ADatP-16(E)

STANDARD OPERATING PROCEDURES

FOR NATO LINK 16

VOLUME 1

FEBRUARY 2006

NORTH ATLANTIC TREATY ORGANISATION

NATO STANDARDISATION AGENCY (NSA)

NATO LETTER OF PROMULGATION

February 2006

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

2. ADatP-16(E) Volume 1 is effective upon receipt. It supersedes ADatP-16(D) Volume 1 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
6	NONE
7	NONE
8	NONE
9	NONE
ANNEX A	NONE
ANNEX B	NONE
ANNEX C	NONE
ANNEX D	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 1

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:

Table of Contents enclosed.

VOLUME 2:

Chapter 1	Introduction
Chapter 2	Guidelines and Procedures for Network Design
Chapter 3	Guidelines and Procedures for Pre-mission Planning and Network Initiation
Chapter 4	Guidelines and Procedures for Network Operation
Chapter 5	Guidelines and Procedures for Cryptonet Management

VOLUME 3:

National Supplement 1	Belgium
National Supplement 2	Canada
National Supplement 3	Czech Republic
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 1
CONTENTS

Chapter Page

LIST OF FIGURES

LIST OF TABLES

ANNEXES

CHAPTER 1

GENERAL INTRODUCTION

1.1 INTRODUCTION

1.1.1 Purpose of Document

1.1.1.1 The purpose of this document is to establish the Standard Operating Procedures (SOPs) for all organisations operating NATO Link 16 on the Multi-Functional Information Distribution System (MIDS). MIDS is the NATO requirement for an ECM-resistant digital communications system and will be met by the Joint Tactical Information Distribution System (JTIDS).

1.1.1.2 ADatP-16 is the standard reference document for operational personnel and those responsible for the planning and design of Link 16 networks. The document is not intended to be a network designer's handbook, but rather a senior operator's guide as to how networks are designed. Designers will use this document to understand the operational functioning of the link. Guidelines are provided for the development of Local Operating Procedures (LOPs) to specify detailed operator-initiated actions.

1.1.1.3 ADatP-16 is an operational manual, rather than a technical one, and as such could be used as a basis for the training of operators.

1.1.2 Scope of Documentation

1.1.2.1 This document addresses all personnel involved in the planning, configuration, execution and management functions of Link 16 and defines their responsibilities in these functional areas.

1.1.2.2 Procedures are defined for the exchange of tactical information between MIDS units (or JTIDS units (JUs)), and procedures for the establishment, operation, management and termination of a Link 16 network. In addition, interoperability procedures are defined to enable effective data exchange with other data links including IJMS.

1.1.2.3 ADatP-16 does not contain a detailed description of all operator actions, but assumes knowledge by the operator of basic system operation.

1.1.3 Document Composition

ADatP-16 is divided into 3 volumes as follows:

a. Volume 1 - presents information and describes standard operating procedures which are of interest to all personnel involved in Link 16 network operations. A Summary of Contents is shown at Table 1.1.

b. Volume 2 - details guidelines and procedures for those personnel specifically involved in the Link 16 planning and management functions. A Summary of Contents is shown at Table 1.1 in Volume 2.

c. Volume 3 – details National/NATO Systems Message Implementation and Link 16 Peacetime Operating Restrictions in the form of National Supplements

1.1.4 Related Documents

In order to obtain a more detailed appreciation of any of the information presented in this document, reference should be made to:

a. STANAG 5516 - for specification of Link 16 in terms of message standards, operational procedures, data link protocols and network management principles.

b. STANAG 4175 - for technical specification of MIDS terminals, including implementation of the messages and protocols defined in STANAG 5516, and terminal interoperability.

c. STANAG 5616 - specifications for data forwarding between tactical data systems employing Link 16 and those employing Link11/11B.

d. NETMAN T/1 - The international standard for the exchange of MIDS/JTIDS network designs.

CHAPTER NUMBER	TITLE	SUMMARY OF CONTENTS
Chapter 1	Introduction	
Chapter 2	General Description of Link 16	Details the operational characteristics of Link 16 and briefly describes the technical functions employed to support them.
Chapter 3	Organisation and Responsibilities	Defines the organisation and responsibilities necessary for the planning, coordination and operation of Link 16 networks.
Chapter 4	Organisation of a Link 16 Network	Covers the Network Design, Pre-mission Planning and Network Initiation functions necessary for the establishment of Link 16 networks.
Chapter 5	Communications Procedures	Details communications procedures for the operation of Link 16 and covers Operational Network (OPNET) Management of the network. Link security procedures are also dealt with in this section.
Chapter 6	Data Exchange Procedures	Details procedures for the exchange of tactical information over Link 16 in support of surveillance, weapons coordination and management and aircraft control.
Chapter 7	Operation of Mixed Link 16 and IJMS Networks	Details procedures for operating a mixed Link 16/IJMS network and highlights the differences between the two communities.
Chapter 8	Interaction with other Links	Details procedures for interactions with other links required to maintain interoperability.
Chapter 9	The Needline Concept	Describes procedures for the operation of Needlines and their interaction with other NPGs.
Annex A	Glossary of Terms and Acronyms/Abbreviations	
Annex B	Link 16 Message List	
Annex C	Link 16 Amplification Data	Contains Tables of Commands, Weapons Engagement Statuses, Mission Assignments, Status Information Discretes and Vector Discretes.
Annex D	Nato Link Management Codes	

Table 1.1 Summary of Contents for ADatP-16 Volume 1

CHAPTER 2

GENERAL DESCRIPTION OF MIDS

2.1 OPERATIONAL CONCEPTS AND CAPABILITIES

2.1.1 General

This section outlines the MIDS Concept of Operations, and describes Link 16 functional areas and operational capabilities.

2.1.2 MIDS Concept of Operations

2.1.2.1 MIDS is a high capacity, ECM resistant digital communications system providing secure data transfer and secure voice in support of joint, air, ground, space and maritime operations. The general concept is to employ MIDS in the tactical environment to simultaneously connect many information contributors to many information users:

a. Tactical command and control systems exchanging information among themselves.

b. Command and control systems exchanging information with weapons systems.

c. Weapons systems exchanging information among themselves.

2.1.2.2 MIDS inherent features of position location and user identification provide additional capabilities within MIDS networks. Multiple communications nets, each with flexible data and voice capabilities, allow for meeting the combat needs of each user by the means of platform dedicated display/interface systems. Interoperability is maintained through the use of common NATO standards.

2.1.2.3 MIDS equipped, interoperable air, maritime and land forces, each using selected portions of a common air, maritime and land picture and tied together in a platform identification and common grid coordinate system, are capable of achieving much improved operational effectiveness in a hostile environment.

2.1.3 Link 16 Information Exchange

MIDS data and voice exchanges are performed according to the formats and protocols specified in the Link 16 message standard. Tactical data is selectively exchanged between MIDS/Link 16 platforms within communities of interest which are defined by functional, radio connectivity (needline) and security requirements. Link 16 also provides for information exchange through free text as well as data forwarded from other tactical data links. Link 16 technical functions support MIDS network management and tactical information exchange related to the twelve warfare tasks as shown in Table 2.1. The Link 16 technical functions are:

a. Systems Information Exchange and Network Management.

b. Precise Participant Location and Identification (PPLI).

c. Air Surveillance.

d. Surface (Maritime) Surveillance.

e. Subsurface (Maritime) Surveillance.

f. Ground Surveillance.

g. Space Surveillance.

h. Electronic Surveillance.

i. Electronic Warfare (EW)/Intelligence.

j. Mission Management.

k. Weapons Coordination and Management.

l. Control.

m. Information Management.

WARFARE TASK TECHNICAL FUNCTION	AIRBORNE OPS	AD AAW AD OPS	AIR OFFENSIVE SAM OPS	AIR RECON SURV OPS	AIRSPACE CONTROL	AIR STRIKE INTERDICT OPS	ASW OPS	CAS OPS	FIRE SUPPORT OPERATIONS	LAND COMBAT OPERATIONS	SEARCH & RESCUE OPS	SHIP TO SHORE OVEMENT
SYSTEM INFO & NETWORK MGT	X	X	X	X	X	X	X	X	X	X	X	X
PPLI	X	X	X	X	X	X	X	X	X	X	X	X
AIR SURVEILLANCE	X	X	X	X	X	X	X	X	X	X	X	X
SURFACE SURVEILLANCE		X	X	X		X	X		X		X	X
SUBSURFACE SURVEILLANCE				X			X				X	X
GROUND SURVEILLANCE	X	X	X	X		X		X	X	X	X	X
SPACE SURVEILLANCE												
ELECTRONIC SURVEILLANCE		X	X	X		X	X	X	X	X	X	X
EW INTELLIGENCE	X	X	X	X		X	X	X	X	X	X	X
MISSION MGT	X	X	X	X	X	X	X	X	X	X	X	X
WEAPONS COORD & MANAGEMENT	X	X	X	X	X	X	X	X	X	X	X	X
CONTROL	X	X	X	X	X	X	X	X			X	
INFORMATION MANAGEMENT	X	X	X	X	X	X	X	X	X	X	X	X

Table 2.1 MIDS User Technical Functions versus Warfare Tasks

2.1.4 Definition of Link 16 Functional Areas

2.1.4.1 System Information Exchange and Network Management

The System Information Exchange and Network Management function provides the information required to establish and maintain an interface via Link 16. This information consists of messages containing synchronisation, timing, capacity allocation, and control designation of relays, reassignment of relays and network control unit, and other data required to ensure interoperability of the participating tactical data systems. This function is divided into sub-functions as follows:

a. Network Initialisation.
b. Network Control.
c. Network Capacity Allocation and Reallocation.

d. Cryptonet Management.
e. Relay Control.
f. Test Requirements.

2.1.4.2 Precise Participant Location and Identification (PPLI)

The PPLI function provides an inherent identification and self reporting capability enabling JUs to report accurate, up-to-date information on own unit network participation status, identification, and position on the Link 16 Interface. PPLI messages also contain information on relative navigation (see paragraph 2.1.7) that allows Link 16 units to accurately determine their position. The PPLI function is essential to network participation.

2.1.4.3 Air Surveillance

Air Surveillance consists of the detecting, tracking, identifying, and reporting of air tracks. Included in the air surveillance function is the computation and reporting of track course, speed, and position, and determination of track identity. The surveillance unit must be able to report the track information to other platforms involved to provide early warning, threat warning, track correlation, and air traffic information.

2.1.4.4 Surface (Maritime) Surveillance

Surface (maritime) surveillance consists of the detecting, tracking, identifying, and reporting of surface tracks. Included in the surface surveillance function is the computation and reporting of track course, speed, and position. The surveillance unit must be able to report the track information to provide early warning, threat warning information, track correlation, and compilation of the surface situation.

2.1.4.5 Subsurface (Maritime) Surveillance

Subsurface (maritime) surveillance consists of the detecting, tracking, identifying, and reporting of subsurface tracks. Included in the subsurface surveillance function is the computation and reporting of track course, speed, and position. The surveillance unit must be able to report the track information to provide early warning, threat warning information, track correlation, and compilation of the subsurface situation.

2.1.4.6 Ground Surveillance

Ground surveillance consists of the detecting, tracking, identifying, and reporting of ground points and tracks. The surveillance unit must be able to report the track information to provide early warning, threat warning information, track correlation, and compilation of the ground situation.

2.1.4.7 Space Surveillance

Space surveillance consists of the detecting, tracking, identifying, and reporting of space tracks, including ballistic missiles. Included in the space surveillance function is the computation and reporting of track trajectory, speed, and position. The surveillance unit must be able to report the track information to provide early warning, threat warning information, track correlation, and compilation of the space situation.

2.1.4.8 Electronic Surveillance

Electronic surveillance consists of the detecting, tracking, identifying and reporting of emitters and jammers.

2.1.4.9 EW/Intelligence

This technical function provides for the amplification of surveillance information and the dissemination of tactical intelligence.

2.1.4.10 Mission Management

Mission Management provides for the exchange of information for overall mission planning and management. It also provides for requesting and directing the allocation of combat resources to satisfy immediate mission support needs and for reporting appropriate information to respond to mission management requests. This includes, but is not limited to, those reports and status required by the tactical commander to effect mission request; air, ground, surface, and subsurface tasking orders; sortie allotments, mission employment and allocation; and in-flight and mission reports. Normally, the command level that implements this technical function does not directly control weapons systems, but is responsible for timely allocation of resources between subordinate command and control (C^2) units. However, this function permits interaction among tactical units at the same levels as well as between senior and subordinate units.

2.1.4.11 Weapons Coordination and Management

Weapons coordination and management consists of the exchange of commands and status necessary to effect optimum employment for all weapons and to prevent mutual interference during tactical operations. This technical function provides information exchange between C^2 units that manage or directly control weapons system/support platforms (e.g., reconnaissance, cargo, etc.). The operational missions of intercept, reconnaissance, strike, close air support, missile/RPV control, submarine warfare, and other missions are supported by this technical function.

2.1.4.12 Control

Control consists of the real-time actions between controlling systems and weapons/supporting systems required to direct weapons systems/supporting platforms in the accomplishment of assigned missions. The control technical function provides for the exchange of information between C^2 units and weapons systems/platforms to accomplish aircraft control, surface control, subsurface control, and ground control. Additionally, the control technical function provides for the exchange of coordination information between weapons systems/supporting platforms, such as nonC^2-to-nonC^2 target data exchange and EW data exchange. The operational mission of cargo delivery, combat surveillance, ground manoeuvres, target acquisition, RPV control, air refuelling, air traffic control, automatic carrier landing control, EW control, ASW air control, search and rescue, etc. are included in this technical function.

2.1.4.13 Information Management

Information Management consists of the procedures and information exchange required to ensure that the platform/systems can properly exchange information when operationally interfaced. The information exchanged for this function consists of track management, information requests, correlation, pointers, track identification, IFF/SIF management, filter management, association, and mission correlator change. Information management data will be exchanged in conjunction with the air, surface, subsurface, ground, and electronic surveillance functions.

2.1.5 Operating Frequencies

MIDS operates at frequencies in the range 960-1215 MHz within D-band and employs spread spectrum and frequency hopping techniques to achieve its anti-jam capability. Measures are employed to reduce the possibility of interference with Identification Friend or Foe/Selective Identification Feature (IFF/SIF) by MIDS and to minimise interference with the Tactical Air Navigation (TACAN) and Distance Measuring Equipment (DME) facilities.

2.1.6 Link Security

Information transfer is cryptographically secure. Cryptovariables are stored at the MIDS terminal but may be changed over the air under the direction of the Network Manager. Information access can be controlled by the distribution of cryptovariables among participating units, forming single or multiple cryptonets.

2.1.7 Relative Navigation

Information contained in PPLI messages is used to provide a Relative Navigation facility, to assist mobile JUs in maintaining an accurate knowledge of their position relative to each other at all times. A network can operate Relative Navigation using both the Geodetic Reference System and a Relative Grid. Where two or more terminals have accurate, independently derived knowledge of their geodetic position, the Relative Navigation facility will provide all participants with accurate geodetic position.

2.2 OPERATIONAL CONSTRAINTS

2.2.1 Line-of-Sight

Direct communication between terminals can only take place over line-of-sight (LOS) range. To support low level operations, and to increase geographic coverage, relay of information may be required to extend the effective range of communications, thus enabling the Operational Commander to receive information and to direct operations throughout his area of responsibility. MIDS relay is a terminal function, requiring no operator action.

2.2.2 Network Capacity

MIDS is a high capacity communications system capable of supporting many users but is constrained by a finite network capacity. As the number of participants increases, the implications of network loading become more significant. Information exchange may become degraded as some messages fail to be received within the required time intervals. However, higher levels of data flow may be maintained at the expense of a reduction in the level of ECM resistance.

2.2.3 Multinet Operations and Interoperability Implications

Capacity problems are most acute when operating a single net, because the transmission capacity available for allocation to all planned participants is fixed by the time sharing structure of MIDS itself. The problem may be alleviated by conducting multinet operations, which increases the overall available network capacity. JUs may be allocated transmission capacity for different functions across a number of nets. However, a JU supported by a single terminal may only operate on one net in any one instant in time. Sub-communities may be established to operate simultaneously on different nets but connectivity cannot be maintained between such groups of JUs. Therefore, multinet operations may be implemented to increase the total network capacity where two or more groups of JUs can be identified which have mutually exclusive communications requirements for particular functions. The allocation of transmission capacity to functions across different nets must be carefully planned to preclude communications conflicts for individual JUs.

2.2.4 Peacetime Operating Restrictions

Frequency clearance agreements define the total emissions which can be generated by a MIDS community within a given geographic area, and also the number of emissions which can originate from a single source within that area. The terminology used to indicate the maximum or actual number of emissions is known as the Time Slot Duty Factor (TSDF) and is usually represented in the form “m/n” where “m” is a percentage indicator of the maximum number of transmissions allowed for the total community, and “n” is a percentage indicator of the maximum number of transmissions allowed for a single user – e.g. 100/50. Some national frequency clearance agreements specify a three part TSDF, e.g. 100/50/20, where the third value represents alternative single user limitations TSDF is calculated by counting time slots (100 TSDF represents 1536 time slots per 12 seconds); the “equivalent TSDF” can be calculated by counting pulses (100 TSDF represents 396, 288 pulses per 12 seconds), as described in paragraph 2.3.3.1e of Volume 2 of this document.

2.3 TECHNICAL FUNCTIONS

2.3.1 General

The operational characteristics of MIDS previously outlined are supported by a number of technical functions. Brief descriptions are given below in order to provide a basic understanding of the operation of a Link 16 network.

2.3.2 Time Division Multiple Access Architecture

2.3.2.1 MIDS is a time division multiple access (TDMA) system. System time is divided into 12.8 minute intervals, known as epochs, with 112.5 epochs per 24 hour day. An epoch is further sub-divided into 98,304 units of time of 7.8125 milliseconds duration, known as time slots. Each time slot defines an opportunity to transmit, thus each net provides 128 transmit opportunities per second. Time slots are used as the unit of allocation of network capacity to users for the transmission of Link 16 messages. It is a network management responsibility to ensure that JUs are allocated sufficient time slots to meet their operational needs.

2.3.2.2 JUs are each allocated a portion of the total network capacity in which they transmit messages. A simplified diagrammatic interpretation of a single net structure supporting two participants is shown at Figure 2-1. The "ring" of time slots depicts a single epoch. Time slots are allocated in blocks on a functional basis according to individual communications requirements. An individual JU's time slot block allocation is distributed evenly through the epoch. JUs receive messages in those time slots in which they do not themselves transmit or in which they have a specific receive assignment.

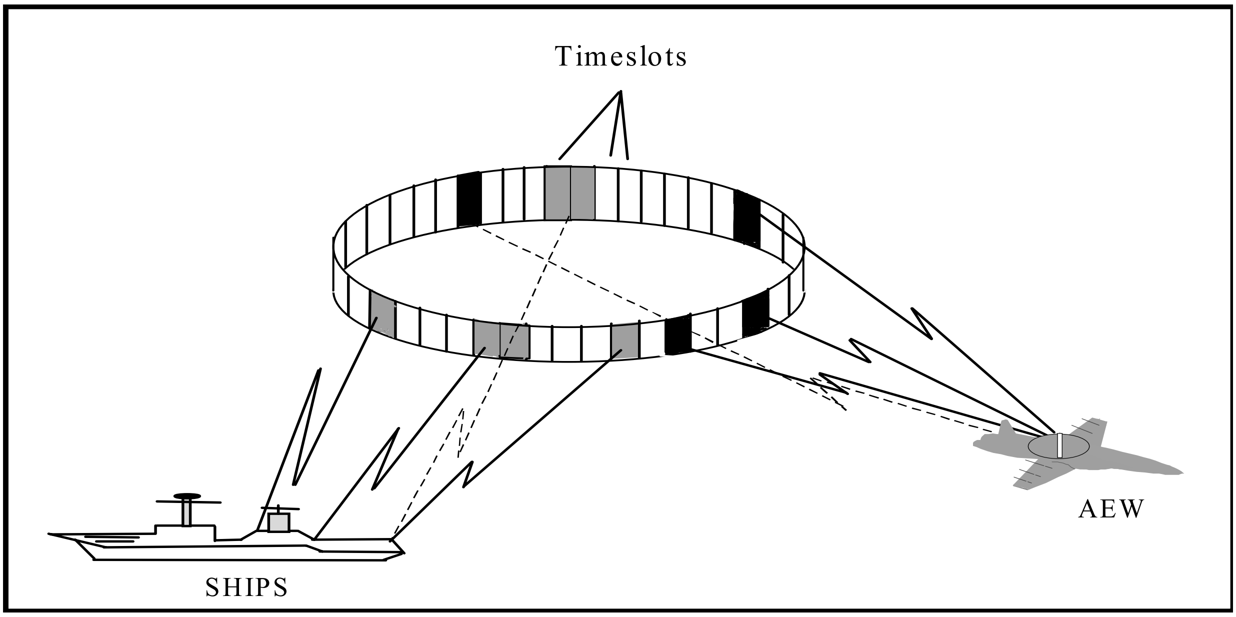


Figure 2-1 Example of Time Slot Block Allocation Within A Single Net TDMA Structure

2.3.2.3 The radio frequency of transmission is varied pseudo randomly across the 51 allowable frequencies within the range 960 - 1215 MHz. The frequency hopping pattern chosen for a given time slot depends on the net number and cryptovariable in use. By using different frequency hopping patterns, MIDS can support multiple nets, up to a theoretical maximum of 128 different nets per cryptovariable. In practice, however, mutual interference and self jamming restricts this; it is expected that between 15 and 20 nets can be operated simultaneously in close proximity.

2.3.2.4 JUs may only transmit or receive on a single net per time slot but may operate on different nets on a time slot by time slot basis depending on the assignment of time slot blocks. Multinetting is the simultaneous use of specific time slot blocks on different nets of a Link 16 network by independent groups of JUs. Connectivity is not maintained among all users of these time slots. Terminals transmit according to their respective time slot block assignments, as defined at initialisation or amended by the Network Manager, leaving the operator with no control over the net number used. Functions, such as Voice and Control, where the operator requires control over the net number employed, should be configured within the network design as Stacked nets; see paragraph 2.3.2.5 below.

2.3.2.5 A specialised form of multinetting, known as Stacked Net operation, can be employed where the operator requires a degree of control over which net is used for transmission and reception, such as for Voice and Control. Stacked Net operation is the coordinated use of simultaneous blocks of time slots, which differ only in channel number and/or cryptovariables assigned . (For Stacked Net operations only, net numbers are referred to as channel numbers). The operator is then able to select a desired channel number from the range 0-126 by switch action during network operations. In a stacked net configuration only, selection of net number 127 means that no channel is in effect for that function. Figure 2-2 depicts a network time-line incorporating stacked nets for the functions of Control and Voice. This creates sub-communities operating independently on separate channel numbers to exchange localised information exclusive to that sub-community. Specific channel designations for each mission are promulgated prior to network operations, via the OPTASK LINK (paragraph 4.3.5). Those functions required for network maintenance (Initial Entry, PPLI, Network Management), Surveillance and Weapons Coordination and Management are carried out on a common or main net.

2.3.3 System Time and Synchronisation

2.3.3.1 In order to communicate, JUs participating in a Link 16 network must be synchronised to a common time standard. Network time is established by the terminal designated as Network Time Reference (NTR). Only one unit can be initialised to perform as NTR for the whole network and his chronometer sets the time standard with which all other JUs must synchronise. The unit designated as NTR will be promulgated via the OPTASK LINK to all JUs prior to initiation of network operations (see paragraph 4.3.5)

.

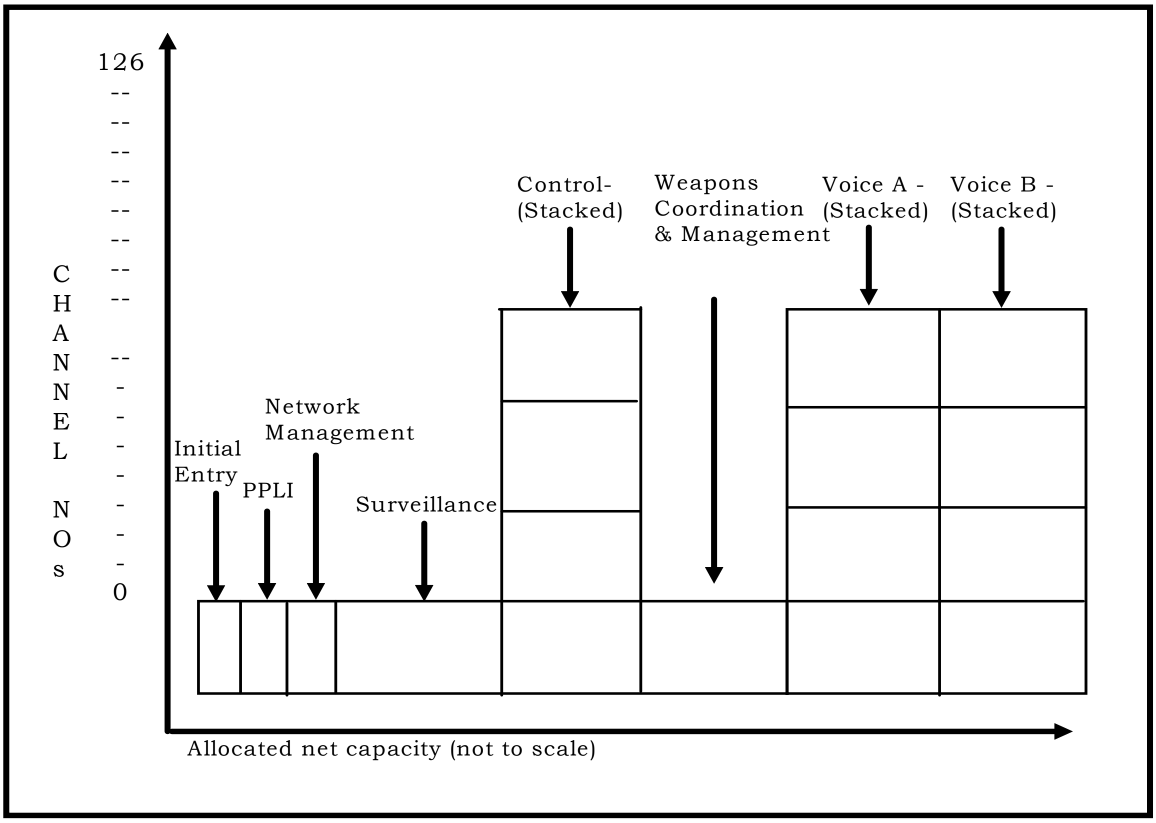


Figure 2-2 Example of Network Time-Line Incorporating Stacked Nets

2.3.3.2 Synchronisation is an automatic terminal function, requiring no operator involvement, and is completed in two stages. Initially coarse synchronisation is achieved which enables the terminal to receive messages but not to transmit. All JUs achieve coarse synchronisation to network time by receiving messages directly from the NTR or from other synchronised JUs initialised to perform the Initial Entry function (known as Initial Entry JUs (IEJUs)). Fine synchronisation of the terminal must be achieved before a JU may transmit and must be maintained to sustain full participation in the network. Fine synchronisation is achieved either actively or passively, depending on the method set at initialisation, by synchronising with any JU which has already achieved fine synchronisation to network time. If fine synchronisation is lost, the terminal will inhibit message transmission and automatically reinitiate the process of achieving fine synchronisation. It is possible for a JU to join the network under conditions of radio silence.

2.3.4 Cryptovariables

2.3.4.1 Cryptovariables are assigned for transmission operations, including determination of the frequency hopping pattern (Transmission Security (TRANSEC) cryptovariable), and data security on the link (Message Security (MSEC) cryptovariable). The use of these cryptovariables determines the crypto mode to be used on a time slot by time slot basis, as follows:

a. Common Variable Mode (CVM) - The MSEC cryptovariable assigned is the same as the TRANSEC variable.

b. Partitioned Variable Mode (PVM) - Two different cryptovariables are assigned, one for TRANSEC and one for MSEC.

2.3.4.2 JUs in possession of the appropriate TRANSEC cryptovariable can determine the frequency hopping pattern used to transmit on the selected net and thus receive the message. If held, the appropriate MSEC cryptovariable enables the platform to interpret received data. Data security is provided by the establishment of cryptonets. A group of JUs which use the same MSEC cryptovariable for a group of time slots operate on the same cryptonet. A JU that does not hold an MSEC for a group of time slots may be used as a relay platform for those time slots if it holds the common TRANSEC cryptovariable.

2.3.4.3 A MIDS terminal may store up to eight cryptovariables at any one time, held in the Secure Data Unit (SDU). The terminal can store cryptovariables for the current cryptoperiod and the next cryptoperiod and automatically rolls over to the new cryptovariable at the required time. Cryptoperiods are of either 24 hours or seven days duration. However, it is NATO policy that 24 hour crypto periods will be used.

2.3.4.4 A facility may be available to enable the Network Manager to supply a cryptovariable over-the-air. This is known as Over the Air Rekeying (OTAR) and may be used to distribute new cryptovariables in response to operational changes or suspected security compromise. However, two of the SDU storage locations are used in the OTAR process, which reduces the number of cryptovariables available for network use to six.

2.3.5 Principles of Message Exchange

2.3.5.1 Participation Groups

Timeslots are allocated to JUs on the basis of Network Participation Groups (PGs). These are defined according to function and therefore the types of messages to be transmitted. A terminal will transmit a message assigned to a PG in a time slot specifically allocated for that PG.

2.3.5.2 Access Modes

Time slots are allocated for message transmission by one of the following access modes:

a. (1) Dedicated Access - time slots are allocated for the unrestricted use of an individual JU. Time slots assigned in Dedicated Access mode for the transmission of a PG's messages are used by the terminal as required in order of occurrence.

(2) Dedicated Reuse - this is a network management technique of allocating the same time slots to more than one JU. Care must be taken when using Dedicated Reuse since this may reduce the probability of a message being received.

b. Contention Access - time slots are allocated to a contention pool which is shared by multiple JUs, with each JU having a predetermined access rate. The access rate determines the number of transmission opportunities allocated to the JU. Contention Access mode is more efficient than Dedicated Access mode in terms of time slot usage, but again reduces the probability of a message reaching its destination. Contention Access is most suitable for those PGs in which data is easily refreshed or repeated, such that the loss of any one message will not be critical.

c. Timeslot Reallocation - time slots are allocated to a pool which is self-managed by the participating terminals, on the basis of reported demands for time slots and connectivity among members of the pool. No operator action is required.

2.3.5.3 Message Format

A time slot may be used to transmit in one of the following formats:

a. Fixed Format - information is transmitted in a fixed, predefined format as defined in the Link 16 message catalogue and summarised at Annex B.

b. Free Text - used for the transmission of voice and alphanumeric data not in a predefined format.

2.3.5.4 Packing Structure

Time slots for transmission use one of the following packing structures:

a. Standard.

b. Packed 2 Single Pulse.

c. Packed 2 Double Pulse.

d. Packed 4.

The amount of data which can be transmitted in each of these packing structures is illustrated in Figure 2-3. A time slot may contain more than one Fixed Format message. The terminal will automatically increase the packing level as required, up to the upper limit defined at initialisation. The use of higher message packing structures increases the volume of data transmitted, but decreases ECM resistance and eliminates the extended range option (see paragraph 2.3.5.5) by decreasing the propagation/guard time.

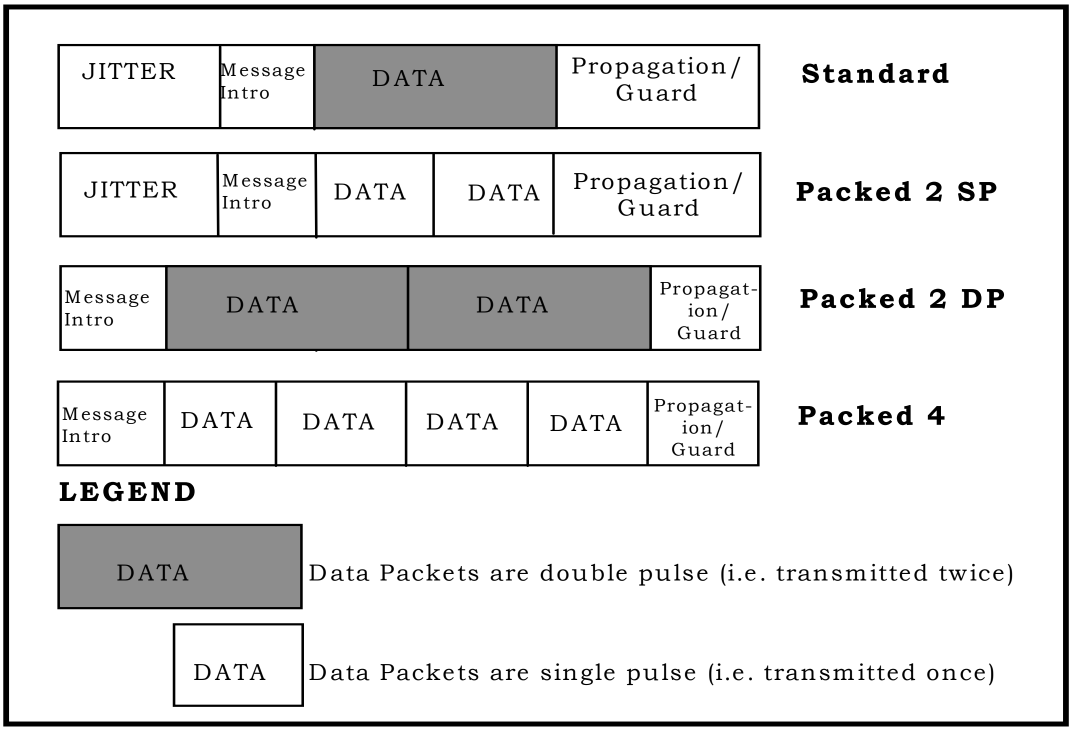


Figure 2-3 MIDS Packing Structures

2.3.5.5 Range Mode

Link 16 networks may be operated in either of two range modes:

a. Normal range mode - up to 300nm (or 550km) LOS range.

b. Extended range mode - up to 500nm (or 920km) LOS range.

All JUs participating in a network must operate in the same range mode. The extended range mode option is only available for use with Standard and Packed-2 Single Pulse packing structures as above.

2.3.5.6 Transmit Modes of Operation

Three transmit modes are available and determine the conditions under which a JU may transmit messages:

a. Normal Mode - a JU achieves and maintains fine synchronisation either actively or passively and can transmit messages unconditionally within its time slot allocation.

b. Conditional Radio Silent Mode - a JU maintains fine synchronisation passively and can receive all messages, but cannot transmit fixed format Link

16 messages or perform receipt/compliance (paragraph 2.3.5.10). MIDS voice capability is retained.

c. Polling Mode - a JU maintains fine synchronisation either actively or passively and may perform receipt/compliance, but may only transmit fixed format Link 16 messages when interrogated by the polling JU. All messages may be received and the MIDS voice capability is retained.

Transmit modes are operator-selectable.

2.3.5.7 Communications Modes

Three communications modes are available and determine whether a network may operate multiple nets and whether messages are encrypted on transmission as shown in Table 2.2. All JUs in a network must operate in the same communications mode.

Mode	Multinet Capability	Data Encryption Employed	Comments
Mode 1	Yes	Yes	Default Mode. Frequency hopping techniques employed between 960 and 1215 MHz
Mode 2	No	Yes	Single net (net 0) at fixed frequency of 969MHz.
Mode 3	-	-	Not used by Link 16.
Mode 4	No	No	Single net (net 0) at fixed frequency of 969mhz. Used for test purposes only.

Table 2.2 Link 16 Communications Modes

2.3.5.8 Interference Protection Feature (IPF) Modes

To ensure compliance with peacetime operating restrictions, JUs will operate in one of three Interference Protection Feature (IPF) modes to provide the necessary control of transmissions from the terminal. Details are provided in Volume 3.

2.3.5.9 Message Exchange and JU Address

Each JU participating on a Link 16 network is assigned a reference number (address) of five octal digits which is used to:

a. Identify the source of a message (Source Track Number(TN)).

b. Address messages to specific JUs (Addressee TN).

Most messages exchanged on Link 16 are broadcast and do not require an Addressee TN. Where it is required to send a message which can be addressed to all JUs, a collective address of 00177 is used. Further details of track number allocation are contained in paragraph 6.2.2.2.

2.3.5.10 Group Identifier Addresses

In addition to a Primary TN, a JU may be assigned up to 16 Secondary TNs to be monitored for addressed messages. Any one or more of these Secondary TNs may be assigned to a group of JUs as a Group Identifier Address. Messages addressed to a Secondary TN which has been designated as a Group Identifier Address will be monitored by all the JUs with that initialised Secondary TN. These messages will not require Receipt/Compliance.

2.3.5.11 Receipt/Compliance

Link 16 messages which are not generated in response to another message are known as original messages. Some messages which are addressed to a specific JU require an acknowledgement from the receiving unit and an indication of the response taken. This protocol is known as Receipt/Compliance and the following responses may be made:

a. WILCO - receiving unit will comply. Response initiated by the operator.

b. HAVCO - receiving unit has complied. Response may be initiated automatically or by the operator.

c. CANTCO - receiving unit cannot comply. Response initiated by the operator.

Other responses may be made automatically without the operator being aware of the transmission, as follows:

d. Machine Receipt - message received error free. In response to network management messages, this will be interpreted as a WILCO.

e. CANTPRO - message cannot be processed.

If a response is not received by the originating terminal within the timeout interval specified, the message is automatically retransmitted a predetermined number of times. If no response or a response of CANTCO or CANTPRO is received, the operator at the originating terminal may be alerted (depending on system implementation). Operator-originated responses of WILCO, HAVCO and CANTCO also require automatic acknowledgement by machine receipt. The operator at a JU which originated such a response may be alerted if this acknowledgement is not received.

2.3.5.12 Message Relaying

Radio relay techniques may be employed to extend effective communications beyond LOS range or in response to enemy jamming. However, the relay function necessarily utilises additional network capacity and the extent of its use should depend on operational priorities. A terminal designated as a relay platform must be operating in Normal mode and must be assigned time slots specifically for relay. A JU that is reporting Limited Status due to a tactical data system failure may still be used as a relay platform. The designated NTR may also be employed as a relay platform. Dynamic management of network capacity for relay is performed by the Network Manager; procedures are contained in Chapter 4 of Volume 2. A terminal will automatically perform relay in accordance with the relay assignment parameters held, with no additional operator intervention required. However, on some platforms the operator is able to enable/disable the relay function.

2.3.6 Voice Communications

2.3.6.1 MIDS provides a secure voice capability. Digitised voice may be transmitted at rates of 2.4kbps and/or 16kbps, depending on platform implementation. All platforms that implement MIDS voice will use at least the 16kbps rate. However, the option to apply error correction coding to voice data is only available at the lower transmission rate.

2.3.6.2 Network capacity may be allocated to up to two voice ports via two Voice PGs (known as Voice Groups A and B) for the transmission and reception of digitised voice. Time slot blocks may be allocated in a stacked net configuration to enable the operator to select by switch action from a range of channel numbers. The terminal will automatically receive in those time slots not used for transmission.

2.3.7 Relative Navigation

2.3.7.1 Relative Navigation is a MIDS terminal function which provides JUs with position information based on a Geodetic Reference System and where necessary, a Relative Grid system, using a selectable grid origin. Relative Navigation depends upon the use of ranging techniques based on time of arrival of PPLI messages.

2.3.7.2 JUs with an accurate knowledge of their absolute geodetic position may be designated as Position Reference (PR). PRs are not essential to the operation of the Relative Navigation function, but the presence of PRs in the network may increase the position quality which can be computed from this function. For this reason, PRs are important and should be provided for in the network design where possible.

2.3.7.3 To implement Relative Navigation with the Relative Grid a JU must be nominated to act as Navigation Controller (NC). The NC is responsible for establishing the relative grid and determining the point of origin and grid north. This is set during initialisation and requires no operator action during network operation.

2.4 MIDS UNIT CAPABILITIES

2.4.1 Classification of Units

JUs are classified according to the extent of their responsibilities as either of the following:

a. Command and Control MIDS Unit (C^2 JU) - a JU with command and control capability communicating directly on Link 16 networks.

b. Non Command and Control MIDS Unit (NonC^2 JU) - a JU other than a C^2 JU communicating directly on Link 16 networks.

2.4.2 Unit Definitions

The following definitions apply throughout the document:

a. Interface Unit (IU) - An IU is a MIDS unit (JU), Participating unit (PU) or Reporting unit (RU) which provides information to the interface.

b. MIDS Unit (JU) - A JU is a unit which communicates directly on Link 16.

c. Participating Unit (PU) - A PU is a unit which communicates directly on Link 11.

d. Reporting Unit (RU) - An RU is a unit which takes part in the exchange or transfer of tactical data on a point-to-point data link to which data can be addressed and from which data can be identified as a source.

e. Indirect Unit - An Indirect Unit is a PU or RU that is being forwarded onto Link 16.

f. Supporting Unit (SU) - An SU is a unit operating in support of a JU, PU or RU which is providing data for the interface but which is not specifically identified as a data source.

g. Forwarding MIDS Unit (FJU) - An FJU is a JU that translates and forwards data among units using Link 16 messages and other message standards. (Different types of FJU are defined in paragraph 7.2.1.2).

CHAPTER 3

ORGANISATION AND RESPONSIBILITIES

3.1 GENERAL

A hierarchy of command, consisting of a number of organisational levels, is required for the planning, establishment and operation of Link 16 networks in NATO. Since the majority of Link 16 networks will be developed to support NATO forces from more than one Service or nation within a given geographical area of operation, specific responsibilities for “Link 16 Network Management” have been assigned within the NATO military command structure.

3.2 NETWORK MANAGEMENT ACTIVITIES

Link 16 Network Management encompasses the interrelated activities of design, pre-mission planning, initiation and control of the network and cryptonet management.

3.2.1 Network Design

Network Design includes the activity of specifying the operational requirements for a Link 16 network and designing the network's structure.

3.2.2 Pre-mission Planning

Pre-mission Planning is the activity required prior to implementing a Link 16 network, including selection of the network design to be used.

3.2.3 Network Initiation

Network Initiation is the activity which encompasses specific platform initialisation and network entry.

3.2.4 Network Operation

Network Operation includes the monitoring and modifying of a functioning Link 16 network.

3.2.5 Cryptonet Management

Cryptonet Management includes the distribution and use of crypto for Link 16 operations.

3.2.6 Network Analysis

Network Analysis covers those post-operations activities conducted off-line for the purpose of network performance evaluation.

3.3 AUTHORITIES AND RESPONSIBILITIES

NATO operational commanders are tasked with the definition, production and dissemination of Link 16 network designs to meet operational requirements. NATO commanders will endeavour to satisfy Link 16 user requirements for all extant NATO operational plans.

3.3.1 Operational Command Responsibilities

The Major NATO Commanders (MNCs) are responsible for the overall management of NATO Link 16 networks to enable them to be used effectively in support of NATO operations and training activities. The Link 16 authorities within the NATO command structure and their specific responsibilities towards network management are as follows:

3.3.1.1 Bi-SC Data Link Management and Interoperability Cell (DLMIC)

a. Defining NATO network management policy.

b. Ensuring that MIDS operations in NATO conform to national FCAs where that responsibility is detailed by national authority. This responsibility is delegated to the RDLMC for activity within the appropriate AORs.

c. Ensuring coordination is carried out between NATO and nations that retain coordination authority within their FIR.

d. Ensuring coordination is carried out between NATO and nations in which NATO intends to operate MIDS or where NATO MIDS activity may have an effect.

e. Coordinating NATO MIDS operational communication requirements.

f. Identifying and resolving inter-regional conflicts in operating needs.

g. Maintaining a NATO network management capability to design, produce, distribute and carry out configuration management of MIDS network designs.

h. Liaison with nations and the NHQC3S/ FMB on FCAs.

i. Identifying requirements for network management and OPNET management equipment.

j. Identifying, reporting and resolving interoperability related problems.

3.3.1.2 Regional Data Link Management Cell (RDLMC)

a. Coordinating regional communication requirements for MIDS operations.

b. Identifying and resolving conflicts in regional NATO/national MIDS network requirements.

c. Referring unresolved conflicts in requirement to the Bi-SC DLMIC for resolution.

d. Designating DLMCs.

e. Maintaining a regional network library of MIDS network plans.

f. Designating the commander responsible for issuing the OPTASK LINK.

g. Issuing maintaining and promulgating Regional Standing OPTASK LINK documentation.

h. Coordinating regional requests for MIDS network designs and referring them to the Bi-SC DLMIC.

i. Investigating and reporting network management related problems.

j. Designating the unit responsible for regional network management.

3.3.1.3 Data Link Management Cell (DLMC)

a. Exercising TACOM of the appropriate MIDS network.

b. Assuming the responsibilities of OPNET manager as directed.

c. Issuing OPTASK LINK.

d. Delegating OPNET Management responsibility.

e. Nominating TACON responsibilities.

f. Compiling, updating and promulgating MIDS schedule of activity.

g. Allocating network resources and resolving conflicts of requirement.

h. Selecting and ordering the appropriate network to be used to meet operating requirements.

i. De-conflicting networks within the CA and with other DLMCs to ensure compliance with national FCAs in accordance with procedures laid down in Annex D.

j. Coordinating the operational requirements of various forces, either operating in or transiting through their area of responsibility.

k. Ensure the efficient and effective transfer of platforms transiting through their areas to adjacent DLMCs.

l. Referring unresolved conflicts in requirement to the RDLMC for resolution.

m. Investigating and reporting network management related problems reported by participating units.

n. Coordinating requests from operational units for MIDS network designs and referring them to the appropriate RDLMC.

o. Maintaining accurate records of all MIDS activity in their area of responsibility.

3.3.1.4 OPNET Manager

a. Ensuring necessary network functionaries are present in the network and operating correctly.

b. Ensuring compliance with frequency clearance restrictions.

c. Maintaining connectivity between units by designating relay platforms.

d. Monitoring communications quality.

e. Monitoring and controlling transmission capacity.

f. Maintaining network security.

g. Ensuring the relative navigation quality is maintained.

h. Contributing to recording and analysis of network performance.

i. Monitoring participant status.

j. Maintaining system timing and network synchronisation.

k. Supporting network entry by new participants.

3.3.2 Network Manager Responsibilities

The Network Manager has overall responsibility for:

a. Network Planning - selection of primary and alternate network structures.

b. Ensuring participants have the necessary identification and crypto data.

c. Allocating network roles.

d. Producing the information necessary for inclusion into the OPTASK LINK.

e. Coordinating network entry and exit.

f. Monitoring network performance and operational effectiveness.

g. Ensuring that peacetime operation of a Link 16 network does not contravene agreed operating restrictions in the given area of operations.

h. Ensuring that the operational effectiveness of a network remains optimal under changing conditions by exercising OPNET Management.

3.3.3 Cryptonet Manager Responsibilities

Responsibility for Cryptonet Management should be assigned to an appointed Cryptonet Manager. However, it should be noted that aspects of cryptonet management are necessarily performed as an integral part of other network functions such as Network Design and Network Operation, and the guidelines produced are equally applicable to these functions. The Cryptonet Manager's duties include:

a. Ensuring that Link 16 network operations are conducted within established COMSEC guidelines to minimise the exposure of sensitive operational information.

b. Allocating cryptovariables to be used during network operations.

c. Ensuring a quick and effective response to detection of a security compromise during network operations.

d. If OTAR is authorised, provide the Network Manager with the information necessary to enable OTAR messages to be generated for any JU participating on the network.

3.3.4 MIDS Unit Responsibilities

Individual JUs are responsible for:

a. Initialising the MIDS terminal according to instructions contained in the OPTASK LINK (as detailed in paragraph 4.3.5).

b. Conducting Link 16 network operations in accordance with agreed operational procedures.

c. Responding to all requests and commands from the Network Manager.

CHAPTER 4

ORGANISATION OF A LINK 16 NETWORK

4.1 GENERAL

4.1.1 Network Management Activities

Link 16 network structures may be designed to cover a wide range of operational scenarios, from a single net supporting only a few users to a complex multinet structure facilitating large scale inter-Service and multinational data exchange. The organisational process involved in planning and establishing Link 16 networks is divided into the following activities:

a. Network Design.

b. Pre-mission Planning.

c. Network Initiation.

d. Network Operation.

e. Cryptonet Management (described in Chapter 5).

f. Network Analysis.

4.1.2 Overview

This division of responsibilities provides for centralised planning and decentralised control. The aim is to maximise the centralised planning and design functions, in order to minimise the need for on-line network reorganisation, thereby reducing the potential for disruption. The remaining sections in this chapter describe the activities involved in this organisational process. Procedures and guidelines for Network Operation are given in Chapter 5. Further details are to be found in Volume 2 of this document.

4.2 NETWORK DESIGN

4.2.1 General

4.2.1.1 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. Network Design comprises the following activities:

a. Specification of Link 16 network requirements to support anticipated tactical operations.

b. Production of Link 16 network designs and their associated Network Description Summaries (NDS) to fulfil these requirements.

c. Validation of Link 16 network designs to ensure that operational requirements have been set.

d. Distribution of approved Link 16 network designs to operational units required to participate in Link 16 operations.

4.2.1.2 The process of NATO Network Design is illustrated in Figure 4-1 and basic procedures are defined in the following paragraphs. Further detailed procedures and additional information regarding network design considerations and implications can be found in Volume 2 of this document.

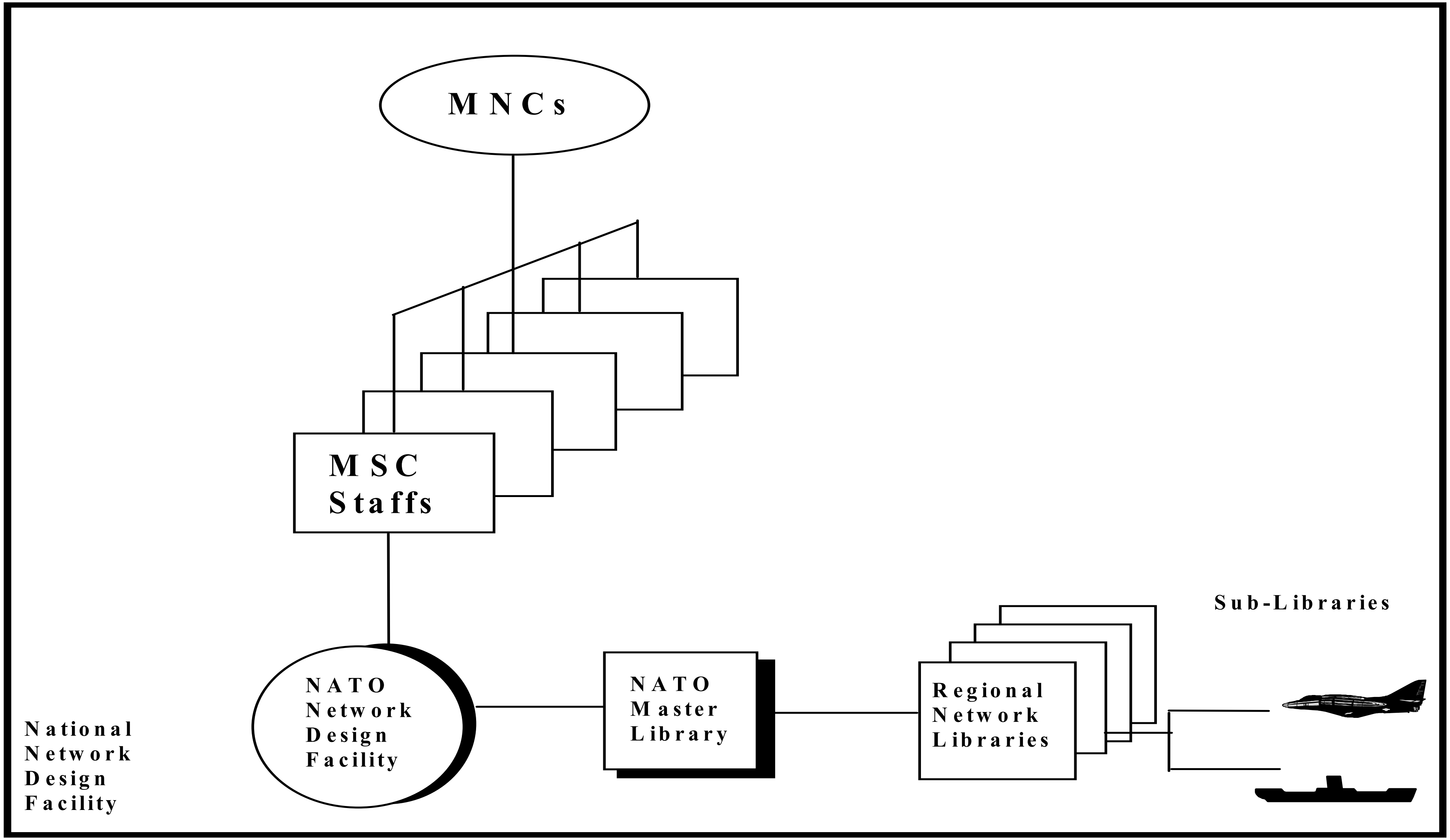

MNCs
MSC Staffs
Sub-Libraries
NATO Network Design Facility
NATO Master Library
Regional Network Libraries
National Network Design Facility

Figure 4-1 Network Design

4.2.2 Network Requirements Specification

4.2.2.1 Each MSC is responsible for coordinating and specifying the Link 16 network requirements necessary to support tactical operations within his AOR. Network requirements specification is accomplished in the following stages:

a. Individual nations and subordinate commanders declare their respective Link 16 user requirements necessary to support NATO operational plans.

b. MSC staffs coordinate individual Link 16 user requirements to determine NATO Link 16 network requirements. This will involve:

(1) Determining operational priorities and trade-offs, as necessary, to resolve conflicting intra-regional Link 16 user requirements.

(2) Liaising with other MSCs/national network design authorities to coordinate regional network operations, involving participation by forces committed from another MSC or reinforcement forces, and to coordinate network operations in adjacent regions involving associated support platforms.

(3) Taking account of national (non-NATO) requirements for Link 16 operations within the MSC's AOR.

(4) Raising inter-regional MSC and NATO/national Link 16 network requirement conflicts to the appropriate MNC for resolution.

c. Coordinated network requirements are passed to a Network Design Facility (NDF) for the development of Link 16 network designs to meet NATO operational requirements.

d. MSC staffs should coordinate with network designers to resolve any design conflicts which may arise during the network design process, and to ensure that network designs are updated and/or new designs are generated in response to changing operational requirements.

4.2.2.2 Network requirements should be specified and issued to the nominated NDF using the standard NATO Network Design Form (see Figure 4-2). This format may be amplified to meet the full requirements of individual nations and situations, but, as a minimum, should contain the following:

a. Requesting agency details and point of contact.

b. Planned utilisation summary, which outlines the objective of the network.

c. Participant list.

d. Connectivity requirements.

e. Operating restrictions.

f. Crypto partitioning requirements.

g. Geographic or relative location and force disposition.

NETWORK REQUEST FORM

1. **Requester Information**:
Identify name & address of requesting agency, point of contact, operational authority, date network required and agency (or agencies) to whom network should be sent.

2. **Planned Utilisation**:
Provide brief description of the objective of the network, particularly in terms of the types of mission the network is required to support.
E.g. “The network will support Exercise XXXXX. It will allow interoperability training among airborne and land-based air defence units.”

3. **Participant List**:
Define number and type of participants.
E.g. “25 total participants, comprising 2 UK E-3D, NAEW E-3A, USAF E-3B, 16 Tornado F3s, 5 IJMS Ground Sites.”

4. **Connectivity Requirements**:
Specify data exchange requirements by functional area (including expected track/target reporting load), relay requirements, voice requirements, free text requirements, data forwarding requirements.
E.g. “The network will support Link 16 (PPLI, Surveillance, Information Management, Mission Management/Weapons Coordination and Management) and IJMS. Relay is desired for all ground unit transmissions. Total surveillance capacity = 250 tracks. Voice A 2.4 kbps coded; Voice B 16 kbps uncoded.”

5. **Operating Restrictions**:
Identify any deconfliction considerations, frequency clearance restrictions in force.
E.g. “The network is designed to operate concurrently with the assignments for Southern Norway, Denmark and Central Europe on Nets 2, 3 & 4. IPF Exercise Override will be authorised.”

6. **Crypto Partitioning Requirements**:
Define crypto connectivity requirements if network is to operate in Partitioned Variable Mode.

7. **Force Disposition**:
Describe geographic or relative location and force disposition (preferably by diagram).

Figure 4-2 Network Request Form

4.2.3 Production of Network Designs

4.2.3.1 Link 16 network designs are produced at a suitably equipped NDF to meet the Link 16 network specifications, within the technical constraints imposed by terminal and host platform implementations. Development of network designs involves determining network initialisation parameters and allocating time slot capacity to planned network participants. The basic tasks to be performed by the NDF include:

a. Assignment of network capacity to required PGs.

b. Designation of CVLL(s) to meet specified crypto connectivity requirements.

c. Assignment of network capacity for relay, as required, to meet specified connectivity requirements.

d. Allocation of time slot blocks to planned network participants for the transmission and reception of Link 16 messages in accordance with specified network data exchange requirements.

e. Specification of other network initialisation parameters, as required.

4.2.3.2 Normally, Link 16 network designs should be produced well in advance of intended network operations. However, the NDF should be capable of responding to a need for network designs to be generated and/or modified at short notice in response to rapidly changing operational requirements.

4.2.3.3 A Network Description Summary (NDS), which is a description of the operational 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. More details and an example are provided in Volume 2, Chapter 2.

4.2.4 Network Design Validation

NATO network designs should be validated to ensure that network designs satisfy the operational requirements specified and comply with any frequency clearance restrictions in force. This may involve exercising the network design in simulated or live training environments to analyse network performance.

4.2.5 Network Design Distribution and Storage

The originating NDF is responsible for distributing network designs as directed by the MSC, in advance of intended operations. The following procedures apply:

a. NATO network designs must be approved by the MSC originating the network requirement prior to operational release.

b. The distribution medium used must be compatible with the receiving units' initialisation facilities.

c. Network designs should be sent to national Initialisation Data Preparation Facilities (IDPFs) (or national NDFs where such facilities have been established) to enable network design data to be generated on the appropriate media for that nation's platforms.

d. Operational units should maintain sub-libraries of distributed Link 16 network designs, to provide safe storage and ready access when required.

e. The originating NDF retains configuration control of all network designs produced. Changes to network design data must only be made on the authorisation of the originating NDF.

4.2.6 Security Considerations

It is the responsibility of the NDF to ensure that all network design data, including NDSs, are appropriately classified in accordance with existing NATO security guidelines. However, network design data originated at the NDF should normally contain only material at the NATO UNCLASSIFIED level until tied to specific operations, operational units, or geographic areas.

4.3 PRE-MISSION PLANNING

4.3.1 General

4.3.1.1 Pre-mission Planning is the process of determining data link connectivity requirements, selecting the appropriate network design, identifying crypto requirements and assigning network duties to meet a specific operational task. Where necessary, this includes the deconfliction of Link 16 operations.

4.3.1.2 The MSC will be responsible for the selection of network designs for regional use. Day-to-day coordination of network use may be delegated to the Tactical Commander. Tactical Commanders will disseminate to all Link 16 participants an OPTASK LINK message detailing specific network configuration information including the period of operation, the platforms involved, crypto loading requirements and network functional responsibilities.

4.3.2 Pre-mission Planning Activities

The process of Pre-mission Planning incorporates the following activities:

a. Coordination with adjacent regions and nations to establish actual inter-regional connectivity requirements and to ensure compliance with national frequency restrictions.

b. Selection of an appropriate network design from the Link 16 network library to satisfy defined operational requirements. Whenever a design is selected that has not been validated, an alternative (validated) design must be selected as back-up.

c. Modification of the selected design, if necessary, to accommodate all required network participants and to achieve desired connectivity among them. Such modifications, however, should always be kept to a minimum.

d. Selection of the Primary and Standby Network Manager responsible for the initiation and management of network operations. Network Managers should be suitably located and equipped to perform their task. If required, sub-network managers may also be designated to manage a portion of the total network, defined according to either function or user group. The Network Manager will normally also be responsible for Cryptonet Management.

e. Allocation of network roles, including standbys, to JUs as required:

(1) Network Time Reference (NTR)

(2) Initial Entry JUs (IEJUs)

(3) Navigation Controller (NC)

(4) Secondary Navigation Controller (SNC)

(5) Position Reference(s) (PR)

(6) Relay Roles

(7) Data Forwarder

f. Allocation of time slot assignment blocks, established by the network design, to actual participants, according to mission requirements and network roles assigned.

g. Allocation of Link 16 TN addresses to network participants. JUs required to report surveillance tracks on the network should be allocated blocks of surveillance track numbers for this purpose.

h. Dissemination of all essential information to operational units via the OPTASK LINK message (as defined in ADatP-3 and explained in paragraph 4.3.5)

4.3.3 Cryptovariables

The designated Network Manager, in coordination with the Cryptonet Manager, should use the distribution list of cryptovariables to each operational unit in order to establish a relationship between available cryptovariables (using short titles) and the cryptovariable logical labels (CVLLs) defined in the chosen network design. This relationship should be promulgated to crypto custodians at each operational unit via the OPTASK LINK.

4.3.4 Multi-link Considerations

The availability of other tactical data links in the Operational Commander’s AOR may influence the selection and modification of a Link 16 network design. More detailed guidance on this subject can be found in Chapter 7.

4.3.5 Operational Tasking Data Links (OPTASK LINK)

For each Link 16 network operation, an OPTASK LINK message must be distributed to all JUs intending to participate. The OPTASK LINK is a Message Text Format (MTF) or character oriented message that is transmitted in advance of operations. This message permits Officers in Tactical Command (OTC), appropriate shore commanders, or other designated authorities to promulgate detailed instructions regarding operation of tactical data links (Link 16, Link 11/11B, Link 1, Link 4, Link 14, and IJMS). The OPTASK LINK should include:

a. Identity of network design to be implemented.

b. Time of initiation and duration of network operations.

c. Modes of operation:

(1) Transmission mode.

(2) IPF mode.

(3) TDMA range mode.

(4) Communications mode.

d. Identity of:

(1) Network Manager and standby.

(2) Cryptonet Manager and standby.

(3) Sub Network Managers (as required).

e. Allocation of source track numbers to platforms; surveillance track number block assignment.

f. Allocation of network roles.

g. Current cryptoperiod designator(CPD).

h. Association of cryptovariable short titles to CVLLs.

i. Net Numbers and cryptovariables for:

(1) Voice Group A.

(2) Voice Group B.

(3) Control.

j. Variable Track Quality (VTQ).

k. Automatic Correlation/Decorrelation.

4.3.5.1 Specifying VTQ Settings

VTQ settings may be specified for some JUs in the OPTASK LINK in the GENTEXT/REPORTING REQUIREMENTS set during operations as the situation dictates. The track correlation process depends on the reporting of accurate TQ (see paragraph 4.3.6). Therefore, VTQ can contribute to the incorrect correlation of two tracks which are actually two separate vehicular objects. If many incorrect correlations occur involving JUs using VTQ, the TDC should consider directing that VTQ not be used.

4.3.6 Automatic Correlation Considerations

JUs use a standard set of automatic correlation tests to test for correlation between two Air or Surface (Maritime) tracks, in order to prevent or detect dual designations. The tests are described in more detail in paragraph 6.2.5.4.1.1. Although the tests are fully automatic, certain parameters to be used in those tests need to be determined and specified in the planning process. They are described below. Two terms that are to be understood in order to understand the use of variable correlation parameters are:

a. Incorrect Correlation: An incorrect correlation occurs when two tracks which are actually two separate vehicular objects are incorrectly correlated, thus losing one of the tracks until it is decorrelated.

b. Missed Correlation: A missed correlation occurs when two tracks which are actually the same vehicular object are not correlated, thus creating a dual or allowing a dual to persist.

4.3.6.1 Variable Correlation Parameters

a. Operational or testing experience may indicate that the correlation tests will result in fewer incorrect correlations and/or missed correlations if parameters used in correlation algorithms are adjusted. Therefore, C^2 JUs' correlation algorithms are programmed with nine different variable parameters that can be modified either in the initialization load or by operator selection in each C^2 JU. Each parameter has a default value, minimum and maximum allowable values, and a prescribed variability increment within the range of allowable values. (These parameters were not specified for implementation until 2001. Therefore, some C^2 JUs may not be able to vary the parameters.)

b. The settings for each of the variable correlation parameters are to be defined in the OPTASK LINK in the GENTEXT/REPORTING REQUIREMENTS section. The default settings should be specified unless data link planners or managers, e.g., DLM/ICO or TDC, are aware of reasons to specify otherwise. Such reasons might include known test results, local operating conditions, recent tracking observations, planned correlation tests, etc. This should be done by inclusion of the statement "USE DEFAULT CORRELATION PARAMETERS" or "USE DEFAULT CORRELATION PARAMETERS, EXCEPT (list parameters to be set to other than default, and the values to be set)". Changes to the variable correlation parameter values may also be directed by voice during operations. However, if the DLM/ICO determines that the automatic correlation process is not to be used, it should be indicated in the OPTASK LINK under Conditional Capabilities or directed by voice.

c. Table 4-1 lists the variable correlation parameters and their default, minimum, and maximum values and variability increments. Each parameter is designated by a letter that corresponds to the variable in systems' correlation algorithm equations. The letters can also be used for brevity in the OPTASK LINK or voice communications. The use of the parameters is described in more detail in paragraph 4.3.6.2.

Ltr	Parameter	Default	Minimum	Maximum	Increments
a	Window Size Multiplier	1.0	0.5	3.0	0.1
b	Minimum Window Size	0.5 dm	0.0 dm	2.0 dm	0.25 dm
c	Minimum TQ	7	3	7	1
d	Maximum TQ	10	8	15	1
e	Restricted TQ	4	2	6	1
f	Course Differential	45°	15°	90°	15°
g	Speed Differential	40%	10%	100%	10%
h	Altitude Differential	10K feet	5K feet	50K feet	5K feet
j	Minimum Q_{pg}	2	1	5	1
k	Maximum Q_{pg}	11	1	15	1
m	Decorrelation Window Multiplier	1.5	1.0	2.0	0.1
n	Consecutive Decorrelation	2	1	5	1

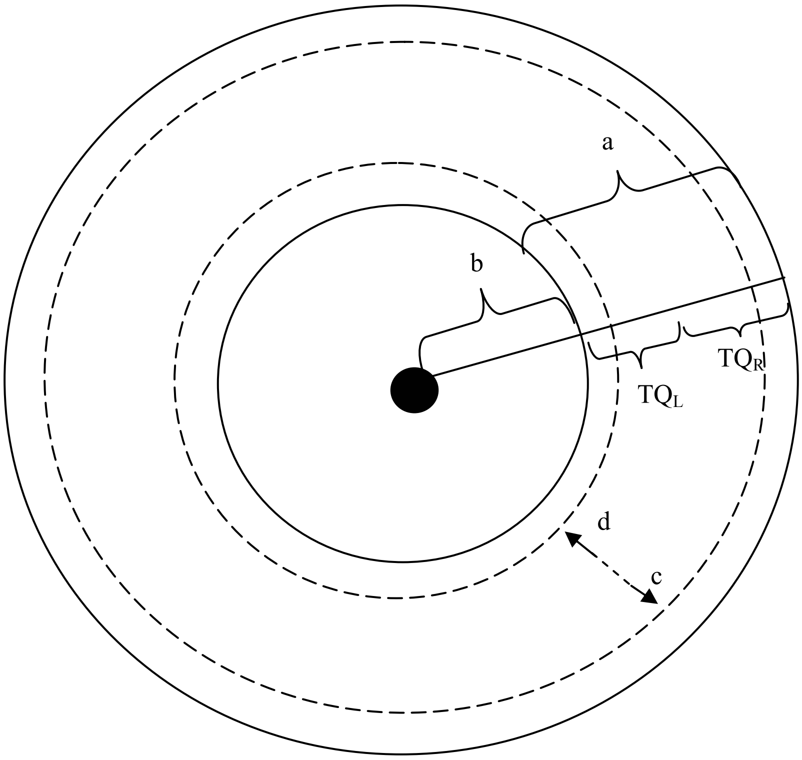
Table 4.1 Variable Correlation Parameters

4.3.6.2 Correlation Parameter Descriptions

Each of the variable correlation parameters is described below in terms of their use in automatic correlation algorithms, and their potential operational effect.

4.3.6.2.1 Correlation Window Parameters

The correlation window is a circle with radius based upon the positional accuracy's associated with the TQs of the two tracks (see Table 6-1a). (The radius is not based on the actual sum of the positional accuracies, but on the square root of the sum of squares, since TQ represents a variance.) The circle is centred on the track being checked against surrounding tracks. Tracks within the circle are eligible for correlation with the track being checked, subject to other tests. Correlation algorithms use the variable parameters a through d to compute the radius of this circle. Figure 4-3 depicts the correlation window and which portions of the radius are affected by the parameters a through d. When the default values for parameters a through d are specified, correlation algorithms compute correlation windows between 0.64 dm (for 2 tracks with TQ ≥ 10) and 4.64 dm (for 2 tracks with TQ ≤ 7) in radius. The purpose of each of these "window" parameters is described below.



TQ_L = Positional accuracy for TQ of local track represented by min TQ and max TQ.
TQ_R = Positional accuracy for TQ of remote track represented by min TQ and max TQ.

Figure 4-3. Effect of Variable Parameters on Correlation Window

4.3.6.2.1.1 Window Size Multiplier (a)

The correlation window can be loosened or tightened uniformly for all JUs in an interface by increasing or decreasing the window size multiplier. The window size multiplier stretches or reduces the entire window radius. This might be necessary if it is determined that there are many incorrect correlations (decrease (a)) or missed correlations (increase (a)) attributable to distances between the tracks.

4.3.6.2.1.2 Minimum Window Size (b)

Essentially an estimation added to the basic window calculated from TQs, to insure that windows are not so small as to prevent valid correlations. The default value insures a correlation window of at least a half-mile, even if the TQs of both tracks are very high.

4.3.6.2.1.3 Min TQ (c)

The minimum TQ to be used in positional correlation calculations. This prevents correlation windows from being unrealistically large. The positional accuracies associated with lower TQs are quite large. TQ = 6 reflects a potential track positional error of almost 6 miles, TQ = 2 almost 30 miles, and TQ = 1 greater than 30 miles to an indefinite distance. Allowing correlation of tracks in a correlation window that is too large would probably result in many incorrect correlations. (As "c" decreases the TQ positional error increases causing the radius of the correlation window to increase.) Therefore, the correlation algorithms treat TQs below a certain value as if they were at least the Min TQ. Experience may show that a Min TQ lower than the default value of 7 (positional accuracy approximately 3 miles) is desirable, if the default value results in many missed correlations of low quality tracks. Note: The value used for c can never be less than the value used for e.

4.3.6.2.1.4 Max TQ (d)

Similar to Min TQ, but prevents correlation windows from being unrealistically small because very high TQs are used. TQ = 11 reflects track positional accuracy of about 300 feet, TQ = 15 about 18 feet. Experience may show that a Max TQ higher than the default value of 10 (positional accuracy approximately 600 feet) is desirable, if the default value results in many incorrect correlations of high quality tracks. (As "d" increases the TQ positional error decreases causing the radius of the window to decrease, resulting in a smaller correlation window.)

4.3.6.2.1.5 Restricted TQ (e)

Tracks with TQ less than or equal to the Restricted TQ are not eligible for correlation, since their low TQ reflects a high degree of uncertainty about their position. Restricted TQ may require lowering if it appears that too many duals involving low TQ tracks are occurring. (As an exception, correlation of new local real-time tracks with any TQ is attempted before they are initially reported, since an incorrect correlation in this instance will not create a dual, and may keep false tracks off the interface.)

4.3.6.3 Kinematic Variable Parameters

Tracks within the correlation window are checked for matches of their course, speed, and altitude with the track being checked. The allowable kinematic differences for correlation between the two tracks are specified by parameters f, g, and h, described below:

4.3.6.3.1 Course Differential (f)

The maximum difference between the reported course of the remote track and the calculated course of the local track, see table 4-1. For surface tracks, if the speed of either track is less than 10 dmh, "course differential" is not applied in the correlation test, since course calculations for slow-moving tracks are subject to large errors.

4.3.6.3.2 Speed Differential (g)

The maximum percentage by which the speed of the faster track may differ from the speed of the slower track. Since the speed of new tracks is usually unreliable for a short period of time until tracking stabilises, this parameter is particularly important in detecting correlation of new, unreported tracks with existing reported tracks.

4.3.6.3.3 Altitude Differential (h)

The maximum altitude difference between two air tracks. This parameter is not applied to surface tracks, and is applied only if the Altitude Source of both air tracks is Sensor, Aircraft Automatic Altitude, or PPLI Report. If many duals appear to be occurring due to altitude differences, the TDC should ascertain if JUs with sensors that do not have accurate altitude finding capability are setting their Altitude Source to Sensor. If so, they should be directed to set Altitude Source to No Statement/Estimated. However, if many incorrect correlations or missed correlations occur for tracks which are both being reported by JUs with accurate 3-D sensors, this correlation parameter may require lowering (to prevent incorrect correlations), or increasing (to prevent missed correlations).

4.3.6.4 Min Q_{pg} (j) and Max Q_{pg} (k)

JU PPLI reports are also tested for correlation with track reports. In this case, the Geodetic Position Quality (Q_{pg}) is used for the JU instead of TQ. Min and Max Q_{pg} are equivalent to Min and Max TQ used in correlation tests of two tracks, and the guidance for their setting is similar. The default Min Q_{pg} = 2 has an associated positional accuracy of almost 4 data miles and the default Max Q_{pg} = 11 has an associated positional accuracy of about 500 feet. Correlation of JUs with Q_{pg} = 0 is not attempted, since this essentially states that the JU's Link 16 Terminal Navigation is not working properly and the PPLI position is considered unreliable. PUs and RUs are tested for correlation as if they were a track with TQ = 7.

4.3.6.5 ID and IFF/SIF Mode II Correlation Capabilities

Normally, two tracks which have conflicting IDs or different nonzero IFF/SIF Mode II codes are not correlated automatically. However, JUs have operator selectable capabilities to selectively remove either or both of these correlation restrictions if operational conditions dictate, e.g., IDs or Mode II codes are unreliable and incorrect IDs or Mode II codes are preventing valid correlations and creating duals. The use of these capabilities is to be controlled by the TDC, and is to apply to all JUs in the interface. They should also be promulgated in the OPTASK LINK/ REPORTING REQUIREMENTS section, including the initial OPTASK LINK if pre-planning indicates the need to use the capability from the start of operations. The default value of each of these capabilities is "on", i.e., the correlation restriction applies unless turned off by an operator.

4.3.7 <u>Automatic Decorrelation Considerations</u>

After two tracks have been correlated to form a single common track, they are then checked for decorrelation upon receipt of each remote track report. Similar to the variable correlation parameters, there are two variable decorrelation parameters that may also require adjustment for reasons similar to the correlation parameters. These are to be defined in the OPTASK LINK/REPORTING REQUIREMENTS section in the same manner as suggested for the variable correlation parameters. If the default values are to be used for all of the correlation and decorrelation parameters, then the single statement "USE DEFAULT CORRELATION AND DECORRELATION PARAMETERS" should be stated. The variable decorrelation parameters are:

4.3.7.1 Decorrelation Window Multiplier (m)

The amount by which the distance between the common and remote track is to exceed the applicable correlation window for the two tracks in order to be decorrelated. The default value is 1.5, e.g., if the correlation window for a common and remote track is 5 miles, the local and remote would decorrelate at 7.5 miles. The multiplier can be varied between 1.0 and 2.0 in increments of 0.1.

4.3.7.2 Consecutive Decorrelations (n)

The number of consecutive remote track reports which must meet the decorrelation criteria before the decorrelation is executed. The default value is 2, variable between 1 and 5 in increments of 1. Excessive incorrect decorrelations may indicate the need to use a higher value.

4.4 NETWORK INITIATION

4.4.1 General

Network Initiation is the process of preparing JUs for network operation. This includes:

a. Provision of crypto and initialisation data.

b. Terminal (platform) initialisation.

c. Start of network operation.

4.4.2 Initialisation Preparation

4.4.2.1 On receipt of an OPTASK LINK message, units are responsible for:

a. Preparation of designated crypto load.

b. Retrieval of nominated network design(s) (alternate network designs as required) from unit sub-libraries.

c. Input of relevant OPTASK LINK data and specification of mission specific data to produce a terminal initialisation load.

An Initialisation Data Preparation Facility (IDPF) may be provided at units for this purpose.

4.4.2.2 Equipment Checkouts and Set-Up

Equipment checkouts and set-up should be started in sufficient time for all checks to be completed before scheduled Link 16 operations. This process will include:

a. Preliminary checks on the data equipment, radios, computers and inter-connections.

b. Equipment checkouts by utilisation of the MIDS terminal's built-in test equipment. (Each system will use the individual checklist or procedure developed from appropriate handbooks of operation and maintenance instructions).

4.4.3 Platform Initialisation

4.4.3.1 The process of Platform Initialisation is a decentralised one, conducted at operational units either acting as JUs or responsible for JUs (e.g. aircraft carriers, airfields). JUs participating in a Link 16 network should be initialised with the necessary initialisation data prior to attempting network entry. Initialisation data is loaded into the terminal to:

a. Define the platform characteristics of the JU.

b. Establish the network role of the JU.

c. Provide network capacity to satisfy the communications requirements of the JU.

4.4.3.2 The Network Manager should be informed of any problems encountered during the initialisation process, enabling him to implement contingencies and appoint standbys as required.

4.4.3.3 Loading of Cryptovariables

4.4.3.3.1 Cryptovariables should be loaded under the direction of the local crypto custodian directly into the SDU of the terminal, separately from the initialisation data. However, close coordination is required between the initialisation organisation and the local crypto custodian to ensure that the cryptovariables loaded into each JU correspond exactly with the parameter set used to initialise the terminal. Incorrect loading of cryptovariables precludes any communication with the network.

4.4.3.3.2 It is the responsibility of the local crypto custodian to direct the loading of:

a. Appropriate cryptovariables in the correct SDU locations as instructed, in the platforms specified by the local initialisation organisation.

b. The correct unique variable for each platform into the designated SDU memory location if OTAR is to be implemented.

Further guidelines on cryptovariable loading are to be found in Volume 2.

4.4.3.4. Loading of Initialisation Data

4.4.3.4.1 Initialisation data includes the following:

a. Parameters defined for the chosen network design.

b. Parameters defined in the OPTASK LINK.

c. Platform-unique parameters.

d. Mission-dependent parameters.

Any changes to parameters identified at (a) and (b) above must be coordinated with the Network Manager.

4.4.3.4.2 Operational units are responsible for the provision of an adequate initialisation capability at associated Forward Operating Bases (FOBs) and detached units as required.

4.4.3.4.3 Initialisation data should be loaded into each JU, according to established operating procedures for each platform type. However, the following guidelines apply:

a. All host platforms must be initialised with the correct CPD prior to joining a network to ensure correct utilisation of cryptovariables:

(1) For host platforms that cannot manually specify the current CPD, initialisation data must be loaded into the terminal during the cryptoperiod for which it was prepared. The terminal will then automatically perform rollover at the end of the cryptoperiod and continue to maintain the correct value of current CPD. Failure to initialise the terminal during the correct cryptoperiod will invalidate the current CPD in the initialisation data.

(2) For host platforms that can manually specify the current CPD, it is permissible to delay loading of initialisation data until the next cryptoperiod. However, in such cases, the operator must amend the value of the current CPD (either 0 or 1) held within the terminal prior to joining the network.

b. Initialisation must take place with the terminal switched to “On” mode. Initialisation data will be retained indefinitely while the terminal is in the “On” mode or for a period of up to 48 hours while in the "standby" mode. The terminal will automatically roll over cryptovariables at the end of the designated cryptoperiod.

c. A terminal which has been powered down must be fully reloaded with its initialisation data and cryptovariables. All parameters, in particular the CPD, should be checked to ensure that they are still in effect.

4.4.4 Network Entry

4.4.4.1 Normal Network Entry

Network Entry will be conducted in accordance with the appropriate OPTASK LINK. After successful initialisation, some systems may require the operator to input a "Start Net Entry" command to initiate the synchronisation process for network entry.

4.4.4.2 Network Entry Without Initialisation

4.4.4.2.1 Where initialisation data is available, JUs should be fully initialised before attempting network entry. This will ensure communication with the desired net(s) and reduce the use of available network capacity for requesting and receiving time slot allocations. However, if problems occur during the loading process, the operator should take action to terminate initialisation and commence emergency network entry, as detailed in paragraph 5.2.5.

4.4.4.2.2 A MIDS terminal holds default values of a subset of initialisation parameters which are automatically loaded in the absence of externally loaded data. Automatic loading of default values allow a JU initialised with the appropriate cryptovariables and current CPD to enter the network and receive messages on the default net. Transmission capacity may then be obtained for those PGs in which the JU is required to participate, as detailed in paragraph 5.2.5.

4.5 NETWORK OPERATION

4.5.1 General

4.5.1.1 The Network Manager is responsible for monitoring and evaluating the performance of the network and has the authority to implement changes to the network in response to:

a. Changing operational requirements

b. Requests from participating JUs, either by voice, Link 16 message or other means.

c. Requirements for the transfer of vital network duties.

d. Communications overload situations leading to degradation of network performance.

e. Planned and unexpected departure/arrival of JUs.

4.5.1.2 During Network Operation, the Network Manager monitors the network operation and makes adjustments to the network to meet changing operational requirements.

4.5.2 Network Monitoring

The Network Manager must monitor the network during operation to ensure that operational requirements continue to be met. Network Monitoring provides the necessary information for modifying the network. Network Monitoring encompasses:

a. Monitoring of the connectivity among JUs.

b. Monitoring of the network load.

c. Monitoring for potential security compromise situations.

d. Analysis of JU requests and platform status reports.

e. Network performance evaluation.

4.5.3 Network Modifying

Network designs should be developed with sufficient flexibility and utility to support operations without the need for modifying an active network. However, if modifications of an existing network structure are required, these may encompass many activities including: the reallocation of network duties and functions: the allocation of unused time slots: changes to the initial allocation of time slots: the reconfiguration of relays and Over The Air Rekeying (OTAR) of cryptovariables. Changes made to a network structure during operation must be authorised by the Tactical Commander through the delegation of OPNET Management functions. Delegated authority may be granted as Full or Limited. These can be defined as follows:

a. Full OPNET Management - The capability to modify an active network by any means, when authorised.

b. Limited OPNET Management - The capability to perform specified modifications to an active network by any means.

4.6 NETWORK ANALYSIS

Network Analysis is the off-line post operations evaluation of previous operations with the aim of modifying or changing future network designs to improve network operations.

CHAPTER 5

COMMUNICATION PROCEDURES

5.1 GENERAL

5.1.1 Data and Voice Communications

Link 16 networks support both data and voice communications. Data exchange is governed by Link 16 data link protocols. Effective use of voice communication relies on operator adherence to established and standardised voice procedures.

5.1.2 Voice Coordination

Data exchange on Link 16 networks should always be supported by a voice capability for coordination purposes. This requirement may be partly fulfilled by the MIDS voice facility but a non-MIDS voice capability should always be available to provide operational flexibility. For information management purposes, the primary method of conflict resolution should be via automatic data exchange. Conflict resolution by voice will only be required between systems with limited capabilities and in cases where automatic procedures fail to achieve a solution. In such cases the operator will be alerted.

5.1.2.1 A voice coordination net (or nets) should be established to support the following:

a. Interface Coordination - to coordinate the employment of certain tactical weapons and for interface command and control coordination.

b. Track Coordination - to control and coordinate procedures used by track surveillance personnel to maintain clear tactical pictures. In the event of TDS automated display malfunctions, this net could be used to coordinate manual track cross tell, handovers and commands.

c. Data Link Coordination - to coordinate the technical operation of data terminal and communications equipment and to enable final coordination of pre-arranged technical data prior to initiation of MIDS operations. This could also include JU-JU coordination if technical problems exist during initialisation, Synchronisation or operation.

5.1.2.2 When voice reports are necessary, agreed 'standard' voice reporting procedures must be used (see Note below). Where voice reports cannot be covered by such standard procedures, or where possible ambiguity may occur, NATO Link Management Codes applicable to Link 16 (as detailed in Annex D) should be used.

Note: NATO Standard Voice Reporting Procedures are contained in the following publications; Navy APP1, Air APP1 or equivalent (i.e. Pub 32/34/35001, Annex C).

5.1.3 Exchange of Alphanumeric Text

5.1.3.1 JU operators may elect to exchange alphanumeric text information either by the Link 16 Text message or by utilising the MIDS Free Text message format facility.

5.1.3.2 Link 16 Text Message

5.1.3.2.1 Link 16 provides the capability to exchange alphanumeric text information by the transmission of Text (J28.2(0)) messages (known to some operators as free text messages). This enables implementing JUs to exchange text information, e.g. in support of mission planning and execution. When required, Text messages may be compiled by the operator. In addition, in order to reduce operator workload, frequently exchanged information may be loaded in a pre-scripted form at platform initialisation.

5.1.3.2.2 The text character set comprises the letters A-Z, numbers 0-9 and other standard characters. The maximum length of a Text message depends on the packing level employed, namely 5,760 characters at Standard Packing and I3,680 characters at Packed-2. However, operators should note that some nonC^2 JUs, particularly fighters, are restricted in the length of Text message that can be received and displayed, and messages exceeding a system's maximum capability could be truncated at the maximum limit or discarded. Reference should be made to the National Supplements in Volume 3 for details of platform restrictions/variations in Link 16 Text message usage.

5.1.3.3 MIDS Free Text Message Format

5.1.3.3.1 In addition to fixed format messages (i.e. the J-series message catalogue). MIDS terminals also provide the capability to exchange data not in a predetermined format (e.g. alphanumeric text. teletype and digitised voice) using the MIDS free text message format (known to some operators as one line free text messages). Operators should note that, unlike fixed format messages, this capability is retained even when operating in Conditional Radio Silence mode.

5.2 JOINING A NETWORK

5.2.1 Network Start-Up

The MIDS terminal which has been initialised as NTR must be the first JU to transmit on the network. At the designated time (as directed in the OPTASK LINK), the NTR must switch on the terminal and enter network time (Z time or local time as appropriate). The terminal automatically sets time quality to 15 and initiates transmission of the Initial Entry message at set intervals in given time slots, thus establishing network time.

5.2.2 Network Entry by Subsequent JUs

5.2.2.1 Once the NTR has commenced transmission, other JUs, which have been fully initialised with network parameters and cryptovariables, may enter the network. The Network Manager may determine the order of network entry of C^2 JUs to facilitate the initiation of surveillance reporting (see paragraph 6.2.3). Each terminal should be initialised with network time and an estimated time error. Operational experience will provide "rules of thumb" for the degree of time error to be entered. JUs initialised as Secondary Users must also enter an estimate of initial position and position quality.

5.2.2.2 Initial Entry JUs (IEJUs)

JUs other than the NTR, which have been initialised to transmit the Initial Entry (J0.0) message will automatically commence transmissions of this message upon achieving fine synchronisation. IEJUs which are in LOS with the NTR will synchronise with the NTR and then begin transmitting the Initial Entry message. IEJUs not in LOS with the NTR will synchronise with those IEJUs which have already achieved synchronisation, thus maintaining one network time.

5.2.3 Synchronisation

5.2.3.1 On activation, the terminal automatically initiates the synchronisation process, which is achieved in two stages:

a. Coarse synchronisation - is achieved by successfully receiving an Initial Entry message.

b. Fine synchronisation - is achieved by either active or passive means according to terminal initialisation.

Once coarse synchronisation has been achieved, a JU may receive all Link 16 messages. However, a JU may only transmit messages and participate fully in the network when in fine synchronisation with network time.

5.2.3.2 Failure to Achieve Synchronisation

Assuming full equipment serviceability, a MIDS terminal may fail to achieve synchronisation with network time for either of the following reasons:

a. Loading of incorrect initialisation data and/or incorrect cryptovariables. The terminal must be reinitialised.

b. JU is beyond LOS of the NTR or an IEJU.

If a JU fails to achieve synchronisation, the operator should contact the Network Manager to seek assistance. The Network Manager should attempt to improve connectivity within the network to ensure that every JU can receive an Initial Entry message.

5.2.4 Network Entry by Non-Initialised JUs

JUs which have no initialisation data, but have access to the Initial Entry TRANSEC cryptovariable, may wish to enter the network. Where this requirement is known in advance, the following procedure should be used:

a. The operator should contact the Network Manager in advance to request permission to enter the network. He should state:

(1) Identity.

(2) Reason for entry.

(3) Time/date of entry.

(4) Anticipated duration of network participation.

(5) Network capacity requirements.

b. The Network Manager should determine the impact on network operations and allocate network capacity, according to availability and network loading, to meet the JU's requirements.

c. The Network Manager should signal the JU (or initialisation facility responsible for the JU) with the appropriate OPTASK LINK, to provide required initialisation data and an effective date/time for network entry.

d. At the required time, the JU should proceed with the normal network entry procedure.

5.2.5 Emergency Network Entry

Where there is no time for advance planning or if initialisation data fails, non-initialised JUs may simply enter the network on the default net, providing the Initial Entry TRANSEC cryptovariable is stored in the terminal's SDU. JUs utilising the Emergency Network Entry procedure will have the following capabilities:

a. Message reception on the default net.

b. Limited transmission capability by obtaining time slot assignments from the Initial Entry message for the following PGs:

(1) PPLI.

(2) RTT-B.

(3) Voice.

(4) Control.

The operator should contact the Network Manager and use voice to state the problem and request full transmission capability for other established PGs. Use of the Initial Entry message to obtain time slots as detailed in (b) above may be inhibited by peacetime operating restrictions (refer to Volume 3). However, when available, its use will reduce the loading on the Network Manager to process requests and reallocate time slots for required PGs.

5.2.6 MIDS Voice Only Participation

JUs, intending to participate in a network for MIDS voice communications only, must join the network initialised to operate in Conditional Radio Silence mode. In this mode, all fixed format data messages are automatically inhibited from transmission, but the MIDS voice and alphanumeric free text capabilities are retained.

5.3 NETWORK OPERATION

5.3.1 Network Monitoring

The Network Manager should utilise whatever aids are available to assist him in monitoring the effectiveness of the current network. The purpose of network monitoring is to ensure that:

a. The network meets operational requirements by employing the most effective allocation of available resources among participating JUs, meeting the communications requirement for different PGs and meeting the connectivity requirements of platforms.

b. Peacetime operation of the network does not contravene established peacetime operating restrictions in the area of operations (see Volum 3 for details).

5.3.1.2 The Network Manager will receive information from participating units, which will help him perform the Network Management function. This information is transmitted via Link 16 messages (e.g. Network Management, Platform & System Status and OTAR messages). MIDS or non-MIDS voice and/or other means.

5.3.2 Network Participation Status

5.3.2.1 The Network Manager must be aware of the network participation status of all JUs on the network to enable him to manage fully the resources available to him. The three levels of network participation status that exist are:

a. Active - Full capability to transmit and receive messages in accordance with time slot allocation. JUs must be operating in the Normal transmit mode and be in a state of fine synchronisation.

b. Limited - Restrictions are imposed on the transmission of messages according to the reason for change to limited status. Details are provided in Figure 5-1.

c. Inactive - Operator selectable to either the "off" or "standby" states. JUs cannot exchange data or voice and cannot act as relay.

5.3.2.2 Impact of Network Participation Status Changes

5.3.2.2.1 When a JU undergoes a change in network participation status, the network is affected to a certain degree, depending on the functions performed by that JU. Such changes, other than a change to Inactive status, are automatically reported in the PPLI message. The Network Manager should assess the impact on the network and reassign critical network functions and time slot capacity as required.

5.3.2.2.2 Conditional Radio Silent and Polling modes are operator selectable and will produce a change to limited status. Polling Mode should only be selected when a JU is directed to participate in a polling community.

LIMITED STATUS	CONDITION	TRANSMIT CAPABILITY	RECEIVE CAPABILITY	VOICE CAPABILITY	RELAY CAPABILITY	IMPACT ON NETWORK
CONDITIONAL RADIO SILENT	Operator Selectable	No	Yes	Yes	No	No further data transmissions from the JU
HIGH MESSAGE ERROR RATE	Errors detected on received messages >10%	Yes	Yes	Yes	Yes	Quality of data exchange on the network could become degraded
NO INITIAL ENTRY MESSAGE RECEIVED	Not received within a 120 sec period	Yes	Yes	Yes	Yes	Affected JU cannot respond to changes in network time. New JUs may not be able to join the network.
TDS FAILURE	Terminal cannot communicate with host	No host-generated message or acknowledgements can be transmitted	Terminal responds with CANTPRO to all messages addressed to the host	Yes	Yes	No data exchange possible between the MIDS terminal and the host. Normal functions not affected but PPLI data may be inaccurate
POLLING	Operator Selectable	Only when polled	Yes	Yes	No	JU will only participate in a PG when Polled

Figure 5-1 Restrictions and Implications of Change to Limited Status

5.3.2.2.3 JUs wishing to cease data transmissions but continue participation in MIDS voice communications only must manually switch to Conditional Radio Silence mode. The capabilities retained are as in Figure 5-1 above.

5.3.2.3 Resumption of Active Status

5.3.2.3.1 Returning to Active status from Conditional Radio Silent or Polling modes is an operator action. A limited status of "High Error Rate", "No Initial Entry Message Received" or "TDS Failure" will automatically revert to Active status upon resolution of the problem.

5.3.2.3.2 JUs may resume Active status from an Inactive status by following the procedure for network entry. JUs which have not retained their time slot allocation, must contact the Network Manager to request a new allocation.

5.3.2.3.3 After initially achieving Active status, or after returning to Active status from Inactive status or TDS failure, C^2 JUs capable of assuming R^2 for air, surface, space or land tracks must also adhere to paragraph 6.2.3.

5.3.3 Monitoring of Cryptovariables

The Cryptonet Manager is responsible for maintaining the desired crypto connectivity among participating JUs and must ensure that the required levels of communications security are maintained within established COMSEC guidelines.

5.3.4 Network Modifying

5.3.4.1 Based on the results of his monitoring of the situation, the Network Manager can order changes to the network by voice or electronic means. These actions can be:

a. Reassignment of network roles and duties.

b. Allocation (and reallocation) of unused time slots to a requesting unit. This allocation concerns blocks of time slots that are built into the network design but are not assigned to an active unit in the network, and does not impact the original network structure.

c. Ordering a switch from one initialised network to another initialised network. The Network Manager must ensure that all the participants hold the alternate set of initialisation parameters. Therefore, this action can only be taken if planned at the Pre-mission Planning stage.

d. Recommending movement of one or more JUs to the Tactical Commander.

e. Reallocation of time slot block assignments.

f. The adjustment of connectivity among JUs by enabling/disabling platforms as relays as required.

g. OTAR of cryptovariables.

5.3.4.2 Under conditions of data overload, individual JUs should consider applying data filters by coordinating with the appropriate authority, to reduce traffic load within functional areas on the network, before contacting the Network Manager to request additional time slots. Procedures for data filtering are to he found in paragraph 6.2.5.7. When filtering is insufficient or undesirable, additional transmission capacity may be required. The JU should contact the Network Manager by voice, Link 16 message or other means to request additional time slot assignments for the required functions, if known. Similarly, a JU should inform the Network Manager if the requirement for transmission capacity is less than that provided, thus releasing unused time slots for reallocation.

5.3.4.3 Network Management messages are available to assist the Network Manager in modifying the network and are dealt with in Volume 2. However, the aim should be to minimise the extent of modification necessary as it introduces a degree of vulnerability into the network structure and uses up available network capacity.

5.3.5 Repromulgation Relay

5.3.5.1 JUs will normally be initialised to conduct relay automatically, according to the connectivity requirements of the network in force. However, there is a second method of relay, known as Repromulgation Relay, which can be operator originated, providing the terminal has been appropriately set at initialisation and depending on platform implementation.

5.3.5.2 The operator may initiate Repromulgation Relay to improve connectivity on a message-by-message basis, specifying the number of relay hops required. No Network Manager intervention is necessary. However, Repromulgation Relay more than doubles the demand for use of the originator's time slots. Therefore the Network Manager may need to assign additional time slots or the originating JU may experience immediate indications of transmission capacity overload. JUs should, therefore, inform the Network Manager whenever Repromulgation Relay is to be operated, to enable him to manage overall network connectivity.

5.3.6 Degraded Communications

Although MIDS has good anti-jam characteristics, when operating in extreme ECM environments, degradation of communications may be experienced. In such a situation, the Network Manager should:

a. Identify network priorities for information exchange, based on PGs and network participants.

b. Attempt to improve connectivity within those areas of priority by:

(1) Increasing network transmission power.

(2) Decreasing packing limits where applicable, to increase ECM resistance capability. Generally it will not be possible to change packing limits for nonC^{2}JUs already operating in the network because of operator workload.

(3) Redefining relay strategy employed.

Individual JUs may be instructed to take whatever measures are available to improve own platform transmission capability within a degraded communications environment.

5.3.7 Modifying Cryptovariables

5.3.7.1 Cryptovariables are loaded at initialisation to produce the crypto connectivity as defined in the chosen network plan. Cryptovariables are then changed:

a. Periodically, according to the cryptoperiod defined.

b. In response to compromise.

c. To meet changing operational requirements.

Any cryptovariable change must be coordinated and controlled by the Network Manager, to ensure that the desired crypto connectivity among participating JUs is maintained. Further details on Cryptonet Management are to be found in Volume 2.

5.3.7.2 Security Compromise

Loss or exposure of cryptovariables during distribution or use constitutes a security compromise. Any JU which has evidence of security compromise, or suspects that a compromise has taken place, should contact the Cryptonet Manager or Network Manager immediately by non-MIDS voice. The Cryptonet Manager should attempt to isolate any JU suspected of compromise by changing the cryptovariables for all other JUs participating on that cryptonet.

5.3.7.3 Over The Air Rekeying (OTAR) of Cryptovariables

5.3.7.3.1 Capabilities

Modifying cryptovariables in a Link 16 network may be achieved by utilising the capability to rekey cryptovariables over the air, depending on platform implementation. OTAR allows the Network Manager to:

a. Provide a new cryptovariable to be stored in a specific location in the SDU and specify the cryptoperiod in which it is to be used.

b. Alter connectivity within cryptonets:

(1) For operational reasons.

(2) In response to compromise.

c. Request a Cryptovariable Status Update from individual JUs.

d. Receive Cryptovariable Status Reports from individual JUs.

Individual JUs may request new cryptovariables for their own use and for the use of JUs under their control.

5.3.7.3.2 Unique Variables

The OTAR function incorporates an extra level of encryption through the use of a second set of cryptovariables known as unique variables. Each JU is assigned a unique variable, held only by that JU and the authorised rekeying facility, which prevents any terminal other than the intended recipient from deciphering the message. When rekeying a group of JUs, a separate message must be transmitted to each JU, using the appropriate unique variable.

5.3.7.3.3 Cryptovariable Request

JUs may request new cryptovariables from the Network Manager. These requests may be originated as follows:

a. By any JU directly to the Network Manager.

b. By a controlled nonC^2 JU determining that it requires a new cryptovariable and requesting its controlling C^2 JU to transmit an Indirect Rekey Request to the Network Manager.

c. By the controlling C^2 JU determining that a JU under its control requires a new cryptovariable and transmitting an Indirect Rekey Request on behalf of the controlled JU.

The Network Manager, in coordination with the Cryptonet Manager, should determine the impact on network connectivity and respond accordingly.

5.3.8 JU Requests

Individual JUs may request network management actions either by secure voice or Link 16 message. Where such requests are made by message, each request should be addressed to the JU address of the unit acting as Network Manager or to the unique Network Manager Address of 77777 (octal).

5.4 LEAVING A NETWORK

5.4.1 Normal Exit

The following procedure should be used to coordinate the exit of JUs wishing to leave the network:

a. A JU wishing to leave a Link 16 network should contact the Network Manager in advance stating:

   (1) Reason for departure.

   (2) Time/date of departure.

   (3) Anticipated duration of non-participation.

   (4) Network functions currently assigned (NTR, NC etc).

   (5) Desire to retain/release assigned network capacity.

b. The Network Manager should inform the JU whether transmission capacity is to be retained.

c. At the designated time of leaving, the JU should cease all Link 16 transmissions.

d. MIDS terminals should be powered down on completion of network participation by a JU or completion of a mission by airborne JUs. The action of switching the terminal to the "Off" state will destroy all initialisation data and cryptovariables.

Controlling C^2 JUs should coordinate with the Network Manager the entry and exit of nonC^2 JUs under their control. This should reduce the number of direct demands made on the Network Manager.

5.4.2 Exit of NTR

If the leaving JU is the current NTR, the exchange of responsibility must be carefully managed to ensure that only one system time is defined at any one time. The change should be coordinated by voice. The replacement NTR must be a member of the network to ensure continuity of network operation. On confirmation that the NTR has ceased all transmission, the Network Manager should instruct the replacement NTR to initialise his terminal accordingly and begin to transmit the Initial Entry message. Selection of the NTR parameter is made by operator action.

5.4.3 Unscheduled Network Exit

If the Network Manager detects that PPLI messages are no longer being received for a particular JU, he should:

a. Attempt to contact the JU to determine:

(1) Reason for departure.

(2) Anticipated duration of non-participation.

b. Determine the operational impact of the loss of the JU on the network and reassign functions to other suitable JUs as required.

c. If the JU is NTR, inform the designated standby to set the required parameter to NTR and assume responsibility with immediate effect. If possible, contact the original JU with instructions to disable his NTR initialisation.

d. Inform all JUs of the departure and instruct those JUs required to assume new network functions to do so with immediate effect.

5.4.4 Temporary Absence from the Network

5.4.4.1 Where a JU is temporarily required to leave the network, such as for refuelling and/or re-arming, the Network Manager may allow a JU to retain his original time slot assignments. The terminal should be set to Standby mode, to retain cryptovariables and initialisation data for the period of absence from the network.

5.4.4.2 If transmission capacity is released for reallocation, the terminal must be reinitialised with a new set of time slot assignment blocks. Wherever possible, this should be done before rejoining the network to reduce the demand for time slot reallocation over the air.

5.5 AUTONOMOUS OPERATIONS

NonC^2 JUs, such as a fighter group, may continue to exchange Link 16 messages when beyond LOS of other network participants. A Flight Leader may undertake limited command and control responsibilities for the fighter group during such autonomous operations. However, no member of the group should be appointed to operate as NTR during autonomous operations, because of potential disruption to the main network when LOS communications are re-established. JUs should continue to exchange data until fine synchronisation is lost and data can no longer be exchanged. In this case, nonC^2 JUs may either:

a. Continue data exchange by non-MIDS voice.

b. Transit to within LOS of a JU transmitting the Initial Entry Message, re-synchronise with network time and continue autonomous operations as before.

5.6 TERMINATION OF A NETWORK

In order to terminate the network:

a. The Network Manager should inform all participating JUs of the expected time of network termination.

b. At the designated time, all JUs are instructed to cease all transmissions.

CHAPTER 6

DATA EXCHANGE PROCEDURES

6.1 GENERAL

Link 16 provides a capability for exchanging tactical data in support of Surveillance, Weapons Coordination and Management and Air Control; each is dealt with in a subsequent section of this chapter. A number of procedures, such as use of Pointers and Data Update Requests, are common to more than one of these functional areas and are dealt with in each of the relevant sections. Link 16 messages are in Annex B; a list of IJMS messages is at Appendix 1 to Annex B.

6.1.1 Track Data Coordinator

The duty of Track Data Coordinator (TDC) is similar to that known as Force Track Coordinator (FTC) in Link 11 operations, but encompasses additional responsibilities. A TDC will be designated for the Link 16 interface. The ability of the TDC to effectively coordinate the efforts of all IUs to maintain a clear tactical picture depends on the information that is directly available to him on a real-time basis. The value of the database information depends on its quantity, quality and timeliness. Therefore, the individual designated as the TDC should have direct access to the maximum number of active tracks and reliable voice net communications with the maximum number of IUs. The TDC should have voice communications with Track Supervisors in all IUs. The TDC has overall responsibility to:

a. Assist in preparation of the OPTASK LINK (see paragraph 4.3.5).

b. Manage the exchange of track data and related actions to ensure clarity of the tactical picture.

c. Supervise the resolution of interface anomalies such as dual designations, duplicate tracks, false tracks, runaway tracks, and identification and category conflicts.

d. Transmit Change Data Orders to resolve Category and Identity conflicts when required.

e. Coordinate changes in areas of responsibility for surveillance as the tactical situation requires.

f. Coordinate and authorise the use of data filters.

g. Designate the EW Data Forwarding mode (see paragraph 7.2.4.2).

The TDC responsibilities do not replace individual IU responsibilities in these areas.

Note: Not all C^2 IUs have the capability to undertake full FTC/TDC responsibilities, as described above. Such units are not to be assigned FTC/TDC duties. Refer to national annexes for details of individual TDL system capabilities and limitations.

6.2 SURVEILLANCE

6.2.1 General

6.2.1.1 Types of Surveillance Report

Surveillance information derived from a number of sources, including data forwarded from other tactical data links (Chapter 7 for Data Forwarding procedures), is compiled by C^2 JUs and exchanged in the form of:

a. Air, surface (maritime), subsurface (maritime) tracks and land (ground) tracks/points and space tracks (J3-series messages).

b. ASW Acoustic Reports (J5.4).

c. EW information, comprising EW contacts and EW products (J3.7).

d. PPLI reports (J2-series) received from all active JUs, providing regular updates on position, identity and network participation status.

e. Emergency Points (J3.1) and Reference Points/Lines/Areas (J3.0) to define tactically significant areas, such as hazard areas, missile engagement zones (MEZs), Hostile Weapon Zones (HWZs) and safe corridors.

f. Intelligence data (J6.0).

g. Threat warning data (J15.0).

6.2.1.2 NonC^2 JU Participation in Surveillance

6.2.1.2.1 NonC^2 JUs do not report tracks directly on to the surveillance net, but may report sensor target data to their controlling C^2 JU on the designated control net. The controlling C^2 JU will compare data received with tracks being reported on the surveillance net and either:

a. Correlate the sensor target data with the appropriate surveillance track if the track already exists on the interface, or

b. Initiate a new Surveillance Track Report on the surveillance net based on the data reported by the nonC^2 JU.

The reporting of target data by nonC^2 JUs is covered more fully in paragraph 6.4.4.

6.2.1.2.2 Subject to system implementation, nonC^2 JUs may receive data directly from the surveillance net. In addition, the facility is provided for C^2 JUs to transmit high interest tracks to non- C^2 JUs under their control on the designated control net.

Error Sources	Cause of Error	Comment	Corrective Action
Geodetic Position	Inability to locate own unit's position relative to an earth model (normally WGS-84).	Error in geodetic longitude. Error in geodetic latitude. Error in altitude.	Active participants in RELNAV. Terminal will provide adjustments to host platform in latitude, longitude and altitude.
Sensor (Alignment and Calibration)	Bias errors in the JU sensor's azimuth orientation, vertical orientation (normal to tangent plane at geodetic position), and ranging measurements.	Error in sensor azimuth. Error in sensor elevation. Error in sensor range. NOTE: Errors in the north seeking device are included in the sensor azimuth error.	Periodic adjustment of sensor registration to compensate for sensor alignment differences. Results will be displayed for operator appreciation.
Data Processing	a. Coordinate systems. b. Transformations and conversions. c. Basic algorithms utilised. d. Track report extrapolation.	These errors are related to considerations such as type of digital filter used, tracking algorithms implemented, accuracy of transformation equations, and consideration of track positional-time relationship.	JUs must ensure that all track positions are extrapolated when local/remote correlation/decorrelation is performed.
Remote Units	Residual errors that are associated with remote units.	Performed on individual remote units which correction factors calculated in terms of mean translation and mean rotational parameters. These factors are applied to positional data received from each individual remote unit.	Periodically monitor data registration relative to a selected JU and make periodic adjustments. Results will be displayed for operator appreciation.

Table 6.1. Summary of Data Registration Error Sources

6.2.2 Protocols for Surveillance Data Exchange

The exchange of surveillance data on the interface requires the following protocols to be adopted by all participating C^2 JUs:

a. Data Registration - is fundamental to the operation of the interface, particularly for track correlation, and is dealt with in paragraph 6.2.2.1.

b. Track Numbers (TNs) - use of TNs on the interface is covered in paragraph 6.2.2.2.

c. Track Quality (TQ) - is used to report the positional reliability of a track and is discussed in paragraph 6.2.2.3.

d. Reporting Responsibility (R^2) - R^2 rules are covered in paragraph 6.2.2.4.

e. Track Correlation - is necessary to resolve dual designations (see paragraph 6.2.5.4.2). Track correlation and procedures for the resolution of dual designations are covered in paragraph 6.2.5.4.

f. Track Decorrelation - is also covered in paragraph 6.2.5.4. Failure to perform decorrelation may result in duplicate track numbers; procedures are contained in paragraph 6.2.5.4.3.

g. Minimum Wait Time - is also covered in paragraph 6.2.3. Failure to wait prior to transmitting surveillance tracks can result in severe degradation of the overall surveillance picture.

6.2.2.1 Data Registration

6.2.2.1.1 Data registration is a condition of correct relative alignment between local and remote track positional data. It involves measuring and adjusting positional data. Optimum interface data registration occurs when all C^2 JUs hold their locally derived track positional data at the same geodetic position as the remote positional data for the same tracks. Poor data registration will degrade a system's ability to correctly correlate local tracks with remote tracks.

6.2.2.1.2 Errors Affecting Data Registration

The errors that affect data registration are:

a. Local unit errors in:

(1) Geodetic position.

(2) Sensors.

(3) Data processing.

b. Remote unit errors.

6.2.2.1.3 Magnitude of Errors

The magnitude of the errors will vary according to the characteristics and configuration of each JU. For example, a stationary JU that has been accurately surveyed has fewer potential errors in the geodetic position than a moving JU with limited navigational capability.

6.2.2.2 Track Numbers

6.2.2.2.1 A Track Number (TN) is used to provide a common reference number for information and directives exchanged within the interface. The reference numbers are used for both digital and voice communications to identify all IUs and the subjects of tactical information reports, e.g. tracks, strobes, LOBs and points/lines/areas, exchanged on the interface. When applied to an IU, such a number is termed an address.

6.2.2.2.2 Track Number Composition

Link 16 TNs are composed of five numeric or alphanumeric characters in the format AAXXX, where A represents a value in the range 0 through 7 and A through Z, less I and O, and X represents a purely numeric value in the range 0 through 7. Table 6.2 indicates the sequence and use of the numeric and alphanumeric TN blocks. Certain numeric TNs are reserved for specific uses, as shown in Table 6.2, and are not available for assignment.

6.2.2.2.3 Unit Address Assignments

The Network Manager will assign each IU a specific TN as its address and promulgate the assignments in the OPTASK LINK prior to initiation of network operations. No two units may be assigned the same address in a network. Link 16/IJMS has the capability to utilise unit addresses up to 77777. Link 11/11B is limited to unit addresses less than 176. When non-addressed messages are forwarded from Link 16/IJMS to Link 11/11B for C^2 JUs having an address between 00200 and 77777, the data forwarder attributes all of the data to a pseudo data source address of 176. Commands or other addressed messages will not be forwarded to Link 11/11B from Link 16/IJMS units having addresses greater than or equal to 00200. Addresses should not be allocated from within a block or blocks which are allocated for use as surveillance TNs, to minimise the occurrence of duplicate TNs. The Network Manager may also assign TNs in the ranges 00001 to 00076 and 00100 to 00175 as Group Identifier Addresses, to be initialised as a Secondary Address by a designated group of JUs. TNs assigned for this purpose cannot also be allocated as an address to a specific JU, but a JU may be assigned up to 16 TNs as Secondary Addresses as well as a separate specific TN as its Primary Address. Group Identifier Address TN assignments will be promulgated in the OPTASK LINK message.

6.2.2.2.4 Track Number Assignments

Block(s) of contiguous TNs will be allocated to each unit that has a requirement to report tracks, points/lines/areas or LOBs and these assignments are also promulgated in the OPTASK LINK. C^2 JUs are capable of accepting a minimum of two separate noncontiguous blocks of TNs, including a low TN block (00200 – 07776) and a high TN block (10000 –

77776 and all alphanumerics). TNs should be allocated to individual units in blocks which are entirely numeric or alphanumeric, but not a mixture of the two types. A system may subdivide its block for allocation to subordinate units. Each unit should be allocated a larger number of TNs than its local track capacity (or, where this is not practical, expected reporting load) to provide the capability to report tracks when some of its assigned TNs are being used by other units as a result of shifts in reporting responsibility.

6.2.2.2.5 Management of TNs on a Multi-link Interface

Special procedures are required to manage the assignment and use of track numbers on a multi-link interface, because of the different track numbering schemes in use for different data links. Details are contained in paragraph 7.1.4.

6.2.2.3 Track Quality

6.2.2.3.1 The positional reliability of air, surface and land real time tracks is reported by its track quality (TQ) which is a numerical value from 1 to 15 (value from 1-7 for IJMS) with the higher values indicating higher accuracy of track positional data, as shown in Table 6.1a. The TQ of a track is assigned based on an area within which there is a 95% probability that the track lies, determined by the unit reporting the track. Non-real time tracks are assigned track quality of zero.

TQ	Maximum Error
15	18 feet
14	36 feet
13	60 feet
12	120 feet
11	300 feet
10	600 feet
9	3500 feet
8	1.18 dm
7	2.93 dm
6	5.92 dm
5	8.87 dm
4	11.82 dm
3	14.78 dm
2	29.61 dm
1	>29.61 dm

Table 6.1a. Maximum Positional Errors Represented by TQ

6.2.2.3.2 TQ of ballistic missile tracks is a measure of the reliability of the kinematic data reported on the track. This will be determined by the C^2 JU with R^2 using a TQ algorithm of both positional and velocity error terms. The TQ algorithm contains a variable parameter, ΔT (Delta T). This variable parameter will be a default value unless a different value is disseminated via the OPTASK LINK.

6.2.2.3.3 Operators must not artificially increase TQ between sensor inputs.

6.2.2.4 Reporting Responsibility

6.2.2.4.1 The purpose of the Reporting Responsibility (R^2) rules is to ensure that new tracks are reported and that existing tracks are maintained with the best data available within the interface. All C^2 JUs are responsible for reporting local tracks that cannot be correlated with remote tracks being received from another unit. When a local track is correlated with a remote track, it is referred to as a common track, and R^2 rules are applied to ensure that only the JU with the best positional data on the track reports it on the interface.

TN Range	No.TNs	Type2	Use
00000	1	N	No Statement
00001-00076	62	N	PU/FPU/FJUA/FJUAB/C^2 JU Address/Group Identifier Addresses
00077	1	N	Illegal (not used)
00100-00175	62	N	RU/FRU/FJUB/C^2 JU Address/Group Identifier Addresses
00176	1	N	Link 16 Pseudo-Source TN
00177	1	N	Collective Address
00200-07776	3,967	N	Link-11/11B/16/IJMS Surveillance TNs or C^2/NonC^2 JU addresses
07777	1	N	Illegal (not used)
0A000-0Z777	12,288	AN	Link-16 Surveillance TNs
10000-17777	4,096	N	Link-16/IJMS Surveillance TNs or C^2/NonC^2 JU Addresses
1A000-lZ777	12,288	AN	Link-16 Surveillance TNs
20000-27777	4,096	N	Link-16/IJMS Surveillance TNs or C^2/NonC^2 JU Addresses
2A000-2Z777 . . .	12,288	AN	Link-16 Surveillance TNs
70000-77776	4,095	N	Link-16/IJMS Surveillance TNs or C^2/NonC^2 JU Addresses
77777	1	N	Network Manager Address
7A000-7Z777	12,288	AN	Link-16 Surveillance TNs
A0000-ZZ777	393,216	AN	Link-16 Surveillance TNs

1. All JUs shall be capable of accepting all legal TNs described in this table. JUs that assign TNs shall also be capable of assigning all legal TNs.
2. N = Numeric TN block. AN = Alphanumeric TN block

Table 6.2. Link 11/11B/16/IJMS Track Number Sequence and Use

6.2.2.4.2 Reporting Responsibility Rules

The R^2 rules are laid down in STANAG 5516 and are summarised below. In some systems these rules are applied automatically without any operator action, whereas in other systems manual operator action is required.

a. The R^2 rules for air, surface, land and ballistic missile tracks are summarised as follows:

(1) A C^2 JU initiating a track report has R^2 for the track until it is relinquished in accordance with the rules below or the track is dropped.

(2) Other C^2 JUs holding local data on a track will compare their local data with that received on the interface and will assume R^2 under any of the following conditions:

(a) Local TQ at the time of transmission exceeds the received TQ by two or more. For ballistic missile tracks, local TQ at or before time of remote time tag exceeds received TQ by 1 or more. NOTE: A JU reporting a ballistic missile Lost Track is assumed to have a TQ of 5 less than reported, e.g., if a JU is reporting a “Lost Track” data with a TQ of 15, a JU holding “Tracking” data may assume R^2 with a TQ of 11.

(b) Real-time data are held locally and non-real time data were received.

(c) A remote report has not been received on a locally held Air or Surface (Maritime) track for approximately 40 seconds, or on a locally held Land (Ground) track for approximately 120 seconds; 25 seconds for a ballistic missile track. For ballistic missile tracks, this rule only applies when the last remote report was received with the Lost Track Indicator set to Tracking.

(d) A non-real time track is updated locally by a new non-real time track report.

(3) Upon receiving a Drop Track Report (J7.0 Action Value (ACT)=0) on a track for which local data is held, a C^2 JU may elect to assume R^2 for the track. Immediately prior to assuming R^2 for an air or surface track after receipt of a Drop Track message, a JU shall test the track for correlation in accordance with paragraphs 6.2.5.4.1.2, 6.2.5.4.1.3, and 6.2.5.4.1.4, except the test shall be conducted only once.

(4) A C^2 JU receiving a PPLI message (with the NPS Indicator set to Inactive, Conditional Radio Silence or TDS Failure) from a C^2 JU that has R^2 of a locally held track, may assume R^2 at the next opportunity to transmit the track if local reporting eligibility remains and a remote report has not been received on that track.

b. There is no automatic shift of R^2 for subsurface contacts.

c. The reporting of Intelligence information is independent of R^2.

d. The R^2 rules for Reference Points/Lines/Areas and Land Points are summarised as follows:

(1) The C^2 JU originating the point/line/area retains R^2 as long as that C^2 JU remains active and reports the point/line/area.

(2) Any C^2 JU may, by operator action, assume R^2 for a point/line/area, using the same Reference TN, under one of the following conditions:

(a) A Drop Track Report is received on the point/line/area.

(b) The C^2 JU holding R^2 goes Conditional Radio Silent or Inactive.

(c) No report is received for three or more consecutive update intervals.

e. The R^2 rules for Emergency Points are as follows:

(1) Any C^2 JU may, by operator action, report on a previously reported emergency point when that C^2 JU has additional or more current information on the point.

(2) A C^2 JU may, by operator action, assume R^2 for an emergency point under one of the following conditions:

(a) A Drop Track Report is received on the point.

(b) The C^2 JU holding R^2 goes Conditional Radio Silent or Inactive.

(c) No report is received for three or more consecutive update intervals.

(3) The latest C^2 JU to report an emergency point has R^2 for that point.

f. The unit that originates an EW fix, Area of Probability (AOP), or LOB report always retains R^2 for it. A C^2 JU shall not assume R^2 for another C^2 JU's EW fix, AOP, or LOB report.

g. The R^2 rules for ballistic missile launch points and impact points are summarised below.

(1) Any C^2 JU may initiate a report of an actual ballistic missile Launch Point or Impact Point. The originator of such report retains R^2 on the point until it is relinquished.

(2) The C^2 JU initially reporting a ballistic missile track may initiate an impact point report and may initiate a report on a related Launch Point. R^2 for the related Impact Point report will remain with the C^2 JU having R^2 for the ballistic missile track.

(3) A C^2 JU assuming R^2 for a ballistic missile track need not assume R^2 for the related Launch Point. A C^2 JU no longer holding R^2 on the ballistic missile track may continue to report the related Launch Point.

6.2.3 Initiation of Surveillance Operations

6.2.3.1 When initialising an entire data link, the Network Manager should determine the order of network entry of C^2 JUs reporting on the surveillance net. Normally the C^2 JU with the largest track load should transmit first. Other C^2 JUs should enter the network with transmission filters imposed for all surveillance tracks. (Procedures for the use of transmission filters are covered in paragraph 6.2.5.7).

6.2.3.2 Each C^2 JU should:

a. Establish itself on the interface by transmission of own PPLI reports.

b. Receive all active remote tracks being reported on the surveillance net and attempt correlation with all local tracks held to determine commonality, to monitor data registration and to eliminate dual designations.

c. The minimum wait time prior to removing transmission filters is 12 seconds before reporting air, surface and space tracks, and 48 seconds before reporting land tracks. This is a minimum wait time and may be extended if necessary to accomplish a. and b. above.

d. Remove transmission filters as required to commence reporting of tracks for which local sensor data is held, in accordance with R^2 rules.

6.2.3.3 This procedure ensures that reporting of surveillance data on the network is commenced in an orderly manner. However, should operational necessity dictate, all or several C^2 JUs may begin to transmit on the link prior to expiration of the minimum wait time. This could result in a severe disruption of the surveillance picture and could last for an extended period of time until correlation between local and remote tracks has been resolved by all units.

6.2.4 Reporting Surveillance Data

6.2.4.1 Reporting of Tracks

6.2.4.1.1 Real-Time Tracks

a. All tracks in the surveillance picture are derived either from real-time or non-real time data. Real-time track reports on contacts are normally based on track data derived from active sensors, usually radar. Real-time air, surface and land tracks are always reported with positional data extrapolated to the time of report transmission. When sensor contact is interrupted, the reporting unit continues reporting the track and decrementing TQ as appropriate.

b. Ballistic missile tracks are normally reported as real-time tracks even if based on data derived from non-organic sensors. Certain systems, e.g. SIS, will report ballistic missile tracks as non-real time tracks. Space tracks are time tagged to the integer second nearest to the measurement time, and all position, velocity and covariance data are extrapolated or interpolated to the referenced time.

6.2.4.1.2 Non-real Time Tracks

Non-real time tracks are reported with TQ = 0. Some systems will automatically degrade TQ to 0 in the absence of sensor contact. However, less capable systems may require operator action to designate the track as a non-real time track. Non-real time track reports are used for contacts if any of the following conditions prevail:

a. The track data originated from a non-tactical data system (non-TDS).

b. The track data have been relayed from another system by other than a digital data link.

c. The track data have been derived from other than integrated sensors.

d. The operator judges that the time elapsed since the last update based on sensor information is such that the validity of the track position is questionable.

6.2.4.1.3 Action on Loss of Sensor Contact

If the loss of sensor contact continues, subsequent track reporting is determined by individual system design which provides one or more of the following alternatives:

a. Automatic purging of the track and initiation of a Drop Track Report if R^2 is held.

b. Operator action to continue reporting the track. The duration of such continuance shall be based on reasonable operator certainty that the track reports are accurate and that the loss of sensor contact will be of short duration.

c. Replacement with a non-real time track.

d. A ballistic missile track will be reported with the Lost Track Indicator set to “Lost Track” when the initial determination of lost track is made and periodically thereafter unless another JU assumes R^2 or the estimated time of impact has passed.

6.2.4.2 Point/Line/Area/Reporting

Data may be exchanged over Link 16 on various types of points/lines/areas for surveillance purposes.

6.2.4.2.1 Reference Points/Lines/Areas

6.2.4.2.1.1 C^2 JUs may transmit Reference Point/Line/Area messages to report tactically significant geographic references in the form of points, segmented lines, multisided areas, circles, ellipses and volumes (e.g. waypoints, Combat Air Patrols (CAPs) Forward Edge of Battle Area (FEBA), Missile Engagement Zones (MEZs), Hostile Weapon Zones (HWZs), safe corridors). Corridor widths are defined such that when reporting a Corridor or Low Level Transit Route, the width value specified represents the value that is closest to but does not exceed the required width. The reported line represents the centre line of the corridor or LLTR. Each point, line or area is assigned a TN by the originating JU. Positional data is reported using geodetic (latitude/longitude) coordinates. Altitude/elevation data may also be reported, as appropriate. Corridor Altitude and altitude ranges apply only to a single word sequence, i.e., a single track number. This is to allow different altitudes to be applied to different segments of the same line. Points, lines and areas may be reported with associated time in hours/minutes and Time Function, to define the meaning of time as used in the report (e.g. Time of Activation, deactivation). A list of the Point Type/Point Amplification values available for transmission on Link 16 is to be found in Table 6.3.

6.2.4.2.1.2 The originator of a reference point/line/area retains R^2 as long as the originator remains active and reports the point. If the point/line/area is dropped, the originator is declared inactive or if no periodic update is received for three consecutive update intervals, another C^2 JU may, by operator action, assume R^2 for the point/line/area. If an operator requires immediate information on a point/line/area for which his unit does not hold R^2, a Data Update Request should be transmitted with the Reference TN set to the TN of the desired point/line/area (see paragraph 6.2.5.3.3.1a).

6.2.4.2.1.3 Procedures for the use of the Exercise Indicator when reporting points/lines/areas are contained in paragraph 6.2.4.4.3.

6.2.4.2.1.4 Any JU may initiate/terminate a Force Tell alert on a point, line or area; emergency alerts are not used on reference points/lines/areas (see paragraph 6.2.5.8.2).

6.2.4.2.1.5 Points must not be correlated with any other point or track. Operators may report an association between a point and another point or track (see paragraph 6.4.10).

POINT TYPE	0	1	2	3	4	5	6	7	8
POINT AMP	HAZARD	REFERENCE POINT (GENERAL)	STATION (GENERAL)	STATION (AIR)	LINE	AREA (GENERAL)	AREA (HAZARD)	ASW	ASW, 1
0	NO STATEMENT	NO STATEMENT	NO STATEMENT	NO STATEMENT	NO STATEMENT	NO STATEMENT	NO STATEMENT	NO STATEMENT	CHARTED WRECK
1	NAVIGAITON	MARSHALL POINT	TOMCAT	COMBAT AIR PATROL (CAP)	FORWARD EDGE OF THE BATTLE AREA	SEARCH	DANGER	SINKER	BOTTOMED NON-SUBMARINE
2	MINE	WAYPOINT	PICKET	AIRBORNE EARLY WARNING (AEW)	GUN TARGET LINE	RESTRICTED	CONTAMINATED	BRIEF CONTACT	ASW STATION
3	IMPACT POINT	CORRIDOR TAB	RENDEZVOUS	ANTISUBMARINE WARFARE (ASW) FIXED WING	CORRIDOR	EXERCISE	MISSILE ENGAGEMENT ZONE	SEARCH CENTRE (ASW)	UNDEFINED
4	GROUND ZERO	POSITION AND INTENDED MOVEMENT (PIM)	UNDEFINED	ANTISUBMARINE WARFARE (ASW) HELICOPTER (HELO)	HOSTILE BOUNDARY	SUBMARINE PATROL AREA	UNDEFINED	ESTIMATED POSITION (EP)	UNDEFINED
5	AIM/WEAPON ENTRY POINT	DISPOSITION CENTRE	REPLENISHMENT	REPLENISHMENT	BUFFER ZONE BOUNDARY	FIGHTER ENGAGEMENT ZONE/FIGHTER AOR	HOSTILE WEAPON ZONE	FIX (ASW)	UNDEFINED
6	MISSILE LAUNCH POINT	FORMATION CENTRE	RESCUE	STRIKE INITIAL POINT	LOW LEVEL TRANSIT ROUTE	GROUND AREA OF RESPONSIBILITY	HOSTILE TACTICAL AREA	NOTACK AREA	UNDEFINED
7	ELECTRONIC COUNTER MEASURES (ECM) DECOY	SEARCH AREA	UNDEFINED	TACAN	TACTICAL ACTION LINE	UNDEFINED	SHORAD	MOVING HAVEN	UNDEFINED
8	ENGAGEMENT POINT	VICTOR LIMA (VL)	UNDEFINED	TANKER	FIRE SUPPORT COORDINATION LINE (FSCL)	UNDEFINED	KILL ZONE	DATUM	UNDEFINED
9	OIL RIG	SUBMARINE POSITION AND INTENDED MOVEMENT (SIM)	UNDEFINED	ORBIT, RACE TRACK	FORWARD LINE OF OWN TROOPS (FLOT)	UNDEFINED	TARGET AREA OF INTEREST	SONOBUOY POSITION	UNDEFINED
10	UNDEFINED	UNDEFINED	UNDEFINED	ORBIT, FIGURE EIGHT	UNDEFINED	UNDEFINED	NAMED AREA OF INTEREST (NAI)	SONOBUOY PATTERN REFERENCE POSITION	UNDEFINED
11	UNDEFINED	UNDEFINED	UNDEFINED	ORBIT, RANDOM CLOSED	UNDEFINED	UNDEFINED	UNDEFINED	LIMITING LINE OF APPROACH	UNDEFINED
12	UNDEFINED	UNDEFINED	UNDEFINED	ORBIT POINT	UNDEFINED	UNDEFINED	UNDEFINED	AREA OF PROBABILITY (AOP)	UNDEFINED

Table 6.3. Point Type/Point Amplification

6.2.4.2.2 Emergency Points

6.2.4.2.2.1 C^2 JUs will use the Emergency Point message to report the location of an emergency condition that requires search and rescue. Operators should include the type of emergency and personnel involved, where this information is known. A C^2 JU may report on a previously reported emergency point when that unit has additional or more current information on the point. The C^2 JU may also report the point if the originator drops the point, is declared inactive or has not updated the point. The latest unit to report on the emergency point has R^2 for it. In both cases, operator action is required.

6.2.4.2.2.2 Emergency points will be forced through data filters and are, therefore, not required to be reported with Force Tell or Emergency alert status. If an emergency point is reported for exercise purposes, the operator must set the Exercise Indicator prior to transmission (see paragraph 6.2.4.4.4). Operators may report an emergency point as related to a previously reported track or point (e.g. to report the position of a downed aircraft - see paragraph 6.2.4.2.2.3 below).

6.2.4.2.2.3 If a JU loses all contact with a friendly track and there is cause to believe that an emergency situation exists, the operator should establish an emergency point at the last reported position of the track. The TN of the previously reported track should be entered as the Related TN and the IFF/SIF modes and codes of the track should also be included in the emergency point report.

6.2.4.2.2.4 The terminate Emergency Point sequence will normally be transmitted by the JU in charge of the Search and Rescue or Emergency Search operation but may be transmitted by a JU delegated to do so by the unit in charge of the operation. The unit will terminate the Emergency Point:

a. By assuming R^2 for the Emergency Point, if not already held.

b. By transmitting the Emergency Point message with the Time Function set to Deactivation Time and the time set to the hours and minutes at which the emergency has been terminated.

c. Following this by transmission of a Drop Track message for the Emergency Point TN.

6.2.4.2.2.5 Following receipt of the Drop Track message, or after a suitable time interval if no updates of the Emergency Point are received, the Emergency Point may be purged by operator action.

6.2.4.2.3 Land (Ground) Points

C^2 JUs will use the Land (Ground) Point message to report the location of fixed ground units or objects; e.g. airbases, radar installations, troop concentrations.

6.2.4.2.4 Moving Points/Lines/Areas

Reference points, lines and areas may be reported with course and speed data to indicate movement. Position and Intended Movement (PIM) and Submarine Position and Intended Movement (SIM) points should be reported with an activation time at which reported position, course and speed becomes effective. Other points/lines/areas established with an activation time in the future will only be reported as moving once the activation time has been reached. Emergency and land (ground) points are only reported as static points. A change in geodetic position must be transmitted to show that an emergency or land (ground) point has shifted.

6.2.4.2.5 Slaved Points/Areas

Certain reference points and regular areas (i.e. squares, rectangles, circles and ellipses) may be slaved to a track being reported on Link 16 (e.g. a marshal point used during aircraft recovery operations onboard an aircraft carrier). The position of the slaved point or area is reported as a constant bearing (true or relative) and range from the related track. Lines and irregular multisided areas cannot be slaved. ASW AOPs cannot be slaved but an operator may associate an ASW AOP to a track or point (e.g. a subsurface track for which contact has been lost or a datum point) by transmitting an Association message (see paragraph 6.2.5.9).

6.2.4.3 Reporting of JU Data

6.2.4.3.1 Active JUs

C^2 JUs should attempt to correlate received PPLI reports with local sensor data. Where correlation is found, a separate track shall not be reported except as in Table 6.4.

6.2.4.3.2 Inactive JUs

When a C^2 JU determines another JU is no longer active on the interface and that C^2 JU holds local data on the inactive JU, it will report the position of the inactive JU in a Surveillance Track Report. The Reference TN will be set to the inactive JU's address.

Network Participation Status	Action Required
No Statement	1
Active	1
Inactive	2
Conditional Radio Silent	2
High Error Rate	1
No Initial Entry Message	1
TDS Failure	1, 3
Polling	1, 2

Actions:

1. Received PPLI accepted in preference to received surveillance data for same TN.
2. A C^2 JU with local track data may immediately assume R^2 for this JU using the JU's address as TN.
3. Errors may exist in received PPLI. C^2 JUs with local track data may initiate an associated track for surveillance using TN from the C^2 JU's assigned TN block.

Table 6.4. PPLI Versus Surveillance R^2

6.2.4.4 Reporting of Exercise Data

6.2.4.4.1 Link 16 provides operators with the capability to report exercise data over the interface. Exercise data constitutes data on real vehicles which may be reported with artificial values for training purposes only. Operators should note that the reporting of artificial data is only permissible when authorised prior to operations and promulgated in the OPTASK LINK, and may only be reported on a track or JU with exercise status, as indicated by the setting of the Exercise Indicator. However, data which impacts directly on platform safety, e.g. positional, navigational and network management data, will always be interpreted as real data and must never be reported with artificial values. Detailed procedures for the reporting of exercise data are contained in the following paragraphs.

6.2.4.4.2 Exercise Tracks

6.2.4.4.2.1 Tracks may be reported with the Exercise Indicator set to enable exercise and non-exercise tracks to be distinguished on the interface. Exercise tracks are live tracks which are participating in an exercise. The Exercise Indicator will be set to “Exercise Track” by operator action, to report exercise status on a track. This status will remain valid until a further operator action is taken to set the Exercise Indicator to “Non-Exercise Track” (see Paragraph 6.2.4.4.7). Operators must not attempt to assign exercise status:

a. To tracks which have a standard identity other than Friend.

b. To tracks which have emergency alert status.

c. To any other active JU (see paragraph 6.2.4.4.6).

6.2.4.4.2.2 When exercise status has been assigned to a track, the exercise identity of that track is for exercise purposes only and may be set to one of the following:

a. Exercise Pending.

b. Exercise Unknown.

c. Exercise Assumed Friend.

d. Exercise Friend.

e. Exercise Neutral.

f. Joker (a friendly track acting as Suspect for exercise purposes).

g. Faker (a friendly track acting as Hostile for exercise purposes).

6.2.4.4.2.3 When authorised, operators may elect to report artificial data in exercise track reports for exercise purposes only. Operators must not report artificial data without first assigning exercise status to the track concerned. Artificial values may be reported for the following data:

a. Special Interest Indicator.

b. Strength.

c. Platform/Platform Activity.

d. Specific Type.

Operators receiving track reports with exercise status set should assume that values reported for the above data are artificial and for exercise purposes only. All other data should be considered real.

6.2.4.4.2.4 Emergency Indicator on Exercise Tracks

Operators must only set the Emergency Indicator on a track with exercise status to report a real emergency over Link 16. Where there is a requirement for training purposes to report a platform with a practice emergency, voice procedures must be used. Alternatively, an exercise emergency point may be established specifically for training purposes (see paragraph 6.2.4.4.4).

6.2.4.4.2.5 Force Tell Indicator on Exercise Tracks

Operators may set the Force Tell Indicator on a track with exercise status. The Force Tell Indicator is always real and never artificial.

6.2.4.4.2.6 Special Processing Indicator on Exercise Tracks

The Special Processing Indicator (SPI) should not be set on a track with exercise status.

6.2.4.4.2.7 Exercise Threat Warning Reports

When a threat warning (J15.0) report is transmitted on the Link 16 interface to report threat information on a track with exercise status, receiving JUs should interpret all threat data pertaining to the reported TN as artificial and for exercise purposes only.

6.2.4.4.2.8 Exercise EW Products

When an EW Product Information (J3.7) message is transmitted on the Link 16 interface with exercise status, receiving JUs should interpret all EW data pertaining to the reported TN as artificial and for exercise purposes only.

6.2.4.4.3 Exercise Reference Points/Lines/Areas

Operators may initiate MEZs or HWZs with exercise status for reporting on the interface. Exercise MEZ or HWZ definitions should be considered artificial and for exercise purposes only. No other reference points/lines/areas can be reported with exercise status. Operators must not change the Exercise Indicator to “Exercise MEZ or HWZ” if the MEZ or HWZ has been previously established with the Exercise Indicator set to “Non-Exercise MEZ or HWZ”.

6.2.4.4.4 Exercise Emergency Points

Operators may initiate emergency points with exercise status for reporting on the interface. All data associated with exercise emergency points should be considered artificial and for exercise purposes only. Operators must not change the Exercise Indicator to “Exercise Emergency Point” if the emergency point has been previously established with the Exercise Indicator set to “Non-Exercise Emergency Point”.

6.2.4.4.5 Management of Exercise Data

The management of exercise data is identical to that for non-exercise data (see paragraph 6.2.5), including frequency and type of updates, R^2 rules, track alert procedures and drop track requirements. Information difference recognition, reporting and resolution procedures are the same, with one exception: in all cases where a conflict occurs between a track with exercise status and one with non-exercise status, the operator will be alerted and the conflict of exercise status must be resolved by voice.

6.2.4.4.6 Exercise Participation by JUs

6.2.4.4.6.1 JUs participating as friendly assets in an exercise will report their exercise status by setting the Exercise Indicator in the PPLI message. An exercise participant acting as a hostile force will not be an active JU on the same Link 16 friendly force net.

6.2.4.4.6.2 When authorised, operators at JUs participating in an exercise may elect to report artificial data in their own PPLIs for exercise purposes only. Operators must not report artificial data without first assigning exercise status to their own unit. Artificial values may be reported for the following data:

a. Command and Control Indicator.

b. Flight Leader Indicator.

c. Strength.

d. Platform.

e. Platform Activity.

Operators receiving PPLIs with exercise status set should assume that values reported for the above data are artificial and for exercise purposes only. All other data must be considered real.

6.2.4.4.7 Termination of Exercise Status

6.2.4.4.7.1 Termination of exercise status is achieved by one of the following methods:

a. By operator action to clear the exercise status of an individual track.

b. By operator action at a JU to clear exercise status of own unit.

c. By operator action to clear all exercise data from the network.

6.2.4.4.7.2 When an operator takes action to clear the exercise status of an individual track, the following automatic actions will be taken:

a. The identity will be set to Exercise Friend.

b. Any artificial data will be reset to real values, if available, or to No Statement/default values.

c. The Exercise Indicator in the track report will be set to "Non-Exercise Track".

This will cause the track to be transmitted with an identity of Friend. If the track is the subject of an engagement, the operator should ensure that the engagement is terminated on the interface. These procedures also apply to inactive JUs.

6.2.4.4.7.3 When an individual JU ceases to participate in an exercise, the operator must clear the exercise status of his own unit. This action will automatically cause all artificial data to be cleared or set to default values immediately and clear the Exercise Indicator in that unit's PPLI message. Depending upon system implementation, artificial data will be automatically replaced with real data or No Statement/default values will be reported until changed by the operator. No JU, including a controlling unit, can change the exercise status of another active JU by Link 16 message. Voice procedures must be used to request/order an active JU to change its exercise status.

6.2.4.4.8 Exercise Status Order

6.2.4.4.8.1 On cessation of an exercise, during which exercise data has been exchanged over the interface, it is essential that all exercise data be rapidly cleared from the network. This requires operator action at the C^2 JU with command authority to initiate an Exercise Status Order for transmission to all other network participants. On receipt of the order, all systems will automatically:

a. Alert the operator.

b. Set the identity of all exercise tracks held to Exercise Friend.

c. Reset all data held, including data on own unit, which may be artificial, to No Statement/default values, until real values are available.

d. Clear the exercise status of own unit and set the Exercise Indicator of all tracks with the status "Exercise Track" to "Non-Exercise Track". This will cause the tracks to be transmitted with an identity of Friend.

e. Where system capabilities allow, inhibit transmission or reception of any further exercise data.

6.2.4.4.8.2 When alerted to the receipt of an Exercise Status Order, C^2 JU operators should:

a. Implement exercise filters (see paragraph 6.2.5.7.3), if own system does not incorporate an automatic exercise inhibition capability, in order to prevent the transmission of exercise data.

b. Ensure that all locally originated engagements involving an exercise track are broken or cancelled.

c. Ensure that all locally originated commands involving an exercise track are terminated.

d. Ensure that all MEZs or HWZs and emergency points generated with exercise status, and for which R^2 is held, are terminated on the network.

e. Enter real values for those data that may have contained artificial values, as appropriate.

6.2.4.5 Reporting of Simulated Data

Simulated tracks (including points, bearings, fixes and AOPs) and units which are not derived from any live sensor data, may be reported on the interface for training or test purposes. All data generated from simulated sensor inputs must be reported with the Simulation Indicator set. The simulation status of a track cannot be changed on Link 16. If for any reason, such as operator or system error, it is necessary to correct the simulation status of a track, the operator must drop the track and initiate a new track report with the correct status. However, operators should note that it is possible for the simulation status to change from “Live” to “Simulated” on a Link 11/11B-originated track being forwarded on to Link 16 by the FJU. Simulated tracks must not be correlated with non-simulated tracks. (See paragraph 7.2.4.3 for restrictions on forwarding simulated tracks/units).

6.2.4.6 SAM Reporting

Land-based Surface to Air Missiles (SAMs) are reported in Land (Ground) Point messages, defining the location and specific type (if known) of the SAM. Ship-based SAMs are reported in Surface (Maritime) Track messages, defining the location and specific type (if known) of the ship on which the SAM is fitted. Airborne assets receiving hostile SAM information will be able to determine doctrinal SAM engagement envelopes from Specific Type information contained in the reports. When required to pass generic doctrinal weapon engagement zones for hostile anti-air threats to provide an avoidance cue to friendly aircraft, these are to be reported in Reference Point messages using Point type Area/Hazard/Hostile Weapon Zone.

6.2.4.7 Cease Reporting

The Drop Track Report may be used by C^2 JUs to report that they have dropped or ceased to report a track or point. Tracks or points that are the subject of a Drop Track Report can still be reported by another unit that holds valid reportable data and that elects to assume R^2.

6.2.5 Information Management

On many occasions messages are exchanged and actions are taken within the interface for the purpose of managing and/or enhancing existing tactical data. These messages, while not reporting track information, manage and effect the flow of the information being reported on the interface.

6.2.5.1 Commonality of Data

When locally held data differ from the corresponding data received from another C^2 JU, a potentially disruptive situation known as a data difference exists. A data difference can only occur when local data is held on a track received from a remote source. Depending on the data involved, some action may be required to cause all C^2 JUs to hold a common value for that data, although it should be noted that many types of data are not subject to this procedure. Operators should be aware that the locally held value for such types of data may vary from C^2 JU to C^2 JU.

6.2.5.2 Difference Reporting and Conflict Resolution

The exchange of surveillance data requires procedures to recognise and resolve data differences that may occur. Recognition, resolution, or some corrective actions are applied to data differences in the following track data items:

a. Track environment/category (Env/Cat).

b. Track identity data.

c. Track IFF/SIF data.

Some data differences of identity or IFF/SIF can be automatically resolved, whereas others are of sufficient importance to demand resolution by operator action. These latter differences are referred to as conflicts.

6.2.5.2.1 Corrective Actions

Many corrective actions and methods may be applied to resolve data differences, depending on the specific data items involved. Actions range from compulsory acceptance of another unit's data to simply reporting the difference without changing local data. Some systems will be capable of performing automatic actions without requiring any operator intervention, whereas other less capable systems will require operator judgement and subsequent action. For this reason, both automatic and manual methods are discussed in the following paragraphs; however, only operators of systems with limited capability will be required to follow the manual procedures.

6.2.5.2.2 Track Environment/Category

When two or more JUs are using different Env/Cats for the same TN, an Env/Cat conflict exists. Such conflicts can occur as a result of erroneous sensor data, operator error or may indicate a Duplicate TN condition (see paragraph 6.2.5.4.3). An operator alert will also be provided if local and received data differ as to whether the TN is assigned to a track or a point. This type of conflict should be resolved using the Env/Cat conflict resolution procedures described below.

6.2.5.2.2.1 Environment/Category Changes Not Permitted

Link 16 does not permit the following changes in Environment/Category (Env/Cat):

a. Between air or land (ground) and subsurface (Maritime), or vice versa,

b. From a known Env/Cat to No Statement/Unknown, or

c. Between space and surface (maritime), subsurface (maritime), or land (ground), or vice versa.

Acceptance or rejection of Env/Cat, except those directed by a Change Data Order (see paragraph 6.2.5.2.5), must be accomplished by a manual operator action. Where changes of Env/Cat are not permitted, or where units cannot agree, a new track report with a new TN must be transmitted.

6.2.5.2.2.2 Methods for Changing Track Environment/Category

The methods for changing track Env/Cat follow:

a. The C^2 JU with R^2 may transmit a new track report using the same TN, containing a new Env/Cat. Depending on system implementation, the operator at the receiving C^2 JU may be alerted.

b. C^2 JUs not holding R^2 may declare differences in Env/Cat in an Information Difference Report (J7.0 ACT=1). In this case, other C^2 JUs, including the unit holding R^2, may be alerted (acceptance or rejection by operator action).

c. Another method of changing track Env/Cat is for a C^2 JU to establish a new track with the required Env/Cat, using a new TN. If the unit has R^2 of the original track, then a Drop Track Report must also be transmitted. Units not agreeing to the change may maintain the original track with the original Env/Cat.

When the Env/Cat changes for a specific TN cannot be resolved using one of the methods described above, voice coordination should be initiated. Differences in Env/Cat must be resolved before differences in Identity.

6.2.5.2.3 Track Identity

6.2.5.2.3.1 Methods of Changing Identity

Each C^2 JU has the capability to independently perform the identification function and to report its unit's assessment of a track's identity. If received identity data are not identical to the corresponding local data held on the same track, an identity difference exists. Individual systems react to these differences by one of the following automatic or manual means:

a. A C^2 JU with R^2 may transmit a track report with the same TN containing a new identity. Receiving C^2 JUs holding local data on the track will alert the operator if an identity conflict exists.

b. C^2 JUs not holding R^2 may initiate identity changes in an Information Difference Report. Upon receipt of an Information Difference Report, the C^2 JU with R^2 will alert the operator if a conflict exists.

c. Operator action following an operator alert may be one of three options:

(1) Accept the received identity.

(2) Return to the original identity.

(3) Select another identity.

When R^2 shifts between two C^2 JUs holding different data, the reported data may change. If the Identity Difference Indicator is set, the new reporting C^2 JU will transmit the latest identity reported on the interface. C^2 JUs not having local data will in many cases not be aware that an identity difference situation exists.

6.2.5.2.3.2 Controlling Unit

A C^2 JU controlling an aircraft is assumed to have the best identity data. All other C^2 JUs shall automatically accept the identity reported by a controlling C^2 JU in an Information Difference Report. The controlling C^2 JU will not accept changes in identity for aircraft under its control, (see paragraph 6.2.5.2.5.2 below).

6.2.5.2.3.3 Subsurface Tracks

Identity differences are not reported for subsurface tracks.

6.2.5.2.4 Platform, Platform Activity and Specific Type

Differences in Platform, Platform Activity, and Specific Type data for friendly platforms may exist on Link 16 without any corrective action required. Such differences cannot be reported on Link 16 unless an Environment or Identity difference is also reported. Receiving JUs with the exception of the controlling unit, will automatically accept the values of Platform, Activity and Specific Type reported on the Link 16 interface, if implemented. Activity differences involving the Activity “Tanking” may cause an operator alert, depending on system implementation. Where Environment or Identity differences are not reported and the operator considers resolution is necessary, voice coordination is required. Alternatively, the Change Data Order may be used by the units with proper authority.

6.2.5.2.5 Change Data Orders

6.2.5.2.5.1 The Change Data Order (J7.0 ACT=2) causes all C^2 JUs, except the controlling unit, to accept the same Env/Cat, Identity, Platform, Platform Activity, Specific Type, Exercise Indicator, and Special Interest Indicator as transmitted from and as held by the C^2 JU issuing the order. Upon receipt, all systems automatically accept the data in the Change Data Order if they are maintaining the specified track in their database, except as described in paragraph 6.2.5.2.5.2 below. The Change Data Order is initiated only by operator action and only by units with proper authority.

6.2.5.2.5.2 Controlling Unit Identity Procedures

A controlling C^2 JU receiving a Difference Report or Change Data Order containing different data for a track under its control will reject that data and transmit a Difference Report containing the local data, with the Controlling Unit Indicator set. This may include differences of Platform, Platform Activity, Specific Type or Special Interest Indicator without any Env/Cat or ID difference. Other C^2 JUs are required to accept the Information Difference reported by a Controlling C^2 JU.

6.2.5.2.6 Track IFF/SIF Data

6.2.5.2.6.1 IFF/SIF information is used by systems as one factor in determining track identity. IFF/SIF information associated with a specific track is reported by the C^2 JU with R^2. All other C^2 JUs are responsible for monitoring IFF/SIF data on the track and reporting any valid data held locally that differs from that received over the interface. IFF/SIF information may be cleared to no data status by any C^2 JU and any C^2 JU may update IFF/SIF information, with the exception of Mode II data (see paragraph 6.2.5.2.5).

6.2.5.2.6.2 Updating IFF/SIF Data

There are several ways to update IFF/SIF information on the interface as follows:

a. The C^2 JU holding R^2 transmits updated data in a Surveillance Track Report.

b. A C^2 JU not holding R^2 generates an IFF/SIFF difference Report (J7.5 ACT=1).

c. A C^2 JU generates an IFF/SIF Clear (J7.5 ACT=0) message to initiate a change to “no data” status for any or all of the currently held IFF/SIF modes for the track. (For use of Mode IV Clear message, see paragraph 6.2.5.2.6.6).

d. A C^2 JU originates a IFF/SIF Update Request (J7.5 ACT=2).

The last two methods of causing an update must be operator-initiated actions. Irrespective of the source, the response to the above is automatic involving no operator action.

6.2.5.2.6.3 Causes of IFF/SIF Data Differences

IFF/SIF data differences and data errors may be caused by any of the following:

a. Malfunction of IFF/SIF equipment or misalignment of Automatic Code Changing (ACC) routine (Mode I or III).

b. Duplicate TN condition which results in different IFF/SIF data being reported for the same TN.

c. Operator error when entering IFF/SIF manually.

d. Operator or system correlation error.

e. Two or more transponding platforms in close proximity.

6.2.5.2.6.4 IFF/SIF Mode I/III Data Difference Procedures

Recognition of an IFF/SIF data difference or error normally occurs when specific local IFF/SIF data is compared with equivalent data obtained from another source (e.g. aircrew report or another JU). This data comparison may be prompted by a TDS-generated alert or by other means, indicating a data difference. Some IFF/SIF data differences may be resolved automatically on the interface without the need for operator intervention. However, when an operator receives an IFF/SIF data difference alert or recognises that a data difference or error exists, he should verify and correct the data involved using the following procedures:

a. Reinterrogate the track and update local data, ensuring that such data are consistent and current. If own unit controls the track, verify the data with the aircrew.

b. After verification of the data, the operator should perform one of the following actions:

(1) If the operator believes that his local data is correct, generate a Clear IFF/SIF message to cause all units to revert the indicated IFF/SIF mode(s) to zero (no data status) in their database, and manually initiate an IFF/SIF Difference Report containing the local data.

(2) If the operator believes his local data to be in error, accept the remote data into own database.

(3) Coordinate by voice with the appropriate TDC/FTC or with the other unit(s) involved to resolve the difference.

<u>NOTE</u> :Current data link protocols specify the no data status for IFF/SIF Modes I and III as all zeros. However, some countries use Mode I code 00 and Mode III code 0000 as operationally valid codes. Operators should be aware that Mode I or Mode III codes of all zeros cannot be processed as such by Link 16 protocols. When such codes are in operational use, operators are advised to use voice procedures to resolve IFF/SIF Mode I or Mode III data differences.

6.2.5.2.6.5 Mode II Data Difference Procedures

The Mode II code requires special consideration because it is normally a unique vehicle identifier. It can be used to advantage in avoiding erroneous track correlations and alerting operators to erroneous entries. Therefore, the maintenance of a clear tactical picture is dependent to a certain extent on the protection and utilisation of Mode II code uniqueness. However, operators must be aware that a Mode II code is not always unique to specific aircraft in certain theatres and operations. Special procedures apply to Mode II data as follows:

a. When valid (i.e. non-zero) data is held for a specific track, that data cannot be changed over Link 16, except in response to a Clear IFF/SIF message on that track. This causes all JUs to revert the Mode II code in their database to zero (no data status) for that track until the next valid code response is received or a valid Mode II code is reported on the interface.

b. If local sensors detect an apparent Mode II change, it should be treated as a potential new track (see paragraph 6.2.5.2.6.7 below).

c. Operators may be alerted if two or more tracks have the same Mode II code. This provides a strong indication that a dual designation exists. Some systems allow the operator to suppress this alert. However, this capability should be used judiciously, and only when it is known that there is a high incidence of multiple aircraft present assigned the same Mode II code.

6.2.5.2.6.6 Mode IV Data Difference Procedures

Mode IV is the primary means of Friend identification. Differences in the Mode IV reported on the interface for a specific track must be resolved immediately. Mode IV data is reported as values of:

a. 0=Not interrogated.

b. 1=Interrogated, no response.

c. 2=Interrogated, invalid response.

d. 3=Interrogated, valid response.

Mode IV upgrades (to a higher value) are automatically accepted by all JUs. However, downgrades are automatically rejected. If an operator believes that a Mode IV downgrade is appropriate, he may use the Mode IV Clear IFF/SIF message. However, it should be noted that, because of the importance of Mode IV data, some systems may not accept a Mode IV Clear request. For this reason operators are advised to reinterrogate and conduct voice coordination with the appropriate TDC/FTC or with the other unit(s) involved to resolve Mode IV data differences.

6.2.5.2.6.7 Resolution of IFF/SIF Data Conflicts

If an IFF/SIF data difference persists after verification of the data using the above procedures, the C^2 JU holding local data that differ from the remote data must decorrelate by establishing a new track with the local IFF/SIF data. This procedure must apply, even though the positions of the two tracks may be identical.

6.2.5.2.6.8 IFF/SIF Voice Coordination

When resolving IFF/SIF data differences by voice, the following common terms and meanings must be used to avoid operator misunderstanding:

a. IFF/SIF Data Held – IFF/SIF code(s) held in the TDS data base and available for display to the operator.

b. IFF/SIF Response – IFF/SIF codes(s) being received as a result of own unit interrogation of an object, track or point in space.

c. SQUAWK – Order to operate IFF as indicated.

d. SQUAWKING – Operating IFF as indicated by the IFF transponder control within the platform.

6.2.5.3 Data Update Requests

6.2.5.3.1 The Data Update Request is used for requesting certain data from one or more other JUs. While this request may occur automatically, it is normally initiated by operator action. The request may be used to update the following:

a. Information purged or dropped locally.

b. Information missed during periods of inactivity.

c. Information missed due to poor data reception.

d. Information missed due to filtering.

6.2.5.3.2 A Data Update Request may be addressed to a specific JU, to several specific JUs or to the collective address. Information may be requested by specific TN (J7.1 ACT=1), or ballistic missile Track Update Request (J7.1 ACT = 2), or Request Indicator Value (RIV) (J7.1 ACT=0). In the latter case, the operator selects the data desired by setting the appropriate RIV. The possible selections are:

a. Multi-point area or line (requiring multiple messages).

b. ECM data.

c. ESM data.

d. EW fixes.

e. Weapon status.

f. Weather data.

g. Intelligence.

h. Filter data.

A request for filter data must only be directed to a specific address. The collective address cannot be used.

6.2.5.3.3 Response to Data Update Request

The response to a Data Update Request from any JU is automatic and requires no operator action.

6.2.5.3.3.1 Response to Request by Track Number

If the data are requested on a specific TN, then the responding JU(s) will reply with all data described below, depending on its relationship to the referenced TN. If the responding JU is a:

a. C^2 JU with R^2 on the referenced TN, then it will transmit a Surveillance Track/ Point Report for that TN. Ballistic missile track data will be requested either with or without error estimate data included. The C^2 JU with R^2 will respond with the requested data.

b. C^2 JU that has originated surveillance amplification data on the track, then it will respond with that data.

c. Controlling C^2 JU of the referenced track, then it will respond with weapons coordination and management information and platform and system status information. This will include the Controlling Unit Report (J10.5) and the Engagement Status (J10.2).

d. C^2 JU responding to a Data Update Request on own TN, then it will report the status of all engagements in progress by subordinates under its control and platform and system status information on itself.

e. C^2 JU controlling an engagement against the referenced TN, then it will report the status of the engagement.

f. NonC^2 JU whose TN address is the referenced TN, then it will respond with platform status information on itself.

6.2.5.3.3.2 Response to Request by Request Indicator Value

If the data are requested by RIVs, then the C^2 JU(s) which originated the data will respond with the requested information.

6.2.5.4 Track Correlation and Decorrelation

6.2.5.4.1 Commonality of track positional data is maintained by the correlation and decorrelation functions of the interfacing systems.

6.2.5.4.1.1 Track Correlation

a. Each JU performs a correlation function to determine if its new contacts are new tracks or duplicates of existing tracks. Correlation occurs when the locally derived data are associated with an existing active TN. If a track does not correlate, a new TN is assigned and the new track is reported to the interface. This process is normally accomplished automatically by C^2 JUs, but may also be accomplished manually by the operator.

b. When tracking manually, the operator correlates the radar return on the current scan with those received on the past three or four scans on the radar. Local tracks are not to be reported to the interface until a correlation with a remote track has been attempted and failed, or an operator action has been taken to selectively release that track for reporting.

c. When attempting to manually correlate a received track with a local track, the following criteria should be followed:

(1) Position: The closer the received report is to the local data, the stronger the correlation. Position comparison should include altitude for air tracks.

(2) IFF/SIF: Common IFF/SIF data provides a strong correlation comparison. Although a Mode II code is normally unique to one aircraft, the operator should be aware that the same Mode II code is sometimes assigned to multiple aircraft.

(3) Motion: A received report that also has a track travelling on the same course and speed as local data provides a strong correlation.

(4) Other Data: Identity, Platform, etc.

d. An R^2 JU makes an automatic correlation check upon receipt of each remote real-time Air or Surface (Maritime) track report or PPLI report, which is not confirmed to have an existing correlation to a local track, or immediately prior to each transmission of a local track. Such tests will compare the received remote track or JU to local tracks of the same E/C, including previously common local tracks for which own unit has R^2.

e. When a correlation is executed, systems combine the two tracks into a single track and the retained track is given the higher ID as determined by the ID difference resolution processing in paragraph 6.2.5.2. For IFF data, any nonzero Mode I, II, or III values from the retained track are to be kept in preference to IFF data from the dropped track, whilst the higher Mode IV value of the two tracks is be kept. E.g. Interrogated Valid Response is to be kept in favour of Interrogated No Response.

f. Conflicting IDs or Mode II data are restrictions against correlation, as described in paragraph 6.2.5.4.1.3. However, these restrictions can be turned off by the operator, as described in paragraph 4.3.6.5. When the ID conflict restriction is turned off, systems will keep the ID from the retained track, automatically treat the last track report on the dropped TN as an ID difference report, and provide operator alerts to resolve the conflict on the retained TN as described in paragraph 6.2.5.2.6.5. When the Mode II conflict restriction is turned off, the Mode II code of the retained TN is retained, and normal IFF/SIF difference resolution procedures as described in paragraph 6.2.5.2.6.5 can be used to resolve the conflict if it remains after the correlation.

6.2.5.4.1.2 Automatic Correlation Tests

The following briefly describes the standard position, altitude, and velocity tests applied by each JU system when testing two tracks for correlation. The parameters used in these tests may be changed based on operational or testing experience, or local operating conditions. The procedures for specifying and changing the correlation test parameters are provided in paragraph 4.3.6.

a. Position Tests. Systems use the TQ of the remote and local track being tested for correlation to determine the maximum distance between the two tracks allowable for automatic correlation. Each TQ has an associated radius of positional uncertainty. The test essentially adds the two TQs together to determine the maximum correlation distance, or the correlation "window". Very low or very high TQs are elevated or lowered for correlation purposes in order that the correlation distance not be unrealistically large or small.

b. Altitude Test. For air tracks which both have an Altitude Source of Sensor, Aircraft Automatic Altitude, or PPLI Report, automatic correlation is allowed only if the altitudes are within a certain number of feet of each other. Otherwise, altitude is not used in the correlation tests.

c. Velocity Tests. Automatic correlation is allowed only if the course and speed differentials between the two tracks are within a certain number of degrees and data miles per hour (dmh) of each other.

6.2.5.4.1.3 Correlation Restrictions and Constraints

The restrictions, constraints, rules and criteria for the resolution of dual designations are as follows:

a. Correlation Restrictions. Two reported tracks that pass the correlation tests will not be correlated automatically if certain conditions exist. These are listed below and summarised in Table 6.5. (For the restrictions marked with an asterisk (*), the tracks are not tested for correlation.)

(1) The two tracks have different Environments.*

(2) Either track is a Subsurface track.*

(3) The two tracks have conflicting basic identities, and the conflicting IDs correlation restriction has not been turned off (see paragraph 4.3.6.5). For this purpose, the basic identities are friendly (FRIEND or ASSUMED FRIEND), enemy (HOSTILE or SUSPECT), and neutral (NEUTRAL). However, a NEUTRAL and an ASSUMED FRIEND may be correlated. A PENDING track may be correlated with any Identity. (When conflicting IDs are the only correlation restriction, an operator will be alerted to attempt to resolve the conflict. When resolved, the correlation will then proceed automatically, unless the two tracks no longer meet the automatic correlation test).

NOTE: On Link 11/11B, NEUTRAL is treated as friendly.

(4) The two tracks have different nonzero IFF/SIF Mode II codes, and the Mode II correlation restriction has not been turned off (see paragraph 4.3.6.5).

(5) Either track is the subject of a pending Environment, Identity, or IFF/SIF difference resolution action. In these cases, the correlation may be performed after the difference is resolved, unless any of the above restrictions apply to the resulting Environment, Identity, or IFF/SIF.

(6) Both tracks are locally derived real-time tracks, i.e., being updated with local positional data.

(7) Either track has a strength greater than one.

(8) One of the tracks is simulated and the other is live.*

(9) Either track is already being considered for correlation with another track.

	Do not correlate if:	
Type of Restriction	**One of the tracks**	**And the other track**
Category	is: any Environment	is: any other Environment*
Subsurface	is: subsurface	is: any other track*
Identity	is: Suspect or Hostile	is: Friend, Assumed Friend, or Neutral**
	is: Neutral	is: Friend**
Mode II	has: any nonzero code	has: any other nonzero code**
Local	is: locally derived real-time	is: locally derived real-time
Strength	has: Strength greater than one	is: any other track
Simulation	is: simulated	is: live*
Dual	is: currently a dual track	is: any other track
Operational Contingency Constraint (OCC)	has: an OCC	has: an OCC

* The tracks are not tested for correlation.

** If the restriction has not been turned off (see paragraph 4.3.6.5.)

Table 6.5. Automatic Correlation Restrictions

6.2.5.4.1.4 Operational Contingency Constraints (OCCs)

When the system determines that two tracks correlate and none of the above restrictions apply the track with the highest TN will be dropped, unless any of the below OCCs apply. In these cases, the correlating JU will automatically request the other track be dropped, unless it also has an OCC. If both tracks have an OCC, the correlation is not to be executed automatically until one of the OCCs no longer exists. (There is one exception to this restriction. Some units automatically correlate an Unknown or Hostile engaged by own unit to a Friend JU or a controlled Friend. This expedites automatically breaking the engagement to prevent a potential fratricide.) These OCCs are checked automatically by systems performing automatic correlation before correlation recommendations are made to the operator.

a. The track is currently engaged; i.e., has an engagement status of assigned, tracking, firing, partially effective, or heads up, either as the target or the engaging unit.

b. The track is the subject of a pending command or mission assignment that a response (WILCO, HAVCO, CANTCO, or CANTPRO) has not yet been transmitted or received.

c. The track is a controlled track.

d. The track is an active or inactive JU.

6.2.5.4.1.5 Manual Correlation

a. Any two Air and Surface (Maritime) tracks, one of which is local or common, may be manually correlated irrespective of the positional tests and correlation restrictions above, except that two tracks are not to be correlated manually if:

(1) The two tracks are of a different environment or either track has an existing environment conflict.

(2) One is simulated and the other is live.

(3) Either track is currently engaged; i.e., has an engagement status of assigned, tracking, firing, partially effective, or heads up, either as the target or the engaging unit. (Not applicable to some nations' platforms.)

(4) Either track is the subject of a pending command or mission assignment for which a response (WILCO, HAVCO, CANTCO, or CANTPRO) has not yet been transmitted or received. (Not applicable to some nations' platforms.)

(5) Both tracks are remote.

In addition to these restrictions, system options may also restrict correlations if:

(6) The two tracks have an identity (ID) difference which constitutes a conflict.

(7) The Dropped TN is currently a controlled track.

b. An JU should not reject the manual correlation of two tracks unless it holds them to be of different environment or one to be simulated and the other live, or if it holds them both as locally derived real-time tracks. Some systems will also reject a received manual correlation if either track is a subject of an engagement message or is the subject of a pending command or mission assignment.

c. Since the OCCs in 6.2.5.4.1.4 do not constrain a manual correlation, an operator performing a manual correlation is to carefully consider the operational effects of such a correlation. Among other things, he should consider all of the OCCs, and not drop a track that has an OCC unless there are overriding operational considerations.

6.2.5.4.2 Track Decorrelation

a. Automatic decorrelation checks are performed for each local track that is a common track; i.e., local track that is correlated with a remote track.

b. The distance at which automatic decorrelation occurs depends upon the setting of the decorrelation window multiplier in paragraph 4.3.7.1. If decorrelation results in two tracks that have matching nonzero Mode II IFF codes, an operator alert may be generated. If the local track has a different nonzero Mode II IFF code than is reported for the track, an automatic decorrelation will occur in most units, unless the Mode II correlation restriction has been disabled (see paragraph 4.3.6.5).

c. Upon completion of decorrelation, the local track is declared a new detection and reported over the link with a new TN. The occurrence of numerous decorrelations is usually the result of poor or improper tracking, or many incorrect correlations. The latter suggest the possible need to adjust the variable correlation parameters.

6.2.5.4.2.1 Operator Action Following Decorrelation

Upon decorrelation, a new track with an initial ID of PENDING will be generated automatically. Various operator actions may be required in order to ensure that accurate current information is being reported for the two resulting TNs. In most cases, an operator alert will be provided in applicable JUs as a cue to the operator to consider the following actions, based on his assessment of the situation after the decorrelation:

a. If the old TN (the TN of the common track before decorrelation) is the subject of a current engagement reported and conducted by own unit, or is the target or engaging track for a current engagement reported by own unit and conducted by another unit. The operator will be alerted to break engage on the old TN if required. The operator must initiate an engagement on the new TN as appropriate.

b. If own unit is the controlling unit for the old TN, automatic decorrelation is prohibited. If manually decorrelated the operator is alerted to terminate control of the old TN if appropriate. However, the old TN must not be changed. Before decorrelating a non C^2 JU by own JU, the controller must carefully assess the situation, since he will probably be controlling the aircraft without local sensor data. Thus, he may prefer to inhibit decorrelation. To take control of the new TN the operator must initiate a controlling unit report.

c. If the old TN is the subject of a command originated by own JU or addressed to own JU, and an operator response (WILCO, HAVCO, or CANTCO) has not yet been received or transmitted, pertinent data for both the old and new TN are displayed to the operator. Any reply already initiated by the operator is withheld by the system to give the operator the opportunity to change the reply if appropriate. The operator is to consider the fact that the WILCO or CANTCO reply is relative to the old TN only, but as a remote track vice a local track.

d. If old TN has a Force Tell or Emergency status that was initiated by own JU, it will retain the Force Tell or Emergency status of the old TN, by initiating the appropriate status for the new TN.

e. If the old TN is paired or associated by own JU, the operator is alerted to terminate the pairing or association on the old TN and initiate a pairing or association on the new TN as appropriate.

f. If the old TN has been associated with an Index Number reported by a controlled aircraft, the controller of that controlled aircraft must assess whether the Index Number should remain with the old TN or the new TN, and take appropriate action.

g. If the old TN is involved in a handover, either as the aircraft being handed over or as the target of an engagement being conducted by that aircraft, the automatic decorrelation is delayed until the handover process is completed or terminated. The pending decorrelation is displayed to appropriate operators. When the decorrelation is executed, the procedure in paragraph b above should be used.

6.2.5.4.2.2 In addition to the normal correlation and decorrelation functions, there are two special cases of correlation/decorrelation that contribute to the commonality of track positional data. Both of these situations, dual designation and duplicate TN, require operator recognition and corrective actions as described below.

6.2.5.4.3 Dual Designations

6.2.5.4.3.1 A dual designation exists when the same track or point is being reported by two or more units using 2 or more different TNs. A dual designation is caused by a JU reporting a track with a new TN where one already exists. Units entering or re-entering an interface must be particularly careful that all correlations have been accomplished prior to commencing track reporting (refer to paragraph 6.2.3). Other situations likely to lead to dual designations are:

a. Units participating with poor reception capability.

b. Existence of data registration errors.

c. Areas of high track density or reporting of tracks which are manoeuvring a great deal.

d. Tracks merging.

e. Poor operator performance.

f. Misuse of data filters by one or more units.

Each C^2 JU shares the responsibility for the prevention and early resolution of all dual designations. If digital resolution of dual designation fails, resolution may be accomplished by voice coordination.

6.2.5.4.3.2 Resolution of Dual Designation

The recognition and resolution of dual designations requires all IUs to periodically compare remote tracks to local tracks. Units with an automatic correlation capability automatically attempt to recognise and resolve dual designations. An R^2 unit makes an automatic correlation check on each track for which it has R^2. The correlation process is automatically initiated on pairs of uncorrelated tracks whose positional difference is within predefined values stored in the host system. In addition, an operator can manually initiate the automated process on any two tracks. There are two methods of resolving dual designations when detected. These are Data Link Resolution and Voice Resolution. The primary method used is Data Link resolution. Voice Resolution is only used when digital resolution fails. The FTC is to ascertain if any JUs have not implemented the Correlation message. If so the FTC is to consider directing JUs to inhibit Data Link Resolution and use only Voice Resolution. When Voice Resolution is to be used, all C^2 JUs are to be directed to inhibit transmission of the Data Link Correlation message (all C^2 JUs that implement this message are also required to have the capability to inhibit its use). Correlation Message inhibition should be specified in the OPTASK LINK, under Conditional Capabilities, or directed by voice.

6.2.5.4.3.2.1 Voice or Manual Resolution

a. Voice Resolution of dual designations is necessary whenever the Data Link Resolution capability does not resolve the problem.

b. Voice Resolution procedures are specified in Table 6.6. They are carried out by the individual identified to coordinate tracks for each unit, and coordinated with the TDC via voice.

c. If the C^2 JU recognising a dual designation has R^2 for one of the tracks and does not hold an OCC for that track or a correlation restriction (see paragraph 6.2.5.4.1.4 and 6.2.5.4.1.3 respectfully), it may drop that track and make the remote track local. That action should resolve the dual designation without voice coordination. However, other JUs do not know that the track was dropped due to a dual designation and, thus, do not know to combine its data with the retained TN. Also, another JU may hold the dropped track as a common track and assume R^2, perpetuating the dual. Therefore, the JU should consider Voice Resolution of the dual designation in the same manner as specified in the following steps.

d. C^2 JU recognises dual designations:

(1) If the C^2 JU recognising a dual designation does not have R^2 for either track, he is to advise the TDC by voice.

(2) If the C^2 JU recognising a dual designation holds an OCC or correlation restriction for the track for which it has R^2, he is to advise the TDC by voice and should recommend that the other TN be dropped.

(3) Since two tracks may be manually correlated irrespective of most correlation restrictions, the C^2 JU must inform the TDC and other C^2 JUs if the correlation was manually initiated, and the reason for the manual initiation. Note that holding OCCs for both TNs is a correlation restriction.

e. The TDC is to request all JUs to drop one of the TNs based on any OCCs held by the TDC. If the TDC holds a correlation restriction, he will advise the C^2 JU reporting the dual designation that it cannot be resolved.

Step	Action
1	Any C^2 JU: Upon recognising dual designation, advise the TDC by voice.
2	TDC: Request units drop a specific track number by voice. All Units: a. Perform manual correlation and attempt track inhibit on specified TN (i.e. TN-2). b. If unable to drop the specified TN due to operational considerations, inform TDC immediately. c. If no OCC or correlation restriction is held for the TN, or if the correlation was manually initiated despite a correlation restriction, take the actions to drop reported TN. Additional voice reports not required.
3	TDC: If any unit reports that it is unable to drop the TN requested, request all other units to drop the other TN as in Step 2. All Units (still holding the first TN): Take actions specified in Step 2.
4	TDC: If any unit reports unable to drop TN as a result of Step 3, inform all units that the dual designation condition exists and will be resolved upon termination of the operational conditions (e.g., engagement status alerts, order pending, conflict, etc.) that would not allow for immediate resolution.

Table 6.6. Voice Resolutions of Dual Designations

f. All C^2 JUs are to determine if the specified TN has an OCC, or if the two tracks have a correlation restriction. If so, the TDC is to be informed immediately. If not, take action to drop the TN.

g. If any C^2 JU reports an OCC, the TDC is to request all JUs to drop the other TN, unless the TDC holds an OCC for it, and step 4 is to be repeated.

h. If the correlation cannot be completed due to a correlation restriction, the TDC is to inform all JUs that the dual designation cannot be resolved until the restriction or OCC no longer applies, unless the correlation was manually initiated.

6.2.5.4.3.2.2 Data Link or Automatic Resolution

a. Data Link resolution is accomplished using the Correlation (J7.2) message. The first C^2 JU to detect a dual designation transmits the message. Depending on system implementation, transmission of this message is either automatic or by operator action. The Correlation message identifies the TN to be retained (TN-1) and the TN to be dropped (TN-2). It also indicates whether a reverse correlation (reversal of TN-1 and TN-2) is acceptable, or that the correlation was manually initiated and therefore cannot be reversed. The determination of TN-1 and TN-2, and whether a reverse correlation is acceptable, are automatic system functions which are performed without operator intervention, depending on system design and mode of operation. Systems utilise the correlation restrictions and constraints in paragraph 6.2.5.4.2.3 to make these determinations.

b. Under certain circumstances, in an interface with C^2 JUs or Link 11/11B IUs that have elected not to implement the Correlation message, Data Link Resolution may not work. This will occur whenever the TN requested to be dropped (TN-2) or reversed (TN-1) is reported or held in common by a

PU/RU or a nonimplementing C^2 JU. The track to be dropped will either be dropped and R^2 picked up by a PU/RU or nonimplementing JU, or it will never be dropped. The dual designation will not be resolved using this method and must be resolved by voice.

c. C^2 JUs capable of reporting air or surface tracks are required to implement the Correlation message for transmission and reception.

d. The Data Link Planner or TDC is to ascertain if any C^2 JUs have not implemented the Correlation message. If so the planner or TDC is to consider directing C^2 JUs to inhibit data link resolution and use only Voice Resolution. All C^2 JUs that can transmit the Correlation message are required to have an operator selectable capability to inhibit its transmission. However, the planner or TDC may decide to allow Data Link Resolution even if some C^2 JUs do not implement the Correlation message. The primary disadvantage of doing so is that a non-implementing JU which has R^2 for TN-2 will not know the correlation has been recommended and will continue reporting TN-2, probably delaying resolution of the dual longer than if voice had been used initially.

6.2.5.4.4 Reception of Correlation Request

a. Systems, which receive the Data Link Correlation message automatically, process the request to determine if it should be accepted, rejected, or reversed. The correlation is accepted and executed automatically unless the conditions for rejection or reversal specified in paragraph 6.2.5.4.4.d below exist. The system acts without prompting, only alerting the operator when operator action is require.

b. Systems, which do not implement the Data Link Correlation message, may provide some degree of assistance to the operator when the operator indicates a voice request for correlation has been received, depending on system design. However, the operator is to respond by voice to reject or reverse a correlation request. Therefore, the following procedures prescribe JU actions that may be performed automatically in some JUs, but manually in others.

c. Upon receipt of a Data Link or Voice Correlation request, the receiving JU has three options:

(1) Accept the correlation.

(2) Reject the correlation.

(3) Propose a reverse correlation.

d. Unless the correlation was manually initiated, it is rejected if any of the restrictions in paragraph 6.2.5.4.1.3 applies, or if own JU would decorrelate the two tracks. In the latter case the JU is to report the new correlation. In the event there is an OCC on TN-2 as specified in paragraph 6.2.5.4.1.4, but a reverse correlation is acceptable, the JU should propose a reverse correlation as opposed to rejecting the correlation request. A reverse correlation is a response to the correlation request that proposes that the dropped and retained TNs be reversed. In the absence of any restrictions, the JU is to accept the normal correlation, and, if own JU has R^2 for TN-2, drop TN-2 from the interface.

6.2.5.4.5 Dual Designation of Reference Points

A dual designation exists when two or more points with different TNs represent the same point type at the same geographic location. Dual designations of points are to be resolved by voice coordination between the reporting JUs and the TDC. Resolution is to consist of establishing a common point. The Data Link Correlation message is not used to resolve dual designation of points.

6.2.5.4.6 Dual Designation of JUs

a. A dual designation exists when an JU is reported as both a track/point and an JU with different TNs.

b. When a dual designation exists, it is to be resolved in the same manner as dual designation of two tracks. The JU is not to be dropped, unless the correlation was manually initiated.

6.2.5.4.7 Duplicate Track Number

A duplicate TN exists when the same TN is being used by two or more units for two or more different tracks. The most common cause of duplicate TN is the failure of two or more systems involved to track two targets accurately through a merge and a subsequent separation. Other situations likely to lead to duplicate TN are:

a. Loss of data communication between units.

b. Erroneous correlation (either automatic or manual).

6.2.5.4.7.1 Detection

Dual designation is comparatively easy to recognise since one track is being reported to the interface using two or more different TNs. In the duplicate TN situation, one TN is being used to report two or more different tracks. The non-reporting unit(s) having common track may have limited or no indication when a duplicate TN situation occurs. Manual operator recognition is hampered or may be impossible since displays are normally biased in favour of, or consist exclusively of, local data. Some systems provide decorrelation processing to alert the operator and/or to resolve duplicate TN circumstances. Recognition of a duplicate TN by units not having common tracking is only possible when observing significant data changes when R^2 changes. Even then, these will generally go unnoticed with a normal track load in spite of major position or other data changes. In some instances, duplicate TNs may appear to some JUs as dual designations while other units may see significant difference of position in the two tracks. In these cases both parties should be alerted to the possibility that duplicate tracking may be occurring, particularly where one of the units does not perform decorrelation processing.

6.2.5.4.7.2 Automatic Resolution of Duplicate Track Number

Some C^2 JUs have an automatic decorrelation capability which will detect, resolve and eliminate some duplicate TNs. Decorrelation checks are performed for every local track for which remote track reports are received. When decorrelation occurs, the local track is assigned a new TN, and the remote track retains the old TN. Automatic decorrelation occurs:

a. When the two tracks have different IFF/SIF Mode II codes. The operator is alerted in this situation.

b. When more than a number (depending on the system) of data miles separate the two tracks. If their IFF/SIF Mode II codes match, the operator may be alerted.

c. When other system parameters are met for automatic decorrelation.

6.2.5.4.7.3 Manual Resolution of Duplicate TNs

Timely elimination of duplicate TNs associated with hostile tracks is essential for threat warning purposes. In situations other than where the two tracks have different Mode II codes, automatic decorrelation requires a relatively large distance between the local and remote track positions. In many cases, therefore, duplicate TNs may require detection and resolution by manual procedures, to avoid confusion of the tactical picture. Any unit observing a jumping track should attempt to determine the data sources of the jumping track and notify at least one of the units involved. The unit(s) so advised should take appropriate action as indicated in the following procedure or resolve with other involved units as to which unit(s) will initiate action to assign new track numbers:

a. Any IU that has reason to believe that one of its common tracks is involved in a duplicate TN situation should immediately initiate action to assign a new TN to its local data.

b. If operational circumstances require, a unit may coordinate by voice with conflicting units to determine which of the two tracks being reported is to retain the TN in use.

c. If a track flagged with a Special Processing Indicator (SPI) is involved in a duplicate TN situation, special procedures may be necessary.

6.2.5.5 Pointers

The pointer (J7.3) message provides a capability for an operator to transmit a specific geographic location to another C^2 JU over the data link. A pointer may be used by an operator at one C^2 JU to direct another C^2 JU operator's attention to a track, point or specific geographic area. It may be addressed to a specific unit, several specific units or to the collective address. By specifying the Pointer Action Value, a pointer can be directed to one or more operator positions, according to function, at the receiving C^2 JU. Pointers are not assigned TNs and will usually require amplification by voice. Use of the pointer capability by nonC^2 JUs on the Control net is covered in paragraph 6.4.4.4.

6.2.5.6 Special Processing

6.2.5.6.1 Certain national systems provide surveillance and warning information of a particularly sensitive nature. Data links, including Link 16, make special provision for the control of data distribution from such systems by use of a Special Processing Indicator (SPI). The SPI is used to protect the source of the data and must not be used for any other purpose. In particular, setting the SPI will not permit any other field of the message to be encoded differently from that defined in the Link 16 message standard. The setting of the SPI by originating units will be in accordance with national requirements; however, when the SPI is set the following procedures apply:

a. All surveillance, warning and amplification data flagged with the SPI are classified SECRET and are to attract the protection and handling procedures commensurate with this classification.

b. Care must be taken to ensure that any transmission by voice of data flagged with the SPI is made only over secure voice circuits which afford the necessary protection.

c. Any unit wishing to record data exchanged on the interface must ensure that, if SPI data is present during the period of recording, the recorded material is classified and handled appropriately.

d. When a C^2 JU assumes R^2 for a SPI track, the SPI status will automatically be cleared unless the R^2 unit is the source of the SPI data, or the operator takes action to retain the SPI IAW national requirements.

6.2.5.6.2 Data Constraints

Data flagged with the SPI must not be transmitted over a data link if any unit on the interface is unable to adhere to the following rules:

a. Data flagged with the SPI must be transmitted on secure communications links only.

b. Data flagged with the SPI must not be forwarded on to an unsecure link.

Operators should note that the setting of Force Tell or Emergency alerts on SPI data will override the above SPI data transmission constraints.

6.2.5.6.3 Setting of SPI on EW Data

Special rules are required for the setting of the SPI on EW data. EW fixes, EW AOPs and EW tracks are usually formed from a number of contributing EW reports, some of which may have the SPI set. The setting of the SPI in a report of a fix, AOP or an EW track should be at the discretion of the reporting unit. However, if all contributory EW reports have the SPI set, the resulting fix, AOP or EW track must also be transmitted with the SPI set.

6.2.5.7 Filters

Two types of filters are used by a JU, message label/sublabel filters and data filters, as described below.

6.2.5.7.1 Message Label/Sublabel Filters

Message label/sublabel filters may be used to inhibit overloading of the terminal-to-host interface, or to reduce demands for TDS processor time on a JU. The message label/sublabel filter will select messages to be filtered by the Link 16 label and sublabel fields. A terminal message label/sublabel filter, once initialised, will prevent any message with the appropriate label/sublabel from being passed to the host TDS, even if the message has the Emergency or Force Tell Indicator set. The filter cannot be overridden; it can only be changed by re-initialising the terminal. The message label/sublabel filter is a separate category of filter and its use is not restricted by the rules of any other category of filter. Use of these filters is restricted to receive only filtering for those messages that the JU does not implement due to the mission or particular capabilities/restrictions of the platform.

6.2.5.7.2 Data Filters

Data filtering is the process of inhibiting data from transmission on a data link or the process of deleting data received on a data link prior to entry into a unit's data base. Filters under operator control can be used to:

a. Avoid overloading a unit's database or data links.

b. Control transmission and reception of SPI, exercise and simulated data.

c. Tailor data exchange to area of responsibility.

6.2.5.7.2.1 Data Filter Management

Initial transmission filter assignments may be specified in the OPTASK LINK. Data transmission filters may be managed through data filter management requests and reports (J7.6); these can be used to request or report implementation or deletion of specific filters. In addition, voice coordination is required for data filter management on the interface.

6.2.5.7.2.2 Types Of Data Filters

Each JU has the capability to implement certain types of filters. The four broad types of filters are:

a. Security (SPI)

b. Simulation

c. Identity

d. Environment/Category (Env/Cat)

e. Geographic

Geographic filters must specify whether filtering is to be conducted inside or outside the defined area.

6.2.5.7.2.2.2 Multiple Filters

Filters may be applied in combination. However, when reporting a combination of SPI and Simulation filters, the settings are to be interpreted independently, not cumulatively. That is, when both the SPI and Simulation Filter Indicators are set, then filtering is to be applied to tracks, EW Products, Reference Points which have either the SPI or the Simulation Filter Indicator set.

The following are examples of multiple filter settings:

a. As applied to Tracks:

   (1) If any or all of the Env/Cat Filter Indicators are set and no other Filter Indicators are set, then all tracks of the indicated Env/Cat are filtered.

   (2) If any or all of the Env/Cat Filter Indicators are set and the Security (SPI) Filter Indicator is set, then any tracks of the defined Env/Cat with Special Processing status are filtered.

   (3) If any of the ID Filter Indicators are set and the Security (SPI) and the Simulation Filter Indicators are set, then any tracks of the defined Identity categories with Special Processing status or Simulation status are filtered.

   (4) If any or all of the Env/Cat filter Indicators are set and the Geographic Area Filter Indicator is set, and the Security (SPI) Filter Indicator is set, then any tracks of the defined Env/Cat within/out the defined geographic area with Special Processing status are filtered.

b. As applied to Reference Points:

   (1) As Reference Points have no Env/Cat or ID, point filters will be requested/reported in separate Filter Management messages to tracks and EW Product information. If the Reference Point Filter Indicator is set in a message, then the only other filters that may be set in that message are the SPI and Simulation Filter Indicators.

   (2) If the Reference Point Filter Indicator and the Geographic Area Filter Indicators are set in a message, then all points within/out the area, all

lines with all points within/out the area, and all areas completely within/out the area will be filtered.

c. As applied to EW Product Information:

(1) EW Product Information filters will be requested/reported in separate Filter Management messages. When the EW Filter Indicator is set, then all other Filter Indicators in the same message apply only to EW Product Information.

(2) The exception to the above is when the EW Filter Indicator is not set but the Unknown Env/Cat Filter Indicator is set. Under these conditions EW product information of Unknown Env/Cat will be filtered, in addition to any other valid filter combination.

(3) If the EW Filter Indicator and the Geographic Area Filter is set in a message, then all EW fixes and tracks within/out the area , and all EW AOPs having their centre within/out the area and all EW LOBs with their origin within/out the area will be filtered.

6.2.5.7.2.2.3 Moving Filters

It is possible to establish and report moving filters. Such filters may be slaved to a particular TN, by setting the slaved indicator in the Filter Management message.

6.2.5.7.2.3 Transmit Data Filter Control

Filters are under operator control and may be used to selectively inhibit data flow.

a. Restraint must be exercised in the use of data filters. Filter implementation should be a coordinated action and directed in the OPTASK LINK. Any system which filters tracks/JUs on receipt must establish a transmit filter that duplicates or is more restrictive than the receive filter, to prevent dual designations.

b. Filters are terminated by operator action and must be reported as such on the interface. Since filters inhibit data from entering a system’s database, C^2 JUs must treat filter deactivation much the same as initiation of surveillance operations, e.g. correlation and minimum wait time before resumption of transmission (see paragraph 6.2.3.2).

6.2.5.7.2.4 Data Filter Restrictions

Unless simulated or exercise, the following data shall not be filtered:

a. IU (PU, RU, FPU, FRU and C^2 JU) position messages.

b. Any track or point indicating Emergency or Force Tell Alert status.

c. Emergency Points.

d. Data Management, controlling unit status and associated messages related to a track, point or unit which is not filtered.

e. The Correlation message is not to be inhibited by any filter.

6.2.5.8 Alerts

6.2.5.8.1 Track Alerts

A track alert provides a method of indicating the presence of a track with an emergency or with a condition of particular interest to units within the interface. Alerts are of such importance that their receipt must be ensured. However, tactical data systems have a finite track capacity that may be saturated by receiving all messages with the Force Tell or Emergency Indicator set. Operators should be aware that there are nonC^2 JU platforms that do not process the Force Tell or Emergency Indicators. Track alerts will be forced through all filters, including those established for SPI data (dealt with in paragraph 6.2.5.6).

6.2.5.8.1.1 Types of Track Alert

There are two types of alerts:

a. Emergency Alert - An operator or automatic action that indicates the existence of a life-threatening condition that requires immediate action or assistance.

b. Force Tell Alert - An operator action that indicates that a condition exists that is sufficiently important to ensure that all systems operating within the interface are apprised of the presence of the track. However, the effectiveness of Force Tell status when applied to a track depends on its use being strictly controlled by the operator.

6.2.5.8.1.2 Use of Track Alerts

Any C^2 JU may initiate or terminate a track alert on any track on the interface other than an active JU. If a C^2 JU loses all contact with a friendly track and believes that an emergency situation exists, (e.g. receipt of PPLI with Bailout Indicator set), an emergency point must be established at the last reported track position. (Emergency points are dealt with in paragraph 6.2.4.2.2). NonC^2 JUs can only report an alert status on themselves. When the alert condition has cleared, the track alert must be terminated by operator action.

6.2.5.8.2 Alert Indicators for Reference Points, Lines and Areas

6.2.5.8.2.1 Any C^2 JU may initiate or terminate a force tell status on any point, line or area being reported on Link 16. Emergency status cannot be applied to an existing reference point/line/area; however, emergency points may be established to report a geographical location requiring search and rescue operations (see paragraph 6.2.4.2.2).

6.2.5.8.2.2 A JU initiating a force tell alert on a slaved reference point or area also initiates an alert on the Related TN, as specified above, if the Related TN does not already have an alert set. When the alert is terminated for the reference point or area, the JU terminating the alert also terminates the alert for the Related TN, unless the Related TN had the alert set prior to the slaved point or area alert being initiated.

6.2.5.8.2.3 A JU terminating a force tell alert on a track also terminates the force tell alert on any reference point or area that is slaved to the track.

6.2.5.9 Track Association

The Track Association (J7.7) message is a tool which may be used by the operator in a C^2 JU to indicate that two TNs, or the information concerning two TNs, are associated with the same contact (e.g. an EW LOB and a track). A track association does not indicate that the two TNs are correlated. Once established, it is the responsibility of the originating unit to terminate the association when it is deemed to be of no further use on the interface. If either data involved in the association is dropped, the association is assumed to be terminated.

6.2.6 Ballistic Missile Data Exchange

Ballistic missile tracks and points are managed and reported on the Surveillance net using the applicable procedures discussed in all sections of this chapter. There are several unique reporting procedures which are discussed in this section.

6.2.6.1 Track Reporting

Ballistic missile track reports (J3.6) provide the positional data, velocity and error estimate data with a precision required for engagements. These reports also include the time of measurement and are not extrapolated by the C^2 JU to time of transmission. The track report also includes a TQ field. A track report is not initiated if the predicted time to impact is less than 16 seconds or the altitude is less than 8 data miles from the estimated impact point.

6.2.6.2 Launch Point Reporting

The Reference Point message (J3.0) is used to report the actual or expected launch point. A time function field is provided to allow reporting of past, present or future launch points. The message also provides the capability to relate the launch point to a ballistic missile track. The positional accuracy of the data is defined as an area within which there is a 95% probability that the point is located. A missile launcher will be reported using the appropriate J-series track report message.

6.2.6.3 Impact Point Reporting

The Reference Point message (J3.0) is also used to report the actual or expected impact point and time. The message provides the capability to relate the impact point to a ballistic missile track. The C^2 JU with R^2 for the ballistic missile track also has R^2 for the related impact point. The positional accuracy of the data is the same as for launch points.

6.2.6.4 Lost Track

A ballistic missile track is considered lost when the JU with R^2 does not receive any local sensor data since the last transmitted update, or the C^2 JU with R^2 uses own criteria to determine that the track is lost. When this occurs, a ballistic missile track report with Lost Track Indicator set to "Lost Track", containing data held at the time of last sensor contact, is transmitted periodically unless another JU assumes R^2 or the estimated time of impact has passed.

6.2.6.5 Data Update Request (DUR)

The DUR (J7.1) provides the capability to request ballistic missile track data either with or without error estimate data included. The inclusion of error data requires more transmission time slots; therefore, it should be requested only when needed. The data may be requested from/provided by the C^2 JU with R^2 only.

6.2.7 <u>Electronic Warfare Data Exchange</u>

6.2.7.1 General

Electronic warfare (EW) data will be exchanged by Link-16 units in two forms. Evaluated EW data will be available to all units operating on the Surveillance Participation Group (PG). Parametric data will be available to those EW capable units operating on the Electronic Warfare PG. Also, units operating on the EW PG can exchange EW control and coordination orders (J14.2).

6.2.7.1.1 EW Terms

Operators involved in combined operations must note that the US operators use some EW terminology that differs from that used by other NATO operators. The equivalent terms for the basic types of EW are shown below.

NATO Terms	US Terms
Electronic Countermeasure (ECM)	Electronic Attack (EA)
Electronic Counter-Countermeasure (ECCM)	Electronic Protection (EP)
Electronic Support Measures or Electronic Warfare Support Measures (ESM)	Electronic Warfare Support (ES)

Table 6.7 EW Terms

6.2.7.2 Products of EW Surveillance

The products of EW surveillance are lines of bearing (LOB), fixes and areas of probability (AOP), all reportable on the Surveillance PG.

6.2.7.2.1 Lines of Bearing

Lines of bearings are derived from ESM, jam strobes, or radio direction finding. Every LOB reported on the interface will have its own track number.

6.2.7.2.2 EW Fixes

An EW fix results from the crossing of two or more LOBs which the operator deems to originate from the same object. EW fixes developed from the crossing of LOBs will be issued a new track number and will not inherit the track number of a LOB. However, an EW fix that is developed from an AOP will inherit the track number of the AOP from which it was derived. Units originating LOBs, that are used by own unit or another unit to create an EW fix, should stop transmitting the LOB after that EW fix has been created. The EW Fix report may also be used to announce the deployment by own forces of active electronic decoys. Information provided will include position of the decoy, Identity, Platform and, for programmable decoys, the Emitter Number.

6.2.7.2.3 Areas of Probability

An AOP is an area in which there is a 95% probability of locating a particular emitter of interest. AOPs can be built from LOBs, analysis of EW fix data, other organic or non-organic data or a combination of all. An AOP will be reported by the originator with a time indicating when the AOP was valid (i.e. there was a 95% chance of locating the emitter within the AOP at the time indicated). An AOP, that is generated from the crossing of LOBs, will be given a new track number by the tactical data system (TDS), not inherit the TN of one of the LOBs. Also, an AOP that is derived from analysis of two previously reported EW fixes with two different TNs, will likewise be issued a new track number by the TDS and will not inherit the TN of one of the fixes. However, when a single EW fix is changed to an AOP for whatever reason, that AOP will automatically adopt the track number of the EW fix that was transformed. Units originating LOBs, that are used either by own unit or another unit to create an EW AOP, should stop transmitting the LOB after that AOP has been created.

6.2.7.3 Electronic Warfare Surveillance Information Management

6.2.7.3.1 Units that originate EW products (LOBs, AOPs, fixes) are solely responsible for product updating or dropping them on the interface.

6.2.7.3.2 Data Update Request

Units may receive updated ECM, ESM or other EW parametric data on an individual TN by transmitting a "Data Update Request" on the TN of interest. Units responsible for EW data respond automatically to such requests. Use of this feature should be reserved for situations requiring immediate updates of essential EW information to avoid unnecessary link loading.

6.2.7.3.3 EW Product Correlation and Association

EW AOPs may be correlated with active real-time surveillance tracks, but this action causes the EW product information to be dropped from the link. EW product information can be associated with active, real-time surveillance tracks. The advantage of association is that the product information is not dropped from the interface.

6.2.7.3.4 An operator, who has originated EW product information, receives an alert that an attempt is being made by another unit to correlate a real-time track with his EW product. The EW product originator has the option to accept or reject the correlation attempt. If he accepts the correlation, his system will cease reporting the local EW products. If he rejects the correlation attempt, a rejection report is automatically transmitted and EW product reports continue to be reported.

6.2.7.3.5 Reporting the Origin of a LOB

An EW unit can report the point of origin of a LOB in any of three different ways:

a. By designating own unit as the origin.

b. By designating another existing unit, track or point of origin.

c. By filling in a lat/long for origin of point.

6.2.7.3.6 Dropping EW Data

As the originator of an EW product, any action to cease reporting or dropping an own unit's EW track will result in other units receiving a drop track message on that TN. EW products, remote or local, may be automatically purged from the interface based on system criteria. However, some systems can prevent purging of this remote data by designating the TN as having special interest.

6.2.7.3.7 EW Information Difference Reporting

Operators may challenge information received in remote EW fix or AOP reports using Information Difference Reports and Change Data Orders as for surveillance tracks. (See paragraph 6.2.5.2).

6.2.7.4 Electronic Warfare Participation Group

A dedicated NPG may be established for the correlation, coordination and analysis of unevaluated, parametric, electronic emission data. The Electronic Warfare NPG, if employed, allows EW operators to exchange parametric data, and send and receive EW commands. Unless transformed into evaluated EW products (as described in Para 6.2.6.2), EW NPG exchanges should not appear on system displays that are dedicated to surveillance information.

6.2.7.5 Reporting Parametric Data

6.2.7.5.1 Parametric EW reports (J14.0) on ESM and ECM contacts may be transmitted automatically. Alternatively, the operator may transmit only information that he selects for exchange. Reports that are transmitted onto the link are under the direct control of the originator and cannot be dropped or manipulated by another unit.

6.2.7.5.2 To update EW data on a fix, AOP or LOB that is being reported on the surveillance PG, the operator must take action to associate the new data with the track number of the existing EW product. Sending parametric data on another unit's track does not affect R^2 of the existing track.

6.2.7.5.3 Parametric reports are transmitted automatically at least once every 48 seconds although operators can manually transmit as often as desired. The change of certain emitter data, however, may cause a report to be automatically transmitted. Automatic transmission takes place when changes to the following occur:

- Fix/Bearing Description
- Special Processing Indicator
- Broad Classification
- Specific Type
- lock-on
- speed >50kt air; 5kt other
- emitter number
- platform
- Threat Evaluation
- Environment/Category
- Amplifying Characteristics
- Frequency >1%*
- wartime reserve indicator
- nationality/alliance
- PRF/PRI >1%*

(* These criteria may be set as desired by the operator)

6.2.7.6 EW Control/Coordination Procedures

EW control and coordination functions provide the capability to control JUs participating in the EW PG, to respond to requests/orders and to coordinate EW activities among participants. EW requests/orders should be tagged for execution at a specific time or flagged for immediate action. Requests/orders will also carry a priority number for those units receiving more than one EW assignment. While systems and implementations will vary, EW Command & Control capabilities available are summarised in Table 6.8, and detailed operating procedures for restricted frequency control are provided below.

- Request Periodic Report.
- Request Manual Evaluation.
- Request Directed Search.
- Cease Report.
- Emitter Association.
- Parameter Association.
- No Find.
- Evaluate Track.
- Direction Finder (DF) Request.
- Jamming Request.
- Deploy Decoys.
- Parametric Data Update Order.
- Set Emission Control (EMCON).
- TN, Reference/Index Number Correlation.
- Request Automatic Evaluation.
- Request Update and Watch.
- Cancel Request.
- Emitter Evaluation.
- Disassociation.
- Response to an Electronic Warfare Request.
- Evaluate Sector.
- Restricted Frequency Control.
- Parametric Data Update Request by TN.
- Parametric Data Update Request.
- Request EW System Status.
- Implement Cooperative Countermeasures.
- Intercept-to-Emitter Association.
- Emitter-to-Platform Association.

Table 6.8. EW Command and Control Functions

6.2.7.6.1 Restricted Frequency Control

The three EW orders "Protect", "Guard", and "Taboo" direct varying degrees of protection against friendly interference to specified frequencies or frequency ranges, for varying reasons. The orders may also specify the time of commencement and duration of the protection. They are briefly defined in ACP-167(F) under the terms Protected Frequency, Guarded Frequency, and Taboo Frequency, respectively. The authority for use, and the specific actions to be taken upon receipt of any of these orders, are functions of EW doctrine and local EW procedures, not the data link operating procedures. Receiving TDS operators need only alert appropriate local EW/Communications personnel that the order has been received. Due to the criticality of the orders, this alert should be made on an urgent basis. If the received EW order requires an operator response, the TDS operator should transmit a WILCO before informing appropriate authority, unless previously directed otherwise, is directed otherwise by local authority present at the time of receipt, or the ordered commencement time is sufficiently far in the future to permit a short delay before responding. For further clarification, the following unclassified explanations of the three terms are provided:

a. Protected - Those friendly frequencies used for a particular operation, identified and protected to prevent them from being inadvertently jammed by friendly forces while active EW operations are directed against hostile forces. These frequencies are of such critical importance that jamming should be restricted unless absolutely necessary or until coordination with the using unit is made. They are generally time-oriented, may change with the tactical situation, and must be updated periodically.

b. Guarded - Enemy frequencies that are currently being exploited for combat information and intelligence. A GUARDED frequency is time-oriented in that the list changes as the enemy assumes different combat postures. These frequencies may be jammed after the commander has weighed the potential operational gain against the loss of technical information.

c. Taboo - Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces. Normally these include international distress, safety and controller frequencies. These are generally long-standing frequencies. However, they may be time-oriented in that as the combat or exercise situation changes the restrictions may be removed.

6.2.7.7 EW Report Termination

Prior to the execution of a scheduled termination of Link-16 operation or withdrawal as an EW participant, the operator should send drop track reports on all own-unit originated TNs that are being reported on the EW PG. If the unit is also reporting that same information, using the same Reference TN, on the Surveillance PG, then drop track reports should also be sent on the Surveillance PG.

6.2.8 Threat Warning Information

6.2.8.1 General

General threat warning data is exchanged within surveillance as previously described in this volume. However, immediate type threats are reported via the J15.0 Threat Warning message. The message should include as a minimum the following information about the threat: location, environment/ category, threat type, threat posture, course, speed, altitude and the friendly unit targeted by the threat.

6.2.8.2 Immediate Threat Reporting

The Threat Warning message is originated by any JU having knowledge of an immediate threat against another friendly unit. This message can be initiated by C^2 JUs even though the threat track is not currently being reported on the interface. However, if the track is not currently on the interface, the Threat Warning track should immediately be followed by a normal surveillance track. NonC^2 JUs can only initiate a Threat Warning message if the Threat TN is already being reported on the interface. In all cases the threat track and the surveillance track should have the same TN. When the threat is no longer deemed to be immediate or is no longer a threat, it is cancelled by sending a Threat Warning Cancellation. The Threat Warning Cancellation has no bearing on the surveillance track of the same TN.

6.2.8.3 Threat Warning Addressing

When possible the Threat Warning message should be addressed to the unit responsible for the protection of the targeted unit (this may be the unit itself). The message is sent to the collective address when:

a. The originator is in doubt as to the unit assigned to protect the targeted unit, or

b. When the targeted unit is not a JU, or

c. The threat is general in nature and applies to many or all JUs and friendly tracks/points.

d. It is tactically desirable for multiple platforms to be aware of a threat against an individual platform, e.g. High Value Assets.

Originators should be aware that some nonC^2 JUs may only have the capability to receive and display Threat Warning messages where own unit is specified as the targeted friendly unit.

6.2.8.4 Relating Threat Warning Information

Threat warning of affected targets or tracks consists of coupling the Targeted TN with the Threat TN. As such, the Targeted TN must be an active surveillance track, point, or PPLI (except as described in 6.2.8 above).

Since the capability exists in the Threat Warning message to report threat to friendly couplings between two TNs regardless of environment/ category, the Threat Warning message should not be used to report normal pairings or engagements.

6.2.8.5 Reception of a Threat Warning

Upon receipt of a threat warning, it is up to the receiving unit to determine what action is appropriate. For example, a nonC^2 JU may receive a collectively addressed threat warning that may or may not specifically apply to own unit. Threat type, location, weapon and all appended information should be used to determine what (if any) action is to be taken.

6.3 WEAPONS COORDINATION AND MANAGEMENT

6.3.1 General

Weapons Coordination and Management is the function of exchanging necessary information between C^2 JUs to effect weapons employment and to prevent mutual interference during their employment. It enables the Operational Commander to direct the activities of controlling units and the employment of weapons systems within his area of responsibility. This function consists of the exchange of certain designated commands, weapon status information, and engagement status information. This section also considers the exchange of platform and system status information which applies to all JUs.

6.3.2 Commands

6.3.2.1 The Command (J9.0) message provides the means for directing weapon system engagements and issuing threat warning conditions (white, yellow, red) and weapon condition orders (free/tight). Annex C identifies all commands available for use on the interface with standard definitions. In addition to the commands of Hold Fire and Salvo/Clear Aircraft, other universally implemented commands are highlighted.

6.3.2.2 Origination of Commands

Hold Fire and Salvo/Clear Aircraft are emergency commands that may be originated by any C^2 JU. All C^2 JUs participating on the interface should have the capability to reply to commands addressed to them. Certain commands, i.e. Weapons Free, Weapons Tight, Hold Fire, Cease Fire and Salvo/Clear Aircraft, may be addressed to all units by means of the collective address. When this occurs, no reply will be sent. Commands may be sent to individual units in which case, replies and responses will be exchanged. (Receipt/Compliance is covered in paragraph 2.3.5.9).

6.3.3 Reporting of Friendly Status

6.3.3.1 In addition to the track reports discussed in the previous section, additional reports can be made on friendly platforms. The type of reports which can be transmitted are:

a. Platform and Systems Status Reports (J13-series).

b. Engagement Status Report (J10.2).

c. Controlling Unit Report (10.5).

d. Pairing Report (J10.6).

Friendly status reports, may be initiated manually by operator action or automatically, depending on the extent of the individual system's implementation. Special uses and interpretations for these reports are discussed in the following paragraphs.

6.3.3.2 Platform and System Status

6.3.3.2.1 Platform and system status information is reported by each JU for its own system. The information reported includes:

a. Operational status.

b. Equipment status.

c. Ordnance status.

d. Fuel status.

This information is reported on re-entering the network, by periodic updates, when significant information changes and when requested by a Data Update Request. C^2 JUs requesting status information on nonC^2 JUs should address the Data Update Request to the controlling C^2 JU.

6.3.3.2.2 A controlling C^2 JU should report status information for those nonC^2 JUs and supporting units under its control which do not report their own status directly on the link. This will include any controlled units operating in Conditional Radio Silent mode.

6.3.3.2.3 Airfield Status

6.3.3.2.3.1 Airfields that are capable of reporting own status, and selected C^2 JUs, will report the status of designated airfields and carrier (CV) flight decks. Which JUs report the status of which airfields and CV flight decks will be determined either by standing SOPs or as directed by the Tactical Commander. Using this message, airfield JUs and selected C^2 JUs can broadcast the following information to other JUs:

a. Airfield/CV flight deck air raid state, SHORADEZ status, NBC contamination state, crash services availability, QFE/QNH and, if known, the airfield ICAO code.

b. Runway information including active runway direction, length in metres, status, GCA/ILS precision approach aids, lighting, barriers, braking action, visual range, etc.

c. CV flight deck information, including designated flying course and landing approach condition.

d. Weather data including wind speed, gust and direction, cloud cover and height, visibility, base weather and wind shear indicator.

e. Support information including the capability to rearm with munitions, nitrogen and liquid oxygen availability.

6.3.3.2.3.2 The Time of Observation set in the message applies to the weather data only and will be the time that the weather observation was taken. If no weather data is included in the message, the time of observation will be set to No Statement. An indication will be provided when more than 60 minutes have elapsed since the Time Of Observation.

6.3.3.2.3.3 A JU could receive airfield status messages on the same airfield or CV flight deck from more than one source. In this case the information stored will be that of the own unit status report or, if only third party reports are available, the latest received message, with the exception of weather data. Weather data with the latest time of observation will be retained.

6.3.3.2.4 Reporting of Artificial Data for Exercise Purposes

6.3.3.2.4.1 The reporting of artificial platform and system status data may be authorised for exercise purposes. The decision to prohibit or allow artificial data reporting should be agreed prior to commencement of an exercise and should be promulgated in the OPTASK LINK. The reporting of artificial data is subject to the following procedures:

6.3.3.2.4.2 If a unit is being reported with exercise status, operators may elect to report artificial values for the associated platform and system status information for exercise purposes only. Operators must not report artificial data without first assigning exercise status to the unit to which the data relates. Artificial values may be reported for the following data:

a. Operational Capability.

b. Specific Type/Site Type.

c. Command and Control status information.

d. Equipment status information.

e. EW status information.

f. Stores status information.

g. ASW status information.

6.3.3.2.4.3 Artificial values must never be reported for the following data:

a. Fuel and Fuel Function data (applicable to air platforms only).

b. Time Report Function, Minute and Hour.

c. Flight Deck Status and Landing/Approach Condition (applicable to aircraft carriers only).

d. Airfield Status data.

6.3.3.2.4.4 When artificial data reporting has been authorised, operators receiving platform and system status information on a unit with exercise status should assume that all platform and system status data pertaining to that unit are artificial and for exercise purposes only (with the exception of those data identified in paragraph 6.3.3.2.4.3 above for which real data will always be reported). On termination of exercise status, all artificial data will be cleared immediately and replaced with real data as they become available.

6.3.3.3 Weapon Engagement Status

6.3.3.3.1 A C^2 JU is responsible for reporting the status of all engagements of air, surface, subsurface and space targets by friendly weapon systems under its control. The tracks of both the friendly weapon system and the target it engages must already exist on the interface. The friendly weapon system can be a JU, a supporting unit or a controlled aircraft. An "engagement" reporting the deployment of an electronic decoy will have the Target TN set to the TN of the threat missile, not to the TN of the threat missile carrier.

6.3.3.3.2 Once initiated the controlling C^2 JU must report the progress of the engagement until it is concluded or the engagement is broken. If control is terminated, the controlling C^2 JU must report a status of either Effective/Target Destroyed/Grand Slam if the engagement has been successfully concluded or Engagement Broken to clear the reported engagement from the interface. Other C^2 JUs may transmit a Data Update Request to obtain the latest information on the weapon engagement status of any currently reported engagement from the controlling C^2 JU. Annex C identifies all weapon engagement statuses available for use on the interface with standard definitions and highlights those which are universally implemented.

6.3.3.4 Controlling Unit Status

All C^2 JUs performing an Air Control function for a designated air track will report its status as controlling unit for that track to the interface. The voice call sign of the controlled track may also be transmitted. This information is reported by a C^2 JU when it assumes control of an aircraft and is updated periodically until control is transferred to a new controlling unit or until control is terminated. In the latter case, the controlling C^2 JU must report the termination of control responsibility for the designated air track.

6.3.3.5 Pairing

6.3.3.5.1 A pairing is used to establish an operational relationship between the two subject TNs, but should not be used to indicate any form of engagement between them. Several friendly tracks may be paired to a single track or point. A single friendly track may be paired to multiple tracks or points. However, system limitations may restrict multiple pairings.

6.3.3.5.2 Any C^2 JUs may report the pairing of a friendly track with another track or point which is being reported on the interface. However, pairings involving friendly tracks under control may only be established by the controlling C^2 JU. The originating C^2 JU should report termination of the pairing relationship when it is no longer valid.

6.4 AIR CONTROL

6.4.1 General

This section describes the general operating procedures required for the establishment, maintenance, and operation of Link 16 Air Control and covers the exchange of data between controlling C^2 JUs and aircraft under their control and between aircraft operating autonomously.

6.4.2 Air Control

6.4.2.1 Establishing Air Control

Either the controlling C^2 JU or the aircrew can initiate control once they are both on the same control net. Initiation will require voice communication if not covered by pre-mission briefings. When the controlling C^2 JU wishes to initiate control, it orders the aircraft to come to own unit's control net. The response may be automatic, but if not the aircraft will respond with a control request. When the aircraft wishes to initiate control, it sends a control request to the controlling C^2 JU on the controlling unit's control net. This is usually performed automatically when the aircrew select the controlling unit's control net or select a new control net.

6.4.2.2 Transfer of Control

6.4.2.2.1 Handover is defined as the coordinated transfer of controlling unit responsibilities for a specific aircraft from one controlling unit to another controlling unit. Handover may be achieved through either voice communication or data link. When the data link is used it is termed a digital handover. Digital handovers may be supplemented by voice communications. There are two types of digital handovers, either of which may occur without direction from higher authority or at the specific direction of the Force Commander.

6.4.2.2.2 Original Controlling Unit Originates Transfer (Handover)

a. The original controlling unit initiates a handover by sending a message requesting another controlling unit to assume control of the aircraft.

b. The receiving controlling unit:

   (1) Acknowledges receipt, and

   (2) Alerts the operator who causes transmission of WILCO or CANTCO.

c. If a CANTCO is sent at any stage in the procedure, the original controlling unit maintains control.

d. If a WILCO is transmitted:

(1) The new controlling unit may provide information such as new Control net number to the original controlling unit for transmission to the controlled aircraft.

(2) The original controlling unit acknowledges receipt.

(3) The original controlling unit transmits a Controlling Unit Change (J12.4) message to the controlled aircraft.

e. The controlled aircraft transmits:

(1) A receipt acknowledgement to the original controlling unit followed by a WILCO or CANTCO.

(2) Requests the new controlling unit to assume control.

f. The new controlling unit:

(1) Acknowledges receipt for the message to assume control.

(2) Transmits a HAVCO confirming assumption of control.

g. The controlled aircraft acknowledges receipt.

h. The new controlling unit transmits the controlling unit report which completes the handover process.

This procedure is summarised in Figure 6-1. Steps (e) - (g) above are accomplished by voice when non-JUs are involved as controllers or controlled aircraft. If, at any stage during the automated procedure, a required response is not received, the operator will be alerted and control will remain with the original controlling unit.

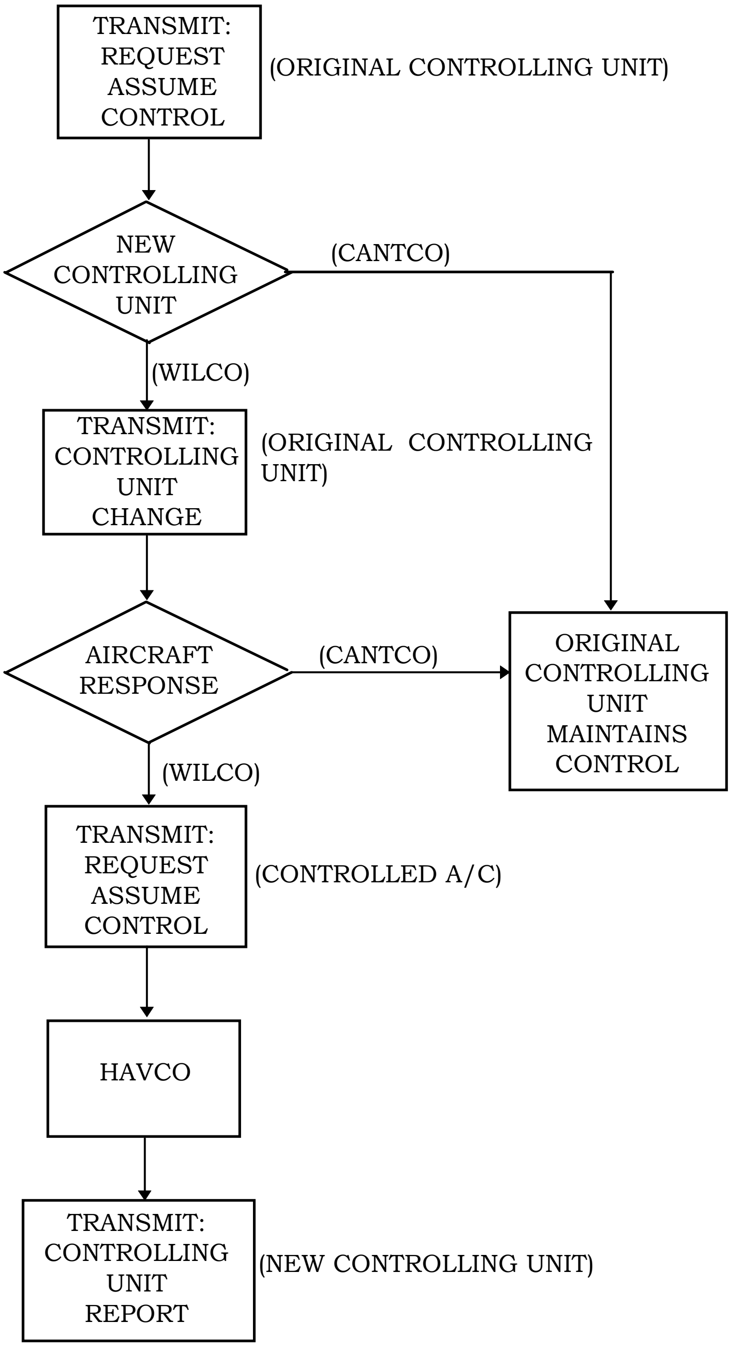

TRANSMIT: REQUEST ASSUME CONTROL
(ORIGINAL CONTROLLING UNIT)
NEW CONTROLLING UNIT
(CANTCO)
(WILCO)
TRANSMIT: CONTROLLING UNIT CHANGE
(ORIGINAL CONTROLLING UNIT)
AIRCRAFT RESPONSE
(CANTCO)
ORIGINAL CONTROLLING UNIT MAINTAINS CONTROL
(WILCO)
TRANSMIT: REQUEST ASSUME CONTROL
(CONTROLLED A/C)
HAVCO
TRANSMIT: CONTROLLING UNIT REPORT
(NEW CONTROLLING UNIT)

Figure 6-1. Procedure for Transfer of Aircraft Control (Handover)

6.4.2.2.3 New Controlling Unit Originates Transfer

a. The new controlling unit initiates handover by sending a message to the original controlling unit requesting transfer of control of the aircraft to the new controlling unit. The new controlling unit may provide information such as the new Control net number to the original controlling unit for transmission to the controlled aircraft.

b. The original controlling unit:

(1) Acknowledges receipt.

(2) Alerts the operator who, by operator action, causes transmission of WILCO or CANTCO.

c. If a CANTCO is sent, the original controlling unit maintains control.

d. If a WILCO is sent, the new controlling unit acknowledges receipt and the handover process continues at paragraph 6.4.2.2.2 d.(3).

6.4.3 Air Control Information Exchange

6.4.3.1 The Link 16 air control capability provides the means for controlling C^2 JUs and aircraft under their control to exchange information necessary for:

a. Directing mission assignments and designating targets.

b. Reporting alert and threat warning information.

c. Reporting track and target data.

d. Correlating sensor target reports with reported surveillance tracks.

e. Providing vector and flight path information to controlled aircraft.

6.4.3.2 Mission Assignments

6.4.3.2.1 The Mission Assignment (J12.0) message provides the capability for C^2 JUs to assign missions, designate targets, direct weapons condition orders and provide information on the threat warning environment to nonC^2 JUs under their control.

6.4.3.2.2 Mission Assignments by C^2 JUs

6.4.3.2.2.1 Controlling C^2 JUs may direct nonC^2 JUs under their control to perform tactical missions for Air Intercept Operations (AIO) or Air Support Operations (ASO) via a Mission Assignment. Missions are categorised according to their nature or type and are divided into Attack and Non-Attack Missions.

6.4.3.2.2.2 When controlling large formations, mission assignments may be directed to a Mission Commander (MC) or Flight Leader (FL) on behalf of the whole formation or flight. The MC/FL may subsequently assign missions to members of the formation using the Mission Assignment (J12.0) or Target Sorting (J12.6) message, albeit the latter for missions against air targets only.

6.4.3.2.2.3 Attack Missions, which are aimed at engagement of enemy forces and therefore contain target information are: Engage (MAD=5); Priority Kill (MAD=6); and Attack (MAD=41). Targets may be specified by TN or by position, course, speed and altitude.

6.4.3.2.2.4 Non-Attack Missions can be directed against enemy units or enemy activity but are normally assigned in response to enemy activity without actual engagement, in support of attack missions or to obtain information about specific enemy forces and/or activities. Examples are: Investigate/Interrogate (MAD=8); Intervene (MAD=11); Close Air Support (MAD=20); Visual Identification (MAD=32); Suppression of Enemy Air Defences (MAD=39). Non-Attack Missions also encompass those that are not directly aimed at enemy forces: e.g. Refuel (MAD=1); RTB (MAD=4).

6.4.3.2.2.5 Not all platforms implement all mission assignments, see National Supplements in Volume 3 for national/NATO platform implementations.

6.4.3.2.3 Acceptance of Mission Assignments

6.4.3.2.3.1 If nonC^2 JUs are able comply with the Mission Assignment, then upon receipt of that Mission Assignment they are to interpret it as an immediate order. NonC^2 JUs are to transmit a WILCO which may be followed by a report of their new platform activity, weapon engagement status or targeting status. Controlling C^2 JUs are to keep a record of the response of the nonC^2 JU's activity, i.e. the type of mission for as long as it is active.

6.4.3.2.3.2 Since different mission assignments may result in similar status reports from nonC^2 JUs, the receipt of a WILCO may be used to commence reporting of the nonC^2 JUs Weapon/Engagement Status (W/ES). This may subsequently be followed by more generic status reports from the nonC^2 JU. For instance the acceptance of an intervention mission assignment may result in the W/ES value 'Intervening' while Shadow results in the W/ES value 'Shadowing', both of which will be followed by a report from the nonC^2 JU with the System Information Discrete (SID) 'Investigating'. The initial W/ES value derived from the acceptance of the mission assignment should normally not be replaced by the subsequent SID value for the same mission received from the nonC^2 JU.

6.4.3.2.4 Multiple Mission Assignments

6.4.3.2.4.1 NonC^2 JUs may undertake multiple Attack missions simultaneously. However, Controlling Units should take care in assigning an 'Engage' mission to nonC^2 JUs that are currently undertaking a mission assignment of 'Attack' or vice versa. The Mission Assignment of 'Priority Kill' should be used to alert a nonC^2 JU of an imminent air threat and to redirect it to engage the air target. Attack missions take precedence over all other assignments.

6.4.3.2.4.2 NonC^2 JUs may only undertake one Non-Attack mission at a time and not simultaneously with an Attack mission. Non-Attack mission assignments may be stacked by a C^2 JU for transmission to a nonC^2 JU; nonC^2 JUs accepting Non-Attack mission assignments are to cancel the previous mission assignment which was being undertaken. When a C^2 JU needs to assign a Non-Attack mission to a nonC^2 JU with an active Attack mission, the C^2 JU is firstly to terminate that assignment. Some platforms, while conducting an Attack Mission, automatically reject any new mission assignment.

6.4.3.2.5 Terminating Mission Assignments

6.4.3.2.5.1 Attack Mission assignments can only be terminated by a controlling C^2 JU, MC or FL via a Break Engagement or Cease Attack, or by the controlled nonC^2 JU via transmission of 'Engagement Broken' or 'Target Destroyed'.

6.4.3.2.5.2 Non-Attack missions can be terminated by subsequent assignment of a new Non-Attack Mission or may be superseded by ordering an Attack Mission. The nonC^2 JU may also initiate the termination of a mission.

6.4.3.2.5.3 Alternatively the general assignments of Air-to-Air and Air-to-Surface may be used, which denote that a nonC^2 JU does not currently hold an active mission assignment but has an assigned primary role, i.e. Air-to-Air or Air-to-Surface.

6.4.3.2.6 NonC^2 JU Response

6.4.3.2.6.1 Upon receipt of a mission assignment from the controlling C^2 JU, the aircrew will be presented with information on the type of mission and target information as appropriate. The operator is required to respond with WILCO, HAVCO or CANTCO as required (paragraph 2.3.5.9 for information on Receipt/Compliance). Once a mission assignment against a specific target has been accepted, target reports to the fighter will be updated automatically until the mission has been completed or is cancelled.

6.4.3.2.6.2 If a mission assigned by a controlling C^2 JU is unattackable, the aircrew should respond with a CANTCO as soon as possible, to enable the C^2 JU to reassign the mission. If a response of WILCO/Engaging was previously transmitted and the target was being engaged, the fighter aircrew should report disengaging if the mission can no longer be executed.

6.4.3.2.7 “Heads Up” Warning

If a fighter is unable to ensure complete destruction of a target assigned in an Attack mission, the aircrew should report a "Heads Up" Warning to indicate that the target still poses a threat to friendly forces.

6.4.3.2.8 Break Engagement

A controlling C^2 JU should transmit a Break Engagement order to the fighter if a previously assigned Attack mission is to be terminated. The aircrew should respond with WILCO/Disengaging and cease the engagement.

6.4.3.2.9 Engagements Initiated by NonC^2 JUs

Engagements may be independently initiated by nonC^2 JUs on discovery of legitimate targets. The status of all such engagements must be reported to the controlling C^2 JU. Fighters report their engagement status by Status Information Discrete (SID). Annex C identifies all SIDs available for use on the interface with standard definitions and highlights those which are universally implemented.

6.4.3.2.10 Engagements Directed by NonC^2 JUs

Engagements may be directed by a nonC^2 JU to another nonC^2 JU when close control is not being exercised by a controlling unit. The Flight Leader may report mission assignments to Investigate, Engage or Disengage a specific target to his wingman. The receiving fighter should report the status of the engagement until its conclusion or until the engagement is broken.

6.4.3.2.11 Weapons Condition Orders

A controlling C^2 JU may assign a weapons condition order of either Weapons Free or Weapons Tight to a fighter under its control. Transmission of Weapons Free or Weapons Tight control orders against specific targets is prohibited. The aircrew should respond to a weapons condition order with WILCO or CANTCO.

6.4.3.2.12 Alert Reporting

The capability is provided for a controlling C^2 JU to report Threat Warning Alert conditions of Red, Yellow or White may also be transmitted, along with information on the threat warning environment, if known. The nonC^2 JU may be requested to respond with WILCO.

6.4.4 <u>Track/Target Reporting</u>

6.4.4.1 NonC^2 JUs may have the capability to monitor surveillance data being reported on the interface. However, some nonC^2 JUs may only receive track/target data from on-board sensors, other fighters and from the controlling C^2 JU. Controlling C^2 JUs may report high interest tracks on the designated control net by broadcast to all nonC^2 JUs under their control or to a specific fighter. If a fighter does not monitor surveillance data, the controlling C^2 JUs should report all track data and certain points necessary for the conduct of assigned missions or for flight safety. Track/target data is reported periodically and as data changes using the Target Sorting (J12.6) message.

6.4.4.2 NonC^2 JUs may report all sensor target data on the designated control net to the controlling C^2 JU. Fighters may exchange sensor target reports to enable them to distinguish targets among themselves. NonC^2 JUs assign index numbers as a means of identifying sensor contacts. Index number usage is automatically self-managed and is transparent to the nonC^2 JU operator.

6.4.4.3 Target/Track Correlation

6.4.4.3.1 Controlling C^2 JUs may monitor sensor target reports received from nonC^2 JUs to determine if targets already exist as surveillance tracks on the interface. When a target is correlated with a surveillance track, the controlling C^2 JU will report the correlation on the same control net to the fighter(s) initiating the sensor target report. Where several nonC^2 JUs hold sensor contact on the same target, each of the reported index numbers should be correlated to the target's surveillance TN.

6.4.4.3.2 Sensor target reports from nonC^2 JUs which fail to meet the correlation criteria may be reported by the controlling C^2 JU as a new track on the surveillance net. The controlling C^2 JU should then report the correlation of the target index number and the new surveillance TN to the nonC^2 JU on the control net.

6.4.4.3.3 Target/Track Correlations (J12.5) will be reported periodically on the control net by the controlling C^2 JU and when any correlation data associated with the surveillance TN changes. Subsequent decorrelations will also be reported by the controlling C^2 JU.

6.4.4.4 Pointers

JUs may use pointers to draw the attention of other JUs to a specific sensor target, track or geographic location on display. Voice amplification should be used to explain the purpose of each pointer.

6.4.4.5 Exercise Data in Control Messages

6.4.4.5.1 Except when reporting exercise alert states (TBD), the setting of the Exercise Indicator in control messages applies only to the exercise status of the track/target. When authorised, operators may report artificial values for Specific Type data only.

6.4.4.5.2 Operators receiving control messages with exercise status set must assume that the values reported for the above data are artificial and for exercise purposes only. All other data must be considered real. On termination of exercise status, all artificial data will be cleared immediately and replaced with real data as they become available.

6.4.5 Air Control Direction

6.4.5.1 Vector Data

6.4.5.1.1 Link 16 provides the capability for controlling C^2 JUs to transmit vector information to fighters under their control. The Vector (J12.1) message includes information on heading, speed, altitude and Vector Discrete, describing vector purpose. Annex C identifies all Vector Discretes available for use on the interface with standard definitions and highlights those which are universally implemented.

6.4.5.1.2 Vectors may be transmitted during any stage of a mission and are normally considered to be advisory in nature. However, for some activities a vector will be treated as a command and the aircrew will be required to respond with either WILCO or CANTCO. Some C^2 JU systems will have the capability to automatically transmit a vector following a mission assignment against a specific target, track or point which is being reported on the interface.

6.4.5.2 Flight Path Data

6.4.5.2.1 Controlling C^2 JUs may transmit multiple-leg flight path information or Restricted Area Boundaries to airborne JUs under their control. The information is transmitted in the Flight Path (J12.3) message as a series of waypoints up to a maximum of 15, each identified with a sequence number, and the time associated with each waypoint. This enables receiving JUs to automatically determine whether the whole sequence has been received and to identify any lost waypoints.

6.4.5.2.2 Protocols are provided to enable receiving JUs to reply with either:

a. All points received.

b. The sequence number(s) of any lost waypoint.

In the event of (b) above, the controlling C^2 JU will retransmit only those waypoints which were not received. These data exchanges are automatic and require no operator intervention. Flight path information will be presented to the aircrew who should respond with either WILCO or CANTCO.

6.4.5.2.3 The controlling C^2 JU should use voice communications to cancel any previously transmitted flight path information.

6.4.5.3 Precision Aircraft Direction

Systems may implement the Precision Aircraft Direction (J12.2) message to allow C^2 JUs to provide precise control positioning information to airborne JUs under their control. Information which can be transmitted includes vertical and lateral flight path corrections and a Drop Discrete for stores delivery. Use of this capability will require the establishment of a dedicated control net.

CHAPTER 7

OPERATION OF MIXED LINK 16 AND IJMS NETWORK

7.1 GENERAL

7.1.1 Until the end of the transition from IJMS to Link 16, some networks must accommodate communications requirements for both Link 16 and IJMS, either for operational reasons or in order to comply with peacetime operating restrictions.

7.1.2 A MIDS network may consist of both MIDS terminals and JTDS Class 1 and Class 2 terminals. The Class I terminal implements only the IJMS messages and protocols. The Class 2 terminal processes some IJMS messages to provide the capability to synchronise with IJMS users. Some Class 2 terminals may have a more extensive implementation of the IJMS messages and are truly “bilingual".

7.1.3 Even though operational data exchange between Class 2 terminals and the IJMS users may not be required, the synchronisation of the terminals into a single network will enable peacetime network operations to comply with frequency clearance restrictions, reduce mutual interference, provide more network entry and synchronisation sources, and may improve relative navigation performance. The additional operational benefits of mutual positional awareness and the ability to communicate by voice should also be taken into account although platform capabilities and the network design may diminish the availability of these additional benefits.

7.1.4 The Link 16 network entry and synchronisation procedures are set out in the main body of ADatP-16. This Annex sets out the planning guidelines and procedures that are necessary if both Class 1 and Class 2 terminals are to be synchronised in a single network.

7.2 TERMINAL CAPABILITIES

7.2.1 Time Slot and Relay Assignments

7.2.1.1 There are a number of significant differences between Class 1 and Class 2 terminals which will impact the network design and its operation. A Class 1Terminal can accept up to three transmit time slot assignments, one assignment for P-message block, one net entry block and six relay pair assignments. In addition, it can accept up to nine receive only assignments for up to three net numbers other than the main net number. All unassigned slots default to the receive mode on the same net as the main net number. When not transmitting, it is in the receive mode on its main net. Other terminal capabilities that differ from the Class 2 are as follows and are summarised in Table 7.1 below:

a. There is only a limited capability to segregate messages for transmission by the following categories:

(1) "P" Messages - position and status data (one time slot block).

(2) "V" Messages - ECM-resistance voice (one time slot block).

(3) "T" Messages - all other data (up to three time slot blocks).

b. The "T" Messages are transmitted using the next available time slot assigned to the terminal for that purpose. Since there is no way of predicting what type of data is contained in each "T" message, information exchange cannot be organised on a functional basis.

c. The maximum relay delay for Voice is six time slots.

d. There is no maximum relay delay for Fixed Format messages.

e. The minimum relay delay for Voice and Fixed Format messages is three time slots.

f. Messages can be transmitted in Dedicated Access and in Standard Packing format only.

	CLASS 1 TERMINAL	CLASS 2 TERMINAL
RELAY DELAY.		
Minimum delay	3 slots	6 slots
Maximum delay	6 slots for Free Text (voice) No limit for Fixed Format	31 slots 31 slots
RELAY BLOCKS	6 relay pairs	Relay pair is one of 64 time slot blocks
RELAY FUNCTION	No selection	PG RELAY for IJMS
NET ASSIGNMENT		
Relay receive	Any net	Any net
Relay transmit	Same as Main Net	Same as receive or any other net (for PG relay)
RELAY ASSIGNMENT		
Relay receive	Explicit time slot block	Explicit time slot block
Relay transmit	Explicit time slot block	Implicit time slot block from relay delay

Table 7.1 Summary of Time Slot Relay Assignment differences between JTIDS Class 1 and Class 2 Terminals

7.2.2 Transmit Modes

Each Class 1 terminal may be operated in one of four transmission modes: Master, Normal, Polling or Radio Silence depending on its role as NTR and the structure of the net. Class 2 terminals are operated in one of three transmit modes; Normal, Polling and conditional Radio Silence, with NTR selection being a separate initialisation parameter entered at the designated terminal. The NTR maintains system time and does not transmit RTT Interrogation messages nor compute local time corrections from information provided by other subscribers. Messages transmitted by the NTR have the highest time quality (15). A description of the Class 2 terminal transmit modes is contained in Volume I, Chapter 2; the transmit modes for the Class 1 terminal are as follows:

a. Master Mode. This mode equates to the NTR function of the Class 2 terminal.

b. Normal Mode. Terminals not designated as NTR usually operate in Normal Mode. Fine synchronisation may be achieved either actively or passively and terminals can transmit IJMS and free text messages unconditionally within their time slot block allocation.

c. Polling Mode. A terminal in the Polling Mode transmits data only on demand, except when passing an RTT interrogation message for active synchronisation purposes, or when automatic message acknowledgement is required: it does not respond to RTT interrogations. The time quality data field in transmitted messages is set to indicate the lowest time quality status.

d. Radio Silence Mode. When a terminal is placed in the Radio Silence Mode, it reports its intention to go Radio Silent in its next P message. It then ceases radiating and further transmissions do not occur while in this mode. Fine synchronisation is achieved by passive means only.

7.2.3 Interference Protection Features (IPF)

The Class 1 terminal implements features to protect against inadvertent or incorrect operation. In order to comply with frequency clearance restrictions, the terminal contains Interference Protection Features (IPF), which is set by operator action, as follows:

a. IPF 0 No Protect (Combat). The COMBAT mode offers no IPF protection, although for the Class 1 terminal, a single terminal may only use a maximum of 59% of the total time slots available when in this mode. This restriction does not apply to the Class 2 terminal. This mode is not authorised for use during peacetime. It is intended for combat or other extraordinary situations where operational requirements dictate. In these cases, deviations in the distribution of limited frequencies, pulse width or energy emitted in the IFF band, which would otherwise result in the cessation of terminal operation in the full or partial IPF protection modes, will be allowed.

b. IPF 1 Partial Protect (Exercise). This is the normal NATO mode of operation. The terminal monitors its own emissions and automatically inhibits transmission if the following parameters do not meet specification requirements agreed by military and civilian aviation authorities:

(1) Frequency hop.

(2) Pulse width.

(3) Spurious emissions in the IFF guard bands.

c. IPF 2 Full Protect (Peacetime). This mode incorporates all protection features of IPF Partial Protect. This mode also provides the following additional protection:

(1) Automatically inhibits transmissions if any attempt is made to transmit in more than 304 time slots (slightly less than 20% of the time slots).

(2) Prevents assignment of adjacent time slots or more than 608 time slots in a network (slightly less than 40% of the time slots).2

(3) Prevents selection of the high power mode, multi-net operation and communications in other than Communications Mode 1. In the Class 1 terminal any net number assignment is accepted but is defaulted to 000.

(4) Prevents transmissions in disallowed time slots.

7.2.4 Cryptovariables

In Class 1 terminals, cryptographic storage is restricted to a single cryptovariable pair.

7.2.5 Relative Navigation

Class 1 terminals do not perform relative navigation processing. Class 1 terminals transmit their position and its associated Position Quality value that are entered by the operator when the terminal is initialised. It is essential that Class 1 terminals are initialised with Position Quality values that accurately reflect the positional accuracy of the JTIDS antenna. This is necessary to ensure that there is no adverse impact on the Relative Navigation function in the Class 2 terminals of other network participants.

7.3 NETWORK DESIGN

7.3.1 The guidelines and procedures laid down in Volume 2 Chapter 2 should be followed and the following additional points should be considered:

a. Class 2 terminal units should be assigned transmit time slots in NPG 30 to provide additional sources for “P”messages to the Class 1 terminals and to enable the Class 2 terminal to transmit IJMS RTT-A interrogations.

b. Class 2 terminal units should also be assigned receive time slots in NPG 30 to utilise additional "P" message sources and to enable the Class 2 terminal to respond to received IJMS RTT-A interrogations.

c. The Class 1 terminal can not be used to relay Link 16 messages.

d. The Class 2 terminal may be used to relay IJMS messages, provided the Relay Function of the relay assignment is Participation Group Relay and the NPG of the assignment is an IJMS NPG, i.e. NPG 30 or 31.

e. If voice exchange is required between Class 1 and Class 2 terminals the time slot assignments should use a single block, a rate of 2.4 Kbps, standard packing and the same net number as the Class 1 unit's main net. On a Class 1 terminal, each ERV channel is activated separately by manual initialisation via Unformatted Message Element (UME), which is the interface between the vocoder and terminal. The UME initialisation data includes the ERV channel number, whether the ERV is to be error-coded or not, the net number, and the relay delay (if the ERV channel is relayed). ERV channels are counted upwards and are assigned in sequence of time slot transmission sequence, starting with channel 000 and time slot 00000 of Set A. Non-Error-Coded voice has 24 channels available while Error-Coded voice can only be assigned a channel number up to 11. This is because twice the number of time slots are required for Error-Coding to be accomplished. Table 7.2 shows the available assignments but note that Channel "0" is illegal in Class 1 terminals.

CHANNEL	NON-ERROR-CODED RECURRENCE RATE 12		ERROR-CODED RECURRENCE RATE 13	
	SET	TIME SLOT	SET	TIME SLOT
0	A	00000	A	00000
1	B	00000	B	00000
2	C	00000	C	00000
3	A	00001	A	00001
4	B	00001	B	00001
5	C	00001	C	00001
6	A	00002	A	00002
7	B	00002	B	00002
8	C	00002	C	00002
9	A	00003	A	00003
10	B	00003	B	00003
11	C	00003	C	00003
12	A	00004		
13	B	00004		
14	C	00004		
15	A	00005		
16	B	00005		
17	C	00005		
18	A	00006		
19	B	00006		
20	C	00006		
21	A	00007		
22	B	00007		
23	C	00007		

Table 7.2 - ERV Allowable Channel Assignments

7.4 PRE-MISSION PLANNING

7.4.1 Selection of Network Time Reference

7.4.1.1 The guidelines and procedures laid down in Volume 2, Chapter 4 should be followed but the selected NTR and any IEJUs should be capable of acting as suitable network entry sources for both Link 16 and IJMS joining units. The appointed NTR should be either:

a. A Class 2 unit that is capable of being initialised to transmit the Link 16 Initial Entry message and the IJMS Net Entry Aid alternately in the Initial Entry time slot. Class 1 terminals can join the network via receipt of the IJMS Net Entry Aid, which must be received on Net 0, and Class 2 terminals can do so using either message.

b. A Class 1 unit that is initialised to transmit the IJMS Net Entry Aid in the Initial Entry time slot. All Class 1 and most Class 2 terminals can gain entry to the network by receipt of this message. However, careful consideration should be given as to whether it is appropriate for a Class 1 unit to be NTR as some Class 2 units may not be able to receive the Initial Entry message when the Class 1 unit's Main Net is other than Net 0. This problem is described more fully in paragraph 7.5 below.

7.4.1.2 If a Class 2 unit, that is only capable of being initialised to transmit the Link 16 Initial Entry message in the Initial Entry time slot, is selected as the NTR for the network, Class 1 units will not be able to join the network using the NTR's transmissions. The Network Manager should ensure that suitable IEJU(s) are appointed (see paragraph 7.4.2 below).

7.4.1.3 If a Class 1 unit is selected as the NTR for a network and that network includes some Class 2 units that are unable to use, for network entry purposes, the “P" message being transmitted by the NTR in a specific time slot, suitable IEJU(s) should be appointed (see paragraph 7.4.2 below).

7.4.2 Selection of Initial Entry JUs

The guidelines and procedures laid down in Volume 2, Chapter 4 should be followed, but the selected IEJUs should be capable of acting as suitable network entry sources for joining platforms using either Link 16 or IJMS.

7.4.3 Selection of Position References

The guidelines and procedures laid down in Volume 2 Chapter 3 apply. A ground-based Class 1 terminal may be selected to act as a PR to support the Class 2 relative navigation function. The PQ value entered in the Class 1 terminal must truly reflect the accuracy of its reported position using values contained in the table below. Ideally, units acting as PR should have a positional accuracy of ±50 feet (1 5m), in which case a PQ value of 15 should be entered, but a lower value can support relative navigation provided it is accurate. An inaccurate PQ undermines relative navigation and severely degrades network performance. Position Quality values are shown in Table 7.3.

Class 1 Position Quality	Geodetic Position Accuracy
15	<50 feet
14	< 71 feet
13	<100 feet
12	< 141 feet
11	<200 feet
10	<282 feet
9	<400 feet
8	<565 feet
7	<800 feet
6	<ll30feet
5	<1600 feet
4	<2260 feet
3	<4520 feet
2	<9040 feet
1	<18080 feet
0	No Statement

Table 7.3 - Position Quality Values

7.4.4 Selection of Navigation Controller(s)

The guidelines and procedures laid down in Volume 2 Chapter 3 apply. The Class 1 terminal does not implement relative navigation and, therefore, cannot act as NC.

7.4.5 Track Numbers

On a Link I6/IJMS interface, TNs greater than 07777 may be allocated. However, the TN blocks should be limited to numeric values only since IJMS does not support alphanumeric TNs. Limiting the TN blocks to numeric TNs only will allow TNs to be equated. Every effort should be made to ensure that a track is identified by a single TN on the interface. Individual system capabilities may not fully support TN equating.

7.5 NETWORK ENTRY AND SYNCHRONISATION

7.5.1 Initial Entry

Class 1 Terminals can gain initial entry to the network via Class 2 terminals using one of two possible procedures as follows:

a. Receipt of IJMS Net Entry Aid - Some Class 2 terminals can be initialised to transmit alternately the IJMS Net Entry Aid message and the Link 16 Initial Entry message in the Initial Entry time slot if they are authorised to transmit in that slot; i.e. if acting as NTR, Main Net Relay or IEJU. The joining platform monitors the Initial Entry time slot which occurs once every 12 secs in time slot A-0-6 on Net 0. On receipt of an IJMS Net Entry Aid message in the Initial Entry time slot, the joining platform gains initial entry to the network.

b. Receipt of Any IJMS Message in a Specified Time Slot - A Class 1 terminal user can also achieve network entry via the receipt of any IJMS message in a specified time slot, normally a time slot assigned for the transmission of another IJMS unit's "P" message.

7.5.1.2 Class 2 terminals gain initial entry to the network using the procedure in Volume 2 Chapter 4. A Class 2 terminal can also use the methods described above subject to the following conditions:

a. Receipt of IJMS Net Entry Aid - Some Class 2 terminal users can also achieve network entry using this method although it needs to be specifically initialised to receive the Net Entry Aid. The Net Entry Aid is transmitted on Net 0 for Class 2 terminals whereas the Class 1 terminal transmits on its main net.

b. Receipt of Any IJMS Message in a Specified Time Slot. Some Class 2 terminals may also be able to use this method by using a specific initialisation parameter ("Alternate Net Entry Slot Designator") together with the additional parameters necessary to identify the time slot to be used. However, this method requires careful pre planning to ensure that the platform to be used to aid net entry is present in the network when the joining platform attempts to enter the network. For this reason, it should be considered to be a secondary procedure.

7.5.2 Fine Synchronisation

7.5.2.1 Following the attainment of network entry and coarse synchronisation, the network joiner must gain fine synchronisation. Both Class 1 and Class 2 terminals can synchronise either passively or actively (as described in the main body of ADatP-16). In all cases the attainment of fine synchronisation requires that the synchronising terminal receives PPLI and/or “P” messages to identify suitable sources. Class 1 terminals will process only messages for this purpose but Class 2 terminals can make use of both "P" messages and PPLI messages. However, if the Class 1 terminal uses a P-message that is transmitted on a different net to its Main Net then it can only use the passive method of achieving fine synchronisation.

7.5.2.2 Passive Method

Class 2 terminals will transmit a "P" message in all assigned transmit time slots for NPG 30 (the IJMS “P” NPG). If the Class 2 terminal is to process received "P” messages, it must have a receive time slot assignment in NPG 30 or NPG 31 so that it recognises and processes messages received in those time slots as IJMS "P" messages.

7.5.2.3 Active Method

7.5.2.3.1 To achieve fine synchronisation actively, the terminal must build a list of candidate sources for RTT interrogations. RTT-A interrogations and RTT replies can be exchanged between Class 1 and Class 2 terminals, although the coding of the message in IJMS is different from the Link 16 coding convention and this results in the bit position being reversed.

7.5.2.3.2 The Class 1 terminal will transmit and process only IJMS RTT-A messages but the Class 2 terminal is able to transmit and process both IJMS and Link 16 RTT-A message types. The Class 2 terminal will record whether a potential RTT interrogation addressee is an IJMS or a Link 16 user. If the selected addressee is a Link 16 user, the Class 2 terminal will transmit a Link 16 RTT-A Interrogation message in an assigned RTT-A NPG (NPG 2) time slot (or an RTT-B Interrogation message in an RTT-B NPG (NPG 3) time slot if one is assigned). If the selected terminal for interrogation is an IJMS source, the Class 2 terminal will transmit an IJMS RTT-A Interrogation message in an assigned IJMS "P" (NPG 30) time slot.

7.5.2.3.3 If the Class 2 terminal is required to act as an RTT-A source for Class 1 terminals, it will require a receive time slot assignment in NPG 30 or 31 so that it recognises and processes the received message as an IJMS RTT-A Interrogation message and responds accordingly.

7.6 NETWORK MONITORING AND DYNAMIC NETWORK MANAGEMENT

7.6.1 The guidelines and procedures laid down in Volume 2 should be followed, but the Network Manager will be additionally responsible for the IJMS participants. Wherever possible, the Network Manager should be capable of monitoring the position and status of both Link 16 and IJMS participants; if this is not possible, the appointment of a sub-network manager to monitor the IJMS participants should be considered.

7.6.2 The Network Manager, when planning changes to the network, will need to consider the impact of such changes on the IJMS units and whether the IJMS units can implement the required changes to maintain their integrated participation in the network.

CHAPTER 8

INTERACTIONS WITH OTHER LINKS

8.1 GENERAL MULTI-LINK CONSIDERATIONS

8.1.1 General

This section provides guidance and considerations for operating Link 16 in a multi-link environment. Specific data exchange procedures for Link 16 are included in Chapter 6.

8.1.2 Management of the Multi-Link Interface

8.1.2.1 Responsibilities

Through the Interface Planning and Management function, the authority for management of the multi-link network will be delegated to an IU with data link network management responsibilities. As part of this task, the designated unit will retain responsibility for its respective link, but will also assume responsibility for integrating the capabilities of all links into an effective system.

8.1.2.2 Multi-Link Interface

The introduction of Link 16 into the NATO environment will significantly increase the overall communications network capacity and flexibility but will also add design complexity. The IU responsible for managing the multi-link interface must consider many technical and operational parameters to achieve effective communications.

8.1.2.3 Multi-Link Network Management

Multi-link network management is an Interface Planning and Management activity. The IU responsible must be concerned with network interface design and operation, including participants, connectivity, and network parameters. Activities associated with multi-link network management include:

a. Ensure multi-link requirements are considered during Pre-mission Planning. The network designers need to know:

   (1) Mission communication priorities.

   (2) Number and types of links.

   (3) Connectivity requirements.

   (4) Security requirements.

   (5) Forwarding requirements.

b. Assist in preparation of technical and tactical plans to ensure the coordination of Link 16 operations via the OPTASK LINK.

c. Prepare a list of participants required to satisfy operational requirements and supervise the allocation of addresses to JUs, PUs, and RUs.

d. Translate the total track exchange requirements to TN block allocations.

e. Establish requirements for FJUs. Assign FJUs including backup and/or replacements.

f. Ensure sufficient Link 16 network capacity is assigned to FJUs so that all required messages can be forwarded.

g. Establish secure voice communications for interface coordination of multi-link operations.

h. Designate one IU to be responsible for Track Data Coordination on the multi-link interface.

i. Direct changes to the networks needed to support the changing operational situation.

8.1.2.4 Network Design Requirements

The design of Link 16 networks to be used within multi-link operations should take into consideration the other interfaces to be involved. This will include planning of C^2 JU capacity on the surveillance net to account for data forwarding. Network Description Summaries should contain details of the operation of all links interfacing with Link 16 in addition to the operating characteristics of the Link 16 network itself.

8.1.2.5 Establishing the Network

For multi-link operations one OPTASK LINK should be issued containing the operational details for all links involved. The selection of suitable units to act as FJUs is covered in detail in paragraph 3.1.4.3 of Volume 2.

8.1.2.6 Multi-Link Voice Coordination

Secure, dedicated voice communications should be established to provide timely management and coordination of all changes (e.g. redesignation of data forwarder) on the multi-link interface.

8.1.3 Types of Multi-Link Operation

8.1.3.1 Data Forwarding

Data forwarding is the process of receiving data on one digital data link and outputting the data in the proper format and protocol of another digital data link. During the process, a message received on one link is translated to an appropriate message on another data link. Those data elements applicable within the messages are translated to the appropriate data elements in the corresponding messages. Within the data forwarding process, data management will be minimised.

8.1.3.2 Concurrent Operations

A concurrent operator is a system/platform that participates on more than one data link simultaneously. The IU transmits only locally derived data and conforms to all the applicable link protocols for the links on which it is transmitting. In concurrent operations remote data received on one data link should not be passed to any of the other data links.

8.1.3.3 The Problem of Loopback Reporting

Within a multi-link interface, certain operating configurations can produce data looping when one or more IUs receive the same information from more than one data path. This can happen when both forwarding and concurrent operations are occurring as in Fig 7.1. In this case unit A1 is receiving AEW data directly and indirectly through the FJUA. Operators should be aware that multi-link configurations incorporating both data forwarding and concurrent operations can result in disruption of the tactical picture unless data looping is prevented. Operational Commanders should consider this impact, together with the operational priorities, when planning the overall multi-link interface configuration.

8.1.4 Track Number Management in a Multilink Interface

8.1.4.1 Different track numbering schemes are used on different links. Link 16 TNs are composed of five numeric or alphanumeric characters, as described in paragraph 6.2.2.2.2. Link 11 uses four octal digit TNs only, whereas IJMS uses 5 octal digit TNs only. In a multilink environment, if a track is reported by a different TN on each link, an additional burden will be placed on operators to associate, either by data link or by voice coordination, those TNs being used to report the same object. Therefore, every effort should be made to ensure that tracks are reported using a common TN on a multilink interface. This can be achieved by equating TNs between links, whereby TNs assigned for use on the multilink interface are limited to the allowable range of the least capable link. Specific procedures for the use of TNs in a Link 16/Link 11/11B interface are contained in paragraph 7.2.5.2; procedures for the use of TNs in a Link 16/IJMS interface are contained in paragraph 7.3.1.

8.1.4.2 Situations may occur when the use of TNs cannot be limited in this way:

a. High track volume requires the use of a greater range of TNs than that provided by the least capable link.

b. Individual system capabilities may not fully support TN equating.

In such cases, TNs will not be able to be equated and the different TNs will need to be associated (see paragraph 8.1.4.3 below). However, IUs should always equate TNs whenever possible to minimise the requirement for TN association.

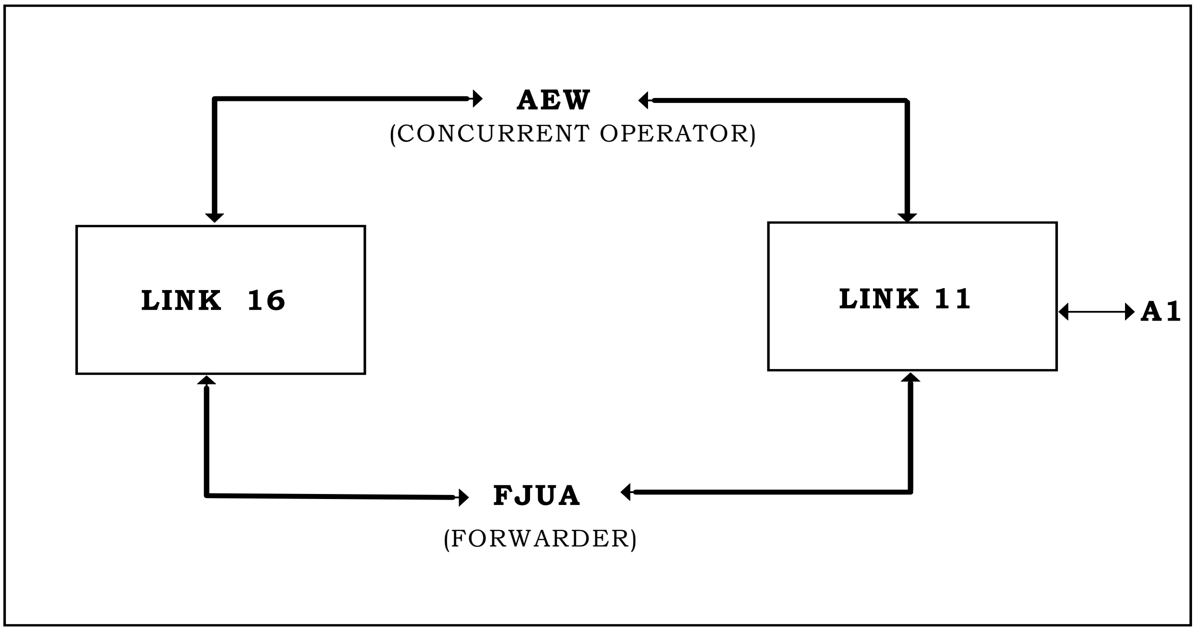


Figure 8-1 Data Looping

8.1.4.3 TN Association

On Link 16, the Track Identifier (J7.4) message provides the capability for an operator to associate a Link 16 Reference TN with other system TNs where they refer to the same object. Association may be made with the following:

a. Link 11/Link 11B TN.

b. NATO Link 1 TN (NTN).

c. IJMS System Reference Number (SRN).

d. Army Tactical Data Link - 1 (ATDL-1) TN.

This information is reported as a result of operator action to initiate a TN association or change any of the associated TNs. There is no management of TN association information; the latest reported association will supersede any previously received data.

8.2 OPERATION OF LINK 16 TO LINK 11/LINK 11B INTERFACE

8.2.1 Participants

8.2.1.1 The possible participants in a multi-link interface are:

a. MIDS Unit (JU):

(1) C^2 JU.

(2) Non-C^2 JU.

b. Participating Unit (PU).

c. Reporting Unit (RU).

d. Indirect Unit.

e. Supporting Unit (SU).

f. Forwarding MIDS Unit (FJU):

(1) F JU A.

(2) F JU B.

(3) F JU AB.

g. Forwarding Participating Unit (FPU).

h. Forwarding Reporting Unit (FRU).

i. Concurrent Interface Unit.

8.2.1.2 Forwarding Unit Definitions

Standard Unit definitions are to be found at paragraph 2.4.2. The following additional definitions apply specifically to data forwarding operations:

a. Forwarding MIDS Unit A (FJUA) - A unit communicating on both Link 11 and Link 16 while forwarding information between Link 11 and Link 16 participants.

b. Forwarding MIDS Unit B (FJUB) - A unit communicating on both Link 11B an Link 16 while forwarding information between Link 11B and Link 16 participants.

c. Forwarding MIDS Unit AB (FJUAB) - A unit communicating on Link 16, Link 11 and Link 11B while forwarding data among Link 16, Link 11 and Link 11B participants.

d. Forwarding Participating Unit (FPU) - A PU which is forwarding data between Link 11 and one or more RUs .

e. Forwarding Reporting Unit (FRU) - An RU which is forwarding data between two or more RUs.

8.2.2 Link 16/Link 11/Link 11B Interface Configuration

Figure 8-2 illustrates one example of a Link 16/Link 11/Link 11B interface configuration. A single data forwarder is designated to serve as the interface between the NATO Link 16 network and a Link 11B network (one or more connected Link 11B circuits). Separate Link 11 and Link 11B networks may be interfaced to the Link 16 network by separate data forwarders.

8.2.3 FJU as a Participant

Subject to all specified data forwarding filters, all translatable messages from Link 16 PGs on which the FJU is a participant shall be forwarded onto Link 11/Link 11B. To accomplish this, the FJU must have each Link11/11B participant's address (up to a maximum of 16) entered as a Secondary TN at initialisation. All translatable messages from Link 11/Link 11B shall be forwarded onto the appropriate Link 16 PGs on which the FJU is a participant. The FJU shall discard messages that cannot be forwarded.

8.2.4 Data Forwarding Considerations

8.2.4.1 Surveillance Data Forwarding

Link 16 uses geographic position reporting. This imposes no limitations on the areas which can be covered, since Link 16 reported track positions are independent of the reporting unit's position. Link 11 utilises the Cartesian coordinate system, which restricts the reporting of tracks to within 511.75 data miles of the reporting unit's System Coordinate Centre (SCC). Therefore, surveillance data forwarding from Link 16 to Link 11/Link 11B is limited to tracks that are positioned within 511.75 miles of the FJU's SCC reported on that link. PPLI reports from all JUs having an address 00200 through 77777, both C^2 and nonC^2, are forwarded as tracks or reference points. The forwarding unit indicates itself as having reporting responsibility for these JUs. Tracks are forwarded with a track quality of 7 in this case (paragraph 6.2.2.3 for Track Quality).

8.2.4.2 EW Data Forwarding

EW data is reported on two Link 16 PGs, EW and Surveillance. Because of the dual PGs some EW data are reported on both PGs simultaneously. When forwarded it means that the same data are reported twice on Link 11/11B, which can cause excessive link loading. The same dual reporting can happen in reverse when one Link 11/11B EW message is forwarded onto both the EW and Surveillance PGs. Because of this the forwarding of EW data is controllable such that it is forwarded to/from either the EW or Surveillance PGs or both. These options will primarily prevent overloading of Link 11/11B with EW data, but will also reduce link loading on Link 16.

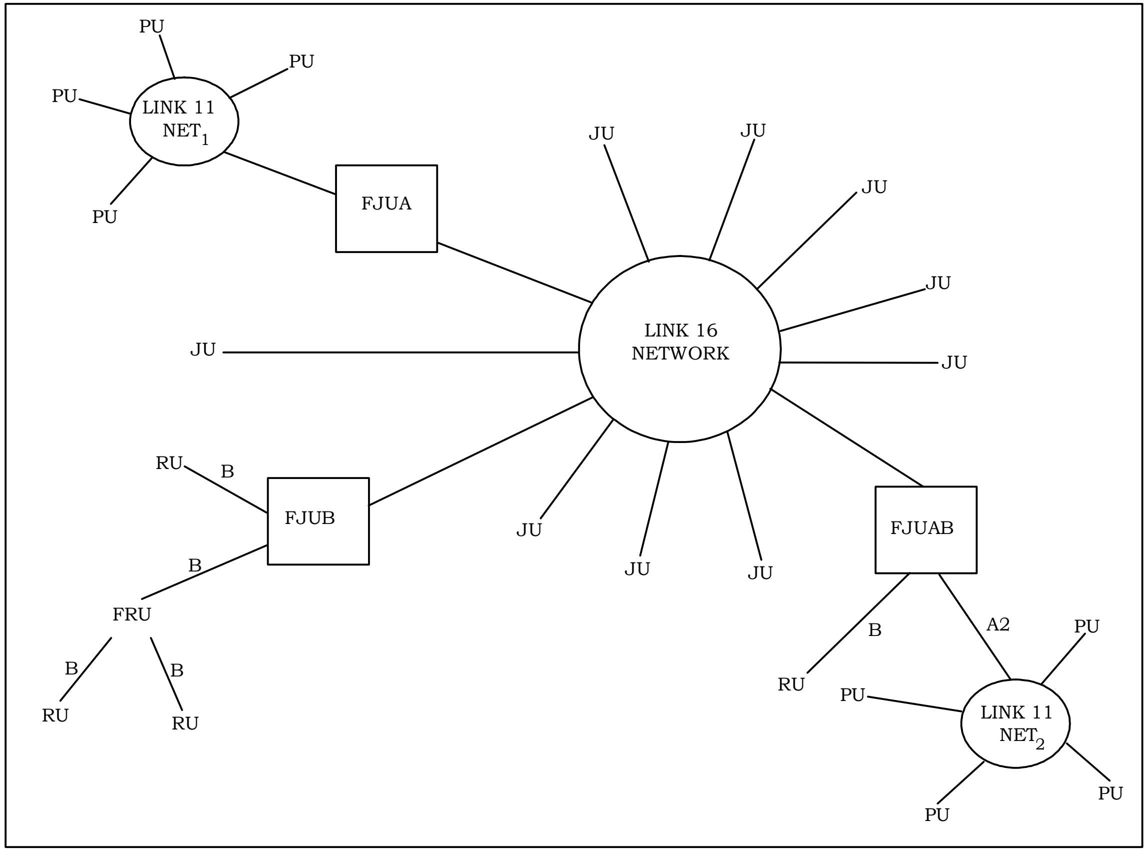


Figure 8-2 Example of Link 16/Link 11/Link11B Interface Configuration

8.2.4.3 Restrictions on Data Forwarding

An FJU will inhibit the forwarding of received data when:

a. The data are received from, or addressed to, a unit not currently held as an active IU. Re-establishing active status of the IU is an exception to this rule.

b. The command or other addressed message is from a JU with a TN address greater than or equal to 00200. Likewise, Link 11/11B messages addressed to the pseudo address, 176, will not be forwarded to Link 16.

c. The coordinate filter criteria for the appropriate data link prohibits forwarding the data.

d. The received data is technically illegal or invalid.

e. A periodically updated report is superseded by a second report before the first message can be forwarded. The new data shall override the stale data and only the most current information shall be forwarded.

f. A simulation transmit filter is selected. Since Link 11/Link 11B units not implementing the simulated track or unit capability would display these as live (real) objects, simulated track or unit data must not be forwarded to Link 11/Link 11B networks containing PUs/RUs that do not implement the simulated track or unit capability.

8.2.5 Data Management

8.2.5.1 Data Filters

Data filters can be used to restrict data flow between links but their use must be managed. An FJU only reports on transmit filters that are used on Link 16. Filters for forwarding data from another link to Link 16 are not reported via Link 16. In order to achieve positive control over the use of data filters by FJUs, such use must be coordinated with the Network Manager prior to implementation. Procedures and restrictions for the use of data filters on Link 16 are contained in paragraph 6.2.5.7.5.

8.2.5.2 Track Numbers

8.2.5.2.1 When operating a Link 16/Link 11/11B interface, the following procedures should be followed:

a. All JUs should be assigned an address below the octal number 07777, to ensure that each JU can be identified by a single address throughout the interface.

b. C^2 JUs which require to exchange addressed messages with Link 11/11B units must be assigned an address below the octal number 00176.

c. Whenever possible, each C^2 JU should be allocated at least one block of low TNs (00200 – 07776) and another block of high TNs (10000 – 77776 octal and all alpha numerics).

d. FJUs should be allocated, in addition to own host unit TN allocation(s), a block (or blocks) of low TNs specifically to allow the forwarding of Link 16 tracks with TNs greater than 07777.

e. Note: Although TNs within the block 00001_8 to 00076_8 are valid for use as Group Identifier Addresses, network planners should allocate all PU/FPU Addresses, Link 11 Terminal Addresses and other C^2 IU Addresses before using this block for Group Identifier Addresses. This procedure is particularly relevant when planning for complex net communities in a multi-link environment.

8.2.5.2.2 C^2 JUs should always attempt to originate tracks with TNs below 07777 whenever possible, to minimise the need for interlink TN association. The high TN block should be utilised only as an overflow block when no low TN is available for use. When a track with a TN greater than 07777 is forwarded to Link 11/11B, the data forwarder will assign a Link 11/11B TN to the track, and report the TN association to other IUs via the Track Identifier message on Link 16 (see paragraph 7.1.4.3) and the equivalent message on Link 11.

8.2.5.3 Data Update Request

A TN specific Data Update Request is not forwardable to Link 11 and therefore will achieve no response. Any Link 16 originated Data Update Request by RIV which is forwarded to Link 11 will result in all classes of information being transmitted in response, irrespective of the RIV settings in the request.

8.2.6 Multi-Link Security Considerations

The IU responsible for Cryptonet Management must be alert to the effects of a compromise of an FJU on the multi-link interface. In such instances, cryptovariables for all links involved on the interface may require changing.

8.2.7 Variable Track Quality (Dial-a-TQ)

8.2.7.1 Some units have a capability to manually enter a maximum TQ value, between 3 and 6, to be assigned by that PU to any track. This Variable Track Quality (VTQ) capability, previously referred to as “Dial-a-TQ”, allows the Track Data Coordinator to direct PUs with less accurate sensors to limit their TQ in order to ensure that the most accurate positional data is reported on the interface. It also provides a means of biasing R2 toward the GRU when necessary to ensure that the GRU reports a sufficient number of tracks to allow proper gridlock.

8.2.7.2 Although 7 is the maximum TQ reportable on Link 11/11B, TQs up to 15 are reportable on Link 16. The Link 16 TQs 8-15 require much greater positional accuracy than link 11 TQ 7, and the higher Link 16 TQ values are only achievable by C^2 JUs with very accurate sensors and navigation. Thus, R2 will naturally tend to migrate towards the C^2 JUs with the most accurate track data and VTQ will not normally be advantageous in a multi-link interface. However, directing certain JUs with less accurate sensors to limit their TQ to 6, or over, may be advantageous. An example might be when the platforms with the most accurate sensors must operate as PUs.

8.2.7.3 VTQ settings may be specified for applicable units in the OPTASK LINK in the GENTEXT/REPORTING REQUIREMENTS set during operations as the situation dictates.

8.2.7.4 Units that are not capable of lowering TQ will not be removed from the interface when VTQ is employed.

8.3 OPERATION OF A LINK 16/IJMS INTERFACE

8.3.1 Track Numbers

On a Link 16/IJMS only interface, TNs greater than 07777 may be allocated. However, the TN blocks should be limited to the numeric values only since IJMS does not support alphanumeric TNs. Limiting the TN blocks to numeric TNs only will allow TNs to be equated on the two links. Every effort should be made to ensure that a track is identified by a single TN on the interface. Individual system capabilities may not fully support TN equating.

CHAPTER 9

THE NEEDLINE CONCEPT

9.1 OVERVIEW

This chapter provides guidance and considerations for operating MIDS in a ground-to-ground environment.

9.1.1 Initial Requirement

Ground units have to move in a small and highly threatened area. They have the following requirements:

a. Contributing to the safety of friendly fixed wing aircraft and helicopters.

b. Improving air defence artillery efficiency by commanding and controlling air defence weapons.

c. Providing real-time control over army aircraft in accordance with Air Force guidelines.

d. Improving survivability against threats, including enemy intelligence gathering, jamming etc.

e. Facilitating the rapid enforcement operational directives.

9.2 NEEDLINE CONCEPT

9.2.1 Needline Repromulgation Relay

Link 16 provides a valuable capability to extend communication coverage to units beyond Line-of-Sight (BLOS), using successive retransmission, a capability referred to as “Repromulgation Relay”. The Needline Concept defines a special use of this MIDS/L16 service by allocating a specific communication role to each MIDS subscriber. A unit can be perform the role of “Source”, “Relay” or “Addressee” (destination), which allows a selective retransmission of repromulgated messages along a selected path.

With the Needline Concept, repromulgation capabilities are optimised by decreasing the relay transmission requirements. Furthermore, message loss, caused by the capture phenomenon, is avoided and peacetime Time Slot Duty Factor (TSDF) constraints can be met more easily. Figure 9-I shows both Classic and Needline repromulgation relay. Selective retransmission of repromulgated messages will only occur along a selected path.

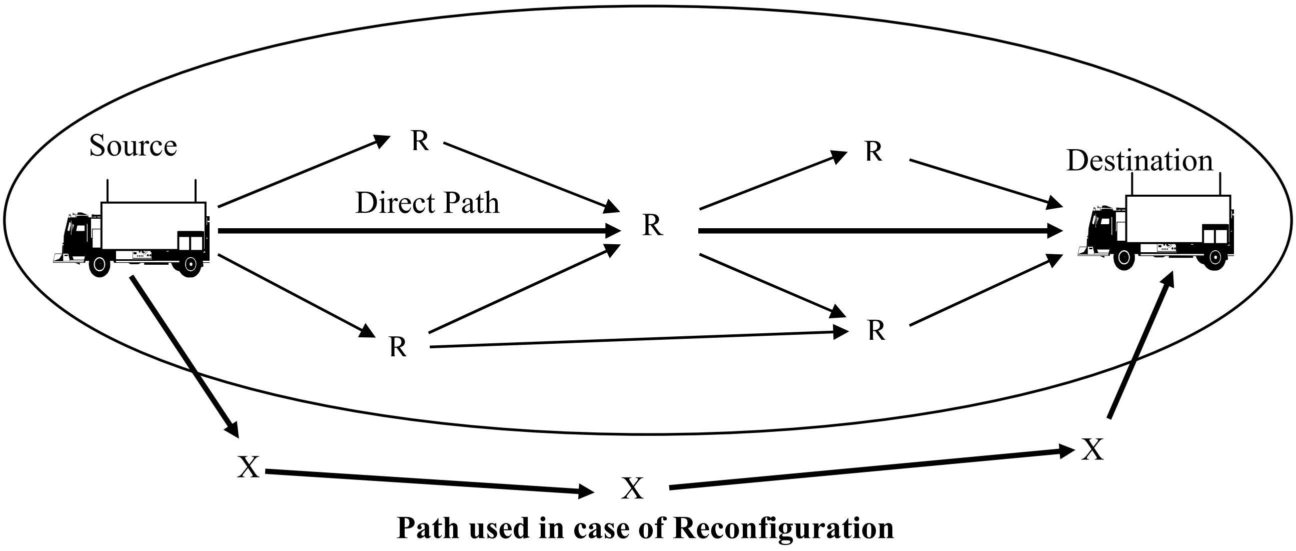


Figure 9.1 Classic and Needline Repromulgation Relay

The following specific Needline functions and procedures have been defined for incorporation in the MIDS LVT:

a. PPLI Needline PG - each ground station must transmit its identification and its location to the others; thus the PPLI messages must be conveyed by the Needline.

b. Extrapolation - the extrapolation process is applied to positional data of some Fixed Word Format (FWF) messages. Therefore, in the MIDS LVT, the extrapolation mechanism is selectable an a PG by PG basis.

9.2.2 Needline-Identification

To enable identification and recognition by transmitters (source terminals) and receivers (destination terminals), a Needline Data Block Identification (NDBI) of 16 bits is used. This NDBI contains:

a. Route Number (RN).

b. Participation Group (PG) number.

c. Terminal Roles (TR).

Routes are numbered between 0 and 15 and are used to define a specific path for message exchange. Needline PGs range from numbered in the range 33 to 511. The network design authority has to define transmission conditions for each PG (e.g. Packing Limits, Time Slot Assignments, etc.). The terminal role can be either Source or Destination; for relay, the Needline identification is not required. Specific Source terminal information, that is to be included in a transmission, consists of a list of addresses, etc. Destination terminals include information on paired Needlines for Receipt/Compliance (R/C) purposes, an End Of Message (EOM) header, etc.

9.2.3 Needline Creation

Within a MIDS network a Needline is created through repromulgation filtering at each terminal. Filters are selected on a PG (33-511) basis for each PG Route (0-15) and are determined by the following three parameters:

a. Action Route Indicator Parameter (ARIP) - indicates to the terminal to activate RIC protocols. The default value is set to 0, which means that the message will not be processed.

b. Interest Route Indicator Parameter (IRIP) - indicates that the host is the message destination. The default value is set to 1, which means that the message is not to be transmitted to the host.

c. Relay Route Indicator Parameter (RRIP) - indicates that the terminal is a relay on the Needline. The default value is set to 1, which means that the message is not to be relayed.

Repromulgation relay can be managed remotely (i.e. via the network) by a specific JTIDS Unit (JU). The J0.4 message will have a capability to change the RRJP and IRIP via the network.

Figure 9-2 gives an example of a typical Needline organisation with all required parameters. The Source unit (S) sends out a message to two destinations units (D).

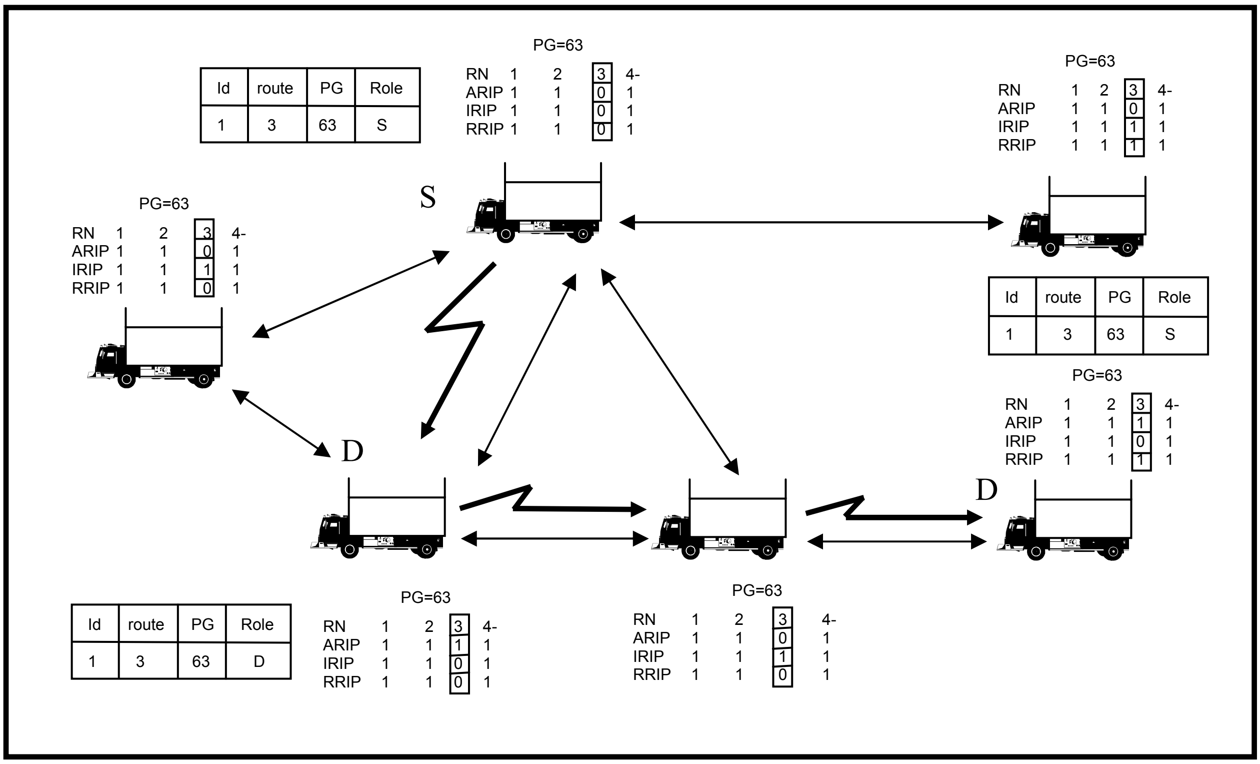


Figure 9-2 Example of Needline Organisation

9.3. SPECIFIC NETWORK MANAGEMENT ASPECTS

9.3.1 Dynamic Network Management

Some of the networks used by ground forces have to be monitored and dynamically managed. Therefore a dedicated organisation has been defined based on a central Network Control Station (NCS). The following specific network management functions have been identified:

a. Allocation of resources among Ground Units (only in the Ground dedicated time slot)

b. Computation of the relay position over the deployment period.

c. Monitoring network status.

d. Checking communication quality between MIDS units.

e. Maintaining network communications.

9.3.2 The NCS role

The dynamic network management role of the NCS can be divided into two main steps as shown in Figure 9-3.

a. Before the deployment of the NCS allocates Time Slot resources among the different units. It computes the positions of the relay stations over the deployment period and defines the message routes in accordance with the operational requirements and the terrain relief characteristics. The result of this first message is the generation of initialisation parameters for the MIDS terminals.

b. During the deployment phase and the following actions, the NCS monitors the network and checks the connectivity quality between MIDS units. The NCS can react or respond to a network problem and will determine new resource allocations; new relay locations and new routes to maintain network communications. It can also perform a complete modification of the communication plan in force to in order to comply with the requirements for either a new operational mission or a new organisation.

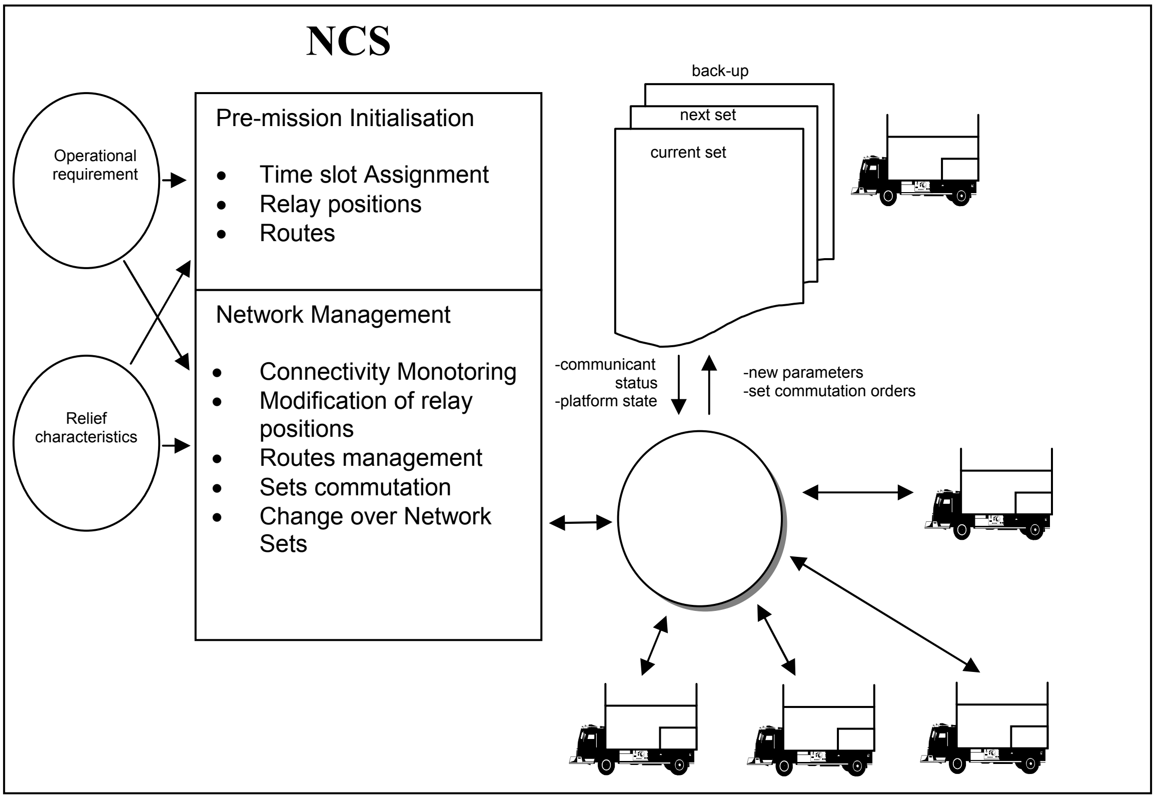


Figure 9.3 Dynamic Network Management - Role of the NCS

9.3.3 Dynamic Network Control

To enable dynamic network control to function, each terminal must hold multiple sets of Network Organisations (MIDS LVT can store 8 sets of initialisation parameters). One network set is needed as the current set, while the others may be used to store other specific Network Organisations, for example back-up configurations (due to NCS destruction) or deployment in small numbers. The stored sets can be modified by the NCS over-the-air in accordance with the current tactical situation. Upon receiving a request from the NCS, all units will switch from the current network organisation to another one, already stored in the terminal. This global change-over avoids network organisation discrepancies and should result in more satisfactory information exchange.

9.4 RELATIONSHIP BETWEEN NEEDLINE AND NETWORK PARTICIPATION GROUPS

9.4.1 Deployment Scenarios

The following points apply to deployments:

a. The tie between the Needline PG and the NPG is made by a Generic Ground Station. The GGS is the upper level of the Needline network and is the interface between the Needline PG and the NPG.

b. The NCS always subscribes to the technical NPG and communicates with army platforms on the Needline PG.

c. Ground platforms are only in receive mode on NPG.

d. All army platforms are capable of communicating within the Needline PG. If direct communication with an external destination is required it is necessary to convey the message up to the GGS.

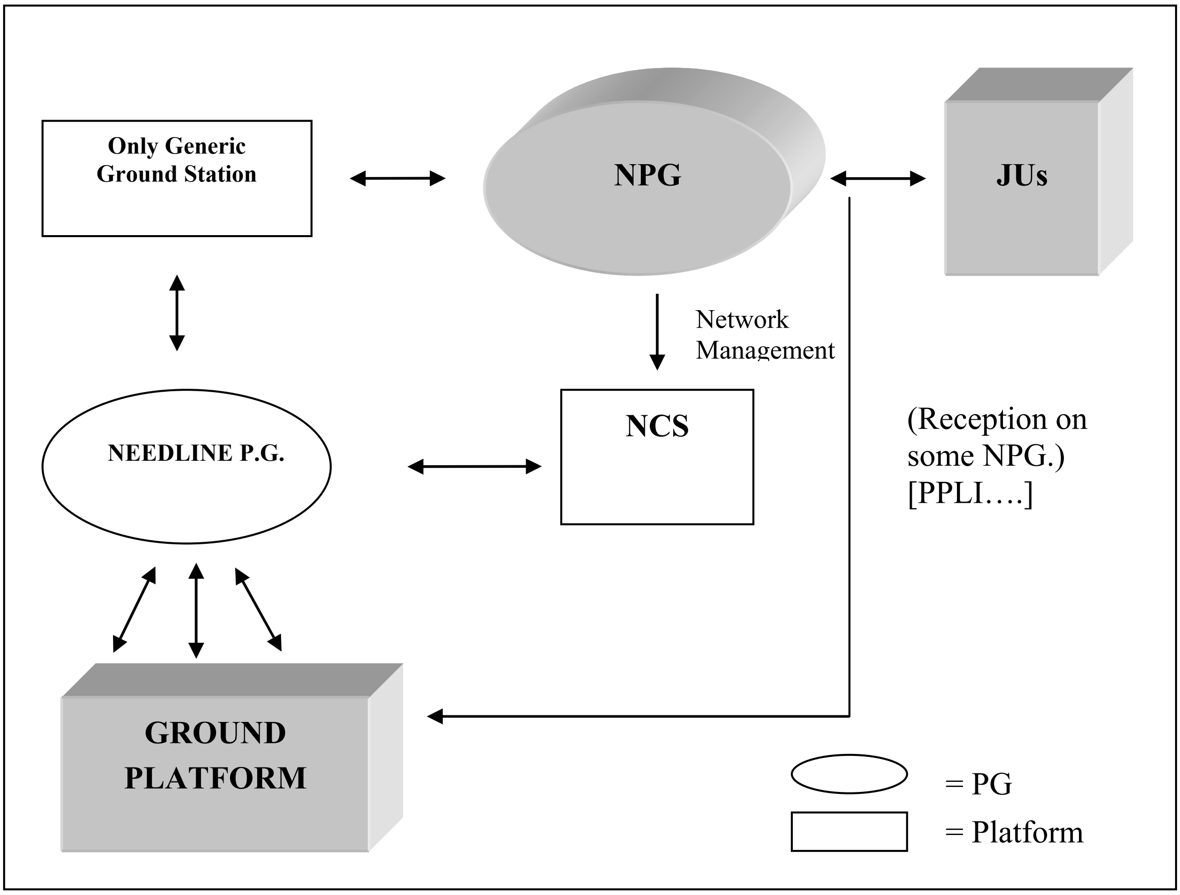


Figure 9.4 Deployment Scenarios

9.5 PROCEDURES ASPECTS

9.5.1 Organisation

The Land Component Commander (LCC) has the responsibility to organise and to implement overall communications and to manage army networks. In particular, he directs the manoeuvre of the technical ground stations (NCS and relay). His action consists of the realisation of fielding ground stations for the operational deployment. The NCS is the dedicated station which is allowed to act in the field. The NCS has the following functional capabilities:

a. Network design

b. Network management.

c. Network control and supervision.

9.5.2 Network Design

The NATO ICD only knows the GGS. The ICD allocates to this ground station all of the time slots required for the manoeuvre (Army dedicated Time slots, Transmit and Receive PPLI Time slots, Transmit RTT Time slots). The NCS, after computing the time slots blocks, distributes them to all ground stations, except for the GGS which has already taken into account in the ICD. The NCS then computes the Needlines and proposes locations for relay using an automated cartographic tool. Once done, all initialisation data for the stations is ready for distribution.

9.5.3 Network Management

In case of connectivity problems or a change of operational requirement, the NCS has the capability to modify relay locations using the JO.4 Repromulgation Relay Control message; to change the initialisation set using the JO.3 Set Management Word message or to transmit a new TS allocation in a defined Needline PG using the JO.3 message. All these messages are addressed in a point-to-point basis on a Needline PG using the technical FWF messages. Other modifications can be held for management and supervision by national VMF messages.

9.5.4 Network Control and Supervision

Each station computes its connectivity table in one jump radius that is transmitted to the NCS in a J1.4 message and the Needline CNN PG. The NCS then computes the global connectivity. Connectivity Needline status is maintaining by each station (source or destination) using an embedded MIDS-LVT connection monitoring function.

9.6 TECHNICAL RESPONSIBILITIES

9.6.1 Network Time Reference (NTR)

A ground unit can assume the role of NTR. It is preferable to ensure that the designated unit within LOS with most, if not all, of other units. The NTR uses the J0.0 Net Entry message allowing other JUs to achieve coarse synchronisation. Fine synchronisation is achieved by either active or passive means according to terminal initialisation. It is not intended to use Helicopters as the NTR due to their missions and their mobility.

9.6.2 Initial Entry JU

Several JUs can assume the role of IEJU. This function is automatically performed by the MIDS-LVT. In the army, all ground units can assume this role, particularly the relay units.

9.6.3 Stand-by Manager

The NCS assumes the role of the Stand-by Manager, corresponding to an internal army Network Manager having the capability of controlling communications, maintaining networks performance and supervising reconfiguration. The dynamic management function of the NCS allows it to:

a. Allocate TS dynamically.

b. Manage relay dynamically.

c. Store all network modifications during the mission.

9.6.4 Cryptonet Manager

The NCS does not have capacity to be Cryptonet Manager. It has only the capability to affect the CVLL when designing army networks and to store the dedicated keys received from the joint staff cryptonet manager before distributing than to ground units.

LIST OF EFFECTIVE PAGES

VOLUME 1

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 XVI (RB)	NATO UNCLASSIFIED	ORIGINAL
1-1 to 1-3 (RB)	NATO UNCLASSIFIED	ORIGINAL
2-1 to 2-17 (RB)	NATO UNCLASSIFIED	ORIGINAL
3-1 to 3-6	NATO UNCLASSIFIED	ORIGINAL
4-1 to 4-22	NATO UNCLASSIFIED	ORIGINAL
5-1 to 5-15 (RB)	NATO UNCLASSIFIED	ORIGINAL
6-1 to 6-67 (RB)	NATO UNCLASSIFIED	ORIGINAL
7-1 to 7-12	NATO UNCLASSIFIED	ORIGINAL
8-1 to 8-12	NATO UNCLASSIFIED	ORIGINAL
9-1 to 9-9 (RB)	NATO UNCLASSIFIED	ORIGINAL
A-1 (RB)	NATO UNCLASSIFIED	ORIGINAL
A-1-1 to A-1-10	NATO UNCLASSIFIED	ORIGINAL
A-2-1 to A-2-4	NATO UNCLASSIFIED	ORIGINAL
B-1 (RB)	NATO UNCLASSIFIED	ORIGINAL
B-1-1 to B-1-7 (RB)	NATO UNCLASSIFIED	ORIGINAL
B-2-1 to B-2-3 (RB)	NATO UNCLASSIFIED	ORIGINAL
C-1 (RB)	NATO UNCLASSIFIED	ORIGINAL
C-1-1 to C-1-2	NATO UNCLASSIFIED	ORIGINAL
C-2-1 (RB)	NATO UNCLASSIFIED	ORIGINAL
C-3-1 to C-3-2	NATO UNCLASSIFIED	ORIGINAL
C-4-1 to C-4-3 (RB)	NATO UNCLASSIFIED	ORIGINAL
C-5-1 to C-5-2	NATO UNCLASSIFIED	ORIGINAL
D-1 (RB)	NATO UNCLASSIFIED	ORIGINAL
D-1-1 to D-17 (RB)	NATO UNCLASSIFIED	ORIGINAL
LEP-1 (RB)	NATO UNCLASSIFIED	ORIGINAL