the NTR will transmit RTT-Rs. This requires that all participating units be within LOS of the NTR in order to interrogate the NTR. To calculate the TSDF, first determine how many platforms are participating in the network. In this example there are only 13 platforms participating, but the total available time slots assigned are 16. The calculation is a dedicated access calculation.

b. The calculation follows:

#RTT-I = number of assigned RTT-I transmit time slots
#RTT-R = maximum number of possible RTT-R transmissions
72 = number of pulses transmitted for RTT-I or RTT-R

NOTE: When calculating the NTR TSDF remember that the NTR DOES NOT transmit an RTT-I, so no platform will transmit an RTT-R for the NTR!

c. Example 1 (Platform assigned as NTR)

SHIP (1) = (#RTT-I) x (72) + (#RTT-R) x (72) = RTT pulses

SHIP (1) = (0) x (72) + (12) x (72) = 864 pulses
[only 12 platforms will be transmitting RTT-I, so the NTR can only transmit the RTT-R to 12 platforms]

d. Example 2 (Non-NTR Platform)

Remember that:

#RTT-I = number assigned RTT-I transmit time slots
#RTT-R = maximum number of possible RTT-R transmissions
72 = number of pulses transmitted for RTT-I or RTT-R.

NOTE: When calculating the non-NTR pulses remember that the NTR DOES NOT transmit an RTT-I so the interrogating platform will not transmit an RTT-R for the NTR. Also, the interrogating platform does not transmit an RTT-R in response to its own RTT-I. So the maximum number of possible RTT-Rs is the total number of participants minus 2 (NTR and interrogating platform).

#RTT-R = (total platforms -2)

E-2C (1) = (#RTT-I) x (72) + (#RTT-R) x (72) = RTT pulses

E-2C (1) = (1) x (72) + (11) x (72) = 864 pulses

A.3 RTT-B

a. The RTT-I and RTT-R are transmitted using 72 pulses each. All platforms that receive the RTT-I can respond with an RTT-R. In this example, SHIP (1) will be assigned the NTR role (TQ = 15). This assignment indicates that the SHIP (1) will not transmit an RTT-I. However, it can and will transmit RTT-Rs. The NTR's only transmission of RTT-R will be on net 15. This requires that all participating units be within LOS of the NTR. To calculate this, first determine how many platforms are participating in the network and how many times each platform is allowed to transmit within a 12 second frame. In this example there are only 13 platforms participating with an assignment of 16-time slots and an access code of 4, which allows 3 time slots every 24 seconds. The equivalent slots per frame is 2 time slots every 12 second frame. Therefore, the platform calculation is 2 transmissions every 12-second frame.

Remember, the NTR DOES NOT TRANSMIT RTT - I MESSAGES.

b. The calculation follows:

#RTT-I = number of assigned RTT-I transmitted time slots
#RTT-R = maximum number of possible RTT-R transmissions
72 = number of pulses transmitted for and RTT-I or RTT-R.

c. Example 1 (Platform assigned as NTR)

NOTE: When calculating the NTR TSDF, remember that the NTR DOES NOT transmit RTT-I so NO platform transmits an RTT-R for the NTR!

Platform total transmission = [(#RTT-I x 72) + ((X or Y which ever is smaller) x 72)]

X = (# of Platforms - NTR) x (equivalent slots per frame)

X = (13 - 1) x 2 = 24 transmissions

Y = (# time slot in pool) = 16

If the number of platforms (X), exceeds the total number of time slots assigned to the pool (Y), then the smaller of the two will be used for calculations, because there are only 16 time slots in which the NTR can transmit an RTT-R, no matter how many RTT-I are transmitted within the pool. The NTR can only respond to one RTT-I message in a single time slot. As with contention, the possibility exists that more than one transmission can occur within a single time slot, but only one is answered by the NTR.

Z = (X or Y which ever is smaller) = 16

SHIP (1) (NTR) = (#RTT-I) x (72) + (Z) x (72) = RTT- R pulses
SHIP (1) (NTR) = (0) x (72) + (16) x (72) = 1152 pulses

This calculation is for RTT - R's transmitted by the NTR (which does not transmit any RTT – I).

d. Example 2 (Non-NTR Platform)

The calculation for transmitted pulses of a non-NTR platform is very similar to that of the platform assigned to be NTR. The major difference is the non-NTR E-2C will transmit RTT-Is as well as possible RTT-Rs. For this example, assume that the E-2C will be the second highest TQ within the network and is in LOS with all participants and is the only one in LOS of the NTR. Under these conditions all participants, except the NTR, will be transmitting an RTT-I to the E-2C and the E-2C will be responding with an RTT-R.

The calculated value for the E-2C RTT-I transmission is as follows:

RTT-I = (Equivalent slots per frame, based on access code) x (72 pulses)

RTT-I = (2 x 72) = 144 pulses

The calculation for the E-2C RTT-R transmission is as follows:

The calculation is preformed much like that of the NTR, with the one exception that the E-2C will not respond to its own RTT-I transmission. Take the total number of participants minus 2 (the NTR and the platform being calculated, since the platform will not transmit and RTT-R while transmitting its own RTT-I), multiplied by the Average access rate, (equivalent slots per frame). Those transmissions are calculated in the above paragraph. The equation is as follows.

X = (# of Platforms - (NTR + 1)) x (Average access rate, (equivalent slots per frame))

X = (13 - (1 + 1)) x (2) = 22 transmissions

Y = [(number of time slots assigned to pool - (Average access rate, (equivalent slots per frame))]

Y = [16 - 2] = 14

If the value of X exceeds the value of Y, then we will use the smaller of the two for our calculations, because there are only 16 time slots in which the participant can transmit an RTT-I or RTT - R. The platform being examined can only respond to one RTT - I message in a single time slot. As with contention, the possibility exists that more than one transmission occurs within a single time slot. However, only one is answered by the RTT-R transmission.

Z = (X or Y which ever is smaller) = 14

NOTE: When calculating the non-NTR pulses remember that the NTR DOES NOT transmit an RTT-I so NO platform transmits an RTT-R for the NTR. The platform who's TSDF is being calculated does not transmit an RTT-R in response to its own RTT-I. So the maximum number of possible RTT-R is total number of participants minus the “Average Access Rate”, or:

#RTT-R = (total - (Average access rate))

E-2C (1) = (RTT-I) + [(Z) x (72)] = RTT pulses

E-2C (1) = (144) + [(14 x 72)] = 1152 RTT pulses

This is the calculation for the E-2C in this example. It can be argued that this would be the worst-case number for all non-NTR participants. There are many more combinations for which calculations can be performed, however, the results for an individual platform will be equal to or less than what was calculated for the E-2C.

CHAPTER 3

GUIDELINES AND PROCEDURES FOR PRE-MISSION PLANNING

3.1 GENERAL

To protect the integrity of an operational MIDS network, staff planners should minimise the need for 'on-line' management of the MIDS network interface by optimising the interface 'off-line'. This is achieved by maintaining a library of network designs and by the use of a combination of MIDS modes and functions to establish a robust data link environment capable of graceful degradation.

3.2 AIM

The aim of pre-mission planning is to organise all the systems necessary to satisfy the information exchange requirements (IERs) of a specific force structure in a given operational scenario.

3.3 PROCESS

Pre-Mission Planning encompasses the following processes:

a. Analysis of the operational planning inputs to determine the communications requirements.

b. Selecting a network design(s) which supports the requirements determined by the planning input analysis.

c. Determining what modifications are necessary to tailor the design(s) selected to the specific requirement.

d. If no suitable network design already exists, requesting a new design to support the specific information exchange requirements.

e. Mapping physical units to the Initialisation Data Load (IDL) files included in the network design(s) selected.

f. Determining how the network architecture is to be established and maintained.

g. Determining how network integrity is to be established and maintained.

h. Determining what on-line network management procedures are to be employed.

i. Determining the cryptographic key requirements.

j. Assigning network roles to support synchronisation, relative navigation, network management and data exchange.

k. Promulgating the OPTASK messages to support necessary interface configuration information to the operational units.

3.4 PLANNING INPUTS

The detailed information needed to configure the MIDS interface to support a specific operational requirement will vary depending on the scenario. The task of allocating network resources and network roles is significantly influenced by the number, type, geographic distribution, operating profile, survivability, and on-task period of the participating JUs. The following operational and platform specific information is thus fundamental to the planning process:

a. Operational Environment:

(1) Joint and component commanders' plans (e.g. command structure, relationships, mission requirements, and enemy threat).

(2) Operational scenario (e.g. geographical area of operations, geographical limitations, forces present, disposition of forces, treaties, host-nation restrictions, political constraints, EMC constraints, frequency assignments, rules of engagement, tactical operating procedures, non-hostile track load, adjacent MIDS operations).

(3) Identification and prioritisation of the IERs by functional area and participants.

(4) Intra-Service data link requirements that impact on the joint interface configuration.

(5) EW considerations (e.g., expected jamming threat).

(6) Cryptographic requirements.

b. Link Participants:

(1) Geographical location, operating areas, operating profile and mission.

(2) Functional area communities of interest (e.g., surveillance) and operational IERs for each participant.

(3) Expected track reporting level and track update rates.

(4) Physical capabilities and limitations of each participating platform that impact planning, such as:

i. Data Links implemented.

ii. Functional areas implemented for each Data Link.

iii. Data forwarding capabilities.

iv. Restrictions on relay capabilities.

v. Data grid/display grid limit.

vi. Operating range.

vii. Track number capacity.

viii. Communications available (for data link traffic and co-ordination nets).

ix. External Time Reference (ETR) capability.

x. GPS capability.

xi. Geodetic positions of fixed-site JUs.

xii. Transmit Power setting.

(5) Any current problems or degraded capabilities of each platform that would affect its ability to operate its data link capabilities as designed.

3.5 PLANNING INPUTS ANALYSIS

The planning inputs and the analysis of these inputs are essentially the same for the pre-mission planning process as it is for the network design process. However, at the pre-mission planning stage, the staff planner should first check the available network design libraries to determine if the requirements derived from the planning inputs analysis can be satisfied by using an existing design. If there is no design that meets the requirements then the output of the planning inputs analysis becomes the input to the network design process.

3.6 NETWORK DESIGN SELECTION

3.6.1 Selection Criteria

The output of the planning inputs analysis is a set of operational criteria, which includes the following:

a. Own forces ORder of BATtle (ORBAT)

b. Enemy ORBAT.

c. IER.

d. Information throughput requirements.

e. Connectivity requirements.

f. Security requirements.

g. Anti-Jam (AJ) requirements .

h. Network Management requirements.

i. EMC requirements.

3.6.2 Selection Process

The network description summary should be used to determine if there is an existing design(s) that satisfies the selection criteria, or one that can be modified. Having selected the most appropriate design(s) and determined what, if any, modifications are necessary to tailor the design(s) selected to the specific requirement, the physical platforms must be mapped to the IDL assignments. This is achieved by either assigning IDL to individual platforms directly, or by assigning a set of IDL to operational units (e.g. airfields/aircraft carriers), for local assignment to individual platforms as required.

3.6.3 Network Specific Parameters

3.6.3.1 Network Specific Parameters (NSPs) are parameters that define the communications structure of a network (e.g. time slot assignments). The NSPs may need to be modified in order to tailor an existing network design to meet a specific requirement. They include the parameters determined at network design and form the major part of a platform IDL.

3.6.3.2 An IDL contain thousands of NSPs and any manual modifications made to an IDL during platform initialisation are extremely vulnerable to operator error. In order to mitigate this risk, modifications must be kept to a minimum. When there is no existing network design that can be employed without the need for extensive modification to platform IDL, then it is essential that the planning staff initiate a request for a custom design.

3.6.4 Mission Specific Parameters

3.6.4.1 Mission Specific Parameters (MSPs) are parameters that are specific to either the mission and/or the network function which a platform is tasked to perform. MSPs may vary from mission to mission and may include such parameters as:

a. Primary Track Number.

b. Secondary Track Number(s).

c. Special Track Number(s).

e. Transmit Mode.

g. Network Time Reference (NTR) selection {Network Function}.

h. External Time Reference (ETR) selection.

i. Initial Entry MIDS Unit (IEJU) selection {Network Function}.

j. Position Reference (PR) selection {Network Function}.

k. Navigation Controller/Secondary Navigation Controller (NC/SNC) selection {Network Function}.

m. Voice Callsign.

n. Initial Voice Net number(s).

o. Initial Control Net number.

p. Current Crypto Period Designator (CPD).

q. Mission Correlators.

3.6.4.2 Planners may specify initial values for all MSPs, when known and applicable. The current CPD must always be in accordance with the standard CPD convention at Table 3.1.

Table 3.1 - Crypto Period Designator Prediction Table

LEAP YEAR CPD PREDICTION TABLES					
YEAR: 2000 2008			YEAR: 2004		
MONTH	DAY		MONTH	DAY	
	ODD	EVEN		ODD	EVEN
Jan	0	1	Jan	1	0
Feb	1	0	Feb	0	1
Mar	0	1	Mar	1	0
Apr	1	0	Apr	0	1
May	1	0	May	0	1
Jun	0	1	Jun	1	0
Jul	0	1	Jul	1	0
Aug	1	0	Aug	0	1
Sep	0	1	Sep	1	0
Oct	0	1	Oct	1	0
Nov	1	0	Nov	0	1
Dec	1	0	Dec	0	1
NON LEAP YEAR CPD PREDICTION TABLES					
YEAR: 2001 2003 2006 2009			YEAR: 2002 2005 2007 2010		
MONTH	DAY		MONTH	DAY	
	ODD	EVEN		ODD	EVEN
Jan	0	1	Jan	1	0
Feb	1	0	Feb	0	1
Mar	1	0	Mar	0	1
Apr	0	1	Apr	1	0
May	0	1	May	1	0
Jun	1	0	Jun	0	1
Jul	1	0	Jul	0	1
Aug	0	1	Aug	1	0
Sep	1	0	Sep	0	1
Oct	1	0	Oct	0	1
Nov	0	1	Nov	1	0
Dec	0	1	Dec	1	0

3.6.5 Platform Specific Parameters

Platform Specific Parameters (PSP) are parameters that are specific to individual platforms, such as antenna cable delays and platform type codes etc. PSPs rarely need to be changed and, where changes are necessary, these are the responsibility of the host platform. PSP data must be merged with both NSP and MSP to form the terminal IDL.

3.6.6 Selection Considerations

3.6.6.1 The most robust method of allocating timeslots to accommodate the information exchange, throughput and connectivity requirements of the total population of JUs is to use a single network design. This strategy minimises the degree of pre-mission and on-line optimisation required for any given operation.

3.6.6.2 In practice, the total population of JUs could exceed that which can be permanently accommodated within a single network design. In this case it may become necessary to;

a. Select different designs and/or IDLs within a design that satisfy different or changing tactical situations.

b. Optimise the interface by the use of automatic reallocation (e.g.TSR) and/or automated reallocation of timeslot and relay functions. However, it must be noted that some nations and/or tactical commanders may limit the extent to which automated management may be employed.

3.6.6.3 If a network is to be optimised on-line, manually or by either an automatic and/or automated process, then the design(s) selected must support these functions. Furthermore, at least one (and preferably more than one) unit must implement the functions necessary to execute the OPerational NETwork (OPNET) Management task as described in Chapter 4.

3.6.7 Multi-load Profiles

A JU is not necessarily constrained to using the same IDL for all phases of a mission. However, some platforms may not have the ability to change IDL during operations. Due consideration must be taken of platform capabilities and operating times when different network designs are considered necessary for different tactical phases.

3.6.8 Off-line Plan

The product of the pre-mission planning process is one or more off-line network plans. An off-line plan must include, but is not limited to, the following information:

a. ORBAT

b. IDLs (which must reflect any pre-mission changes to timeslot and relay block assignments).

c. IU Address-IDL-platform mapping.

d. Relay assignments.

e. Network Role assignments (including 'standby' functions).

f. Voice net assignments.

g. Control net assignments.

h. Fighter-to-Fighter net assignments.

i. Crypto load requirements.

3.6.9 Operational Tasking Datalinks Message

The off-line plan, which may include several different network designs, IDL assignments, MSPs and any new or modified IDL NSPs are promulgated using the Operational TASKing Datalinks (OPTASK Link) message. The date and times of activation, any pre-planned changes from one plan to another and any restrictions on the use of on-line network management (OPNET Management) must also be detailed.

3.7 NETWORK ROLES AND FUNCTIONS

3.7.1 Network Roles

In order to support the efficient operation of a network, an OPNET Manager (NM) should be appointed. Additionally, dependent upon the operational scenario, it may be desirable to appoint a Subordinate OPNET Manager (SubNM) to assist with the on-line management of the network. When such roles are employed, 'standby' units should also be identified. These management roles define operator actions and are not terminal settings or functions. The responsibilities of a NM and a SubNM are discussed in Chapter 4.

3.7.2 Network Functions

3.7.2.1 The following functions, which are terminal or host parameter settings, may be utilised in the operation of a MIDS network (including 'standby' functions where appropriate):

a. Network Time Reference (NTR).

b. Initial Entry MIDS Unit (IEJU).

c. Navigation Controller (NC).

d. Secondary Navigation Controller (SNC).

e. Position Reference (PR).

f. Primary User (PRU).

g. Secondary User (SU).

h. Data Forwarding Unit.

3.7.2.2 The functions of NTR, IEJU, PRU and SU support network time synchronisation. The functions of NC, SNC, and PR support the Relative Navigation (RELNAV) function. Table 3.2 shows which of the synchronisation and RELNAV functions can be performed simultaneously by a MIDS terminal.

3.7.2.3 Network roles and functions are assigned to each unit on the basis of capability, survivability, Radio Line-of Sight (RLOS) coverage, period of operation, operating area and operating profile. Assignment criteria are given in the subsequent sections that deal with network time and RELNAV.

3.7.2.4 Network roles and functions should be promulgated in the OPTASK LINK. A platform operator may be able to change a JU's network function during operation. However, there is no network management protocol that allows the NM to change a JU's function directly (i.e. automatically, using J-series network management messages).

Table 3.2 - Network Function Assignment

NTR	--						
IEJU	No	--					
PR	Yes	Yes	--				
NC	Yes	Yes	Yes	--			
SNC	Yes	Yes	Yes	No	--		
PRU	Yes	Yes	Yes	Yes	Yes	--	
SU	No	Yes	Yes*	No	No	No	--
	NTR	**IEJU**	**PR**	**NC**	**SNC**	**PRU**	**SU**

LEGEND:

Yes	= Can be assigned this combination of roles.
No	= Cannot be assigned this combination of roles.
--	= Not applicable
*	= Possible but not recommended.

3.8 TRANSMIT MODES

3.8.1 General

Transmit modes determine the conditions under which a JU will transmit data. Transmit Modes are promulgated in the OPTASK Link and entered either by initialisation or by operator action. There are four mutually exclusive transmit modes: TDMA OFF, NORMAL, POLLING and CONDITIONAL RADIO SILENT. Not all platform types implement the Polling mode and some platforms implement additional modes described in the following paragraphs. On certain platforms (mainly C^2 platforms), transmit modes can be changed during operation by a platform operator. However, there is no network management mechanism which allows the NM to change a JU's transmit mode directly (i.e. automatically, using J-series network management messages).

3.8.2 TDMA Off

In TDMA OFF, a JU will not transmit any formatted or unformatted data. The TACAN function, if implemented, will continue to operate.

3.8.3 Normal Mode

In NORMAL mode, a JU transmits messages as required, in its assigned time slots.

3.8.4 Polling Mode

In POLLING mode, a JU will transmit fixed format messages for the following purposes only:

a. RTT interrogation messages for synchronisation.

b. In response to a communications control message (J0.6) addressed to own unit.

c. For receipt compliance.

A JU in Polling Mode may transmit unformatted digital voice and free text messages but will not relay either voice or fixed format messages.

3.8.5 Conditional Radio Silent/Data Silent Mode

In CONDITIONAL RADIO SILENT mode, a JU will transmit unformatted voice and free text messages, but it will not transmit fixed format messages or relay either voice or fixed format messages. Fine synchronisation is achieved and/or maintained passively. The TACAN function, if implemented, will continue to operate. The Conditional Radio Silent mode is not an Emission Control (EMCON) condition, as the MIDS terminal can still transmit unformatted messages and TACAN signals. Some platforms refer to the Conditional Radio Silent mode as the Data Silent mode and feature an additional mode which is known as Radio Silent mode.

3.8.6 Radio Silent/Transmit Inhibit Mode

In Radio Silent mode, all MIDS terminal transmissions are inhibited and fine synchronisation is achieved and/or maintained passively. The TACAN DME function, if implemented, will also be inhibited, however, the TACAN will continue to provide bearing information. Some platforms implement a mode known as TRANSMIT INHIBIT (also known as LONG TERM TRANSMIT INHIBIT), which is similar to the RADIO SILENT mode.

3.8.7 Test Mode

There are two terminal test modes, Test Mode 1 and Test Mode 2. These modes are not normally used operationally. However, the NM may request that a platform operator select a test mode momentarily, in order to determine in which timeslots the JU is initialised to transmit (as described in Chapter 4).

3.8.8 Selection Criteria

3.8.8.1 To participate fully on the interface, a JU must operate in the NORMAL transmit mode. Furthermore, a JU's transmit mode affects its ability to function in one or more network roles. Ideally, therefore, all JU's should operate in the NORMAL transmit mode. When this is not practical, then all C^2 JUs and nonC^2 JUs which function as tactical data sources (i.e. exchange track data) must operate in the NORMAL transmit mode when not restricted by EMCON measures. JU's that participate as information clients only (i.e., primarily as receivers of tactical data), may operate in either POLLING or RADIO SILENT mode.

3.8.8.2 In CONDITIONAL RADIO SILENT or RADIO SILENT mode, a terminal must maintain synchronisation by passive means. Conversely, a terminal in POLLING mode can maintain synchronisation by either active or passive means, and it will respond to communications control messages. The NM may interrogate a JU in polling mode for information about its position and interface status. Therefore it is preferable for JU's that are not required to operate in the NORMAL transmit mode, to operate in POLLING rather than RADIO SILENT mode.

3.9 TDMA COMMUNICATIONS MODES

3.9.1 General

Communications mode determines whether a network employs frequency hopping and/or data encryption. The Communications mode is set at network design and all JUs must use the same mode.

3.9.2 Selection Criteria

Mode 1 is the normal and most secure communications mode. Mode 1 uses encryption and frequency hopping and can therefore be multi-netted. Mode 2 is encrypted but operates on a single net at a fixed frequency of 969 MHz. Mode 4 is also transmitted at 969 MHz but is not encrypted. Communications mode can be modified during initialisation but not during network operation. Only Mode 1 should be used operationally. Modes 2 and 4 are essentially for test purposes. The characteristics of the Communications Modes are shown in Table 3.3.

Table 3.3. Communications Modes

Communications Mode	Multiple Nets/AJ Capability	Data Encryption Capability
1 (Operational Use)	Yes	Yes
2 (Test Only)	No/Reduced AJ	Yes
3 (Class 1 only)	Not used	Not used
4 (Test only)	No	No

3.10 RANGE MODE

3.10.1 General

Range mode determines the proportion of a timeslot that is reserved for MIDS signal propagation. There are two mutually exclusive range modes: NORMAL or EXTENDED.

3.10.2 Normal Range Mode

In NORMAL Range mode there is sufficient propagation time available to ensure that all types of J-series messages, irrespective of packing structure, can be received by a JU at 300 nm from the originating JU (assuming RLOS). All Anti-Jamming (AJ) and variable data capacity features of the MIDS signal are available and both active and passive synchronisation is supported.

3.10.3 Extended Range Mode

The EXTENDED Range mode increases the time available for signal propagation by reducing message start jitter. In Extended Range mode, JUs will receive only Standard and Pack 2 Single Pulse messages at ranges between 300 and 500 nm from the originating JU. However, JUs within 300 nm can receive all messages, irrespective of packing structure. Furthermore, a JU that receives an RTT interrogation from another JU, which is more than 300 nm away, may not respond to the interrogation. Thus active fine synchronisation between JUs which are more than 300 nm apart is not guaranteed. Units beyond this range should select SU vice PRU to enable active aided passive synchronisation (see 3.12.6.1.2).

3.10.4 Range Mode Setting

3.10.4.1 Range mode is determined at network design and **all JUs in a MIDS network must operate in the same range mode**.

3.10.4.2 Range mode and maximum packing limits are set during terminal initialisation and can not be modified by the NM directly. Some platforms allow an operator to change both the range mode and the maximum packing levels (on an NPG basis) during operation. Any change to the maximum packing level/limit may have adverse effects on message reception and cause non-compliance with the existing frequency clearance, therefore any changes must be coordinated with the NM.

3.11 INITIAL ENTRY MESSAGE

3.11.1 The Initial Entry Message (IEM) supports the automatic allocation of transmission capacity to JUs entering the network with a minimum set of initialisation parameters. The IEM supports contention and dedicated reuse allocations only, in the following PGs:

a. Voice.

b. RTT-B.

c. PPLI.

d. Control.

3.11.2 The NM may elect to use the Initial Entry Message (IEM) to automatically assign timeslots to JUs entering the network, in order to reduce the loading on the Network Management PG. However, this facility is available only when a network is being operated in Communications Mode 1.

3.11.3 **National and/or service operational employment concepts may not allow the use of IEM allocation for MIDS operations**. Furthermore, the use of certain access modes may be prohibited by a MIDS frequency assignment agreement (see Section 3.20).

3.12 NETWORK TIME

3.12.1 Architecture

3.12.1.1 A MIDS network is a Time Division Multiple Access (TDMA) communications architecture in which transmissions are made in specific time intervals. A network can either operate on a time basis relative to a single participant (NTR), or can be synchronised to an external absolute time standard.

3.12.1.2 ‘Relative’ or ‘system time’ is the marking of events in an unambiguous and traceable manner, by referencing a single JUs MIDS terminal clock. ‘Absolute time’ is the marking of events by referencing an external time standard (such as the United States Naval Observatory time standard used by GPS).

3.12.1.3 A MIDS network operating on a relative time basis may be referred to as a 'System Time Referenced Network' (STRN). A MIDS network operating using an external absolute time standard may be referred to as an 'External Time Referenced Network' (ETRN).

3.12.2 Time Quality

Time quality (Qt) is a measure of the accuracy of a JU’s terminal time with respect to a Network Time Reference (NTR) or an External Time Reference (ETR). Qt is a data element in the Precise Participant Location and Identification (PPLI) and Initial Entry Messages (IEM). Qt is expressed as an integer from 0 to 15 that represents a deviation from the chosen time reference.

3.12.3 Synchronisation

Synchronisation is an automatic, two-stage process by which a MIDS terminal acquires and maintains network time. The PRU and SU functions, in conjunction with a JUs Transmit Mode, determine the method used by a terminal to maintain synchronisation with the time reference.

3.12.4 Initial Entry

3.12.4.1 A JU synchronises to the time reference by receiving an IEM transmitted by either an NTR, an IEJU or a main net relay JU. The acquisition of network time by this process is called 'initial entry' and results in the joining terminal achieving coarse synchronisation with the time reference.

3.12.4.2 A terminal in coarse synchronisation will receive messages transmitted by other JUs already in fine synchronisation with the time reference. The terminal uses the PPLI messages it receives to achieve and maintain fine synchronisation with the time reference. This is achieved either by monitoring other JU's PPLIs (passive synchronisation) or by exchanging Round Trip Timing (RTT) messages (active synchronisation) with other JUs.

3.12.5 Active Synchronisation

Active synchronisation is employed by JUs operating in the role of PRU, NC or SNC. Active synchronisation requires the synchronising JU to transmit either an addressed or broadcast RTT message. Fine Synchronisation is achieved by processing the RTT reply messages from active JUs already participating in the network. A terminal in coarse synchronisation with the time reference can receive messages but is prohibited from transmitting any messages other than RTT interrogations.

3.12.6 Passive Synchronisation

There are two passive synchronisation modes; passive mode and active-aided passive mode.

3.12.6.1 Passive Mode

3.12.6.1.1 Passive synchronisation is performed by SUs, JUs in CONDITIONAL RADIO SILENT or JUs in LONG TERM TRANSMIT INHIBIT. If a JU conducting passive synchronisation receives PPLI data from three or more JUs, then the MIDS terminal can use these sources to fix its own position. Fine synchronisation is then achieved by computing the temporal position of timeslot boundaries, from the Time-Of-Arrival (TOA) measurements and position information within the PPLI messages received. However, if a JU who is trying to passively synchronise to the network receives PPLI data from less than three JUs, then it cannot fix its own position. In this situation, the geodetic position with which the JU’s terminal is initialised must be accurate to within 2 nm, in order to achieve fine synchronisation.

3.12.6.1.2 It is not possible for a JU to achieve fine synchronisation if the only PPLIs it can receive are from JUs that are within the range defined by its Geodetic Position Quality (Qpg).

3.12.6.2 Active-Aided Passive Mode

Active-Aided passive synchronisation is performed by JUs that are operating as SUs. In aided passive mode, a JU uses passive synchronisation techniques primarily. However, a SU that is not CONDITIONAL RADIO SILENT, will transmit an RTT message to aid the passive synchronisation function, under certain conditions.

3.12.7 System Time Referenced Network

3.12.7.1 A System Time Referenced Network (STRN) is a network in which a single JU is assigned the function of NTR. The NTR JU has zero time error and declares the highest Qt (15). The time qualities of all other JUs reflect an estimate of their time error relative to the NTR’s clock.

3.12.7.2 In a STRN, there is no requirement for the network to be tied to any particular absolute time standard. However, some time datum is required in order for a terminal to know approximately where to look (in time) for the IEM message. In practise, therefore, it is necessary to specify a time datum against which the STRN will be loosely correlated.

3.12.7.3 The time datum used to establish the network architecture must be determined at the planning stage and promulgated in the OPTASK Link. The standard time datum for NATO operations is GMT (Zulu time). The NM may also specify a time uncertainty to be used by JUs when joining the network, although this is not essential and may be dictated by platform SOPs. In some JUs, the time uncertainty parameter is fixed and can not be modified either during operation or at initialisation. Therefore, if required, the NM must select a network time uncertainty value that is equal to or less than that of the JU type with the smallest, fixed, time uncertainty value. Typical time uncertainty values range from 12 to 36 seconds.

3.12.8 STRN Function Assignment

3.12.8.1 NTR

3.12.8.1.1 The NTR is essential to the correct operation of an STRN and only one JU may operate as the NTR. The first JUs to synchronise to an STRN do so by receiving an IEM transmitted by the NTR. The NTR function may be transferred between JUs when operationally necessary.

3.12.8.1.2 The ideal NTR is one which:

a. Provides RLOS coverage of the entire operating area.

b. Is continuously available.

c. Is in a low threat environment or a well defended location.

3.12.8.1.3 In practice, it is unlikely that any single JU satisfies all these criteria. However, these attributes can be used to identify a typical ‘set’ of potential NTR candidates.

3.12.8.1.4 All JUs function as either C^2 or nonC^2 JUs. C^2 JUs are generally large entities such as CRCs, naval units or large multi-engined aircraft. Airborne C^2 JUs normally provide extensive RLOS coverage, have predictable operating profiles and are typically available for several hours. However, if a specific tactical station, such as an AEW or ELINT orbit, is being manned continuously, then the airborne C^2 JUs exhibit, collectively, many of the attributes of an ideal NTR. Similarly, surface C^2 JUs can operate continuously for weeks at a time. Their coverage is limited by the RLOS nature of MIDS, but otherwise they also exhibit a number of the attributes of the ideal NTR. NonC^2 JUs however, are generally small, highly dynamic entities (such as fighter aircraft) that operate for 2-3 hours at a time. The coverage they provide is highly variable and therefore they do not make the best NTR.

3.12.8.2 IEJU

Given that there is unlikely to be a single JU which provides RLOS coverage of the entire operating area, then IEJUs are required to support initial entry in conjunction with the NTR. The IEJU function is not mutually exclusive and all JUs can be initialised to operate as IEJUs. However, certain operational circumstances, such as nonC^2 aircraft operating in close formation, or the requirements of some FCAs may preclude the use of IEJUs in this way. In order to reduce the effects of mutual interference or to comply with FCA it may be necessary to limit the number of IEJUs by, for example having only Flight Leader nonC^2 aircraft operating as IEJUs.

3.12.8.3 PRU and SU

A PRU uses active synchronisation techniques and is capable of achieving and maintaining the maximum Qt possible. A SU uses passive synchronisation techniques primarily and does not maintain optimum Qt. Ideally, all JUs should operate as PRUs. However in certain circumstances, such as when there are more than 256 platforms or if some units are more than 300nm from NTR/IEJU , then it may not be practical to support either dedicated or broadcast RTT exchanges for every JU. In this situation, all C^2 JUs and nonC^2 JUs that transmit data derived from on-board sensors (e.g. radar, ESM, sonar etc) should operate as PRUs. All other JUs should operate as SUs.

3.12.9 External Time Referenced Network

3.12.9.1 An External Time Referenced Network (ETRN) is a network in which all JUs are either directly or indirectly synchronised to an external absolute time standard via a Precise Time and Frequency Service1 (PTFS), which is utilised as an ETR. The ETR may be any system that provides a precise frequency reference and time-of-day marker to the required accuracy (such as GPS). A JU that is initialised to use an ETR, is referred to as a JU^E.

3.12.9.2 In an ETRN, a JU^E's time error is measured against the ETR (rather than against an NTR JU). A JU^E's Qt will thus reflect an estimate of its clock error relative to the absolute standard established by the ETR.

3.12.9.3 A JU^E will normally obtain and maintain fine synchronisation with the time standard by observing the ETR directly. However, any JU^E will RTT with other JUs if its own ETR input is not the best source of timing information. Importantly, a JU^E does not have to be within RLOS of other network participants in order to synchronise to the network, but it does have to be able to observe the common ETR.

3.12.9.4 Within an ETRN, not all of the participating JUs need to be equipped with ETR equipment. Non-ETR JUs may still synchronised to the network by receiving an IEM from an existing participant (NTR, IEJU or main net relay) and conducting synchronisation in the normal way (either as a PRU or a SU). The Qt declared by such a JU still reflects that unit's time error relative to the ETR even though the JU is not observing the ETR directly. A Non-ETR JU must gain RLOS with a network participant before synchronisation can be achieved.

3.12.10 Direct Network Entry

3.12.10.1 In order to commence MIDS transmissions, a JU^E must still first achieve fine synchronisation. This may be achieved either by synchronising to the ETRN in the normal way (by synchronising to the NTR or IEJU) or by using the time input from the ETR. To utilise the ETR, however, the JU^E must first select NTR - this procedure is called Direct

[1] Free-running time or frequency references that are external to the MIDS terminal but organic and internal to the host platform (e.g. a ships chronometer) can not be used as an ETR.

Network Entry (DNE). In an ETRN in which DNE is being employed, it is thus possible to have 2 or more NTRs simultaneously, however, unlike a STRN, this situation is not necessarily disadvantageous. As an NTR JU^E is not the custodian of network time but is merely referring to another, shared time standard, the existence of multiple NTRs will not result in the establishment of multiple, asynchronous networks.

3.12.10.2 The advantage of DNE is that it dispenses with the need for a JU^E to receive an IEM in order to synchronise to an ETRN. This makes initial entry for a JU^E independent of all other participating JUs. However, once time alignment with the ETR has been achieved, an NTR JU^E should deselect the NTR function and revert to operating as an IEJU^E.

3.12.11 ETRN Function Assignment

3.12.11.1 The function assignment criteria when planning to establish an ETRN are essentially the same as for an STRN. However, when operating a STRN, the NTR function is critical for correct operation of the link this is not necessarily the case in an ETRN.

3.12.11.2 In practice, a NTR JU^E is almost identical to an IEJU^E and for general synchronisation purposes, it is possible to operate without any NTRs or with several simultaneously. However, in order to ensure that the protocols for updating the IEM and initiating a Network Time Update (NTU) are protected, one JU should operate continuously as a NTR and **this JU must always be a JU^E**. In order to support the synchronisation of non-ETR JUs and the dissemination of IEM and NTU management functions, further participants (either JUs or JU^{E}s) should be designated as IEJU/IEJU^{E}s.

3.13 NETWORK INTEGRITY

3.13.1 Direct Connectivity

A JU that receives a J-series message in the timeslot in which it was originally transmitted, has direct connectivity with the originating JU.

3.13.2 Indirect Connectivity

A JU that receives a J-series message only if the message is relayed by one or more relay JUs, is considered to have **indirect connectivity** with the originating JU.

3.13.3 Connectivity and Network Time

When a JU has RLOS with the time reference (either NTR or ETR) it has direct connectivity with the time reference. If a JU is not referencing the network time directly but is maintaining synchronisation via another JU, it has indirect connectivity with the time reference.

3.13.4 Isolation and Fragmentation

In a situation where a JU cannot maintain either direct or indirect connectivity with the time reference, its Qt will begin to degrade. If connectivity is not re-established, the JU's Qt will degrade to zero within a few hours. At Qt zero, a MIDS terminal will eventually declare itself to be out of fine synchronisation and cease to transmit. Any JU, or tactical grouping of JUs, that cannot maintain connectivity with the time reference is referred to as isolated and the network is considered to have fragmented.

3.13.5 Participant Disposition

Whenever the geographic distribution of JUs provides multiple, redundant direct or indirect connectivity paths to the time reference, then the integrity of the network is good, as there is very little chance that the network will fragment. If there is only one connectivity path between a JU and the time reference, then the integrity of the network maybe reduced, as the unavailability of a single JU could cause the network to fragment.

3.13.6 Dispersed Area Operations

3.13.6.1 When planning to support dispersed area operations, the NM must first determine how to achieve and maintain initial entry and synchronisation over the area. If the natural (uncoordinated) geographic and temporal distribution of JUs does not provide the connectivity necessary, it will be necessary to position, or reposition and then retain, one or more high altitude JUs in specific geographic areas. This may entail additional, dedicated flying effort and incur restrictions on the tactical employment of the JUs in question.

3.13.6.2 When determining wide-area relay requirements, the primary object is to achieve redundant coverage of the entire operating area. The secondary objective is to minimise the degree of on-line reallocation of the relay functions required to satisfy the primary object.

3.13.7 System Time versus External Time Referenced Networks

3.13.7.1 There are three key factors that affect the integrity of a wide-area network:

a. The coverage of the time reference.

b. The redundancy of coverage of the time reference.

c. The number and geographic distribution of IEJUs and wide-area relay JUs.

3.13.7.2 System Time Referenced Network

3.13.7.2.1 To achieve maximum integrity when operating within a STRN, the primary objective is to assign the NTR function to a JU that is expected to have the greatest RLOS coverage of the operating area. Furthermore, as the NTR function cannot be reassigned by the NM automatically, then the secondary objective is to minimise the need to transfer the NTR function during the lifetime of the network. As the IEJU function is not exclusive, and IEM redundancy enhances network integrity, it is pragmatic to have all airborne C^2 JUs operating as IEJUs.

3.13.7.2.2 When relying on dynamic tactical elements to provide both the time reference and the redundancy of coverage necessary to achieve good STRN integrity, the number, type, operating profile and geographic distribution of the participating JUs are significant and critical factors. Indeed, in a highly dynamic tactical environment, it may be difficult to establish a single wide-area STRN.

3.13.7.3 External Time Referenced Network

3.13.7.3.1 Operating an ETRN can mitigate many of the critical factors that affect the integrity of a STRN as follows.

3.13.7.3.2 If there is only one JU^E operating in an ETRN, then this JU performs the same function as the NTR in an STRN. In this case, the two types of network are essentially identical and nothing is gained by attempting to establish a wide-area ETRN. It is inadvisable to attempt to establish an ETRN (if there is only one JU^E) as the Qt is determined by the performance of the ETR and, if this performance is anything other than optimal, the network Qt will be degraded.

3.13.7.3.3 If all the participating JUs are JU^{E}s, and the ETR provides continuous, redundant radio coverage of the entire operating area (e.g. GPS), then all operations are local area and high integrity. In this situation, the integrity of an ETRN is unaffected by the number, type, operating profile, on-task period or geographic distribution of JUs, as every JU can maintain direct connectivity with the ETR. This removes the need for any ‘time’ related co-ordination and management beyond monitoring the availability and performance of the ETR.

3.14 RELATIVE NAVIGATION

3.14.1 General

RELNAV is an automatic terminal function that utilises information received via PPLI messages and navigation inputs from a JU’s on board systems. RELNAV supports two basic co-ordinate systems: the standard geodetic system, and a flat-plane grid system tangential to the earth’s surface at an arbitrary grid origin. RELNAV is an essential function as it facilitates the accurate correlation of datalink objects. A MIDS terminal can operate simultaneously in both co-ordinate systems.

3.14.2 Geodetic Grid

The Geodetic Grid (GEOGRID) is an earth-based curved co-ordinate system (WGS-84) used to report positions by latitude, longitude and altitude. The GEOGRID is the principal grid and is maintained continuously.

3.14.3 Relative Grid

The Relative Grid (RELGRID) is a three axis, flat-plane co-ordinate system used to report position as U,V,W co-ordinates from a relative grid origin. For this grid to be active, a NC must be operating in the network.

3.14.4 Relative Grid Origin

RELGRID co-ordinates are valid only when network participants are <1,024 nm from the RELGRID origin. The RELGRID origin should be a point at the centre of the region of activity.

3.14.5 Position Quality

Geodetic Position Quality (Qpg) is a measure of the accuracy to which a MIDS terminal fixes its own position in the GEOGRID. RELGRID position quality (Qpr) is a measure of the accuracy to which a MIDS terminal fixes its own position in the RELGRID. Both are expressed as an integer from 0-15. The maximum or best quality value is 15.

3.14.6 Navigation Controller

A NC establishes the relative grid co-ordinate system, including grid origin and grid orientation. By definition, the NC has zero relative grid co-ordinate error and declares the highest Qpr (15). All other JUs align to the grid reported by the NC and their relative position and azimuth qualities reflect an estimate of their position with respect to the NC.

3.14.7 Secondary Navigation Controller

The SNC may enhance the stability of the RELGRID. When a SNC is employed, it must be in direct connectivity with the NC at all times and must exhibit motion relative to the NC in order for it to assist in refining the RELGRID.

3.14.8 Position Reference

3.14.8.1 A Position Reference (PR) is a JU that can determine its geodetic position to a high degree of accuracy. As the geographic position reported by a fixed-site JU does not change, there is no requirement for it to use inputs derived from the MIDS RELNAV processing.

3.14.8.2 A PR provides a stable geodetic reference for other JUs to determine their own position via RELNAV. PRs will also assist a NC in refining the accuracy of the Relative Grid. The absence of PR support does not significantly degrade the Rel Grid, however, PRs are essential if the accuracy of the position data reported over the link cannot be maintained at a level that is sufficient to support navigation and track correlation functions.

3.14.8.3 The disposition of force assets is not a consideration in assigning a PR. However, favourable geometry (as described in paragraph 3.14.11.1), enhances a JU's ability to improve its position accuracy using the PRs. The key factor for assigning the PR role is a JU's ability to accurately fix the geodetic position of its MIDS antenna. Any fixed site JU which has independently derived knowledge (external to RELNAV) of the geodetic position of its MIDS antenna, to an accuracy of ≤ 50 feet (in 3 dimensions), should operate as a PR and report a Qpg of 15. When two or more PRs are available, other JUs, in direct connectivity with the PRs, can achieve a geodetic accuracy approaching that of the PRs'.

3.14.8.4 A JU satisfying both PR and NC criteria can perform both roles simultaneously and there is no limit to the number of JUs operating as PRs.

3.14.8.5 Mobile JUs should not select PR. Ground units should only select PR if they have a surveyed position accurate to 50 ft (as above) unless they are directed by the NM to act as a Pseudo PR.

3.14.9 Pseudo Position Reference

3.14.9.1 The ‘position reference’ terminal parameter (as distinct from the PR network function) determines whether or not a RELNAV-capable MIDS terminal attempts to navigate using information derived from the MIDS interface. A terminal that is operating with the position reference parameter set, but does not declare a Qpg of 15 is called a 'pseudo PR'.

3.14.9.2 If, for example, the geodetic position accuracy of a fixed-site JU is known only to ≤ 300 feet, then the position and height uncertainties must be set to values which ensure that the Qpg declared by the terminal is ≤ 10. In this case, although the terminal’s position reference parameter is set, it is, by definition, functioning as a pseudo PR.

3.14.10 Position and Height Uncertainty Parameters

3.14.10.1 When the position reference parameter is set, a MIDS terminal will not perform geodetic RELNAV updates using the position data contained in the PPLI messages of other JUs. In this case, a mobile JU will derive position and height uncertainty values from its non-MIDS navigation system(s), and a fixed site JU will set position and height uncertainties values at terminal initialisation.

3.14.10.2 A terminal’s position and height uncertainty values must always encompass the accuracy to which a JU’s geodetic position is known. If the geodetic position of a fixed-site JU’s MIDS antenna is known to an accuracy of ≤ 50 feet (in 3 dimensions), then the position and height uncertainty parameters can be set to their maximum value (Qpg =15).

3.14.10.3 If RELNAV-capable fixed-site JUs do not operate as either a PR or a pseudo PR, their reported position will vary slightly, even though they are not actually moving. Furthermore, MIDS terminals designed for use as a fixed-site JU require position and height uncertainty values to be set at initialisation and the RELNAV process does not modify these values. Therefore the Qpg reported by the JU will be inaccurate if the JUs computed RELNAV position falls outside that described by its Qpg (the consequences of which are described in Chapter 4).

3.14.11 RELGRID Function Assignment

3.14.11.1 The criteria for assigning NC and SNC are based on the following factors:

a. The number of JUs to be assigned a RELGRID role.

b. JU mobility.

c. JU relative motion.

d. LOS Connectivity.

e. Inter-JU geometry.

f. Minimum range.

g. The quality of GEOGRID data (in some cases).

3.14.11.2 Assignment criteria are as follows:

a. If only one JU is to be assigned a RELGRID role, then this JU must operate as a NC. The JU must be mobile and exhibit significant relative motion with respect to all other JUs who intend to operate in the RELGRID and should have RLOS with as many units as possible.

b. If two JUs are to be assigned a RELGRID function then:

(1) If both JUs are fixed site PR JUs (Qpg = 15) then both JUs can operate as NC. Positional accuracy is critical when more than one NC JU is assigned. If either JU is not a PR, or does not have Qpg = 15, then the JU with the lower Qpg must operate as a SNC.

(2) If one JU is a fixed site JU and the other JU is mobile, or if both JUs are mobile, then one JU must operate as NC and the other as SNC. Either JU may be designated NC.

(3) Any NC/SNC combination must be in direct connectivity with one another in one or more of the PPLI NPGs. However, if both JUs operate as NC, then there is no requirement for them to be in connectivity.

c. If three or more JUs are to be assigned a RELGRID role then all JUs must be fixed site JUs.

3.14.12 Relative Grid Geometry

The purpose of having more than one NC or NC/SNC combination is to create bearing separation so that other JUs can calculate grid positions accurately in two axes. The ideal situation is where the angle between the bearing from any JU to the NC, and the bearing from the same JU to the SNC (or second NC), is approximately 90 degrees.

3.14.13 Range Factors

If the NCs (or NC/SNC combination) are in close proximity to one another, then this reduces the bearing separation observable from other JUs and also affects the ability of a NC/SNC combination to accurately define the grid orientation.

3.15 DATA FORWARDING

3.15.1 General

Data forwarding is the process of receiving data on one datalink (the subject link) and then transmitting this data in the proper format and protocol on a different datalink (the object link).

3.15.2 FJU Assignment

3.15.2.1 Assigning the Forwarding MIDS Unit (FJU) (and Standby FJU (SFJU)) function is a multi-link planning activity. Therefore only general guidance is provided in this document.

3.15.2.2 A JU may be designated to perform data forwarding in any multi-link operation involving Link 16 and other tactical data links. Units that forward data between Link 16 and Link 11 are designated FJUAs. Units that forward data between Link 11B and Link 16 are designated FJUBs.

3.15.2.3 A FJU must be a C^2 JU with the software capabilities to perform the data forwarding function. When there are multiple FJU capable units available, the FJU function should be selected on the basis of RLOS coverage, availability and survivability.

3.15.3 Data Looping

Data looping is the exchange and then re-exchange of the same data between one datalink and another, such that duplicate instances or reports of single items may occur. Data looping is a damaging situation that must be avoided at all cost. Therefore, **one data forwarder only should be assigned to forward data from one datalink to another at any one time**. However, the total data forwarding responsibility may be functionally divided between two or more FJUs; e.g. one FJU may be designated to forward EW data and a second to forward all other data.

3.16 CONCURRENT DATALINK OPERATION

3.16.1 General

Concurrent datalink operation is the transmission of locally-held tactical data on two or more different datalinks simultaneously. A platform that operates in this way is called a Concurrent Interface Unit (CIU). The CIU will comply with all of the procedures and protocols of each link.

3.16.2 Considerations

When CIUs and FJUs are operating simultaneously, the potential for data looping and dual reporting is considerable. To mitigate this risk, a FJU must not forward any data that originates from a CIU on a subject link (which includes participant status messages), to any object link on which the CIU is scheduled to be active. **This is irrespective of whether or not the FJU is receiving the data on the object link**.

3.17 IU ADDRESS

3.17.1 General

An IU Address is a unique octal TN, which is assigned to each unit on the interface. Numerically equivalent 2-digit, 3-digit, and 5-digit Addresses are the same Address; e.g., 45, 045, and 00045. IU Addresses must be promulgated in the OPTASK Link. **Duplicate Addresses must not be assigned**. Multilink-capable IUs should, where possible, be assigned the same address in all applicable link data sets.

3.17.2 Handover and Daily Changing IU Address

3.17.2.1 A JU is not constrained to using the same IU Address and IDL for all phases of a mission. For example: an AEW aircraft which is relieving another aircraft already on-station, will normally join a network using a 'handover' IDL and IU Address. The handover procedure requires the two aircraft to 'swap' IDL and IU Addresses by reinitialising their MIDS terminals at the on/off task time specified. Furthermore, this procedure is executed with both aircraft active on the interface. Reinitialising a MIDS terminal whilst it is active on the interface is called 'on-line re-initialisation'.

3.17.2.2 Handover and on-line re-initialisation is a standard procedure for C^2 JU's. However, the procedure may 'confuse' a MIDS terminal if the handover procedure requires the JU's concerned to 'swap' IU Addresses. The same is true if a daily changing IU Address procedure is implemented. In this case however, the magnitude of the problem is considerably greater than for the handover procedure. Therefore **the reallocation of IU Addresses either at handover or on a periodic basis is not recommended**.

3.17.3 IU Address-to-IDL Mapping

If the OPNET management role is to be implemented effectively, then the NM's record of platforms' IDL must be accurate. Therefore **the IU Address-to–IDL mapping specified in the OPTASK Link must not be modified at either unit or platform level, except as directed by the NM**.

3.17.4 Assignment Criteria

3.17.4.1 When assigning IU Addresses to JUs, the NM must consider on which other datalinks a JU may be capable and required to operate.

3.17.4.2 The following are the criteria for IU Address assignment:

a. C^2 JUs may be assigned an Address anywhere in the range 00001-77776, except 00077, 00176, 00177, and 07777. However, in order to allow C^2 JUs to exchange addressed messages with Link 11 and Link 11B units, every effort should be made to assign C^2 JUs with Addresses in the range 001-175. If this is not possible, TNs greater than 175 should be assigned to the C^2 JUs which are least likely to exchange addressed messages with Link 11 and Link 11B units. C^2 JUs with Command authority or likely to originate Handover requests or EW orders addressed to Link 11 and Link 11B units, must be assigned an address below 176. These orders and requests cannot be forwarded to Link 11 and Link 11B units if the source TN is 00200 or greater.

b. A JU that is capable of both Link 16 and Link 11 operations should be assigned an Address in the range 01-76, even when the JU is a C^2 JU. This expedites the JU's activation of Link 11 and prevents confusion if the JU's Link 16 capability becomes unusable. For similar reasons, JUs capable of both Link 16 and Link 11B operation should be assigned an Address in the range 100-175.

c. NonC^2 JUs may be assigned an Address anywhere in the range 00200-77776, except 07777. To facilitate operator recognition, it is highly desirable that all nonC^2 JU Addresses be taken from a common block of TNs reserved for that purpose. As nonC^2 JUs' position reports may be forwarded to Link 11 as Surveillance Tracks, it is also highly desirable for nonC^2 JU addresses to be ≤ 07776 to facilitate forwarding and operator recognition.

d. TN 177 is the Collective Address and cannot be assigned as an IU address.

e. Because IU addresses greater than 177 cannot be used on Link 11 or Link 11B, FJUs use the Pseudo Source Address 176 when forwarding data from a C^2 JU whose TN is 00200 or greater. FJUs use the host platform IU Address for indicating R^2 when forwarding nonC^2 JU PPLI reports as tracks on Link 11 or Link 11B.

f. An FJUA or FJUAB must be assigned a single Address in the range 01-76, because it participates actively as both a PU and a JU and uses a single Address for both Links and for data forwarding. For a similar reason, an FJUB must be assigned an Address in the range 100-175. A Standby FJUA/ Standby FJUAB or Standby FJUB must also be assigned an Address in the range of 01-76 or 100-175, respectively.

g. The Address 77777 is reserved as a generic address for the Network Manager and must not be assigned as an IU Address. It is used for certain Link 16 management functions when the IU Address of the NM is not known.

h. TNs 00077 and 07777 are illegal for any purpose.

i. Table 3.4 summarises the above IU Address assignment criteria.

Table 3.4 - IU Address Assignment Criteria

JU Type/Function	Legal Range(8)	Preferred Range(8)
C^2 JU	00001-77776	00001-00175
Non-C^2 JU	00200-77776	00200-07776
FJUA/FJUAB	01-76	01-76
SFJUA/SFJUAB	01-76	01-76
FJUB	100-175	100-175
SFJUB	100-175	100-175
Link 11 Capable C^2 JU	00001-77776	01-76
Link 11B Capable C^2 JU	00001-77776	100-175
Pseudo Source Address	176	176
Collective Address	177	177
Network Manager	77777	77777

3.18 OPERATIONAL NETWORK MANAGEMENT

3.18.1 General

OPNET management is the real-time, on-line monitoring, control and maintenance of MIDS operations. Network monitoring provides the information required by the NM to identify non-optimal conditions or technical problems. Network maintenance is the actions taken to resolve these problems (OPNET management is the subject of Chapter 4.)

3.18.2 Monitoring and Maintenance

Network monitoring is the analysis of specific parameter values to determine the operational status of a network. The monitoring process feeds the maintenance process by providing the information required by the NM to identify and then rectify, non-optimal conditions or technical problems.

3.18.3 Considerations

3.18.3.1 Network Design

If the NM is to monitor and manage a wide-area network effectively, then the network design in use must support the OPNET management activities described in Chapter 4. Ideally, if a wide-area network is to be managed by a single unit, then the unit supporting the NM role should achieve and maintain connectivity with every participating JU. Therefore the network design should support the theatre-wide relay of applicable NPGs. If this is not possible, then one or more Subordinate-OPNET Managers (SubNM) may be employed as described in Section 3.19.

3.18.3.2 Manpower, Workload and Training

3.18.3.2.1 When the number of JUs is small and the total communications demand does not exceed the network capacity, the allocation of network resources, initiation and maintenance of a MIDS network is relatively straightforward. However, as the total number, type and geographical deployment of JUs increase, the task may becomes considerably more complex.

3.18.3.2.2 Monitoring the operation of a MIDS network is a routine and essentially passive task. Inevitably, human factors such as operator multi-tasking, distraction, misinterpretation and finite attention span will significantly degrade an individual's ability to function effectively in this role.

3.18.3.2.3 There are a considerable number of planned, reported, inferred and computed parameters that must be monitored in order to evaluate the operational status of the interface. The degree to which these parameters can be monitored and the extent to which a network can be actively maintained, will depend on:

a. The extent to which OPNET management is to be exercised.

b. The level of NM functionality implemented by the systems operating on the interface.

c. The level of NM expertise and training afforded to the operators of this system.

d. The complexity of the network.

3.18.3.3 Automation

The need for continuous physical monitoring of the interface can be reduced considerably by the implementation of automated monitoring and alerting functions.

3.18.4 <u>OPNET Management Role</u>

3.18.4.1 The unit chosen to support the NM role should be selected on the basis of:

a. NM functional capability.

b. Operational network management expertise.

c. Multi-link capability.

d. Transportability / mobility

e. Survivability.

f. Connectivity to critical network participants.

3.18.4.2 The Standby OPNET Manager (NMSby) is responsible for assuming the NM role if the NM suffers a significant loss of operational capability. The NM must maintain close co-ordination with the NMSby at all times and the NMSby must maintain an up-to-date copy of the on-line plan, either verbally or electronically.

3.19 SUB-OPNET MANAGEMENT

3.19.1 General

MIDS terminal users can be grouped into distinct tactical communities (e.g. a USN battlegroup or a French Army Needline community). Invariably MIDS implementations are optimised for intra-community interoperability and tactical communities will often employ specific MIDS features which are in some way particular to the tactical organisation in question (e.g. the USN prefers the double pulse signal structure). If the NM is to monitor and manage a network effectively, he must both understand and accommodate the specific requirements of each tactical community. It may not always be practical (or possible) for a single NM to manage all aspects of a wide-area network. In such instances the NM may delegate certain management functions to SubNMs who may be better placed and equipped to manage a local environment. Within the tactical community, SubNMs should be experienced personnel with knowledge of the tactical community platform implementations, capabilities and limitations.

3.19.2 Unique Roles and Functions

The management functions that may be performed by a SubNM, are essentially the same as those which must be performed by the NM (See Chapter 4). However, network functions that are either unique (e.g. the NTR function) or required to support inter-community information exchange (e.g. the main net relay function) should remain the responsibility of the NM. Therefore, management of the following functions or areas should not be delegated:

a. NTR, IEJU and main net relay.

b. NC/SNC.

c. Wide area PPLI assignments.

d. RTT A PG.

e. RTT B PG.

f. Network management PG.

g. Wide area relay function.

3.19.3 SubNM Responsibilities

The PGs that are assigned to a tactical community may be a structured and encapsulated subset of the network. This would allow a SubNM to manage a tactical community at the tactical community level, as if it were a network in its own right. When delegated management authority, the SubNM may change or modify assignments within the specified area, however, he must report such changes to the NM by voice or datalink. A SubNM may be used to manage stack nets used by platforms assigned to a tactical community including voice and data PG (e.g. voice A/B, fighter to fighter and air control). If necessary, the NM may delegate the management of one or more segments to one or more SubNMs.

3.19.4 SubNM Nomination

The availability of a SubNM within a tactical community may be notified by the tactical community commander to the NM, stating equipment, capabilities and limitations. If required the SubNM(s) and his assigned responsibilities must be promulgated in the OPTASK LINK. If the NM appoints a SubNM after a network has been initialised, then the NM must ensure that the SubNM has accurate information regarding the current state of the network including any modifications that have been incorporated.

3.20 FREQUENCY ASSIGNMENT

3.20.1 General

MIDS operates in the Air Radio Navigation frequency band 960 to 1215 MHz. Within the Flight Information Regions (FIR) of most nations, this band is controlled by the national Civil Aviation Authority (CAA). Many national CAAs have agreed to the use of MIDS on a non-interference basis and national frequency agreements may prohibit the use of certain MIDS network structures, modes and functions and place significant conditions on the extent to which MIDS communications resources may be utilised.

3.20.2 Operating Conditions

National Frequency Agreements may place conditions on the use of MIDS with regard to the following:

a. Terminal type. (eg. Class 1 or Class 2).

b. Signal structure. (i.e Packing levels).

c. Radiated Power.

d. Individual and total transmission duty factors.

e. Frequency selection characteristics.

f. Timeslot Access Method. (eg. Dedicated/Contention).

g. Simultaneous Transmissions.

h. Automatic Electromagnetic Compatibility (EMC) Protection Features2.

i. Geographic restrictions with respect to the proximity of navigation aids.

j. Co-ordination and monitoring of MIDS operations.

k. Operational records of MIDS usage.

3.20.3 Operating Clearance

It may be necessary for the planning staffs to initiate a request(s) for operating clearance and/or waivers to national frequency agreements as part of the planning process. These agreements and the procedures for requesting operating clearances are included as Annexes to this document.

3.20.4 Electromagnetic Compatibility Protection Features

EMC Protection is an automatic terminal function which will shut down a MIDS transmitter either semi-permanently (i.e. until the EMC Protection is reset manually) or temporarily (i.e. until the condition that triggered the shutdown clears). EMC Protection is a requirement in all national frequency assignments and all MIDS terminals incorporate EMC Protection. However, the basis on which the various EMC Protection modes operate may differ depending on the terminal type and the version of terminal software in use. Therefore the EMC Protection modes described in this section are for guidance only, and the NM must ensure that the actual protection provided by the EMC Protection mode selected for any given terminal, conforms with the restrictions applicable to the geographic area in which a terminal is expected to operate. A MIDS terminal provides at least three levels of EMC Protection: FULL, EXERCISE and COMBAT.

a. FULL EMC Protection mode – In the FULL EMC Protection mode all EMC protection automatic shutdown features are active.

b. EXERCISE EMC Protection mode – In EXERCISE EMC Protection mode the EMC protection features will shut down the terminal if the transmitted frequency hopped carrier is not uniformly distributed over the allowable bands of operation; if, during operation, the transmitted pulse width is excessive; or if the radiated energy in either of the bands 1030 ±7MHz or 1090 ±7MHz is excessive.

c. COMBAT EMC Protection mode – In COMBAT EMC Protection mode all EMC protection features are inhibited from shutting down the MIDS transmitter.

[2] Previously referred to as Interference Protection Features (IPF).

CHAPTER 4

GUIDELINES AND PROCEDURES FOR OPERATIONAL NETWORK MANAGEMENT

4.1 GENERAL

OPerational NETwork (OPNET) Management is the real-time, on-line monitoring and maintenance of MIDS operations. OPNET Management includes monitoring and analysing network and platform parameters, and reassignment of network functions (NTR, IEJU, NC/SNC, etc) and assets (timeslot allocations).

4.1.1 Aim

The aim of OPNET Management is to achieve and maintain optimal network performance and information exchange by monitoring the interface, and responding quickly and efficiently to changes in network use, JU availability and JU geographic distribution.

4.1.2 Functional Areas

4.1.2.1 The OPNET Management process includes the following functional areas:

a. Network Initialisation.

b. Network Plan Maintenance.

c. Synchronisation and Network Time Maintenance.

d. Relative Navigation Maintenance.

e. Network Participation Status Monitoring.

4.1.2.2 There are often significant interdependencies between these functional areas. For example, synchronisation and RELNAV are dealt with as two distinct functions, however, these processes are closely related and the degree of interdependency between the two will depend on a JU’s network function (eg. PRU, SU, NTR, NC)

4.2 NETWORK INITIALISATION

4.2.1 Network Initialisation

4.2.1.1 Network initialisation is the co-ordinated activation of a MIDS network in accordance with the OPTASK Link. The aim of network initialisation is to synchronise all JUs to a common time reference.

4.2.1.2 Network initialisation comprises the following tasks:

a. Processing the network configuration information at unit level and producing platform specific IDL.

b. Platform initialisation.

4.2.2 Platform Initialisation

Platform initialisation is the transfer of a platform specific IDL, merged with platform specific and mission specific parameters, to a MIDS terminal. This is normally achieved by electronic means.

4.2.3 Critical Parameters

To synchronise to a network, a JU must be initialised with at least the following minimum parameters:

a. JU Address.

b. Default Transmission SECurity (TSEC) cryptovariable.

c. Default Message SECurity (MSEC) cryptovariable (if different from the TSEC cryptovariable).

d. Network time uncertainty.

e. Network time (accurate to within the specified network time uncertainty).

f. Current Crypto Period Designator (CPD).

g. Initial Position.

h. Default Net Number.

4.2.4 Co-ordinated Network Entry

Prior to attempting network entry, a JU is initialised with a complete set of parameters that determine the JU's transmission capacity, modes and roles as specified in the OPTASK Link and derived from the network design in use.

4.2.5 Uncoordinated Network Entry

In the absence of an IDL, all terminal parameters are automatically set to default values. However, any JU capable of initialising its MIDS terminal with the minimum parameters listed in paragraph 4.2.3.1 may synchronise to a network. The JU must then obtain transmission capacity from the NM for those PGs for which it has information exchange requirements. If over-the-air initialisation (OTAI) messages are authorised (and implemented by the unit supporting the NM) then the NM may use OTAI to initialise a JU which has entered with only default initialisation data.

4.2.6 Connectivity

4.2.6.1 For a MIDS unit, a JU enters a network by capturing an initial entry message transmitted by the either the NTR or an IEJU (or active Main Net relay platform) which has achieved fine synchronisation. For this to occur, a JU attempting to synchronise must be in direct connectivity with at least one of these network functionaries. A JU equipped with a Class 1 terminal, enters a network by receiving a specified P message or N7-1 test message.

4.2.6.2 PRUs, NCs and SNCs transmit RTT messages to achieve and maintain fine synchronisation with the NTR. However, in order for an RTT exchange to take place, the originating JU must have received a PPLI message from at least one active JU that is already in fine synchronisation with the network and that is:

a. In RLOS and within approximately 300 nm of the originating JU.

b. Capable of responding to an RTT interrogation.

c. Declaring a Q_t that is greater than that of the originating JU.

4.2.6.3 RTT Reply Status Indicator

4.2.6.3.1 The RTT Reply Status indicator is part of the PPLI message data set and indicates whether or not a JU is capable of replying to an RTT interrogation. If a MIDS terminal detects a fault which may result in message TOA measurements being inaccurate, the terminal will set its RTT Reply Status to NOT OPERATIONAL, and the terminal will not transmit any RTT reply messages. Furthermore, all PPLI messages transmitted by a terminal in polling mode have the RTT Reply Status set to NOT OPERATIONAL.

4.2.6.3.2 If, at network initiation, the NTR reports that its RTT Reply function is inoperative, JUs that are initialised as PRUs will be unable to achieve fine synchronisation. **Corrective action must be taken or the network will not function**. Therefore, the NM should activate the standby NTR platform as soon as possible. If the NTR reports that its RTT function is inoperative after network initiation, when other JUs are already synchronised, then the consequences are less severe. However, the NM should still seek to transfer the NTR function to another platform in order to maintain optimum network integrity.

4.2.7 Monitoring and Maintenance

Network entry and exit are distinct and significant events as they may affect the integrity of a network. Furthermore, as the actual configuration of a JU is essentially unknown until it begins to exchange data over the network, then the monitoring processes detailed in this chapter must be intensified in the initial stages of participation. This facilitates the early identification and rectification of technical and/or configuration problems.

4.2.8 Handover and On-line Re-initialisation

The NM may modify the timeslot and/or relay assignments of a JU. These changes must be documented in the OPTASK LINK and provided to any JU assigned to relieve the modified unit. The unit supporting the NM should be able to validate the handover platform's IDL after initialisation**. Failure to control the configuration of the network may result in a serious loss of operational capability**.

4.2.9 System Time Referenced Network

4.2.9.1 Network Initialisation

The NTR establishes a STRN. The first JUs to synchronise to a STRN do so by receiving an IEM transmitted by the NTR. Thereafter, IEJUs support initial entry in conjunction with the NTR, by providing what is in effect, a wide area relay of the IEM. As the NTR's system time defines the architecture of the network, then by definition, there must be **only one NTR**.

4.2.9.2 Monitoring Network Initialisation

4.2.9.2.1 The NM should establish communications with the NTR prior to network initialisation in order to facilitate the monitoring and maintenance of the network. Positive network start up is achieved when the NTR confirms synchronisation with a JU. If the JU designated as the NTR does not initialise in this role, then all other users will remain in a net-entry condition indefinitely. In this case, consideration should be given to reassigning the NTR function. Care must be taken to ensure that the original unit, designated as NTR, deselects that function.

4.2.9.2.2 The NM should monitor the ability of JUs to join the network according to pre-briefed arrival times.

4.2.9.3 Multiple STRNs

4.2.9.3.1 There is no physical way to prevent two or more JUs from selecting the NTR function simultaneously. If this occurs at network initialisation, then each NTR will establish a separate STRN. These networks are likely to be closely correlated in time to the order of a second. However, the two networks are unlikely to be synchronised to the order of a millisecond, therefore, no data exchange between them is possible.

4.2.9.3.2 To safeguard against this situation, a STRN should be initiated from a JU over which the NM has direct control, whenever possible. Furthermore, the NM should monitor all initial network joins and ensure that there are no missing JUs, which could indicate that there are two or more networks.

4.2.9.3.3 The principal difficulty with multiple STRN situations lies in recognising when the situation exists. Monitoring the on-line plan is the key method by which this is achieved. This scenario may also be identified by the following indications:

a. Different JUs, that have achieved fine synchronisation, report that they are unable to receive data from JUs with whom they have RLOS. If a network monitoring facility is available to the NM he may be able to confirm this fragmentation by non-receipt of active JUs PPLIs.

b. More than one unit has a Time Quality of 15 (assuming time separation allows receipt of both units).

c. Units periodically reverting to "no synchronisation" as their position changes.

4.2.9.4 Maintaining a Single STRN

4.2.9.4.1 If a multiple STRN environment is detected, then the NM must take steps to correct the situation as soon as practicable. The co-ordination and time required to achieve this is determined by the following factors:

a. The number of errant NTRs (i.e. the number of STRNs in operation).

b. The number of JUs synchronised to each errant NTR.

c. The number of IEJUs synchronised to each errant NTR.

d. The degree of non-MIDS communications between JUs.

4.2.9.4.2 Recovering from a multi-STRN situation is essentially procedural, as it is unlikely that the unit supporting the NM will have connectivity with more than one of the STRNs. The recovery procedure is a 3 stage process as follows.

a. Stage 1 - Irrespective of which JU has been assigned the NTR role, the NM should retain the NTR to which the greatest number of JUs are synchronised. Having determined which NTR to retain, the NM should then instruct all non-NTR JU's, which are synchronised to NTRs **other than** the nominated NTR, to switch their MIDS terminals to standby (i.e. exit their respective networks). Before proceeding to the next stage of the recovery process, the NM must receive positive confirmation that:

   i. The MIDS terminals of all IEJUs (which includes main net relay JUs), have been switched to standby.

   ii. The NTR JUs, other than the nominated NTR, are not receiving any data over the interface.

If any of the NTRs is receiving data, then there is one (or more) JU which has not set its MIDS terminal to standby. This situation must be rectified before proceeding to the next stage of the recovery process.

b. Stage 2 - When Stage 1 is complete, the NM must instruct each NTR which has not been directed to retain this role, to deselect the NTR function and then switch its MIDS terminal to standby, **in that order**. Before executing the next stage of the recovery process, it is essential that the NM receives positive confirmation from each of these NTRs, that:

i. The NTR function has been deselected.

ii. The MIDS terminal is in standby.

c. Stage 3 - when the errant NTR network shutdown phase is complete, the NM may then instruct all JU's whose MIDS terminals are in standby, to switch their terminals back on and then execute the start net entry procedure.

4.2.9.4.3 If any errant NTRs, or IEJUs which were not synchronised to the nominated NTR, are still transmitting when Stage 3 of the recovery procedure is executed, then it is highly probable that some JU's will re-synchronise to these units. In which case the multi-STRN environment will still exist and the recovery procedure must be repeated.

4.2.10 External Time Referenced Network

4.2.10.1 Monitoring Network Initialisation

Monitoring the initialisation of an ETRN is essentially the same as for a STRN. However, in an ETRN, **only a JU^E may operate in the NTR role**. Furthermore, a NTR JU^E must achieve fine synchronisation with the ETR, before it can begin to transmit IEMs. All other JUs, including non-NTR JU^{E}s, can acquire network time by capturing an IEM. Having acquired network time, any JU^E can then achieve and maintain fine synchronisation either by interrogating or observing other JUs or by observing the ETR. A non-JU^E however, can achieve and maintain fine synchronisation by observing or interrogating other JUs only. The NM should monitor the network initiation process to ensure that the network is established as pre-briefed. In the event that the NTR JU^E cannot synchronise to the ETR then it will not transmit IEMs and non-JU^{E}s will not be able to synchronise to the ETRN. However, if one or more additional IEJU^{E}s are scheduled to join an ETRN (by DNE) then access to the ETRN will be established once the first of these IEJU^{E}s achieves fine synchronisation with the ETR. If the scheduled NTR was the only available JU^E then a STRN must be established.

4.2.10.2 Multiple NTRs

4.2.10.2.1 In contrast to STRN operations, the existence of multiple NTRs is not detrimental to the integrity of an ETRN **providing they are all JU^E NTRs**. If a non-JU^E initialises as a NTR, then the situation is the same as for multiple STRNs.

4.2.10.2.2 Notwithstanding the fact that it is not detrimental to have more than one NTR JU^E operating in an ETRN, once fine synchronisation with the ETR has been achieved, a JU^E which executes DNE and is not designated as a NTR in the OPTASK Link, should deselect the NTR function and revert to operating as an IEJU^E. This ensures that the JU is able to receive updated IEM and NTU messages.

4.3 MONITORING AND MAINTENANCE PROCEDURES

Within each of the functional areas listed in para 4.1.2, there are two distinct tasks:

a. Monitoring.

b. Maintenance.

4.3.1 Monitoring

Network monitoring is the analysis of specific parameter values to determine the operational status of a network. The monitoring process allows the NM to identify and resolve non-optimal conditions or technical problems. By performing this task continuously, the NM can maintain network integrity and optimal information exchange. The ability of the NM to monitor the network will be dependent on several factors including monitoring equipment capabilities, operator training, and platform implementations.

4.3.1.1 Monitored Parameter Sources

4.3.1.1.1 Precise Participant Location and Identification Messages

The transmission of PPLI messages is an automatic terminal function by which JUs report their position, identity and interface status. The PPLI message is the NM's primary source of information as to the state of the interface. However, in addition to the data provided by a JU in its PPLI message, there are a considerable number of other parameters that may be monitored. Ideally these parameters should be monitored continuously to ensure that both gradual and instantaneous changes in platform and network status are detected in a timely manner. The parameters that may be monitored are listed in Table 4.1 and are grouped into three 3 distinct categories:

a. On-line Plan.

b. Individual.

c. Network.

These 3 categories are not mutually exclusive and some parameters appear in more than one category.

Table 4.1 - Monitored Parameters

On-line Plan	Individual	Network
Network start/stop time Network Design(s) IEM Assignments Range Mode Comm Mode Packing Limits Default Parameters Power Settings Grid Origin IFF codes Connectivity TNs IU Number Platform Type Platform Activity ID Load Max TSDF Relay Functions Relay Modes Operating base Operating base ETD Operating area, route and/or station On-station time Handover Off-station time Recovery Base Recovery Base ETA Network Role(s) Geodetic position of fixed-site JUs Crypto short titles Platform unique key SDU serial number SDU/CVLL Pairings Control net Voice nets Special Nets NonC^2 Net	Physical presence Entry Time Exit Time IU Number Platform Type Platform Activity Course Speed ID Load Q_t Average Q_t Reported position Predicted position Q_{pg} Average Q_{pg} Altitude/Height Bearing and Range from a specified point RELGRID position Q_{pr} Average Q_{pr} Q_{ar} Relay Status RTT Reply Status Timeslot utilisation TSDF Network Role Connectivity (Q_c) NPS Average error rate Average IEM failure rate SDU/CVLL Pairings SDU serial number Control net Controlling Unit Voice nets NonC^2 Net NonC^2 net activity Range Mode IFF codes	Time Roles TSDF End-to-end connectivity IEM failure rate Message error rate Q_t Q_{pg}

4.3.1.1.2 On-line Plan Parameters

On-line plan parameters may be used to evaluate the current configuration of the interface.

4.3.1.1.3 Individual Parameters

Individual JU parameters may be used to evaluate the actual participation status of a specific JU.

4.3.1.1.4 Network Parameters

Network parameters provide a ‘quick-look’ indication of the integrity of the interface.

4.3.1.2 Monitored Parameter Derivation

4.3.1.2.1 The value of a parameter is determined by one of the following four methods or processes:

a. Planning.

b. Reporting.

c. Inference.

d. Computation.

4.3.1.2.2 The parameters that may be monitored are re-listed in Table 4.2. However, in this table the parameters are grouped under headings that describe the method or process by which their values are determined.

4.3.1.3 Planning Parameter Values

The value of a Planning parameter is derived from either the network design, the OPTASK Link, the ATO or other related operational tasking messages.

4.3.1.4 Reported Parameter Values

The value of a Reported parameter is derived from:

a. A MIDS message which is transmitted by a JU on a periodic basis (e.g. a PPLI message) or in response to an interrogation message (e.g. Cryptovariable status request message).

b. A platform operator reporting a parameter setting (e.g. range mode selected) via a voice net.

4.3.1.5 Inferred Parameter Values

The value of an Inferred parameter is determined by observing one or more reported and/or computed parameters. For example: if all PRU JUs in direct connectivity with the unit supporting the NM are maintaining a Q_t of 14, then the NM can infer that there is at least one JU, operating as a NTR (ie. Reporting a Q_t of 15).

4.3.1.6 Computed Parameter Values

A Computed parameter is produced, via a specific calculation (normally a sum or average), from other reported or computed parameter values (e.g. Network Q_t, which is the mean average reported Q_t of all active JUs, averaged over a defined period).

4.3.1.7 Indeterminate Parameter Values

An indeterminate parameter value is one that is not reported explicitly, and for which a value can be neither inferred nor computed. For example: in many nonC^2 JU's, the operator-system interface does not allow the operator to access a terminal's Range mode setting. However, if a JU is initialised with the wrong range mode setting, then this can have a catastrophic effect on the RELNAV function (see Section 4.7). There are a number of parameters, which the NM or platform operator may not be able to determine on-line. These parameters are listed in column 5 of Table 4.2.

Table 4.2 - Methods for Determining Monitored Parameter Values

Planned	Reported	Inferred	Computed	Indeterminate
Network start/stop time Network Design(s) Operating base Operating base ETD Operating area, route and/or station On-station time Off-station time Recovery Base Recovery Base ETA Network Role(s) Handover	Network Time Entry Time Exit Time Physical presence IU Number Platform Type Platform Activity Course Speed Q_t Position Q_{pg} Altitude/Height RELGRID position Q_{pr} Actual Connectivity (Q_c) RTT Reply Status Relay Status (for main net, control and voice relay functions) SDU serial number SDU/CVLL pairings Control net Voice nets NonC^2 Net IFF codes IEM assignments	Physical presence (if receiving data but no PPLI) ID Load Relay Status (for PG, directed and Zoom relay functions) JU Timeslot utilisation (including relay functions) JU TSDF (including relay functions) Theoretical Connectivity Network Role(s) Handover	Network TSDF Network End-to-end connectivity Network IEM rate Network Message error rate Network Q_t JU average Q_t Network Q_{pg} JU average Q_{pg} Position JU average Q_{pr} JU average error rate JU average IEM failure rate Bearing and Range from a specified point JU TSDF (not including relay functions) JU Timeslot utilisation (not including relay functions) Operating area, route and/or station	Time Uncertainty IEM Assignment inhibits Range Mode Comm Mode Packing Limits Default Parameters Power Settings Grid Origin ETR setting Crypto short titles loaded Platform unique key loaded

4.3.2 Maintenance

When non-optimal conditions and/or technical problems are identified, it may be necessary to modify the configuration, function, or network participation status of one or more JU's. This activity is called network maintenance, and is achieved in one of 4 ways:

a. By the use of specific J-series messages (J0.3 Time Slot Assignment, J0.4 Radio Relay Control, J0.6 Communications Control) to modify the timeslot and/or relay assignments of one or more JUs, directly.

b. By the use of a J-series command message (J9.0, if implemented) to instruct a JU's operator to assume or relinquish a specific network roles or functions.

c. By transmitting a free text message (if implemented) to the JU.

d. By issuing verbal instructions to a platform operator.

4.3.2.1 Tactical Situation

The NM must be aware of the tactical situation at all times and it is essential for the NM to consult with the appropriate tactical staff before attempting any extensive, procedural on-line maintenance. There may be other operational activities, of a higher or vital nature that would be jeopardised or degraded by immediate OPNET management actions. Therefore, it may be prudent to delay the desired management until after the activity and subsequent liaison with the tactical authority.

4.3.2.2 Direct Modification of Timeslot and Relay Assignments

There are a significant number of parameter values that must be compiled and validated before any interface modification instruction can be transmitted. Furthermore, all changes made to a JU's timeslot and relay assignments must be recorded accurately and tracked continuously. If a few minor changes, which require only a small volume of instructions are used then these alterations may be executed manually. However the potential for error must be considered. If a change results in a large volume of instructions then the potential for error would be increased considerably.

4.4 NETWORK PLAN MAINTENANCE

4.4.1 Off-line Plan

4.4.1.1 The product of the pre-mission planning process is an off-line network plan, which is described and promulgated using the appropriate OPTASK messages. However, once a network has been activated, it may become necessary to modify the plan if the conditions on which the plan was predicated change.

4.4.1.2 Permanent or long-term minor changes may be promulgated by issuing an OPTASK Link update. The NM should be aware that changes which require a change to the network design should be co-ordinated with the issuing Network Design Facility, as some platforms cannot change initialisation data changes at the platform level. It is impractical to use the OPTASK Link to promulgate temporary changes that result from a highly dynamic tactical situation (e.g. the re-assignment of network roles and resources). Therefore it is essential that the NM maintain an on-line plan which reflects the actual configuration of the interface at any point in time.

4.4.2 On-line Plan

When a network is initiated, the off-line plan becomes the initial on-line plan, which must include, but is not limited to, the following information:

a. ORBAT: which must reflect any attrition and redeployments.

b. Air Tasking Order (ATO).

c. IDL: which must reflect any pre-mission and/or on-line changes to timeslot and relay block assignments.

d. IDL-to-platform mapping: which must reflect any on-line platform re-initialisations.

e. Relay assignments: which must reflect any on-line re-assignment of relay functions.

f. Network Role Assignments.

g. Voice net assignments.

h. Control net assignments.

i. Fighter-to-Fighter net assignments.

j. Crypto load-to-platform mapping based on unique platform identifier (if OTAR is to be employed).

k. EMCON condition.

4.4.3 Monitoring the On-line Plan

Monitoring the on-line plan is the process of comparing the values of parameters which are elements of the on-line plan, against those being reported, derived or inferred from information being received (i.e. checking that a JU is present and operating as expected).

4.4.3.1 Transmit Assignments

4.4.3.1.1 If the NM is required to monitor the transmit timeslot assignment of a JU, then ideally, he should have access to equipment that:

a. Compares the timeslots in which a JU’s transmissions are received, with that JUs transmit assignments record held in the on-line plan.

b. Provides a facility to alert the operator of transmissions received in timeslots that have not been allocated to the JU transmitting in those slots.

c. Provides a visual display of actual timeslot utilisation against the on-line plan allocation to verify timeslot usage.

4.4.3.1.2 A JU will not necessarily transmit information in every NPG in which it has been initialised to transmit, on a regular basis. Furthermore, the unit supporting the NM may not be in connectivity with every JU in all NPGs at all times (e.g. due to multi-netting). Therefore in practice, the NM's record of a JU's timeslot utilisation will never be 100% complete. However, the principal reason for monitoring a JU's transmissions is to verify that the JU has initialised with the correct IDL. If this is not the case then the majority of transmissions received by the NM from the JU being monitored, will not concur with the on-line plan. When this is the case, the NM may use a visual timeslot utilisation display to infer which IDL the JU is actually using.

4.4.4 Maintaining the On-line Plan

4.4.4.1 The NM must ensure that the on-line plan reflects the actual configuration of the interface at all times. Furthermore the NM must use the ATO and real-time information to maintain an accurate mission status record for each JU.

4.4.4.2 The NM's response to a disparity between the on-line plan and the information derived from the network, will depend on the nature of the disparity and the specific parameter(s) in question. The options and methods for rectifying a non-optimal situation or technical problem are covered in the sections that follow.

4.4.5 Maintenance Issues

4.4.5.1 IDL Modifications

4.4.5.1.1 If the OPNET management function is to be implemented effectively, then the NM's record of a platform's IDL must be accurate. Therefore **the Network Specific Parameters (NSP) parameters of an IDL should not be modified at either unit or platform level, except as directed by the NM/SubNM or appropriate authority**. This includes modifications that appear to have no apparent affect on the communications functionality of an IDL (eg packing limits).

4.4.5.1.2 If a unit or platform experiences problems in either creating or loading an IDL, then the exact nature of the problem must be reported to the NM as soon as possible.

4.4.5.2 Maintaining IDL Integrity

If it is determined that a JU's IDL is incomplete or incorrect, then the NM must either: instruct a platform operator to re-initialise with the correct IDL or, if this is not possible[1], then the NM must reinitialise the JU directly, using OTAI. If the unit supporting the NM does not provide this facility, or the JU cannot process these instructions, then the NM must determine if the JU's state of initialisation will have any detrimental impact on information exchange or on the network. If so, then the JU must be instructed to either operate in CONDITIONAL RADIO SILENT or exit the network.

4.5 NETWORK TIME MAINTENANCE

4.5.1 Definitions

4.5.1.1 JU Time Quality

Q_t is a measure of the accuracy of a JU's terminal time with respect to the time reference. JU Q_t is an important reported parameter used to monitor the integrity of a MIDS network.

4.5.1.2 Synchronisation

4.5.1.2.1 If a non-NTR JU becomes isolated, its Q_t will begin to degrade at a rate which is determined by its terminal's 'oscillator drift rate' parameter and its state of synchronisation with the time reference at the moment of isolation. If connectivity with the time reference is not re-established, the Q_t of an isolated non-NTR JU will reach zero within a few hours. At Q_t zero, a terminal will eventually revert to coarse synchronisation status and cease to transmit data. Therefore, in order for a JU to continue to pass data over the interface, connectivity with the time reference is essential.

4.5.1.2.2 The oscillator drift rate[2] parameter reflects the expected performance of the MIDS terminal clock oscillator. However, oscillator drift rate is not applied if a JU is operating as the time reference (i.e. a NTR's oscillator is uncorrected or 'free running'). Synchronisation, therefore, is the process by which a non-NTR JU tracks the time reference, by continuously correcting and refining own terminal time to compensate for the oscillator drift rate in both own terminal and that of the time reference.

4.5.1.3 Network Time Quality

Network Q_t is the mean Q_t of all active JUs averaged over a defined period (typically 12 seconds). Network Q_t is a derived network parameter the value of which provides a 'quick look' indication of overall network integrity.

[1] Not all JUs provide a facility for a platform operator to access and modify timeslot assignments.

[2] Oscillator drift rate is a terminal software parameter. It can not be changed by an end-user and its absolute value may vary from one platform and/or platform variant to another.

4.5.1.4 Dishonest Time Quality

The accuracy or 'honesty' of the Q_t reported by a JU is critical to the synchronisation function. If a JU's time error is actually greater than its reported Q_t, then its Q_t is described as 'dishonest'.

4.5.1.5 Unstable Time Quality

When a JU initiates an RTT exchange with another JU, the initiating JU will expect the TOA of the RTT reply to lie within predicted maximum and minimum values. If the TOA of the reply does not lie within the values predicted (i.e. the interrogated JU is declaring a dishonest Q_t), then the anomaly will cause the JU to degrade its estimate of network time. This re-evaluation of a terminal's state of synchronisation with the time reference will be reflected in the JU's reported Q_t, which will drop significantly. If this situation persists, the JU's terminal will eventually initiate a 'synchronisation reset' and revert to coarse synchronisation status. However, if the TOA values do not consistently fall outside the values predicted (e.g. one TOA in range and the next out, cyclically), then this results in the JU's Q_t fluctuating significantly, from one report to the next. This condition is called 'unstable Q_t' and is the key indicator to problems relating to network time.

4.5.1.6 Optimum Time Quality

4.5.1.6.1 The NTR has by definition, zero time error and declares the highest Q_t (15). The time qualities of all other JUs reflect an estimate of their time error relative to the NTR's clock. The highest Q_t that may be achieved by an active, non-NTR JU is 14. To achieve this a JU must be in direct connectivity with the NTR. Q_t degrades by one with each intermediate JU. However, the actual value will depend on other factors such as interference levels, propagation anomalies, individual system performance.

4.5.1.6.2 The ratios of PRUs and SUs operating in a network will also affect the Network Q_t. SU JUs use passive synchronisation techniques, primarily. However, a SU may transmit a RTT message to aid the passive synchronisation function. The practical effect is that a SU's Q_t will invariably fluctuate between the maximum value possible (which depends on whether or not the SU JU has direct connectivity with the NTR) and a value approximately equal to that of its Q_{pg}. If there are a significant number of SU JUs operating, then the Network Q_t will be lower than that which would be expected when all JUs are PRUs.

4.5.1.7 Network Time Transient

A Network Time Transient is caused when a dishonest Q_t reported by a JU causes timing synchronisation problems in other JUs. This problem is most apparent when JUs have intermittent connectivity with the correct system time reference and/or the dishonest Q_t source. Network Time Transients are characterised by sudden drops in individual JU Q_t. along the connectivity path between the JU which is source of the timing error and the most distant JU. When the time disparity between the correct and incorrect sources is relatively large (typically 18 microseconds), it can also lead to loss of synchronisation.

4.5.2 Maintaining Synchronisation

4.5.2.1 Maintaining IEJUs

The NM must maintain connectivity to support initial entry across the entire operating area. This is achieved by either activating additional IEJUs or, if this is not possible, by requesting that one or more existing IEJUs reposition themselves to provide the connectivity necessary.

4.5.2.2 Maintaining Primary and Secondary Users

4.5.2.2.1 If a PRU does not achieve optimum Q_t consistently (and there are no other indications of a degraded link environment), then the NM should confirm with a platform operator that the JU's ORGANISATIONAL USER TYPE is set to PRIMARY USER.

4.5.2.2.2 If a SU consistently achieves optimum Q_t, then the JU may actually be operating as a PRU, in which case it will be transmitting RTT messages at regular intervals. A SU is not normally initialised to transmit in an RTT PG (if it is, then it can operate as a PRU). If the SU is actually operating as a PRU but has no assigned RTT timeslots, then it will pre-empt every 3rd or 4th PPLI transmission and transmit a RTT instead. If the unit supporting the NM provides an incremental missed reports counter, then this can be used to monitor for this behaviour. If such behaviour is observed, then the NM should confirm with a platform operator that the JU's ORGANISATIONAL USER TYPE is set to SECONDARY USER.

4.5.3 Maintenance Issues – Common

4.5.3.1 Network Time Update

4.5.3.1.1 To maintain or change the correlation between Network Time and a designated absolute time standard, it may be necessary for the NM to initiate a J0.2, Network Time Update (NTU) message.

4.5.3.1.2 **Only the NM or a unit directed by him should initiate NTU messages**. The size of the time adjustment and the execution time are specified in the NTU. A NTU message is disseminated in the same way as the IEM. Therefore the authorised unit must transmit a NTU to the NTR, in any timeslot except the initial entry timeslot. The NTR will process a NTU received in a timeslot other than the initial entry timeslot and will retransmit it with the IEM in the Initial Entry time slot. Other JUs, including IEJUs and main net relay JUs, will process a NTU only if it is received in the initial entry timeslot. Like the IEM, the NTU is received, interpreted and implemented by a MIDS terminal automatically and no operator action is required. Furthermore a NTU should not be scheduled to execute within 15 minutes of cryptographic key rollover. NTUs are not interpreted by Class 1 terminals and so **NTU messages should not be used in networks which include Class 1 terminals**. Because of their ability to disrupt network operation, **NTU messages should be used only when absolutely necessary**.

4.5.3.1.3 The NTR, IEJUs and main net relay JUs will transmit the NTU until the execution time specified. At execution time, all JUs that have received the NTU will apply the time correction specified and then purge the message.

4.5.3.1.4 Within STRNs, NTU messages should only be employed when the network system time has deviated from the original time datum (eg ZULU time) to such an extent that new participants experience net entry problem due to the time drift. The use of NTU messages should not be necessary within ETRNs as, by definition, the network time is continuously correlated with the external time source.

4.5.3.1.5 The period of time between the time of transmission of a NTU and the time of execution must be sufficient to allow the message to be distributed to all JUs. However, NTU message dissemination is dependent on a number of factors (e.g. network integrity, IEJU density) and can not be determined with any certainty. Therefore a considerable margin of error must be applied.

4.5.3.1.6 Once a NTU has been initiated and disseminated, it can not be modified or cancelled. Therefore, the NM must not attempt to make a further adjustment to network time when there is already a NTU pending execution.

4.5.3.1.7 IJMS Class 1 Units

IJMS Class 1 JUs do not implement the J0.2 NTU. Therefore they will be de-synchronised from network time when a NTU is executed. As a general rule, the NM should not use the NTU message if a significant number of Class 1 JUs are present in the network. However, if there are relatively few Class 1 JUs participating, then the NM may update the MIDS JU's using a NTU and instruct the Class 1 JUs to re-synchronise to the network at a specified time (assuming the NM has communications with the Class 1 JUs).

4.5.3.2 Range Mode Effect

4.5.3.2.1 Jitter

4.5.3.2.1.1 A MIDS terminal operating in normal range mode, applies a pseudo-random 'jitter' period to the beginning of all standard and packed-2 single pulse messages it transmits. When operating in extended range mode the jitter applied is approximately half that applied in the normal range mode. Therefore to determine an accurate TOA, a terminal must compensate for the pseudo random jitter applied to all messages it receives.

4.5.3.2.1.2 All MIDS terminals calculate jitter on a timeslot by timeslot basis. However, there is no provision made for one terminal to determine the range mode setting of another terminal. Thus a receiving terminal will compensate for jitter based on its own range mode setting. If one terminal is operating in extended range mode and another in normal range mode then the jitter calculated by each will be different. The effects which occur as a result of JUs selecting different range modes are the same as the effects noted when dishonest Q_{pg} are reported by JUs.

4.5.3.2.2 Active Fine Synchronisation

Active fine synchronisation is achieved by the exchange of RTT messages. As jitter is not applied to an RTT message, a JU's range mode setting will not affect its ability to achieve and maintain fine synchronisation when the JU is operating as a PRU.

4.5.3.2.3 Passive Fine Synchronisation

In the passive mode, fine synchronisation is achieved by processing TOA measurements and position information of PPLI messages received from active JUs. If the jitter calculated by the synchronising JU is different from that actually applied, then the TOA calculations will be in error, and the size of the error may vary considerably (hundreds of miles) from one report to the next. Therefore the range derived from the TOA will bear little relation to the actual range of the JU, when compared to the position of the JU as reported in its PPLI message. In this situation, a JU operating in RADIO SILENT will never achieve fine synchronisation.

4.5.3.2.4 Aided Passive Fine Synchronisation

In the aided passive mode, a SU uses passive synchronisation techniques primarily. However, it will eventually resort to transmitting RTT messages if it fails to achieve fine synchronisation within a certain period. In which case, the SU essentially becomes a PRU momentarily and will, therefore, eventually achieve fine synchronisation.

4.5.3.3 Class 1 Unit

If a IJMS CLASS 1 TERMINAL loses connectivity with its synchronisation source then its Q_t invariably freezes at whatever value it achieved before connectivity was lost. Given that the IJMS CLASS 1 TERMINAL oscillator will continue to drift, then its Q_t will eventually become dishonest. If the IJMS CLASS 1 TERMINAL has achieved optimum Q_t before connectivity with its synchronisation source was lost (Q_t = 14) then its Q_t will become dishonest within a few minutes. IJMS CLASS 1 TERMINAL terminals in this condition are a common source of network time transients as described in paragraph 4.5.1.7.

4.5.4 System Time Referenced Network Operations

4.5.4.1 Monitoring STRN operations

4.5.4.1.1 Monitoring the NTR

The NM may determine which platforms are operating as NTRs by monitoring the Q_t of each participating JU. Within a STRN, only one JU should be declaring a Q_t of 15 and the identity of this JU should correspond with the on-line network plan. The Q_t of all non-NTR JUs should always be less than 15. Furthermore, if the NM or the unit supporting the NM does not have connectivity with all the participating JUs, then it is possible to infer the presence of one or more NTRs by either monitoring individual JU Q_t or monitoring the Network Q_t.

4.5.4.1.2 Monitoring IEJUs

4.5.4.1.2.1 A NTR transmits an IEM every frame in the initial entry timeslot. IEJUs (which includes main net relay JUs) transmit an IEM in every other frame in the same timeslot. Therefore it is possible to determine if a JU is operating as an IEJU by monitoring its IEM transmissions. However, all IEM messages are transmitted in contention on Net 0 and a MIDS terminal can only receive one transmission in any given timeslot.

4.5.4.1.2.2 When two or more JUs transmit in the initial entry timeslot, the unit supporting the NM will receive the transmission from the JU that is closest to it. If the NTR is the closest JU to the NM's location, then the unit supporting the NM will receive the NTR's IEM only. However, when this is not the case, the unit will receive from the closest IEJU that initiates an IEM transmission. Therefore, the receipt of an IEM from a JU confirms that the JU is operating as an IEJU (or the NTR). However, the fact that an IEM has not been received from a JU, does not necessarily mean that the JU in question is not operating as an IEJU. If the NTR is the closest JU to the unit supporting the NM it will receive the NTRs IEM only.

4.5.4.1.3 Monitoring Primary and Secondary Users

4.5.4.1.3.1 A PRU uses active techniques to maintain synchronisation with the NTR. Optimal Q_t for a PRU is one less than that of the JU with which it is exchanging RTT messages. Therefore the average Q_t of a JU assigned to operate as a PRU, should be one less than the highest Q_t of whichever JUs, is in direct connectivity with the PRU. .

4.5.4.1.3.2 SUs use the aided passive synchronisation technique and will transmit RTT messages if required. Optimum Q_t for a SU is in the range bounded by its average Q_{pg} and one less than whichever JU, in direct connectivity with the SU, has the highest Q_t.

4.5.4.1.4 Monitoring Criteria

To ensure that optimum Q_t is maintained and that the anomalous situations that may occur when operating within a STRN are detected quickly, the NM should monitor JU Q_t and Network Q_t for the following conditions:

a. Two or more JUs report a Q_t of 15.

b. The JU assigned as the NTR reports a Q_t of < 15.

c. The NTR reports RTT Reply Inoperative.

d. The NTR reports Conditional Radio Silent.

e. The NTR reports Tactical Data System Failure.

f. The NTR reports Inactive.

g. The NTR reports Polling.

h. Any JU reporting a Q_t of < 6.

i. Unstable Q_t.

j. Network Q_t degrading.

k. Own terminal reverting to coarse synchronisation.

l. One or more JUs reporting loss of fine synchronisation.

m. Own terminal time > reference timebase ± network time uncertainty.

4.5.4.2 Maintenance Issues

4.5.4.2.1 No NTR

Loss of the NTR will have little immediate effect on synchronisation or data exchange providing that at least one IEJU continues to operate (to support initial entry/re-entry) and that at least one other JU has achieved a reasonably high Q_t (>12). However, from the moment the NTR is lost, the Q_t of all participating JUs will begin to degrade and this will adversely affect RELNAV and track correlation functions. These functions are seriously degraded if a JU's Q_t is < 6 (see paragraph 4.6.1.3.2). Furthermore, if there is no NTR, then a terminal that has achieved a Q_t of 7 or greater will lose fine synchronisation with the time reference after approximately 3-5 hours. If a terminal loses fine synchronisation with the time reference it will cease to transmit data. Therefore it is essential that the NM activates the standby NTR well before the Q_t of any participating JU is degraded significantly (< 7). If no action is taken and optimal Network Q_t existed at the moment the NTR was lost, then interface functions will be significantly degraded after approximately 15 minutes.

4.5.4.2.2 Multiple NTRs

If a second JU selects the NTR function then by definition, there are two STRNs operating simultaneously. In this situation, there will be little immediate effect on synchronisation or data exchange as the second STRN will be highly correlated in time to the first. However, as the errant NTR's terminal is no longer attempting to maintain synchronisation with the designated NTR, then the NTRs' clocks will drift apart and the two STRNs will gradually de-synchronise. JUs that process information from both NTRs will experience synchronisation anomalies and this will adversely affect RELNAV and track correlation functions. Furthermore, if a JU enters an established STRN and then erroneously selects the NTR function very shortly thereafter (< 1 minute), the STRN de-synchronisation process will be accelerated. Therefore it is essential for the NM to instruct the errant NTR to deselect the NTR function, well before the two networks become significantly de-synchronised. If no action is taken and optimal network Q_t existed at the moment the errant JU selected the NTR function, then interface functions will be significantly degraded after approximately 3 hours.

4.5.4.2.3 Indirect Connectivity with NTR

4.5.4.2.3.1 If the NM or the unit supporting the NM does not have connectivity with the NTR, synchronisation may be maintained via an intermediate JU. If an intermediate JU is maintaining a Q_t of 14, then the NM can infer the presence of a NTR. If subsequently the NTR exits the network (e.g. due to equipment failure) and is not replaced, then the Network Q_t and the Q_t of the intermediate JU will begin to degrade. In this situation the NM can infer that the NTR has either become isolated, or is no longer active in the network.

4.5.4.2.3.2 In circumstances when two JUs have selected NTR in a STRN, the NM may not be immediately aware of this situation due to a lack of connectivity with the JUs. An intermediate JU in direct connectivity with both NTRs and the NM will maintain synchronisation by RTT exchange with one of the NTRs. If this intermediate JU subsequently loses direct connectivity with the first NTR, it will attempt to RTT with the second NTR. The intermediate JU will calculate expected maximum and minimum values for the RTT reply. However, as the two NTRs are not maintaining synchronisation with each other, then the RTT reply from second NTR will invariably be outside the maximum and minimum values predicted. This will cause the JU's Q_t to become unstable and may cause it to lose fine synchronisation. Unstable JU Q_t is, therefore, a key indicator to multi-NTR situations, especially when the NM does not have connectivity with any of the NTRs.

4.5.4.2.4 NTR Network Re-entry

If a NTR leaves a STRN and then restarts network entry with NTR still selected, it will not re-synchronise to the existing STRN, but will initiate a second STRN which is unlikely to be synchronised in time (to the order of a millisecond) with the existing STRN. It is thus fundamental that any JU which is attempting to synchronise (or resynchronise) to an established STRN **must ensure that the NTR function is deselected**. There are no exceptions to this rule.

4.5.4.2.5 NTR Handover

4.5.4.2.5.1 The NTR role should be re-assigned only when operationally essential (e.g. the NTR is mission complete or it becomes unserviceable). NTR handover is procedural and the handover sequence may be included in the special instructions section of the OPTASK Link. When this is the case, the handover should be co-ordinated by the JU which is assuming the NTR role. Otherwise handover must be initiated and co-ordinated by the NM.

4.5.4.2.5.2 The NTR handover procedure should be as follows:

a. Step 1 – The current NTR deselects the NTR function at the time specified or as directed by the JU responsible for co-ordinating the handover. A JU's terminal Q_t is arbitrarily reduced to 13 when the NTR function is deselected. If the JU assuming the NTR role is capable of monitoring this parameter, then this event can be taken as positive confirmation that the current NTR has relinquished the role. Otherwise the current NTR must inform the JU assuming the role, that the NTR function has been deselected (i.e. by voice or free text message).

b. Step 2 – The JU assuming the NTR role selects the NTR function and confirms that its terminal is declaring $Q_t = 15$ (either by internal monitoring or by checking with a JU which is capable of monitoring this parameter).

4.5.4.2.5.3 The use of a 'mark' or 'hack' call to co-ordinate the handover of NTR (i.e. the selection/deselection of the NTR function) is unnecessary and not recommended.

4.5.5 External Time Referenced Network Operations

4.5.5.1 Monitoring ETRN Operations

4.5.5.1.1 Monitoring the NTR

4.5.5.1.1.1 A NTR JU^E will not necessarily be the JU with the highest Q_t, as other non-NTR JU^Es may achieve a higher Q_t due to more favourable ETR coverage, lower levels of interference or enhanced equipment capabilities. In this situation, a NTR JU^E may begin to RTT with a non-NTR JU^E. This situation is quite normal when operating an ETRN. Furthermore, a JU^E that does declare a Q_t of 15 may not necessarily be operating in the NTR role.

4.5.5.1.1.2 Therefore it is not possible for the NM to determine which JU^Es are operating as NTRs by simply monitoring the Q_t of each JU. The exception to this rule is when a JU that is not ETR capable, reports a Q_t of 15. In this case, the non-ETR capable JU must be operating as a NTR, which is illegal in an ETRN. If one or more non-ETR capable JUs operate as a NTR within an ETRN, the consequences are the same as those for multiple NTRs operating within an established STRN (see paragraph 4.5.4.2.2).

4.5.5.1.2 Monitoring Criteria

To ensure that the anomalous situations that may occur when operating within an ETRN are detected quickly, the NM must monitor JU Q_t and Network Q_t for the following conditions:

a. A JU that is not ETR-capable reports a Q_t of 15.

b. No JUs which are scheduled to operate as a JU^E are reporting a Q_t of >= 9.

c. A JU that is not ETR-capable, or an ETR-capable JU that is not scheduled to operate as a JU^E, reports a Q_t greater than or equal to the highest Q_t reported by a JU^E.

d. No active JUs are registered as NTR JU^Es or as $IEJU^E$s.

e. Any JU reporting a Q_t of < 6.

4.5.5.2 Maintenance Issues

4.5.5.2.1 No NTR JU^E

An ETRN will function normally without a NTR providing there is one or more IEJU^{E}s operating. Thus loss of a NTR JU^E is only detrimental to the integrity of an ETRN if it is the only JU^E operating in the network. In which case, the consequences are the same as for a STRN. Furthermore, if the standby NTR is not a JU^E then the network will have reverted to a STRN.

4.5.5.2.2 NTR JU^E Unable to Synchronise to the ETR

If a NTR JU^E is unable to synchronise to the ETR, non-ETR capable JUs will be unable to enter the ETRN. However, if one or more IEJU^{E}s are scheduled to join the ETRN by DNE, then access to the ETRN will be established once the first of these IEJU^{E}s achieves fine synchronisation. If the NTR JU^E is the only JU^E scheduled to operate, then the NM must establish a STRN by instructing the NTR JU^E to deselect the ETR function and revert to operating as a NTR, or by instructing a non-ETR capable JU to operate as NTR.

4.5.5.2.3 NTR JU^E Loss of ETR Interface

If a NTR JU^E experiences an ETR hardware/interface failure from which it is unable to recover, **it must not deselect the ETR function without first deselecting the NTR function**. If it does, then at the moment the ETR function is deselected the NTR JU^E will revert to operating as a NTR and thus initiate a STRN, which will be highly correlated in time with the ETRN. As the JU in question is now operating as a NTR, it will cease to maintain synchronisation with the ETR and immediately start declaring a Q_t of 15. Any JU^E that has not achieved a Q_t of 15 against the ETR will attempt to use this NTR as a synchronisation source. However, if the NTR JU's Q_t against the ETR was actually less than that achieved by another JU^E, then this may cause a synchronisation reset in any JU using the NTR as a source of timing information.

4.5.5.2.4 Reverting to a System Time Referenced Network

When ETR performance is degraded (e.g. poor satellite coverage when using GPS) the NM may decide to revert to a STRN in order to improve overall network Q_t and RELNAV performance. Furthermore when only one JU^E is operational in a network and no other JU^{E}s are expected, the NM may wish to revert to a STRN.

4.5.5.2.5 NTR Handover

When there is one or more IEJU^{E}s operating, an ETRN will function normally even if there is no JU operating in the NTR role. Furthermore, it is possible for two or more NTR JU^{E}s to operate simultaneously in the same ETRN. Therefore the NTR handover procedure is essentially redundant when operating an ETRN.

4.6 GEODETIC GRID MAINTENANCE

4.6.1 Definitions

4.6.1.1 Position Quality

Q_{pg} is a measure of the accuracy to which a MIDS terminal fixes its own position in the GEOGRID. JU Q_{pg} is an important parameter used to monitor the performance and stability of the GEOGRID.

4.6.1.2 Navigation

4.6.1.2.1 When a non-PR JU first enters a network it will declare a Q_{pg} based on the accuracy of its initial three-dimensional position. It will then attempt to improve its geodetic position accuracy using the PPLI messages of other JUs meeting the criteria detailed in paragraph 4.6.1.2.2. To achieve this, a JU's terminal calculates the slant range from itself to another JU by measuring the TOA of the PPLI messages of the observed JU.

4.6.1.2.2 A subject JU will attempt to perform navigation updates using the geodetic positions declared by one or more source JUs, whenever all the following conditions are true:

a. The Q_{pg} of the source JU is greater than the subject JU's Q_{pg}.

b. The Q_t of the source JU is greater than or equal to the subject JU's Q_t.

c. The source JU's PPLI message has not been received via relay.

d. The subject JU's position reference terminal parameter is not set.

4.6.1.3 Minimum Performance Criteria

4.6.1.3.1 A JU's computed geodetic position is based on the TOA of PPLI messages transmitted by other JUs. TOA is measured with respect to a terminal's determination of the start of the timeslot in which the message was transmitted. Therefore the accuracy of a TOA measurement is affected by the magnitude of the relative clock error between any two JUs, and the Q_{pg} that a JU may achieve by this technique is directly related to its Q_t.

4.6.1.3.2 It has been determined, through trials and testing, that optimum RELNAV performance only occurs when values for $Q_{pg} > 5$. This requires a JU to achieve and maintain both a Q_{pg} and a Q_t of at least 6.

4.6.1.4 Network Position Quality

Network Q_{pg} is the mean Q_{pg} of all active JUs averaged over a defined period (typically 12 seconds). Network Q_{pg} is a derived network parameter the value of which provides a 'quick look' indication of the overall performance and stability of the GEOGRID.

4.6.1.5 Dishonest Position Quality

The accuracy or ‘honesty’ of the Q_{pg} reported by a JU is critical to the RELNAV function. If a JU’s position error is actually greater than its reported Q_{pg}, then its Q_{pg} is described as ‘dishonest’.

4.6.1.6 Unstable Position Quality

A JU that reports a dishonest Q_{pg} will induce an error in the position and Q_{pg} reported by any subject JU that uses the errant JUs TOA information for RELNAV. If the Q_{pg} error is constant, then the position and Q_{pg} computed by other JUs will be inaccurate, but likely to remain stable for as long as the subject JU continues to observe the same set of JUs. If the Q_{pg} error is not constant, then the position and Q_{pg} computed by other JUs will fluctuate considerably from one report to the next. This condition is called ‘unstable Q_{pg}’ and is the key indicator to problems relating to the stability of the GEOGRID.

4.6.1.7 Position Jumps

If the disparity between actual Q_{pg} and declared Q_{pg} is significant (tens of miles), then a JU’s terminal will eventually initiate a ‘navigation reset’, which will cause its reported Q_{pg} to drop to zero. Terminals that use the RELNAV function exclusively will also exhibit ‘impossible’ changes in their reported positions (called ‘position jumps’) from one report to the next. Position jumps are the key indicator of an impending catastrophic failure of the GEOGRID. This is described in detail in paragraph 4.6.4.2.5.1.

4.6.2 Monitoring the Geodetic Grid

RELNAV is a fully automatic process that requires no operator intervention. Therefore the GEOGRID will recover automatically from a harmful situation, providing that **any source(s) of error are identified and eliminated quickly**.

4.6.2.1 Monitoring Geodetic Position Quality

4.6.2.1.1 The NM should monitor JU Q_{pg} and Network Q_{pg} to ensure that the minimum performance criteria detailed in paragraph 4.6.2.3 are achieved and maintained.

4.6.2.1.2 The errant conditions (such as dishonest Q_{pg}) which give rise to GEOGRID anomalies (such as unstable Q_{pg}) have the same characteristics as the anomalies that result from two or more active JUs operating in different range modes.

4.6.2.2 Monitoring Position References

The NM can determine which platforms are operating as PRs by monitoring the Q_{pg} of each participating JU. Only PR JUs should declare a Q_{pg} of 15 and the identity and position of each PR JU should correspond with the on-line network plan. The Q_{pg} of all non-PR JUs should, therefore, always be less than 15.

4.6.2.2.1 Position Reference Terminal Parameter

By definition, a PR JU does not navigate. Therefore the latitude, longitude and Q_{pg} (15) values in a PR's PPLI message should not change. However, if a PR is RELNAV capable and its position reference parameter has not been set, then the PR is in fact, operating as a non-PR JU. Therefore its terminal will be performing RELNAV updates. In this situation, its reported position will begin to change slightly, even though the JU is not actually moving. Furthermore, the Q_{pg} reported by the JU will not reflect the error induced by the RELNAV process, as the position and height uncertainty parameters, which determine a JU's Q_{pg}, are fixed at initialisation. Therefore the errant PR's Q_{pg} will be dishonest.

4.6.2.3 Monitoring Criteria

To ensure that the minimum GEOGRID performance criteria are being maintained and that GEOGRID anomalies are detected quickly, the NM should monitor for the following conditions:

a A PR reports a geodetic position that does not equate to the position recorded in the on-line plan.

b. A PR's reported geodetic position is seen to change.

c. A PR reports a Q_{pg} of < 15.

d. A JU not registered as a PR reports a Q_{pg} of 15.

e. A pseudo PR reports a Q_{pg} of 15.

f. A PR sets its NPS to Conditional Radio Silent.

g. A PR sets its NPS to Tactical Data System Failure.

h. A PR sets its NPS to Inactive.

i. A PR sets its NPS to Polling.

j. Any active JU reporting a Q_{pg} of < 6.

k. Any active JU exhibiting unstable Q_{pg}.

l. Network $Q_{pg} <= 6$.

m. Any active JU displaying 'impossible' changes in its position, from one report to the next.

4.6.3 Maintaining the Geodetic Grid

Whenever the GEOGRID shows signs of instability (e.g. unstable Q_{pg}, position jumps etc.) then the NM should take immediate action to determine the source of error.

4.6.4 Maintenance Issues

4.6.4.1 GEOGRID Instability – Possible Causes

4.6.4.1.1 If the GEOGRID is unstable from the outset, then the problem must lie with one or more of the initial entrants. If all non-PR JUs exhibit anomalous behaviour then the source(s) of error is most probably a JU(s) that is in direct connectivity with all other JUs. Furthermore, if there is one or more PRs operating, then a PR is the most likely source of error in this scenario.

4.6.4.1.2 If the GEOGRID becomes unstable in a specific area only (i.e. a group of JUs that are in mutual RLOS begin to exhibit unstable Q_{pg}), then the source of error is likely to be either a PR, or a pseudo PR, which is in direct connectivity with that set of JU's only. The presence of pseudo PR complicates the analysis of GEOGRID anomalies considerably, and this scenario is discussed separately in paragraph 4.6.4.9.

4.6.4.2 Range Mode Effect

4.6.4.2.1 Jitter

4.6.4.2.1.1 A MIDS terminal operating in normal range mode, applies a pseudo-random 'jitter' period to the beginning of all standard and packed-2 single pulse messages it transmits. When operating in extended range mode the jitter applied is approximately half that applied in the normal range mode. Therefore to determine an accurate TOA, a terminal must compensate for the pseudo random jitter applied to all messages it receives.

4.6.4.2.1.2 All MIDS terminals calculate jitter on a timeslot by timeslot basis. However, there is no provision made for one terminal to determine the range mode setting of another terminal. Thus a receiving terminal will compensate for jitter based on its own range mode setting. If one terminal is operating in extended range mode and another in normal range mode then the jitter calculated by each will be different. The effects which occur as a result of JUs selecting different range modes are the same as the effects noted when dishonest Q_{pg} are reported by JUs.

4.6.4.2.2 Jitter Correction Error

When a non-PR JU first synchronises to a network it will declare a Q_{pg} based on the accuracy of its initial three-dimensional position. It will then attempt to improve its geodetic position accuracy using the PPLI messages of other JUs. However, if the synchronising JU is operating in a different range mode to that of all other JUs, then any jitter correction it applies will be in error. Furthermore, the magnitude of the error will vary pseudo randomly between 0 and hundreds of miles, from one PPLI to the next. These 'impossible' range variations will cause frequent navigation resets in the JU's terminal.

4.6.4.2.3 Dissimilar Range Mode Effect

As a result of the dissimilar range mode effect, the JU's Q_{pg} value will be unstable and will fluctuate randomly. These fluctuations will be between zero, and a value one less than the highest Q_{pg} observed by the JU. Given the magnitude of the error that can exist from one observation to the next, if the JU is utilising the RELNAV function, then frequent position jumps of tens, if not hundreds of miles will be observed. In this situation, the dissimilar range mode effect will have a catastrophic effect on the JU's track correlation and picture compilation functions.

4.6.4.2.4 Initial Position Quality

If the initial Q_{pg} of a JU operating in the wrong range mode is less than or equal to the Q_{pg} of all other JUs in direct connectivity with it, then only the errant JU will be affected by the dissimilar range mode effect. Furthermore, the errant JU is unlikely to achieve a Q_{pg} that is greater than that of any other JU whilst the dissimilar range mode effect is inducing frequent navigation resets in its MIDS terminal.

4.6.4.2.5 GEOGRID Collapse

4.6.4.2.5.1 If there are no PRs operating, a JU operating in the wrong range mode can eventually achieve the highest Q_{pg} in the network. Once it does, then it will cease to be subject to the dissimilar range mode effect. However, any JUs in direct connectivity with the errant JU will experience frequent navigation resets induced by the dissimilar range mode effect, even though they may all be operating in the correct range mode. In this situation the Network Q_{pg} will drop to a figure close to zero, and this condition is referred to as GEOGRID 'collapse'. Furthermore, if the errant JU can maintain a reasonable Q_{pg} (>=6) by means other than RELNAV, then the GEOGRID will not recover automatically. **At best, a GEOGRID collapse will degrade the track correlation and tactical picture compilation functions of all non-PR JUs, significantly. At worst, the tactical picture will become completely unstable and unusable**.

4.6.4.2.5.2 If a JU enters a network with the wrong range mode setting and immediately declares a Q_{pg} that is greater than the Q_{pg} of any other JU already operating in the network, then GEOGRID collapse will occur within approximately one minute. However, if there is one or more PRs in direct connectivity with the errant JU, then the presence of the PR should prevent the GEOGRID from collapsing, as the errant JU is unlikely to achieve a Q_{pg} that is equal to that of the PRs. In this situation, only the errant JU will be affected by operating in the wrong range mode.

4.6.4.2.6 Position References

A PR that is initialised correctly does not navigate or perform RELNAV updates. Therefore it will be unaffected by either itself, or any other JU, operating in the wrong range mode. However, a PR that does operate in the wrong range mode **will have a catastrophic effect on the GEOGRID**. When there is more than one PR operating, then the errant PR's effect on Network Q_{pg} will depend on the geometry and the degree of direct connectivity that exists between the total population of PRs and each individual JU. However, the RELNAV function of any JU that is observing the errant PR will be completely ineffective.

4.6.4.2.7 Pseudo Position References

4.6.4.2.7.1 As for a PR, a pseudo PR which is initialised correctly, does not perform RELNAV updates and will not be affected by either itself, or another JU operating in the wrong range mode (or declaring a dishonest Q_{pg}). Paradoxically, however, it is still possible for a pseudo PR to exhibit fluctuating Q_{pg} and position jumps.

4.6.4.2.7.2 As with a PR, if the pseudo PR's position reference parameter is not set, then the pseudo PR is in fact, operating as a non-PR JU. Therefore its terminal will be performing RELNAV updates, and any positional instability exhibited by the JU will be as a result of one or more of the RELNAV anomalies discussed in previous paragraphs. However, if the pseudo PR's position reference parameter is set, then any positional instability exhibited by the pseudo PR must be the result of inputs which are not related to the MIDS interface (e.g. inputs from on-board navigation systems).

4.6.4.3 Relative Navigation and the Class 1 Terminal

4.6.4.3.1 A IJMS CLASS 1 TERMINAL is not RELNAV capable and will not be affected by another JU either operating in the wrong range mode or declaring a dishonest Q_{pg}. However, although unaffected itself, a IJMS CLASS 1 TERMINAL is quite capable of destabilising a GEOGRID by declaring a dishonest Q_{pg} and/or operating in the wrong range mode.

4.6.4.3.2 In the pre-MIDS era, EXTENDED range mode was used regularly and Q_{pg} settings were arbitrary. The 'master' or NTR terminal would set its Q_{pg} to 15 and all other units would set their Q_{pg} to 13. Being arbitrary, these Q_{pg} were also dishonest, although this is of little consequence to a IJMS CLASS 1 TERMINAL. However, in a mixed MIDS/IJMS CLASS 1 TERMINAL network, a IJMS CLASS 1 TERMINAL equipped JU adhering to these procedures would ultimately have a catastrophic effect on the MIDS GEOGRID. The same is true for range mode, which is not mutually exclusive when operating a IJMS CLASS 1 TERMINAL only network, but is mutually exclusive when operating a mixed MIDS/IJMS CLASS 1 TERMINAL network, or a MIDS only network.

4.6.4.4 Unstable PR Position and/or Q_{pg}

If the position and/or Q_{pg} reported by a PR is seen to change, then the NM must remove the PR from the GEOGRID immediately. This may be achieved by either instructing the PR to set its position and height uncertainty parameters to a value of <= 6 (preferred, but not possible for all JUs), or to switch its terminal to CONDITIONAL RADIO SILENT. The PR must then verify that the terminal's position reference parameter is set. If so, then the parameter must be cleared and then reset. If not, then the parameter must be set and the terminal's geodetic position values must then be reset to their correct values. Once this is complete, a NAV RESET command must be executed. The terminal may then be switched back to NORMAL transmit mode. If the position and/or Q_{pg} reported by a PR continues to change, then the terminal is in some way unserviceable. However, the JU may continue to operate as a non-PR JU either in NORMAL transmit mode, with its uncertainty parameters set to <= 6, or in CONDITIONAL RADIO SILENT mode, if required.

4.6.4.5 Unstable Q_{pg}

4.6.4.5.1 If there are no anomalous indications other than unstable Q_{pg}, then the problem is likely to be the result of an error in the initial geodetic position determined for a PR. In this scenario, the NM must remove each PR from the GEOGRID, in turn, starting with the PR that is in direct connectivity with the greatest number of JUs. Having removed a PR from the GEOGRID, if the grid does not recover within approximately 5 minutes then the NM should remove the next PR in the list. Furthermore, any PR that has already been removed from the grid **must maintain this condition until the analysis process has been completed**. If all PRs are removed from the GEOGRID, then Network Q_{pg} is unlikely to recover appreciably if there are no non-PR JUs capable of determining their geodetic position to a high degree of accuracy, independently. This will be irrespective of whether or not one or more of the PR JUs was a source of error. However, the GEOGRID will still stabilise, at a low network Q_{pg}, if the last PR removed from the grid was a source of error. If the grid remains unstable, then the PR JU's are unlikely to be source(s) of error.

4.6.4.5.2 If the grid stabilises after a PR is removed, then the last PR removed is most probably a source of error. However, the PR in question may not be the only source of error. Therefore the PRs that have already been removed from the GEOGRID must now be re-introduce, one at a time and in reverse order. If the grid does not remain stable after a PR is reintroduced, then this PR is most probably another source of error, therefore it must be removed from the grid again.

4.6.4.6 Position Jumps

If the majority of JU's are reporting impossible dynamic changes in position, then there is either a large error in the position reported by one or more PRs, or one or more PRs is operating in the wrong range mode. If the position error is considerable (e.g. tens of miles), then the NM may be able to determine when one or more PRs is reporting an incorrect position, directly. If this is not possible, then the maintenance procedure is the same as for unstable Q_{pg}.

4.6.4.7 Position Jumps, Single JU

4.6.4.7.1 If the NM observes position jumps from a single JU only, then this JU is almost certainly operating in the wrong range mode. In this case the NM must instruct the JU to verify its range mode setting. If the setting is correct, and the problem cannot be cleared by a platform operator, or the operator is unable to access this parameter, then the JU must either switch to CONDITIONAL RADIO SILENT or exit the network.

4.6.4.7.2 Whenever the NM determines that a JU may be a source of GEOGRID error, then the JU must be removed from the GEOGRID. Furthermore, if the JU is operating as a PR, then it must be instructed to verify both the geodetic position of its MIDS antenna and the following terminal parameters:

a. Geodetic position.

b. Position uncertainty.

c. Height uncertainty.

d. Position reference Setting.

e. Range mode.

4.6.4.8 Platform Initialisation

If the GEOGRID becomes unstable shortly after a JU first synchronises to an established network, then the new entrant JU is highly likely to be a source of error. The NM should investigate this possibility before proceeding with any of the more extensive analysis detailed in the previous paragraphs.

4.6.4.9 Pseudo PRs

4.6.4.9.1 The consequences of a pseudo PR operating in the wrong range mode and/or declaring a dishonest Q_{pg}, are dependent on the value of the pseudo PR's reported Q_{pg} in relation to that of other JUs. If the pseudo PR is declaring a Q_{pg} that is less than or equal to the Q_{pg} of any other JU (with which it has direct connectivity), then no JU will use the pseudo PR for RELNAV updates. Similarly, if there are a number of JUs (at least 3) with a higher Q_{pg} than the pseudo PR, then JUs with a lower Q_{pg} than the pseudo PR will observe these JUs in preference to the pseudo PR. In both these situations the errant pseudo PR will have no effect on the operation of the network. **However, when these conditions cease to be true, then the presence of an errant pseudo PR will have a catastrophic effect on the interface**.

4.6.4.9.2 This condition is extremely difficult (if not impossible) to detect, as an errant pseudo PR will not exhibit any unusual characteristic itself and it may have no effect on network operation unless specific conditions are true.

4.6.4.9.3 As the presence of an errant pseudo PR can have a catastrophic effect on the interface, the participation and operation of pseudo PRs must be closely monitored and controlled at all times.

4.6.4.10 Minimum Performance Criteria

If the minimum performance criteria detailed in paragraph 4.6.1.3.2 are to be achieved and maintained, there must be at least one active JU (e.g. a PR), which is capable of determining its geodetic position to < 1520 feet, by a means other than RELNAV. If there is no such unit available, then the NM should activate the RELGRID.

4.6.4.11 Simulated Positions

4.6.4.11.1 When conducting training and exercises, it may be necessary for a unit to simulate that it is at a different location than it actually is. This form of operation must be carefully controlled so as not to degrade Relative Navigation. In particular these units must become Pseudo PRs with the following properties:

a. The PR bit must be set to prevent the terminal from using JTIDS relative navigation

b. The units must have a lower Q_{pg} than any other JUs in the community, in order to prevent other users from using the reported position to aid their navigation solutions.

4.6.4.11.2 In view of the potential for reporting dishonest positions and thereby disrupting network operation, the use of this procedure must be coordinated with the NM and carefully controlled.

4.7 RELATIVE GRID MAINTENANCE

4.7.1 Definitions

4.7.1.1 Relative Position Quality

Qpr is a measure of the accuracy to which a MIDS terminal fixes its own position in the RELGRID. JU Qpr is the principle parameter used to monitor the performance and stability of the RELGRID.

4.7.1.2 Function

A NC JU establishes the relative grid co-ordinate system, including grid origin and grid orientation and a SNC JU enhances the stability of the RELGRID. When the NC role is selected, the NC JU begins to transmit a RELGRID continuation word in its PPLI message. All other RELNAV capable JUs then 'acquire' and align to the RELGRID reported by the NC. A JU's Qpr then reflects an estimate of its position with respect to the NC JU.

4.7.1.3 Monitoring Navigation Controllers

4.7.1.3.1 The NM can determine which platforms are operating as NCs by monitoring the Qpr of each participating JU. Only NC JU's should declare a Qpr of 15 and the identity of each NC should correspond with the on-line network plan. The Qpr of all non-NC JUs should, therefore, always be less than 15. Furthermore, if the NM does not have connectivity with all the participating JUs, then it is possible to infer the presence of an NC JU whenever there are other JUs which are reporting and updating RELGRID parameters.

4.7.1.3.2 However, it is not possible for the NM to determine by passive interface monitoring which platforms are operating as SNCs. As the SNC cannot be monitored directly, then the NM should determine via a means other than MIDS (e.g. voice), whether or not a JU is operating in the SNC role.

4.7.2 Monitoring the Relative Grid

The performance of the RELGRID is determined by the degree of relative motion between JUs. Therefore the NM should ensure that the potential for relative motion exists. However, relative motion is a highly dynamic parameter that may quickly vary from zero to its maximum value. Therefore, the performance of the RELGRID is more localised than that of the GEOGRID. This characteristic is reflected in individual Qpr values that will be highly variable. However, consistently low Qpr values across the network are an indication that the RELGRID configuration is not optimal (i.e. the NC is not achieving the necessary relative motion with respect to other JUs).

4.7.2.1 Monitoring Criteria

To ensure that the potential for relative motion exists, and that GEOGRID anomalies are detected quickly, the NM should monitor for the following conditions:

a. The NC is operating at the periphery of the operating area.

b. The SNC is not in direct connectivity with the NC.

c. The SNC is within 10 nm of the NC.

d. A NC reports a Qpr of < 15.

e. A JU not registered as a NC reports a Qpr of 15.

f. A NC/SNC sets its Network Participation Status (NPS) to Conditional Radio Silent.

g. A NC/SNC sets its NPS to Tactical Data System Failure.

h. A NC/SNC sets its NPS to Inactive.

i. A NC/SNC sets its NPS to Polling.

j. The NM loses connectivity with the NC/SNC.

4.7.3 Maintaining the Relative Grid

Maintenance of the Relative Grid is based on maintaining the availability and connectivity of Navigation Controllers (NCs) and Secondary Navigation Controllers (SNCs).

4.7.4 Maintenance Issues

4.7.4.1 No NC

As the RELGRID is established by a NC JU, if the JU designated as the NC can not select this role then the RELGRID will not be initialised. Similarly, if the NC JU ceases to operate (e.g. due to unserviceability) then the RELGRID will cease to operate. In either case, the NM must activate the standby NC as soon as possible.

4.7.4.2 Single NC

When there is a single NC JU only, then this JU must be mobile, close to the centre of operations and exhibit significant relative motion with respect to all JUs who intend to operate in the RELGRID. Therefore, the NM should monitor the position of the NC JU and transfer the NC function as required to maintain these criteria.

4.7.4.3 Single NC and SNC

4.7.4.3.1 **There must be only one SNC and one NC active at any one time**, and the SNC must be in direct connectivity with the NC JU at all times. Either the NC or the SNC (but not both) may be a stationary JU, however, the SNC and NC JUs should exhibit relative motion in order for the SNC to assist in refining the RELGRID.

4.7.4.3.2 The purpose of having an NC/SNC combination is to create bearing separation so that other JUs can calculate accurate grid positions in two axes. The ideal situation is where the angle between the bearing from a JU to the NC, and the bearing from the same JU to the SNC, is approximately 90 degrees. Furthermore, the NC and SNC JU should not be in close proximity to one another (i.e. members of the same combat air patrol or tactical formation), as this reduces the bearing separation observable from other JUs and also affects the ability of an NC/SNC combination to accurately define the grid orientation. Therefore the NM should monitor the relative positions of the NC and the SNC JU and transfer the NC/SNC functions as required to maintain these criteria. If a second JU selects the NC function then this will significantly degrade the RELNAV process.

4.7.4.4 NC/SNC Handover

The NC/SNC handover procedure is essentially the same as the NTR handover procedure described in paragraph 4.5.4.2.5. The new NC/SNC must ensure that the outgoing NC has deselected NC/SNC before assuming the role. The NM should assist and/or coordinate this procedure.

4.8 NETWORK PARTICIPATION STATUS MONITORING

4.8.1 <u>Definitions</u>

4.8.1.1 Network Participation Status Indicator

4.8.1.1.1 The Network Participation Status (NPS) indicator is part of the PPLI message data set and describes the degree to which a JU is participating on the interface. There are 7 conditions defined for the NPS parameter as follows:

a. Active.

b. Inactive.

c. Conditional radio silent

d. High message error rate.

e. No IEM received.

f. Tactical Data System (TDS) fail.

g. Polling.

4.8.1.1.2 The ACTIVE, CONDITIONAL RADIO SILENT and POLLING conditions identify a JU's transmit mode. The NO IEM RECEIVED, INACTIVE, HIGH MESSAGE ERROR RATE and TDS FAIL describe failure and degraded performance conditions.

4.8.1.2 NPS Hierarchy

All MIDS transmit modes are mutually exclusive. However, it is possible for one or more NPS failure or degraded performance condition to exist simultaneously.

Therefore, the NPS modes and conditions are reported in the following order of precedence (highest precedent first):

a. Conditional radio silent.

b. TDS fail.

c. High message error rate.

d. No IEM received.

e. Polling.

f. Active.

4.8.1.3 Active Mode

A MIDS terminal will set its NPS to ACTIVE when it is operating in the NORMAL transmit mode and is in fine synchronisation with the time reference. An ACTIVE JU is capable of transmitting and receiving all types of J-series messages.

4.8.1.4 Conditional Radio Silent

4.8.1.4.1 If a platform operator changes a MIDS terminal's transmit mode from NORMAL to RADIO SILENT, then the terminal will set its NPS to CONDITIONAL RADIO SILENT and then transmit a single PPLI message. Once the PPLI message has been transmitted the terminal will cease to transmit any further fixed format messages. However, the terminal will continue to transmit unformatted voice and free text data as required.

4.8.1.4.2 If a platform operator changes a MIDS terminal's transmit mode from RADIO SILENT to NORMAL, then the terminal will set its NPS to ACTIVE, automatically. However if a TDS FAIL, INACTIVE, HIGH MESSAGE ERROR RATE or NO IEM RECEIVED condition already exists, then the extant condition with the highest precedent will be reported.

4.8.1.5 Polling

4.8.1.5.1 If a platform operator changes a MIDS terminal's transmit mode from NORMAL to POLLING, then the terminal will set its NPS to POLLING and then transmit a single PPLI message[3]. Once the PPLI message has been transmitted the terminal will then transmit fixed format messages only when required, as follows:

a. RTT interrogation messages for synchronisation.

b. In response to a communications control message (J0.6) addressed to own unit.

c. For receipt compliance purposes.

d. Unformatted voice and free text data.

Furthermore, the RTT Reply Status parameter will be set to NOT OPERATIONAL in all PPLI messages transmitted by a terminal in polling mode.

4.8.1.5.2 If a platform operator changes a MIDS terminal's transmit mode from POLLING to NORMAL, then the terminal will set its NPS to ACTIVE automatically. However if a TDS FAIL, HIGH MESSAGE ERROR RATE or NO IEM RECEIVED condition already exists, then the extant condition with the highest precedent will be reported.

4.8.1.6 High Message Error Rate

A MIDS terminal monitors both transmitted and received messages for irrecoverable message decode errors. If the ratio of irrecoverable message errors to the total number of messages received in any 12 second interval exceeds 10%, then the terminal will declare a high message error condition. If a TDS FAIL condition does not already exist, then the terminal will set its NPS to HIGH MESSAGE ERROR RATE, otherwise the TDS FAIL condition will continue to be reported.

4.8.1.7 No IEM Received

If a MIDS terminal does not receive an IEM in any 120 second interval then it will declare a 'no IEM received' condition. If a TDS FAIL or HIGH MESSAGE ERROR RATE condition does not already exist, then the terminal will set its NPS to NO IEM RECEIVED, otherwise the extant condition with the highest precedent will continue to be reported.

[3] Current Class 2 JTIDS terminals do not set NPS to POLLING and then transmit a single PPLI message before entering the Polling mode.

4.8.1.8 Inactive and TDS Fail

If a MIDS terminal experiences a host interface failure, then it will set its NPS to either TDS FAIL or INACTIVE, depending on platform implementation.

4.8.1.9 Limited Operational Status

A JU's NPS affects its ability to operate in one or more network functions. Therefore a JU which is declaring an NPS of anything other than ACTIVE is considered to be in a LIMited OPerational (LIMOP) status. The impact of LIMOP status and the OPNET management actions required when a JU's NPS changes from ACTIVE to LIMOP, are described in the following section and summarised in Table 4.3.

4.8.2 Monitoring the NPSI

When a JU's NPS changes from ACTIVE to LIMOP, its affect on the interface is dependent on the network, relay and mission roles assigned to the JU.

4.8.3 Maintenance Issues

4.8.3.1 TDS Failure

4.8.3.1.1 A MIDS terminal which experiences a host interface failure will invariably continue to operate normally on the interface at the system level (i.e. it will continue to function as the NTR if it was the NTR at the moment the host interface was lost). However, not all the data in the JU's PPLI messages may be valid, specifically those fields that contain position related data. Furthermore, the system operator may no longer have an interface by which to control the MIDS terminal, as this interface is normally provided by the host system. In this situation, the system operator will be unable to handover exclusive network functions as it will not be possible for the operator to deselect them.

4.8.3.1.2 If the JU holds an exclusive network or relay function (e.g. NTR), then the NM must first determine if the JU is able to recover from the TDS failure. If so, an estimate of how long it will take the JU to return to ACTIVE status is then required. If this time is less than that which the NM estimates would be required to reconfigure the interface, then the NM should not attempt to do so. However, if the JU is operating as a PR, NC or SNC JU, then the NM should monitor the GEOGRID closely. If the integrity of the GEOGRID is seen to degrade, then the NM can infer that the JU's position related data is inaccurate, and a platform operator should be instructed to switch the JU's MIDS terminal to standby. Similarly, if a platform operator reports that the host interface is unserviceable, then the platform operator should be instructed to switch the JU's MIDS terminal to standby. Following either event, the NM should then take immediate action to re-assign all the exclusive roles held by the JU.

4.8.3.2 Timeslot and Mission Assignments

It may be necessary for the mission(s) assigned to an unserviceable JU to be re-assigned to one or more other JUs. In this case the JU(s) assuming the unserviceable JU's missions may require modifications to their timeslot assignments in one or more PGs.

4.8.3.3 Re-initialisation

It is not essential for a JU's MIDS terminal to be re-initialise whenever the JU's NPS changes from TDS FAIL to ACTIVE. However, if a JU's host system is restarted as a result of an irrecoverable software failure, then the host restart process will normally require the terminal to be re-initialised. When this is the case, if the NM has modified the timeslot and/or relay assignments of the JU, then these changes will not be reflected in the hosts record of the JU's on-station ID load. Therefore the NM should ensure that any assignments changes are reapplied to the JU.

4.8.3.4 Radio Silent and Polling Modes

4.8.3.4.1 A JU which switches to either the POLLING or the RADIO SILENT transmit mode has, in effect, decided to stop transmitting tactical data over the interface. In either of these modes, a JU will continue to receive data. However, in RADIO SILENT mode the JU itself will not be 'visible' to other interface users and its terminal must maintain synchronisation by passive means. Conversely, a terminal in polling mode can maintain synchronisation by either active or passive means, and its terminal will respond to communications control messages. Therefore, it may be possible for the NM to interrogate a JU in polling mode for information about its position and interface status.

4.8.3.4.2 The NM should try to determine the reason for a JU's change of transmit mode, if the mode change is not reflected in the on-line plan. It is not possible for the NM to determine by passive interface monitoring alone whether or not a JU that has switched to RADIO SILENT has also initiated a Transmit Inhibit. If this is the case then the JU will not be able to communicate with the NM by either MIDS voice or free text message.

4.8.3.5 High Message Error Rate

4.8.3.5.1 A high message error rate indicates that an appreciable amount of data is being lost due to one or more of the following conditions:

a. Radio frequency interference that results from:

   i. Jamming.

   ii. Non-MIDS interference from the principle users of the MIDS frequency band (e.g. air navigation equipment).

   iii. Mutual interference from co-channel transmissions originated by JU's operating simultaneously on more than one MIDS nets.

   iv. Multi-path propagation effects when employing single pulse message structures.

b. Concurrent IJMS/Link 16 operations.

c. Platform integration anomalies (e.g. number and location of antennas, airframe shielding, etc.).

d. MIDS Receiver/Transmitter (RT) malfunction.

4.8.3.5.2 The detailed effects of intentional jamming are beyond the scope of the classification of this document. However, jamming is often characterised by persistent HIGH MESSAGE ERROR RATE conditions. Furthermore, a terminal may alternatively declare a 'no IEM received' status. However, this status will not be reported if the HIGH MESSAGE ERROR RATE condition is persistent, as the NO IEM RECEIVED condition has a lower precedence than the HIGH MESSAGE ERROR RATE condition.

4.8.3.5.3 Mutual interference may result from the use of network structures that employ extensive multi-netting and/or stacked nets. There is little the NM can do to mitigate the effects of mutual interference, other than take action to reduce the number of nets in use, which is unlikely to be appropriate, tactically.

4.8.3.5.4 Multi-path is an effect which results from the same radio signal being received via two (or more) different paths. The difference in signal path length can cause the two signals to cancel each other and when this occurs the data that the signal carries is lost. The double pulse signal structure mitigates the multi-path effect almost completely, however, the single pulse structure does not mitigate the multi-path effect. Therefore any JU that is operating within the multi-path range band, and is receiving a significant amount of messages at packed-2 single pulse or packed-4, may begin to report a HIGH MESSAGE ERROR RATE condition on a regular basis.

4.8.3.5.5 A MIDS terminal that is not initialised to receive IJMS data explicitly will default to J-series message processing. Therefore, if default processing is applied, and the message received is an IJMS message, then the process will fail and an irrecoverable message decode failure will be recorded. The converse is also true for an IJMS Class 1 terminal, which does not process J-series messages under any circumstances.

4.8.3.5.6 When operating a network that supports both IJMS and Link 16 data exchange, any JU that is not initialised to process the IJMS PGs and is receiving IJMS data, will invariably report a HIGH MESSAGE ERROR RATE persistently.

4.8.3.5.7 If a single JU is reporting a HIGH MESSAGE ERROR RATE persistently, and none of the high error rate conditions described previously are either anticipated or apparent, then this normally indicates that the JU is operating with an incomplete set of IJMS explicit receive assignments. Incomplete or incorrect ID load maintenance is described in paragraph 4.4.5.

4.8.3.6 Network Message Error Rate

4.8.3.6.1 Network message error rate (NMER) is the ratio of the number of JU's reporting a HIGH MESSAGE ERROR RATE persistently, to the number of JU's reporting a HIGH MESSAGE ERROR RATE intermittently, or reporting any other NPS condition of a lower precedence (e.g. ACTIVE). The NMER is a derived network parameter that is calculated over a defined period (typically 1 minute). The magnitude of the NMER provides a 'quick look' indication of the level of interference across the network as a whole.

4.8.3.6.2 The term 'intermittent' in this context describes an NPS which changes from HIGH MESSAGE ERROR RATE to any other NPS condition with a lower precedent, at least once during the period over which the NMER is calculated. As PPLI messages are generally transmitted only once in any 12 second interval (other than high update rate), if the period over which the NMER is calculated is small (e.g. 12 seconds), then a JU's NPS will never exhibit 'intermittent' behaviour. Therefore the utility of the NMER parameter is significantly diminished if the period over which the NMER is calculated is less than 1 minute.

4.8.3.7 Mitigating the Effects of Interference

4.8.3.7.1 Radio Frequency Interference

A degree of radio frequency interference from other authorised users of the MIDS band is considered to be normal. This is also true of the effects that result from a specific platform integration. These effects are characterised by a JU reporting a HIGH MESSAGE ERROR RATE occasionally, and essentially at random. For example, a fighter JU that is performing highly dynamic manoeuvres will invariably report a HIGH MESSAGE ERROR RATE intermittently.

4.8.3.7.2 Anti-jam Characteristics

4.8.3.7.2.1 The MIDS system is designed to be ECM resistant. However, the NM has little control over these characteristics other than those which apply to signal structure and jitter. Essentially, single pulse message structures and extended range mode reduce the anti-jam margin of the system. However, there is no method for the NM to modify the packing levels and range mode of a MIDS terminal directly. Furthermore, some JU's, often nonC^2, do not provide an interface for an operator to modify these parameters either.

4.8.3.7.2.2 A C^2 JU's operator interface may provide the facility for an operator to alter a terminal's maximum message packing levels. If a C^2 JU's message packing is not already set for maximum anti-jam performance, then the NM may instruct (by voice or free-text) any C^2 JU which is significantly affected by jamming or the multi-path effect, to modify the message packing levels of its MIDS terminal, so that the terminal transmits data using double pulse message structures only. However, this may also reduce a JU's data throughput, the effects of which must be considered before any action is taken.

4.8.3.7.2.3 **All active JU's must operate in the same range mode at all times**. Therefore range mode is a network parameter which may be modified by executing a co-ordinated network structure change only. However, a network structure change is an extensive and highly co-ordinated procedural OPNET management action. Therefore any attempt to execute a structure change when the interface is under attack has a low probability of success and is not recommended.

4.8.3.8 No IEM Received

4.8.3.8.1 A 'no IEM received' condition is caused by:

a. A lack of direct connectivity between a JU and either the NTR, an IEJU or a main net relay JU.

b. Interference.

c. A MIDS RT malfunction.

4.8.3.8.2 If a JU persistently reports NO IEM RECEIVED, then the NM should attempt to determine (by voice or free text) if the JU's terminal is reporting any RT related failure conditions. If the JU reports both HIGH MESSAGE ERROR RATE and NO IEM RECEIVED persistently, then the problem may be the result of interference. However, in the absence of any indications of interference, degraded performance or hardware failure, the NM may infer that the JU has become isolated. If the JU is not an IEJU or a main net relay JU, then any other JU that is attempting to synchronise to a STRN (or any non-ETR capable JU attempting to synchronise to an ETRN), which is in the same geographic area as the isolated JU, may be unable to synchronise to the network. Furthermore, a JU that is not receiving an IEM, will not receive IEM updates or NTUs.

4.8.3.8.3 In this situation the NM should attempt to establish an indirect connectivity path between any JU which is not receiving an IEM, and the NTR. This may be achieved by either activating additional IEJUs or, if this is not possible, by requesting that one or more existing IEJUs reposition to provided the connectivity necessary.

4.8.3.9 Network IEM Rate

Network IEM Rate (NIR) is the ratio of the number of JU's that report NO IEM RECEIVED, to the number of JU's that report an ACTIVE NPS over a defined period (typically 1 minute). The magnitude of the NIR provides a 'quick look' indication of the IEM coverage across the network as a whole.

Table 4.3 - Impact of a JU Changing from ACTIVE to LIMOP Status

		RECEIVE	TRANSMIT CAPABILITY			NETWORK FUNCTION CAPABILITY						
LIMOP STATUS	CONDITION	CAPABLE	MESSAGE	VOICE	RELAY	NTR	IEJU	NC/SNC	PR	PRU	IMPACT	NM ACTIONS
CONDITIONAL RADIO SILENT	Operator selectable.	Yes	No	Yes	No	No	No	No	No	No	No further data transmissions from JU.	Re-assign the Network Roles and relay functions held by JU.
HIGH MESSAGE ERROR RATE	More than 10% of messages received in error.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Data loss.	Determine cause and attempt to mitigate.
NO INITIAL ENTRY MESSAGE RECEIVED	No IEM received in 120 second period.	Yes	Yes	Yes	Yes	N/A	Yes, but function degraded	Yes, but function degraded.	Yes, but function degraded.	Yes, but function degraded	JU will not receive IEM and NTU updates. If IEJU then may not be transmitting latest IEM. JU probably isolated, therefore network fragmented.	If JU not IEJU then Initial entry support in area suspect. Attempt to re-establish connectivity with NTR by activating additional IEJUs or repositioning existing IEJUs.
TDS FAILURE / INACTIVE	Terminal cannot communicate with host.	Terminal responds with CANTPRO to all messages addressed to the host.	Terminal generated messages only.	Yes	Yes, if function held at time of failure.	Yes, if role held at time of failure.	Yes, if role held at time of failure.	Yes, if role held at time of failure. However, PPLI data may not be valid.	Yes, if role held at time of failure. However, pseudo PR PPLI data may not be valid.	Yes, if role held at time of failure.	Loss of automated tactical data exchange with JU. Terminal system functions not affected but PPLI data may be inaccurate.	Re-assign all roles and functions if host interface not recoverable. Re-assign NC/SNC roles immediately if GEOGRID or RELGRID degraded.
POLLING	Operator Selectable.	Yes	JU transmits RTT and R/C messages as required. Transmits data in response to a communications control message only.	Yes	No	No	No	No	No	Yes, but will not reply to RTT message.	JU will transmit tactical data only when requested.	Re-assign the Network Roles and relay functions held by JU.

4.9 SUB NETWORK MANAGER

4.9.1 Unique Roles and Functions

Network functions that are either unique (e.g. the NTR function) or required to support inter-community information exchange (eg the main net relay function) should remain the responsibility of the NM. Therefore, management of the following roles, functions or areas should not be delegated:

a. NTR, IEJU (NECT) and other IEM transmission unit functions.

b. NC/SNC functions.

c. Wide area PPLI assignments.

d. RTT A PG.

e. RTT B PG.

f. Network management PG.

g. Wide area relay function.

4.9.2 On-line Plan Integrity

4.9.2.1 A SubNM must maintain an on-line plan for the forces within a community for which the SubNM has some OPNET management responsibilities. Furthermore, the NM should record all changes to role, resource and relay assignments made by a SubNM.

4.9.2.3 The NM and SubNM(s) should co-ordinate and inform each other of all role changes made within their respective areas of responsibility (if the change cannot be determined automatically by passive interface monitoring). Furthermore, if the SubNM modifies timeslot assignments and relay functions procedurally, then the SubNM must communicate these changes to the NM as soon as possible.

4.9.3 IDL Integrity

If a subset of a JU's assignments are managed by the NM (e.g. a wide-area relay element) and a different subset is managed by a SubNM (e.g. timeslot transmit assignments), then the NM and SubNM must ensure that all potential changes are coordinated prior to activation. This is to prevent both the NM and the SubNM from modifying the assignments of a single JU in an interleaved fashion, as this may result in an invalid condition, e.g. a condition where an attempt is made to assign more than the allowable 64 timeslot block assignment.

CHAPTER 5

GUIDELINES AND PROCEDURES FOR CRYPTONET MANAGEMENT

5.1 DEFINITION OF RESPONSIBILITY

5.1.1 Cryptonet Management Responsibility

The Cryptonet Management function is responsible for ensuring that all Link 16 network operations are conducted within established COMSEC guidelines (see note) to minimise the exposure of tactically significant and sensitive information passed over a Link 16 network.

5.1.2 Cryptonet Manager Responsibilities

To achieve this aim, the Cryptonet Manager should:

a. Promote secure distribution, handling and accounting procedures for the use of cryptovariables, in accordance with local crypto custodian and NATO COMSEC procedures.

b. Establish and maintain a relationship of available cryptovariables to defined cryptonets, to ensure desired crypto connectivity is maintained.

c. Promulgate all required information concerning cryptovariable to cryptonet association (via CVLLs) and SDU cryptovariable loading plans, to all JUs required to participate in a Link 16 network. This should ensure correct and effective loading of cryptovariables at the distributed sites, under the direction of local crypto custodians.

d. Maintain records of the allocation of cryptovariables during network operations, to ensure that:

(1) Designated crypto connectivity is maintained.

(2) Required COMSEC controls and accountability are maintained.

e. Initiate a quick and effective response to the detection of a security compromise during network operations.

f. Develop contingency plans for operation in the event of a short notice situation or compromise.

g. Establish access control measures for cryptonet access by users.[6]

[6] Cryptonet Management procedures are based on applicable NATO documents, e.g.:
AMSG 293 - NATO Cryptographic Instructions.
AMSG 505 - NATO Distribution & Accounting Publication.
AMSG 725 - Controlling Authorities for Crypto Rekeying Material and Management of Manual Crypto Systems.

5.2 CRYPTO PLANNING

5.2.1 General

The use of cryptovariables in Link 16 network operations requires a degree of preplanning to ensure that:

a. Link 16 network designs meet connectivity and communications security requirements.

b. Cryptovariable distribution is coordinated to ensure that JUs are issued with common cryptovariables, as required by the network design to be used.

c. Information concerning cryptovariable usage is promulgated to all units prior to network operation.

5.2.2 Definition of Cryptonets

5.2.2.1 Cryptonets should be defined by the Network Design function to support defined communications connectivity requirements, through the allocation of CVLLs. The following guidelines apply:

a. CVLLs should be allocated to authorised JUs on a PG basis, according to individual requirements, such that all JUs requiring interoperability are assigned to a common CVLL.

b. Multiple cryptonets may be defined for Link 16 networks as follows:

(1) Partitioned Variable Mode (PVM) - one TRANSEC, multiple MSECs.

(2) Common Variable mode (CVM) - Multiple TRANSECs.

c. Each CVLL pair will normally be assigned to two SDU loading locations for each platform. Associated tables should be produced and distributed to define the CVLL-to-SDU loading plan for each platform. CPDs must be assigned in accordance with the standard NATO CPD convention to identify which of the pair should be used for the current and next cryptoperiods.

d. Where practical, JUs of the same platform type should be allocated the same SDU loading plan to facilitate quick and accurate cryptovariable loading.

e. Where OTAR is to be implemented, the loading plan must reserve two SDU locations; location 5 to store the unique variable and location 4 for temporary storage of the new cryptovariable while processing.

5.2.2.2 To incorporate flexibility of network configuration, it is advantageous to allow Link 16 data distribution to a large number of participating JUs. However, the larger the user-base, the greater the risk of security compromise. Cryptonet configuration should minimise exposure of cryptovariables to human access, maintain accurate accounting procedures and maintain control of the information.

5.2.3 Guidelines for Cryptovariable Distribution

5.2.3.1 The following guidelines should be followed for the distribution of cryptovariables for Link 16 network operation:

a. All cryptovariables used, including unique variables, will be identified by a short title for ease of reference. The format for short titles is standardised within NATO to facilitate their promulgation.

b. Cryptovariables should be distributed directly from the issuing authority to all operational units requiring Link 16 network operation, in accordance with established COMSEC procedures.

c. Where possible, cryptovariable distribution and handling procedures should be automated, to reduce the probability of error introduction.

d. All potential Cryptonet Manager Stations (CMS), including NMSs, should be provided with details of the distribution of all cryptovariables, referenced by short titles, to participating JUs.

e. Storage and accounting of cryptovariables on site should be the responsibility of the local crypto custodian.

5.2.3.2 Additional Guidelines for OTAR

If OTAR is to be implemented, appropriate crypto material will be issued to the authorised crypto rekeying facility to enable unique variables and/or traffic cryptovariables to be generated. The correct unique variables must be distributed to their respective destination platforms. Each unique variable is unique to each platform. The following additional procedures are required:

a. Unique variables must be generated for each platform in a secure environment. Platform-unique information, such as platform identity and Unique Variable Update Number (UVUN), must be incorporated into the generation of each unique variable to ensure that it is unique to that platform.

b. Each unique variable will be referenced by short title and marked with the identity of the intended platform to ensure accurate distribution.

c. Spare cryptovariables may be made available to operational units and held at the crypto rekeying facility, to enable rekeying as required. Potential CMSs should be provided with a list of spare cryptovariables and details of their distribution.

d. The Cryptonet Manager must be aware of the unique variable stored in each SDU.

5.2.4 Pre-Mission Planning

5.2.4.1 During the Pre-mission Planning stage, the Cryptonet Manager is responsible for ensuring that:

a. An accurate record is maintained of which cryptovariables have been distributed to each operational unit and the relationship of unique variables to individual JU platforms.

b. All cryptographic information required for network operation is disseminated to all participants via the OPTASK LINK.

c. CPDs are determined prior to initiation of network operations and each crypto-custodian on site is aware of the CPDs in force for the duration of network operations. CPD alternates between 0 and 1 starting with CPD = 0 for January 1, 1985.

d. A cryptovariable distribution list is provided, by short titles, to enable him to assign cryptovariables to CVLLs so as to achieve and preserve the required communications connectivity.

5.2.4.2 Cryptovariable/CVLL Association

The Cryptonet Manager is responsible for associating the cryptovariables held by JUs with the CVLL plan of the network to be implemented. He must ensure that all platforms assigned to use a common CVLL have access to and can be loaded with the same cryptovariable. This is particularly important when planning joint and combined Link 16 networks. Cryptovariables should be referenced by short title and the association of short titles to CVLLs must be distributed to all JUs prior to commencement of network operations. He must also have a contingency CVLL plan in order to respond to quick reaction situations.

5.2.4.3 Definition of the Crypto Period

The cryptoperiod will be a standard 24 hours. Rollover will occur at 2400Z. Greenwich Mean Time (GMT) will be the common time standard to ensure common crytovariable usage in networks that span more than one time zone.

5.2.4.4 Promulgation of Cryptographic Information

The following crypto information should be promulgated to all participating JUs via the OPTASK LINK:

a. CVLL to cryptovariable short title association, as defined by the Cryptonet Manager.

b. CPD in use at commencement of network operations (either 0 or 1).

5.2.5 Cryptovariable Loading

Cryptovariable loading should be performed as part of the general initialisation process. The following guidelines apply:

a. All loading of cryptovariables should be under the control of the local crypto custodian.

b. Reference should be made to the current CPD and the CVLL/cryptovariable short title association contained in the OPTASK LINK, together with the CVLL to SDU memory location association tables held for each platform type, to ensure that the required cryptovariables are loaded into the correct SDU locations for each JU.

c. Local operating procedures should be developed and standardised for each platform type for the loading and accounting of cryptovariables.

d. The local crypto custodian should maintain close coordination with the local initialisation organisation to ensure that:

(1)The correct associations between TRANSEC and MSEC cryptovariables, CVLLs and SDU memory locations are implemented for the selected network design.

(2)Initialisation data sets are prepared using the correct predetermined CPD for each JU to enable correct change over of cryptovariables, as promulgated in the OPTASK LINK, and continuity of communications.

(3)Platforms that cannot manually specify the current CPD are issued initialisation data sets to be loaded while the CPD is still in effect. For platforms with the capability to modify the current CPD, it is permissible to delay loading of initialisation data sets until the next cryptoperiod (see paragraph 4.4.3.4.3.a(1) of Volume 1).

5.3 MANAGEMENT OF CRYPTOVARIABLES

5.3.1 General

The Cryptonet Manager is responsible for cryptovariable management during Link 16 network operations through:

a. Maintenance of records.

b. Detection of any actual or suspected security compromise.

c. Modifying of cryptovariables, under the direction of the Network Manager.

5.3.2 Maintenance of Records

The Cryptonet Manager should ensure that records are maintained of:

a. Desired and actual crypto connectivity among JUs for each PG.

b. Current CVLL to cryptovariable short title association.

c. CVLL association for each net and PG (for crypto connectivity).

d. Cryptovariables held by each JU and the respective locations within the SDU.

e. Unique variable held by each JU and its associated UVUN.

f. The current CPD in force.

g. Erased/destroyed cryptovariables.

5.3.3 Link 16 Security Compromise

The Cryptonet Manager should ensure that a quick and effective response is made to the detection of a security compromise during network operations by:

a. Determining the extent of security compromise and identifying JUs involved.

b. Providing the Network Manager with the information required to conduct the required cryptovariable change to isolate affected JUs.

c. Assessing the impact of security compromise on future network operations and advising the Network Manager accordingly.

5.3.4 Modifying Cryptovariables

5.3.4.1 Modification of cryptovariables must be coordinated by the Network Manager. The Cryptonet Manager should advise the Network Manager of all significant implications to overall Link 16 network connectivity for any proposed cryptovariable change. Any changes made must be consistent with the COMSEC instructions in force. Modification of cryptovariables may be used to:

a. Provide JUs with cryptovariables for the next cryptoperiod.

b. Provide JUs with new cryptovariables in reaction to a detected security compromise.

c. Provide JUs with the required cryptovariable(s) to participate in other PGs or Link 16 networks.

d. Change the crypto mode for a PG.

e. Change the MSEC cryptovariable assigned for a PG.

5.3.4.2 Methods of Changing Cryptovariables

Cryptovariables may be changed during network operations by the following methods, depending on system implementation:

a. Direct reloading of the terminal. JUs should hold sufficient crypto to meet anticipated operational requirements. However, some JUs must return to an appropriate base to enable reloading of cryptovariables.

b. Reassignment of time slot blocks accessed by a new cryptovariable, providing the cryptovariable is already held in the terminal's SDU.

c. Over the air rekeying (OTAR), if this function is implemented.

If the reason for performing cryptovariable change is a detected or suspected security compromise, option (b) above should only be used if a single cryptovariable is compromised. In the event of terminal capture, all cryptovariables held in that terminal's SDU are compromised and should be changed.

5.3.4.3 Over the Air Rekeying of Cryptovariables

When authorised, OTAR may be used to:

a. Request cryptovariable status update reports from individual JUs.

b. Provide terminals with new cryptovariables by direct rekeying and own terminal by over the MUX rekeying (OTMR).

Individual JUs may use OTAR to request new cryptovariables, either directly or indirectly from the Network Manager. Details are provided in Chapter 5 of Volume 1.

5.3.4.3.1 Cryptovariable Status Update Request

The Network Manager may use the OTAR Management message to request a cryptovariable status update report from a JU. The receiving terminal should automatically respond with the following information without any operator involvement required:

a. CVLL for each SDU location.

b. CPD for each SDU location.

c. UVUN.

d. Current CPD.

5.3.4.3.2 Rekeying of Cryptovariables

A separate message must be transmitted for each JU to be rekeyed. The procedures are as follows:

a. The Network Manager must inform the crypto rekeying facility of the requirement for an encrypted key load for a particular JU, specifying:

   (1) Platform Identity of the JU to be rekeyed.

   (2) SDU location destination of the new cryptovariable.

   (3) New cryptovariable to be rekeyed.

   (4) Current UVUN.

b. The crypto rekeying facility should provide the Network Manager with the information specified in (a) above, encrypted by the unique variable of the JU to be rekeyed.

c. The Network Manager must specify a time of execution for the terminal to perform the rekeying action (see paragraph 5.3.4.3.3 below).

d. The J31.0 OTAR Management message and J31.1 OTAR message are transmitted to the required JU to be stored in the receiving JU's SDU until the specified time of execution. These messages may be transmitted individually (J31.0 (AC = 1) message followed by a J31.1 message) or packed (J31.0 (AC = 6) Packed OTAR message and J31.1 message in the same time slot). When transmitted individually, the terminal provides Receipt/Compliance for both messages. When the J31.0 and J31.1 messages are packed into a single time slot, the terminal provides a Receipt/Compliance response to the J31.0 OTAR Management message only.

e. Irrespective of which method is used, individual or packed, the receiving terminal is capable of processing the required action. The Network Manager should retransmit the messages and attempt to contact the JU by other means should the receiving terminal fail to respond.

f. The Cryptonet Manager should be informed of each successful rekeying action, to enable him to update his records of crypto connectivity.

The above procedure must be repeated for each JU required to be reloaded. The Network Manager must rekey own terminal using OTMR (J31.0, AC = 7). Procedures for rekeying of a Network Manager's own terminal using OTMR messages are similar to the above steps, except that the terminal does not perform Receipt/Compliance for messages sent to the terminal by the host.

5.3.4.3.3 Time of Execution in OTAR Management Messages

The Network Manager must specify a time of execution, in Hours and Minutes, for the new cryptovariable to be loaded into the specified SDU location at receiving JUs. The time of execution is transmitted in the OTAR Management message, prior to the associated OTAR message containing the new cryptovariable. Where a group of JUs are to rekeyed, the same time of execution should be specified to ensure continued crypto connectivity. The Network Manager should ensure that the time of execution specified allows sufficient time for OTAR Management messages and associated OTAR messages to be transmitted to, and processed by, all JUs requiring to be rekeyed. Failure to do so could result in some JUs not performing the rekey action until the equivalent time in the next cryptoperiod (i.e. almost 24 hours later). The Network Manager would be alerted to such an event by the non-receipt of a HAVCO response from affected JUs, and should take action to reinitiate the OTAR process immediately with a new time of execution for these JUs.

5.3.4.4 Change of Crypto Mode or MSEC Cryptovariable for a PG

The Network Manager may use the Time Slot Assignment message to change the crypto mode of a PG or the MSEC cryptovariable of a PG operating in Partitioned Variable Mode. The time of implementation of the change must be coordinated with all affected JUs. The Network Manager must ensure that all JUs participating in the PG, including those JUs performing relay, have access to the new MSEC cryptovariable.

LIST OF EFFECTIVE PAGES

VOLUME 2

PAGE NUMBERS	CLASSIFICATION	AMENDMENT STATUS
I to III (All RB)	NATO UNCLASSIFIED	ORIGINAL
IV to VI (RB)	NATO UNCLASSIFIED	ORIGINAL
VII (RB)	NATO UNCLASSIFIED	ORIGINAL
VIII to XV	NATO UNCLASSIFIED	ORIGINAL
1-1 to 1-3 (RB)	NATO UNCLASSIFIED	ORIGINAL
2-1 to 2-41 (RB)	NATO UNCLASSIFED	ORIGINAL
3-1 to 3-31 (RB)	NATO UNCLASSIFIED	ORIGINAL
4-1 to 4-43 (RB)	NATO UNCLASSIFIED	ORIGINAL
5-1 to 5-9 (RB)	NATO UNCLASSIFIED	ORIGINAL
A-1 to A-11 (RB)	NATO UNCLASSIFIED	ORIGINAL
LEP-1 (RB)	NATO UNCLASSIFIED	ORIGINAL