NATO OTAN

NATO STANDARDIZATION AGENCY
AGENCE OTAN DE NORMALISATION

NSA

27 April 2007 NSA/0429(2007)-C3/4211

STANAG 4211 C3 (EDITION 3) – THE NATO MULTI-CHANNEL TACTICAL DIGITAL GATEWAY AND THE STANAG 5040 ANALOGUE GATEWAY - SYSTEM CONTROL STANDARDS -

References:

a. MAS/413-EL/4211 dated 15 November 1993(Edition 2)
b AC/322(SC/6)(DS(2006)0001, dated 6/03/2006, Para 10.2 and Annex 38
c. AC/322(SC/6)N/418, dated 29 November 2001 (NU) – Ratification Request

1. The enclosed NATO Standardization Agreement, which has been ratified by nations as reflected in the **NATO Standardization Document Database (NSDD)**, is promulgated herewith.

2. The references listed above are to be destroyed in accordance with local document destruction procedures.

ACTION BY NATIONAL STAFFS

3. National staffs are requested to examine their ratification status of the STANAG and, if they have not already done so, advise the NHQC3S, through their national delegation as appropriate of their intention regarding its ratification and implementation.

J. MAJ
Major General, POL(A)
Director, NSA

Enclosure:
STANAG 4211 (Edition 3)

STANAG 4211
(Edition 3)

NORTH ATLANTIC TREATY ORGANIZATION
(NATO)

NATO STANDARDIZATION AGENCY
(NSA)

STANDARDIZATION AGREEMENT
(STANAG)

SUBJECT: THE NATO MULTI-CHANNEL TACTICAL DIGITAL GATEWAY AND THE STANAG 5040 ANALOGUE GATEWAY - SYSTEM CONTROL STANDARDS -

Promulgated on 27 April 2007

J. MAJ
Major General, POL(A))
Director, NSA

RECORD OF AMENDMENTS

No.	Reference/date of Amendment	Date Entered	Signature

EXPLANATORY NOTES

AGREEMENT

1. This NATO Standardization Agreement (STANAG) is promulgated by the Director NATO Standardization Agency under the authority vested in him by the NATO Standardization Organisation Charter.

2. No departure may be made from the agreement without informing the tasking authority in the form of a reservation. Nations may propose changes at any time to the tasking authority where they will be processed in the same manner as the original agreement.

3. Ratifying nations have agreed that national orders, manuals and instructions implementing this STANAG will include a reference to the STANAG number for purposes of identification.

RATIFICATION, IMPLEMENTATION AND RESERVATIONS

4. Ratification, implementation and reservation details are available on request or through the NSA websites (internet http://nsa.nato.int; NATO Secure WAN http://nsa.hq.nato.int).

FEEDBACK

5. Any comments concerning this publication should be directed to NATO/NSA – Bvd Leopold III - 1110 Brussels - BE.

NATO STANDARDIZATION AGREEMENT
(STANAG)

THE NATO MULTI-CHANNEL TACTICAL DIGITAL GATEWAY
AND THE STANAG 5040 ANALOGUE GATEWAY
- SYSTEM CONTROL STANDARDS -

Annexes:-
A. Tactical Information and Communication Plans
B. Details for the Deployment of a Gateway
C. Re-deployment of Gateways
D. International Routeing and Directory Information
E. Management
F. COMSEC Management
G. Engineering Order Wire (EOW) Operation
H. Subscriber Assistance
I. NPICS Proforma

Related Documents:-

STANAG 4206 - The NATO Multi-Channel Tactical Digital Gateway System Standards.

STANAG 4207 - The NATO Multi-Channel Tactical Digital Gateway Multiplex Group Framing Standards.

STANAG 4208 - The NATO Multi-Channel Tactical Digital Gateway Signalling Standards.

STANAG 4209 - The NATO Multi-Channel Tactical Digital Gateway Standards for Analogue to Digital Conversion of Speech Signals.

STANAG 4210 - The NATO Multi-Channel Tactical Digital Gateway Cable Link Standards.

STANAG 4212 - The NATO Multi-Channel Tactical Digital Gateway Radio Relay Link Standards.

STANAG 4213 - The NATO Multi-Channel Tactical Digital Gateway Data Transmission Standards.

STANAG 4214 - International Routing and Directory for Tactical Communications Systems.

STANAG 4249 - The NATO Multi-Channel Tactical Digital Gateway Data Transmission Standards (Packet Switching Service).

STANAG 4290 - NATO Multi-Channel Tactical Digital Gateway Cable Link (Optical) Standards.

STANAG 5040 - NATO Automatic and Semi-automatic Interfaces between the National Switched Telecommunications Systems of the Combat Zone and between these Systems and the NATO Integrated Communications System (NICS) - Period from 1979 to the 1990s.

STANAG 5048 - The minimum scale of communications for the NATO Land Forces - Requirements, Principles and Procedures.

STANAG 4484 - Overall Super High Frequency (SHF) Military Satellite Communications (MILSATCOM) Interoperability Standard.

STANAG 4578 - The NATO Multi-Channel Digital Strategic - Tactical Gateway.

INTRODUCTION

1. This STANAG is used in the specification of 2 gateways as follows:

a. This STANAG is one of a series which, when taken together, specify all the technical characteristics, parameters and procedures necessary for two NATO tactical digital communications systems (networks) to interconnect and exchange traffic via a gateway.

b. This STANAG specifies the system control standards to be used for analogue gateways according to STANAG 5040.

2. STANAG 4206, the NATO Multi-Channel Tactical Digital Gateway (DG) - System Standards, provides an overview of the gateway concept and summarises the key

requirements and characteristics contained within this and other STANAGs of this series.

AIM

3. The aim of this agreement is to define the common standards including the information which must be exchanged to enable the establishment, operation, restoration, disengagement of Gateway Facilities and the data base required to provide planning and operation of gateways between NATO tactical analogue and digital communications systems. This agreement also defines the common standards for assistance of subscribers in gaining full accessibility to an adjoining network via gateway facilities.

AGREEMENT

4. The participating nations agree to use the standards contained in this STANAG as the system control standards in the exchange of traffic between tactical digital and analogue systems via a gateway.

GENERAL

5.1 The establishment, management and control of Gateways will be the responsibility of the Tactical Communications Control Elements of the adjoining tactical digital networks. The necessary exchange of information between national network control elements shall include, but shall not be limited to, the following:

a. tactical information and communication plans;
b. details for the deployment of gateways;
c. re-deployment of gateways;
d. international routeing and directory information;
e. management;
f. COMSEC management;
g. EOW operation.

5.2 Subscriber assistance will be the responsibility of the Tactical Communication Control Elements of the adjoining tactical digital networks.

The subscriber assistance to be provided by voice shall include, but shall not be limited to, the following:

a. set up assistance;

b. information on modes;
c. information on subscriber numbers. (See Annex H).

The 7 digit address of Subscriber Assistance is identified in STANAG 4214.

5.3 System management will be the responsibility of the Tactical Communication Control Elements of the adjoining tactical digital networks. System management is responsible for tactical and technical planning and control of the communication system within its area of responsibility.

The 7 digit address of System Management is identified in STANAG 4214.

6. Some information is to be exchanged in specially-formatted messages. These are detailed in Annex E Appendices 1, 2, 3 and 11.

IMPLEMENTATION OF AGREEMENT

7. This STANAG is implemented by a nation when it has adopted the multi-channel tactical digital gateway system control standards as specified in this agreement and has reflected their adoption in the relevant documentation.

TACTICAL INFORMATION AND COMMUNICATION PLANS

1. TACTICAL INFORMATION REQUIREMENTS

Communications must support the tactical plans. Since tactical involvement is necessary, information must be exchanged relating to the deployment and management of trunk nodes close to the boundaries between national tactical forces. This information must include timings as well as locations.

2. COMMUNICATION PLANNING INFORMATION

Based on tactical requirements, the national tactical communication control elements will develop detailed gateway deployment information which shall include, but shall not be limited to, the following:

a. responsibilities for gateway management in accordance with STANAG 5048;

b. geographical data regarding the deployment of gateway facilities;

c. type of interface or gateway (5040 analogue interface, 4206 digital gateway, 4578 Digital Strategic – Tactical Gateway);

d. available type of link (electrical cable, optical cable, radio-relay, or satellite).

e. gateway usage (formations reached through the gateway: NIACs in own area under control).

f. own system link security status (crypto secure, physically secure, insecure).

g. own system limiting factors (for example: frequency band, antenna polarisation, restricted areas of coverage, type of signalling).

This Page is Blank

DETAILS FOR THE DEPLOYMENT OF A GATEWAY

1. Communications orders pertaining to a gateway (both active and for contingency plans) will be issued within each national network and will be made available to those control elements which are responsible for nodes scheduled to operate gateway links. These orders will be co-ordinated between the national communication control elements of the adjoining networks to ensure availability of the necessary interface equipment and to ensure conformity of the essential interface parameters. The information contained in these communications orders shall include, but not be limited to, the information contained in paragraphs 2 to 13 of this Annex.

2. Interfacing Networks

a. Nation A (left/higher formation).

b. Nation B (right/lower formation).

c. Gateway node type, identity, and grid reference.

3. Type of Link.

a. Cable.

(1) Cable terminal grid reference.
(2) Transmission bit rate - 256 or 512 kbit/s.
(3) Electrical or optical.

b. Radio Relay. (radio relay terminals to be provided by each nation):-

(1) Grid references of radio relay terminals.
(2) Azimuth A to B, B to A.
(3) Antenna polarisation.
(4) Operating and alternative frequencies.
(5) Frequency deviation.
(6) Transmission bit rate - 256 or 512 kbit/s.

c. Satellite. (satellite ground terminal to be provided at each end of the satellite link):-

(1) Latitude and Longitude for each Satellite Ground Terminal
(2) Azimuth and elevation for each Satellite Ground Terminal
(3) Transmit and receive frequencies for each Satellite Ground Terminal.

(4) Maximum allowed transmitted power for each Satellite Ground Terminal.
(5) Satellite Beacon frequency
(6) Antenna Polarisation for each Satellite Ground Terminal
(7) Modem type. Modulation scheme may include:
  i. Hop Rate.
  ii. Hop Bandwidth.
  iii. Forbidden Frequency Bands.
(8) Transmission bit rate – 256 or 512 kbit/s
(9) Time satellite is available.
(10) The terminal sensitivity (G/T) value (receive gain to noise temperature ratio(dB/K))
(11) Miscellaneous modem settings (i.e. manufacturer specific settings).
(12) The required gain step on the satellite transponder.

4. Planned operational statuses. (working, standby, reserve).

5. Planning Times. Standard time duration of stated activities for planning purposes (eg establishment, closure, conversion to another planned operational status, of the gateway).

6. Gateway Security Status. (crypto secure, physically secure, insecure). In the case of a crypto secure link, refer to Annex F for COMSEC parameters.

7. Trunk Bit Rate. 256kbit/sec or 512kbit/sec.

8. Channel Planning. (5040 - numbers of analogue and of digital channels; DG - numbers of non-dedicated channels).

9. Directory. Telephone directory numbers of responsible system managers.

10. Gateway Limiting Factors. Frequency band, antenna polarisation, restricted areas of coverage, type of signalling.

11. Engineering Orderwire (EOW)

  a. COMSEC Parameters (See Annex F).
  b. EOW Activation Time: Date Time Group.

12. Type of Signalling

  a. 4 block ARQ.
  b. 6 block ARQ.

c. Long Delay Link (e.g. satellite)

13. Routeing Prefixes (See Annex D).

a. NIACs for the circuit switched networks at each side of the gateway.

b. NIACs of other circuit switched networks accessible via the gateway seen from both sides of the gateway.

14. Permanent Connections

a. Duration for each permanent connection

b. Timeslots used for each permanent connection (dedicated channels)

c. Application of each permanent connection, (e.g. X.75 Packet Switching).

d. Application parameters, (e.g. for packet switching, Class 1 or class 4).

e. NIACs for the “Application” (e.g. packet switching) networks at either side of the gateway. (Note 1)

f. NIACs of the other “Application networks” accessible via the gateway seen from both sides of the gateway. (Note 1).

Note 1: The NIACs used by the Application networks using the Permanent Connection may be different from the NIACs used by the circuit switching network.

This page is Blank

RE-DEPLOYMENT OF GATEWAYS

1. Dynamic changes of the national networks necessitate re-deployment of gateways. Appropriate communications orders will be developed and issued when possible. These orders shall include:

a. definition and schedule of specific active gateways;

b. definition and schedule of alternate (standby) gateways.

2. Local co-ordination between nodal control elements of the gateway nodes shall be exercised in the event that scheduled activities cannot be implemented. Changes of schedule or gateway parameters shall be locally determined in the absence of appropriate communications orders.

This Page is Blank

INTERNATIONAL ROUTEING AND DIRECTORY INFORMATION

1. The following information should be provided to Gateway Facilities when a new gateway is brought into operation:-

a. neighbouring network NIAC;

b. networks reached via outgoing transit calls from gateway (NIAC)1......(NIAC)n;

c. formations under command (See Note below).

2. From the above information, it will be possible for the Gateway Facility to compose a list of NIs and ACs reachable through the Gateway for routeing purposes or to use the information directly, if an `interim' system is only able to route on a complete 6 digit prefix. In addition, whenever a gateway to a new network becomes available or when all gateways to a network are closed or whenever a new formation comes under command or a formation ceases to be under command, the controlling system management function will inform all other system management functions in concerned national networks in order that routing tables may be updated.

3. See also STANAG 4214 (International Routeing and Directory for Tactical Communications Systems) Annex D (Routeing Information to be exchanged Between System Managers).

NOTE:

It is the ultimate aim of this STANAG that the information exchange associated with formations under command should become unnecessary as all networks achieve the capability for multiple routeing and duplicated prefixes.

4. The NIACs used by the Application using a Permanent Connection may be different from the NIACs used by the circuit switching network. It is therefore necessary to specify the NIACs used by the Circuit switching network and Application networks using the permanent connection separately.

This page is Blank

MANAGEMENT

1. Information Exchange

After prior contact on System Executive and Planning (SEP) level for planning purposes, further information exchange will take place, via pre-existing communications methods, between the Operational System Control (OSCs) appointed by SEP.

For system control purposes, information will be exchanged as set out in Table 1. Some information is most conveniently exchanged in specially formatted messages. These are detailed in Appendices 1, 2, 3,and 9.

Table 1 - Information Exchange

		Voice		Tg, Data orFax	
1.	To Establish	Nation		Nation	
		A	B	A	B
	a. Contact on Staff level	------> <------			
	b. Locations and identities of suitable trunk nodes of both Nations A and B	------> <------		-------> <-------	
	c. Identity and location of selected trunk nodes of Nations A and B	------> <------		-------> <-------	
	d. Path Analysis by Nation A - if necessary			------->	
	e. RR frequencies (transmit & receive)			-------> <-------	
	f. Antenna azimuth and polarisation			-------> <-------	
	g. Crypto Information (traffic & EOW)			------->	
	h. Status (working, standby, reserve)			-------> <-------	
	j. Time gateway is to be available			-------> <-------	

Table 1 - Continued

		Voice		Tg, Data or Fax	
1.	To Establish (continued)	Nation		Nation	
		A	B	A	B
	k. Special facilities (usage of dedicated channels for permanent connections).			-------> <-------	
	l. Satellite parameters for each ground station.			-------> <-------	
2.	To Control				
	a. Traffic Load			-------> <-------	
	b. Frequency changes			------->	
	c. Crypto Information (traffic & EOW)			------->	
	d. Change of Status, operational/security.			-------> <-------	
	e. Change of channel utilisation			-------> <-------	
	f. Change of plans	-------> <-------		-------> <-------	
	g. Change of quality reports			-------> <-------	
	h. Changes in accessible NIACs			-------> <-------	
3.	To Close Down				
	a. Time of closing gateway			-------> <-------	

LEGEND:- 1. Nation A - left or higher formation.
2. Nation B - right or lower formation.

2. Types and Formats of Messages

Four types of messages have been identified which require special formats. These are set out in Appendices 1, 2, 3 and 9.

They are:

a. Appendix 1: Request message - may be sent by left or right or higher or lower formation;

b. Appendix 2: Acceptance message - sent by the recipient of the request message. It need not be sent if the recipient of a Request Message can respond promptly with a Warning Order or Executive Order.

c. Appendix 3: Warning order/Executive Order - sent by left/higher formation. Sent as Warning Order if the full information for the Executive order is not yet available.

d. Appendix 9: Gateway status message - sent by the responsible FC up the system management command chain for dissemination within their SEP area whenever the status of a gateway changes. This SEP area is that of the SEP currently commanding the FC involved: the FC and SEP may be of different nations. There is no need for the routine exchange of this information between system managers on either side of the gateway to which it refers, because they will have the same information already from their own FCs.

NOTE:- Other information is exchanged as shown in Table 1 but this does not require specially formatted messages.

3. Gateway Engineering

3.1 General

Responsibility for the set-up and fault location on gateways will be in accordance with STANAG 5048 (left to right and higher to lower).
Radio relay sections will be engineered on the initiative of the responsible party, using the quality monitor equipment specified in STANAG 4212, Annex E, to a BER better than 1 in 10^4 and be brought into operation.

Cable sections (both electrical and optical) will be checked via voice EOW contact and be brought into operation.

Satellite sections will be engineered on the initiative of the responsible party.

3.2 Fault Location

If the responsible nation judges the link not to fulfil the STANAG 4206 specified requirements, it will initiate fault location on the basis of looping back the link on all local and transmission relay interfaces ie, in the example configuration at Figure 1, on points A, B, D, D, B and A. The other party will be instructed to install and remove the loop-back via voice commands on the EOW. It is up to the responsible nation to decide what signal he uses to measure the link: loop- back requires the same crypto key in both send and return directions. Nations shall have a loopback capability at all local and transmission relay interfaces.

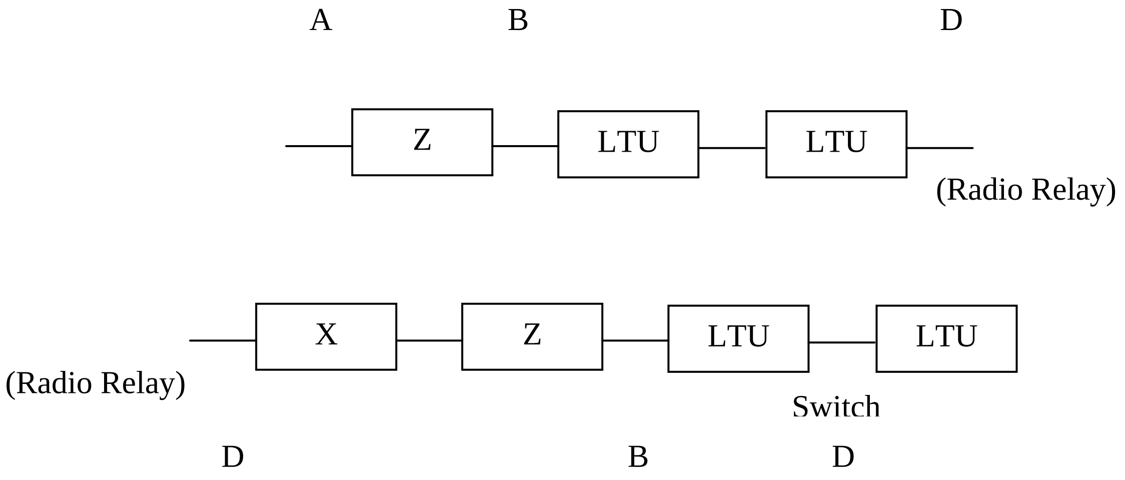


FIGURE 1 - EXAMPLE OF LOOPING BACK POINTS

3.3 Opening a Gateway Link

a. This paragraph describes in detail the procedures to be followed in opening a gateway. Prior distribution of crypto variables is assumed.

b. The actual interconnection point on the gateway link can be either on radio (`in the air') (radio relay or satellite) or on cable (electrical or optical).

c. Start State

The facilities controller at each end of the gateway will have been given the information necessary to establish the link.

d. End State. All EOW circuits are established and working.

e. The link is opened, quality checked and put into service. The link is available for traffic and link quality is monitored.

f. The sequence of events from start to end states is given in the following appendices:-

Appendix 4, Sequence to Open Radio Link;
Appendix 5, Sequence to Open Cable Link;
Appendix 6, Sequence to Engineer Satellite Link;
Appendix 7, Sequence to Open Switch to Switch Traffic;
Appendix 8, Sequence to Open a Permanent Connection;
Appendix 9, Sequence to Monitor Switch to Switch Traffic.

3.4 Closing the Gateway Link

When the OSC's determine that a gateway is to be closed, the Facilities Controllers (FCs) will be instructed accordingly and will carry out the sequence given in Appendix 8.

List of Appendices:

1. Request Message.
2. Acceptance Message.
3. Warning Order/Executive Order.
4. Sequence to Open Radio Link.
5. Sequence to Open Cable Link.
6. Sequence to Engineer Satellite Link.
7. Sequence to Open Switch-to-Switch Traffic.
8. Sequence to Open a Permanent Connection.
9. Sequence to Monitor Switch-to-Switch Traffic.
10. Sequence to Close the Gateway.
11. Gateway Status Message.

This page is Blank

REQUEST MESSAGE

From: ....

To: ....

Gateway Request

1. Gateway request number ....

2. From ....[Formation]

3. To ....[Formation]

4. Times - establishment, closure, [conversion to planned status 2 - optional].

5. Type of Gateway

   a. 5040

   b. Digital Gateway (STANAG 4206)

   c. Digital Strategic Tactical Gateway (STANAG 4578)

6. Type of Link – copper cable, radio relay, satellite, optical cable

7. Status

   a. identity of controlling side.

   b. security status - crypto secure, physically secure, insecure.

   c. operational status 1 - working, standby, or reserve.

   [d. operational status 2 - working, standby, or reserve - optional].

8. Special facilities required.

9. Available Gateway nodes (in order of preference) by Identity and Location (UTM grid)

10. For each Gateway node, any limiting factors (for example: frequency band, antenna polarisation, restricted areas of coverage, type of link, type of signalling).

11. NIACs:

a. NIAC of requesting side (for the circuit switching network).

b. NIACs accessible from requesting side (for the circuit switching network).

12. Satellite link parameters if relevant: Latitude and Longitude for each Satellite Ground Terminal, Azimuth and elevation for each Satellite Ground Terminal, Transmit and receive frequencies for each Satellite Ground Terminal, Maximum allowed transmitted power for each Satellite Ground Terminal, Satellite Beacon frequency, Antenna Polarisation for each Satellite Ground Terminal, Modem type (including Hop Rate, Hop Bandwidth, Forbidden Frequency Bands), Transmission bit rate – 256 or 512 kbit/s, Time satellite is available, The terminal sensitivity (G/T) value, miscellaneous modem settings, the required gain step on the satellite transponder.

13. Permanent Connection

a. Times - establishment, closure

b. Timeslots used for each permanent connection

c. Application of each permanent connection, (e.g. X.75 Packet Switching).

d. Application parameters, (e.g. for packet switching, Class 1 or class 4)

e. NIAC of requesting side (for the Application network). (Note 1)

f. NIACs accessible from requesting side (for the Application network). (Note 1)

Note 1 only required when the NIACs for the Application network using the Permanent Connection are different from the NIACs for the circuit switching network.

ACCEPTANCE MESSAGE

From: ....

To: ....

Gateway Acceptance

1. Gateway request number .... of .... (DTG)

2. From ....

3. To ....

4. Available Gateway nodes (in order of preference) by Identity and Location (UTM grid).

5. For each Gateway node, any limiting factors (for example: frequency band, antenna polarisation, restricted areas of coverage, type of signalling).

6. NIACs:

   a. NIAC of accepting side (for the circuit switching network).

   b. NIACs permitted to be accessed from accepting side (for the circuit switching network).

7. Type of connection (Type of Gateway and Link) (only if different from Request Message).

8. Times (only if different from Request Message).

9. Status (only if different from Request Message).

10. Satellite link parameters if relevant: Latitude and Longitude for each Satellite Ground Terminal, Azimuth and elevation for each Satellite Ground Terminal, Transmit and receive frequencies for each Satellite Ground Terminal, Maximum allowed transmitted power for each Satellite Ground Terminal, Satellite Beacon frequency, Antenna Polarisation for each Satellite Ground Terminal, Modem type (including Hop Rate, Hop Bandwidth, Forbidden Frequency Bands), Transmission bit rate - 256 or 512 kbit/s, Time satellite is

available, The terminal sensitivity (G/T) value, miscellaneous modem settings, the required gain step on the satellite transponder.

11. Permanent Connection

a. Times - establishment, closure

b. Timeslots used for each permanent connection

c. Application of each permanent connection, (e.g. X.75 Packet Switching).

d. Application parameters, (e.g. for packet switching, Class 1 or class 4)

e. NIAC of accepting side. (Note 1)

f. NIACs permitted to be accessed from accepting side. (Note 1)

Note 1 only required when the NIACs for the Application networking using the Permanent Connection are different from the NIACs for the circuit switching network.

WARNING/EXECUTIVE ORDER

From: ....

To: ....

Gateway Warning/Executive(*) Order
(* Delete whichever is inappropriate)

1. Gateway request number .... of .... (DTG)

2. Selected node Nation A (left or higher formation) (identity and location)

3. Selected node Nation B (right or lower formation) (identity and location)

4. Times - establishment, closure, [conversion to planned status 2 - optional].

5. Status

   a. identity of controlling side.

   b. security status - crypto secure, physically secure, insecure.

   c. operational status 1 - working, standby, reserve.

   d. operational status 2 - working, standby, reserve - optional].

6. Special facilities required

7. Crypto key settings:-

   a. EOW.
   b. Traffic.

8. Type of Link.

   a. Cable:
      (1) cable terminations grid references;
      (2) transmission bit rate - 256 or 512 kbit/s;
      (3) electrical or optical.

   b. Radio:
      (1) grid reference of radio terminals;

(2) azimuth A to B, B to A;
(3) antenna polarisation;
(4) operational and alternative frequencies;
(5) frequency deviation;
(6) transmission bit rate - 256 or 512 kbit/s.

c. Satellite (satellite ground terminal to be provided at each end of the satellite link):-

(1) Latitude and Longitude for each Satellite Ground Terminal
(2) Azimuth and elevation for each Satellite Ground Terminal
(3) Transmit and receive frequencies for each Satellite Ground Terminal.
(4) Maximum allowed transmitted power for each Satellite Ground Terminal.
(5) Satellite Beacon frequency
(6) Antenna Polarisation for each Satellite Ground Terminal
(7) Modem type. Modulation scheme may include:
i. Hop Rate.
ii. Hop Bandwidth.
iii. Forbidden Frequency Bands.
(8) Transmission bit rate – 256 or 512 kbit/s
(9) Time satellite is available.
(10) The terminal sensitivity (G/T) value (receive gain to noise temperature ratio(dB/K)).
(11) Miscellaneous modem settings (i.e. manufacturer specific settings).
(12) The required gain step on the satellite transponder.

d. Type of Gateway :–

a. 5040.
b. DG STANAG 4206.
c. DSTG STANAG 4578

9. Type of Signalling:-

a. 4 block ARQ.
b 6 block ARQ.
c. Long Delay Link (e.g. satellite).

10. Accessible NIACs - own and other NIACs on both controlling and subordinate sides.

11. System Manager Information - DNs of SEP, OSC, and FC on both controlling and subordinate sides of the gateway.

12. Channel Allocation.

a. 5040. Numbers of analogue and digital channels.

b. DG. Numbers of common user channels, dedicated channels, and channels reserved for packet switching.

13. Special instructions (if necessary).

Note. Serial 12 is used only for the Executive Order.

This page is Blank

SEQUENCE TO OPEN RADIO LINK

1. Content of executive order known in the nodes at both sides of the gateway to be opened.

2. Mast erected using established operational procedures with appropriate antennas directed approximately in the specified azimuth and using the specified polarisation.

3. Radio relay set to appropriate transmission bit rate and send-and-receive frequencies; antenna cables connected and receivers switched on.

4. Crypto variable for engineering order wire (EOW) initial key variable (KVO(I)) shall be inserted on the EOW unit.

5. Transmitter switched on at highest output power 15 minutes before the gateway is due to be available or upon reception from the other party.

6. Master calls via EOW using a uniform calling procedure as specified (see Annex G).

7. On both sides quality monitoring equipment is connected to traffic input or transceiver and is switched on.

8. Under control of master, antenna direction alignment starts. Master aligns first, then slave, then master, etc.

9. Under control of master, masts are lowered and/or transmit power is reduced but ensuring an adequate fade margin (10 dB) is maintained.

10. If the quality is satisfactory the quality monitoring equipment is removed and traffic switched through.

11. If the transmission quality is not satisfactory perform fault location procedure as stated in Annex E, paragraph 3.2.

This page is Blank

SEQUENCE TO OPEN CABLE LINK

1. Content of executive order known to nodes at both sides of the gateway.

2. Detachment of Nation A with detailed instructions set out to install the cable link.

3. Detachment of Nation A arrives with cable at the relevant location of Nation B where cable is hooked up to* LTU of Nation B.

4. KVO(I) is inserted.

5. The Master contacts the Slave via EOW.

6. Quality monitoring equipment is connected to the traffic input to measure quality of transmission.

7. If the quality is satisfactory, the quality monitoring equipment is removed and traffic switched through.

8. If the transmission quality is not satisfactory, perform fault location procedure as stated in Annex E, paragraph 3.2.

*NOTE: The term LTU used here to include the termination of an optical cable as an option.

This page is Blank

SEQUENCE TO ENGINEER SATELLITE CONNECTION

Note: this text is intended to apply to the combination of the Satellite Ground Terminal and SATCOM mode.

1. Content of executive order known in the nodes and Satellite Ground Terminals (SGT) at both sides of the gateway to be opened, and by the Satellite anchor.

2. Satellite antenna set-up using established operational procedures with antenna directed approximately in the specified azimuth and elevation, and with the specified polarisation.

3. Satellite Ground Terminal set to appropriate transmission bit rate and send-and-receive frequencies; antenna cables connected and receivers switched on.

4. Set speed buffers in the Satellite Ground Terminal.

5. Load necessary crypto variables (EOW and traffic as required).

6. Set loop backs.

7. Transmitter at SGT switched on at specified maximum output power 15 minutes before the gateway is due to be available or upon reception from the other party t check link is workable.

8. Master calls via EOW using a uniform calling procedure as specified (see Annex G).

9. On both sides quality monitoring equipment is connected to traffic input or transceiver and is switched on.

10. Both terminals to align on the satellite.

11. Under control of master, transmit power is reduced but ensuring an adequate fade margin (10 dB) is maintained.

12. If the quality is satisfactory the quality monitoring equipment and loopbacks are removed and traffic switched through.

13. If the transmission quality is not satisfactory perform fault location procedure as stated in Annex E, paragraph 3.2.

This page is Blank

SEQUENCE TO OPEN SWITCH-TO-SWITCH TRAFFIC

1. Equipment set to appropriate parameters. KVB(I) is inserted. Once frame alignment and crypto synchronism under KVB(I) is achieved, the gateway is now available for engineering purposes.

2. A gateway that is engineered but not yet enabled for traffic is only available for calls between `engineering' terminals. A nation may decide to allow a gateway link in this state to accept incoming calls in the normal manner, but outgoing calls (other than engineering calls) will not be allowed.

3. If neither crypto synchronism, nor alignment can be achieved, the responsible nation shall initiate fault location as described in Paragraph 5.

4. When the gateway is available for engineering under KVB(I), the master FC shall set-up a connection via a traffic channel of that gateway to the other FC, to declare the gateway available for regular traffic.

5. If the set-up of a connection under KVB(I) is not successful the master FC shall contact the other FC via the EOW to establish the proper functioning of the channel by using the procedures of Appendix 7.

NOTE:- Subject to national COMSEC approval, nations may, on a bilateral basis, prefer to use an agreed engineering key setting for their crypto equipment as a first step in the process of setting up the gateway. This would allow a check that the established link is properly functioning, before any KVB(I) has to be inserted. It should be noted that links which are operating under an engineering key setting are never to be declared `secure'. When the gateway is properly functioning under the engineering key setting, the procedure to open switch to switch traffic, as laid down in this Appendix must be followed.

This page is Blank

SEQUENCE TO ENGINEER PERMANENT CONNECTIONS

1. Content of executive order is known in the nodes at either end of the Gateway.

2. Gateway link is engineered.

3. Channels are made available for the Permanent Connection and are not available for circuit switched traffic.

4. Higher layer protocol stack is engineered, (e.g. X.75 packet switching using the parameters defined for the permanent connection.

This page is Blank

SEQUENCE TO MONITOR SWITCH TO SWITCH TRAFFIC

1. Both gateway switches shall raise appropriate alarms when link failures occur.

2. When either crypto synchronism, frame alignment or signalling ability is lost, the gateway shall be closed for regular traffic.

3. If the EOW is still functioning but after some time gateway synchronism is not automatically re-achieved, the master FC shall initiate fault location as described in Annex E, paragraph 3: Gateway Engineering.

4. If this fault location results in a supposed malfunctioning of the bulk-encryption equipment, the KVB(I) shall be re-inserted upon instruction of the master FC.

5. Once crypto synchronism and frame alignment are achieved, the gateway is available for engineering and the master FC may initialise and direct channel testing, if needed.

6. When no (more) testing is needed under KVB(I), the master FC shall set-up a connection via a traffic-channel of that gateway to the other FC. If successful, the master FC shall inform the other FC that the gateway is now available for regular traffic again. If not successful, the FC's will contact each other via EOW and re-engineer the Gateway, if necessary with a new KVB(I). If again not successful, the master FC shall inform his OSC.

7. If a single channel failure is detected, that channel shall be closed for regular traffic. If needed, the master gateway switch sends a control message that specifies a channel loop-back request. Upon reception, the called gateway switch effects the specified channel loop-back and returns the related control message to the master gateway switch.

8. The master FC performs the needed tests, following national procedures. When finalised, the master gateway switch sends a release message that specifies a `normal release' for the looped channel. Upon reception of this release message, the called gateway switch shall remove the loop-back provision from the specified channel.

9. The master FC contacts the other FC to initialise and direct the appropriate procedures to re-establish the proper functioning of the channel. If such can be achieved, the master FC shall inform the other FC that the channel can be made available for regular traffic again.

10. If proper functioning of a single channel cannot be achieved the gateway as such shall not be closed for regular traffic, but the master FC shall inform his OSC.

SEQUENCE TO CLOSE THE GATEWAY

1. At the time the gateway is to be closed, the master FC informs the other FC that the gateway is no longer available for the set-up of new calls.

2. New calls are to be barred from the gateway to be closed. Ten minutes later, calls which are still existing will be released. The barring method is the responsibility of each nation's FC.

3. When all channels are idle, the master FC contacts the other FC to inform him that the gateway is now closed for regular traffic.

4. If any further information is to be exchanged between the FCs, it should be done now.

5. If no (more) information is to be exchanged, the master FC informs the other FC that the gateway is closed. Following its own procedures, each nation is now free to disconnect equipment, including radio-relay equipment, from the closed gateway.

This Page is Blank

GATEWAY STATUS MESSAGE

1. Link identity - node nation A/higher formation, node nation B/lower formation.

2. Real status - working, standby, reserve, closed, out of service: time at which status achieved.

3. NIACs accessible from controlling side - NIAC of subordinate network, NIACs accessible through subordinate network.

4. NIACs accessible from subordinate side - NIAC of controlling side, NIACs accessible through controlling side.

5. Security status - secure or insecure.

6. Channel status:

   a. For 5040 gateway - number of analogue channels and number of digital channels.

   b. For digital gateway - number of packet channels in service, number of common user channels in service, number of sole user channels in service.

7. Comment (up to 5 lines of free text).

This Page is Blank

COMSEC MANAGEMENT

Management of COMSEC information shall be performed at the appropriate levels within each national system. Co-ordination among networks shall be exercised regarding COMSEC provisions required at the network interfaces. Specific COMSEC management and control requirements are contained in (to be determined).

This page is Blank

ENGINEERING ORDER WIRE (EOW) OPERATIONS

BASIC PRINCIPLES

1. Configuration

a. An example of an EOW circuit is shown in Appendix 1, the following communication capabilities shall be provided:-

(1) Facility Control (FC) - Facility Control (FC);

(2) Operator - Operator (on either side of the interface point).

b. The equipment used to access an EOW circuit shall be called an EOW terminal. Such terminals may function as either a terminating or an intermediate EOW terminal. A terminating terminal (TEOW) in connection with a multi-EOW access equipment (MEAE) may be in an FC function or not as shown in Appendix 1.

c. An EOW link is defined as the connection between one EOW terminal and its neighbour.

d. An EOW circuit is defined as a number of EOW links in tandem, connecting two terminating EOW terminals.

e. Interconnection of EOW circuits is not required.

2. General

a. An encrypted EOW circuit shall be provided on all Gateways.

b. An EOW circuit provides 16 kbit/s digital speech communication in a half-duplex mode of operation.

c. EOW terminals shall be able to access the EOW circuit for the purpose of making and receiving calls.

d. The EOW shall be operationally independent of the group traffic signal. The EOW circuit shall continue to be usable, to a certain extent, when the quality of the group traffic has become unacceptable.

3. User Facilities

a. Communication Mode

(1) Half duplex speech communication facilities shall be provided to enable EOW communication between any terminals on the same circuit. Only one

EOW terminal shall be able to originate traffic at any time. All terminals connected to the circuit shall receive the transmitted EOW signal.

(2) It shall be possible to connect any EOW terminal to an idle EOW circuit for the purpose of transmitting. This shall include connection during idle intervals when the direction of the half duplex communication is changing.

b. Subscriber Calling

It shall be possible to call all EOW terminals on the same circuit or in a selected direction simultaneously by use of the `alert' signal.

c. Call Interruption

The EOW terminals used by the FC shall be able to break down (not necessarily automatically) an existing connection for the purpose of making an urgent call.

d. Control and Indicator Facilities

Control and indicator facilities shall be provided for EOW terminals.

CONVERSION

4. Analogue/Digital Conversion

Speech signals shall be transmitted on the EOW using delta modulation conforming to STANAG 4209.

TIMING

5. Autonomy

A transmitting EOW terminal shall use its own free-running clock which shall be independent of the traffic clock.

6. Clock Accuracy

The accuracy of the free-running EOW clock shall be better than ±1 part in 10^4 of the nominal frequency.

7. Timing During Operation

a. Terminals providing a through-path shall retransmit digital signals maintaining bit count integrity for a minimum of 90 seconds.

b. A receiving EOW terminal shall derive timing from the incoming signal.

EOW TRANSMISSION CHARACTERISTICS

8. General

a. The EOW link on radio or cable shall have, for both directions of transmission, one channel each.

b. The limit for operation of an EOW circuit under worst case conditions shall be a random error rate of 1 in 10.

c. EOW transmission shall be possible both in the presence of, and in the absence of, group signals (signalling and/or traffic).

d. The EOW circuit timing shall be independent of the group traffic clocks. The error rate on an EOW link shall be lower than 1 in 10^3 at a group traffic error rate of 1 in 10^4 and lower.

9. Cable Transmission

(a) EOW signals on electrical cable shall be transmitted on the cable phantom as specified in STANAG 4210.

(b) EOW signals on optical cable shall be transmitted in accordance with STANAG 4290 (under development).

10. Radio Transmission

The transmission method of EOW signals for radio relay links is defined in STANAG 4212.

EOW SIGNALLING

11. The signalling system shall be unencrypted.

12. Signalling codes shall be transmitted at a bit rate of 16 kbit/s.

13. The EOW signalling system shall use an 8 bit cyclically permutable codeword (CPC) as specified in Table 1, having a strong analogue frequency component.

14. The CPC word shall be transmitted in blocks of 16 with and without inversion as shown in Table 1. The inversion shall be controlled by 4 bit phase shift codewords (PSC).

15. The signalling transmission shall start with a non-inverted block as shown in Table 1.

16. The criterion for the reception of a valid signal shall be the detection of 6 consecutive error-free CPC codewords or the detection of 2 consecutive error-free PSC codewords of transmitted block sequence. The use of PSC codewords enable analogue detection to be used.

17. The CPC codeword allocation shall be as specified in Table 1.

18. The PSC codeword allocation shall be as specified in Table 1.

19. The order of transmission of bits shall be such that the left-hand bit of the CPC codeword, as shown in Table 1, is transmitted first.

20. EOW signalling shall conform to the signalling sequence given in Figures 2 and 3 of Appendices 2 and 3 respectively.

21. The ‘alert’ signal is used to set up the EOW circuit. when the EOW detects the ‘alert’ signal, the ring indication should be provided to the operator.

22. The ‘pressel on’ signal is used to capture the EOW circuit and allow the operator to become the speaker. From time to time any listener may become the speaker through the use of the ‘pressel on’ signal.

23. For call interruption, the TEOW sends the `alert' signal on a busy circuit. The detection of `alert' on a busy circuit implies breaking down the current connection. (This function need not be fully automated).

24. Block sequence should be transmitted for at least 500 ms.

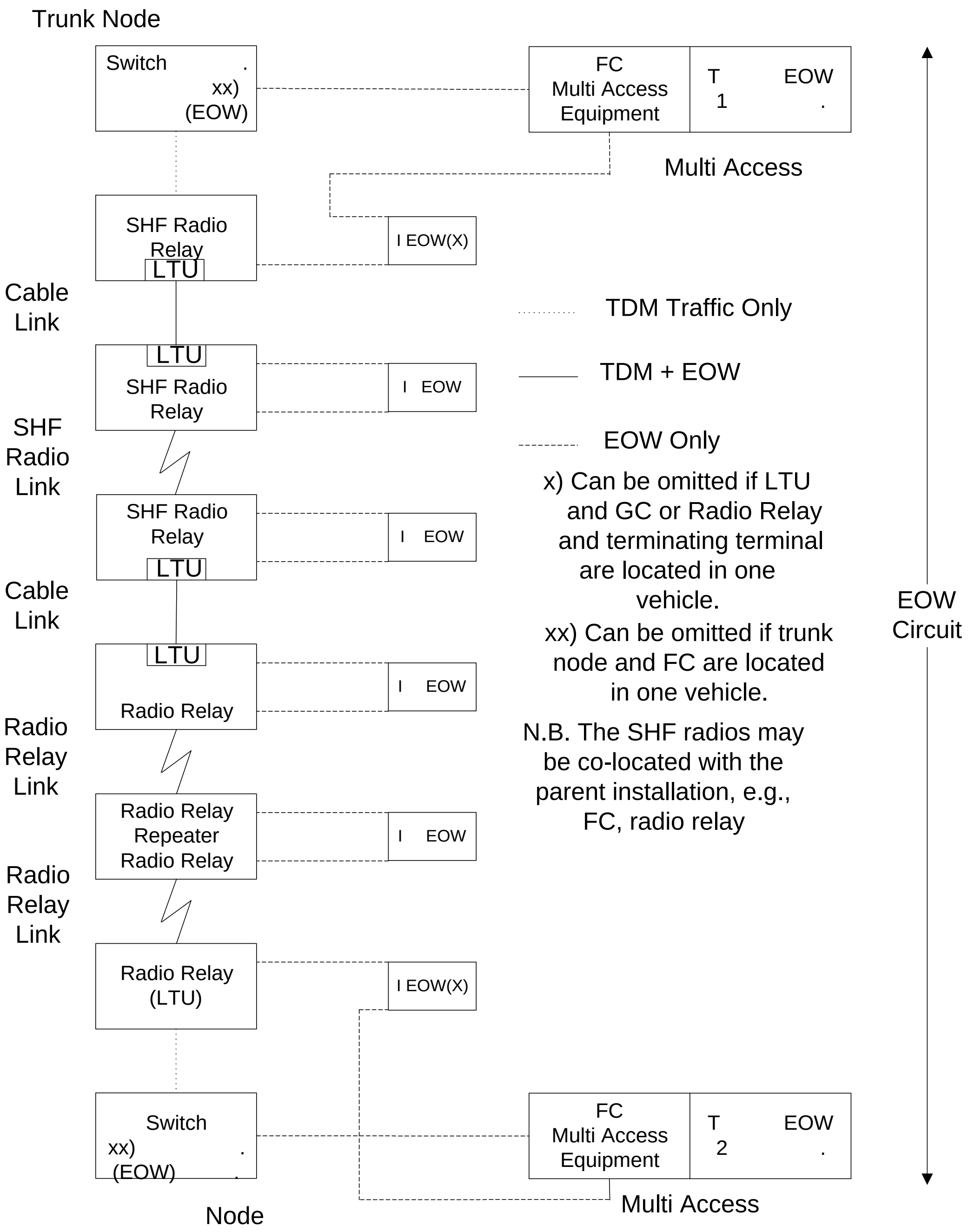
SIGNAL	CPC CODEWORD	TRANSMITTED BLOCK SEQUENCE	PSC CODEWORD
Alert	10011100	N/ININININININININ/I	1111
Pressel On	10101010	N/NNNNNNNNNNNNNNNN/N	----

TABLE 1 - EOW CODEWORD ALLOCATION

N = Non-inverted block of 16 CPC codewords.
I = Inverted block of 16 CPC codewords.

NOTE:-

In the transmitted block sequence a transition from N to I or vice versa is equivalent to a `1' of the PSC codeword.  No transition is equivalent to a `O'. The signal `pressel on' is used for bit synchronisation prior to each transmission of speech signals.



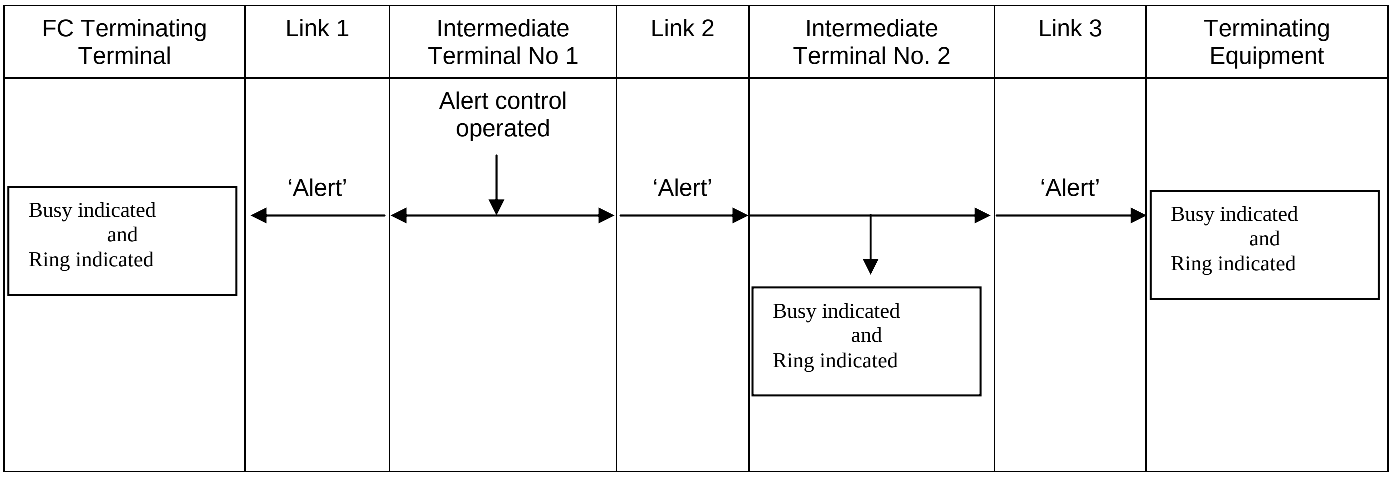
x) Can be omitted if LTU and GC or Radio Relay and terminating terminal are located in one vehicle.

xx) Can be omitted if trunk node and FC are located in one vehicle.

N.B. The SHF radios may be co-located with the parent installation, e.g., FC, radio relay

FIGURE 1 - EXAMPLE OF AN EOW CIRCUIT

This Page is Blank

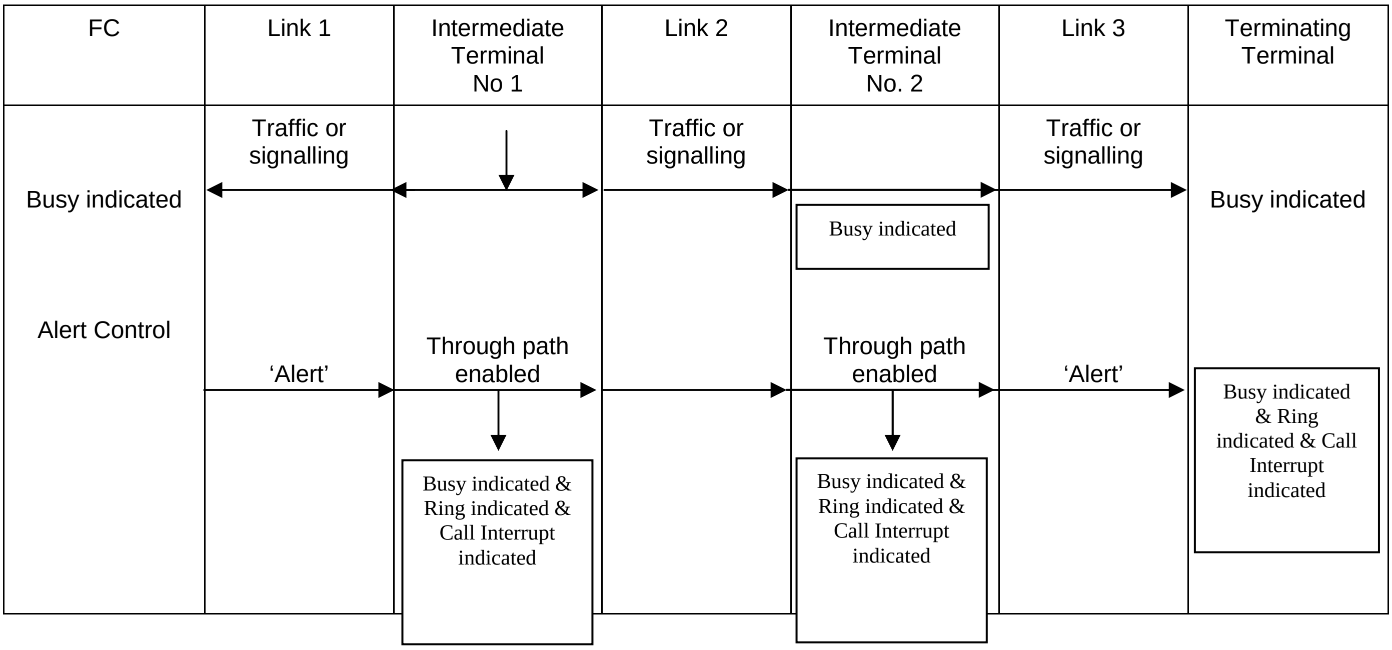

FC Terminating Terminal
Link 1
Intermediate Terminal No 1
Link 2
Intermediate Terminal No. 2
Link 3
Terminating Equipment
Alert control operated
'Alert'
'Alert'
'Alert'
Busy indicated and Ring indicated
Busy indicated and Ring indicated
Busy indicated and Ring indicated

Notes:

1. `Alert' is transmitted for the duration of alert control operation.
2. Busy indication is given for the duration of `alert' reception.

FIG. 2 - EOW Call to Intermediate EOW Terminals

This Page is Blank


FC
Link 1
Intermediate Terminal No 1
Link 2
Intermediate Terminal No. 2
Link 3
Terminating Terminal
Traffic or signalling
Traffic or signalling
Traffic or signalling
Busy indicated
Busy indicated
Busy indicated
Alert Control
'Alert'
Through path enabled
Through path enabled
'Alert'
Busy indicated & Ring indicated & Call Interrupt indicated
Busy indicated & Ring indicated & Call Interrupt indicated
Busy indicated & Ring indicated & Call Interrupt indicated

Notes:

1. `Alert' is transmitted for the duration of alert control operation.
2. Busy indication is given for the duration of `alert' reception.

Fig 3 - EOW Call Interrupt FC to EOW Terminals

This Page is Blank

SUBSCRIBER ASSISTANCE

1. SET-UP ASSISTANCE

A subscriber may experience difficulty in establishing a communications path with a subscriber of an adjoining network. If the call set-up attempt results in a number unobtainable condition, the subscriber may request subscriber assistance from the adjoining tactical digital network.

2. INFORMATION ON MODES

A subscriber may request subscriber assistance to determine the communications mode available to the subscriber of the adjoining tactical digital network with which he wishes to communicate.

3. INFORMATION ON SUBSCRIBER NUMBERS

A Subscriber may request subscriber assistance for information on subscriber numbers of the adjoining tactical digital network. These subscriber numbers may or may not be deducible from the NATO DIRECTORY Structure as described in STANAG 5046.

This Page is Blank

MULTICHANNEL DIGITAL GATEWAY AND STANAG 5040 ANALOGUE GATEWAY SYSTEM CONTROL STANDARDS NPICS PROFORMA

1 Introduction

1.1 A nation implementing system control facilities, which include procedures and communications for system managers, for the multichannel digital gateway and the STANAG 5040 analogue gateway, which are claimed to conform to STANAG 4211, shall complete the following NATO Protocol Implementation Conformance Statement (NPICS) proforma. No later than the date of implementation, the nation shall send it to NACISA through its ATCA or ANCA representative.

1.2 For a NATO standard, the NPICS corresponds to the Protocol Implementation Conformance Statement (PICS) defined in ISO/IEC 9646-1 for an international standard. The term NPICS is used to avoid confusion where the requirements for NPICS and PICS differ.

1.3 The NPICS proforma is a document, in the form of a questionnaire designed by the responsible group in the TSGCE, which, when completed for an implementation or system including any Additional Information and Exception Information, becomes the NPICS for the implementation in question.

1.4 The NPICS is a statement of which capabilities and options of the protocol have been implemented. The NPICS can have a number of uses, including use:

a. By the protocol implementer, as a check list to reduce the risk of failure to conform to the standard through oversight.

b. By the supplier and acquirer - or potential acquirer - of the implementation, as detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided for by the standard NPICS proforma.

c. By the user - or potential user - of the implementation, as a basis for initially checking the possibility of interworking with another implementation. (Note that while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible NPICS.)

d. By a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

2 Abbreviations and Special Symbols

2.1 Status Symbols

M	Mandatory
O	Optional
O.<n>	Optional, but support of at least one of the groups of options labelled by the same numeral <n> is required.
X	Prohibited
<pred>:	Conditional-item symbol, including predicate identification, see 3.4
	Logical negation, applied to a conditional item's predicate

2.2 Abbreviations

N/A	not applicable
NPICS	NATO Protocol Implementation Conformance Statement
NIAC	National Identifier and Area Code (see STANAG 4214)

2.3 Item References. Items in the NPICS proforma are identified by mnemonic item references. NPICS items dealing with related functions are identified by item references sharing the same initial letter or letter pair (in capitals). There follows a list of those initials, in the order in which the groups of items occur in the NPICS proforma.

CP	Communications planning information
IE	Information exchange means
GM	Gateway messages
GL	Gateway links
GE	Gateway engineering
EOW	Engineering order wire
CM	COMSEC management
DN	Directory numbers
SA	Subscriber assistance

2.4 Base Standard References. The generic format of a reference of the NPICS proforma is:

<Paragraph>

for a reference to the main part of the STANAG, and

[<Part>]<Annex>[<Appendix>]/<Paragraph>

for all other STANAG references.

<Part>	= A capital Roman number	(I, II, etc)
<Annex>	= An upper case character	(A, B, etc)

<Appendix> = A number or upper case character (A, B, etc, 1, 2, etc)
<Paragraph> = <n>.[<n>] or <n>.[<x>] as appropriate

[ ]	enclose an optional entry
< >	denote a generic identifier
<n>	a numeral (1, 2, 3, etc)
<x>	a lower case character (a, b, c, etc)

In the case when there are references to one or more CCITT or ISO base standards in addition to STANAG references, the STANAG references shall be prefixed by "STnnnn", while the CCITT or ISO references are direct to chapters, paragraphs, etc. Such CCITT or ISO base standards shall be listed in the "Related Documents" sections of this STANAG or STANAG Annex, to which this NPICS Proforma is attached. If more than one CCITT or ISO standard is referenced in the NPICS Proforma, only one reference should be used in each table, with the reference stated above the table.

3 Instructions for Completing the NPICS Proforma

3.1 General Structure of the NPICS Proforma.

a. The first part of the NPICS proforma - Implementation Identification and Protocol Summary - is to be completed as indicated with the information necessary to identify fully both the nation and the implementation.

b. The main part of the NPICS proforma is a fixed-format questionnaire, divided into a number of major subclauses: these can be divided into further subclauses each containing a group of individual items. Answers to the questionnaire items are to be provided in the rightmost column, either by simply marking an answer to indicate a restricted choice (usually Yes or No) or by entering a value or a range or set of values. There are some items where two or more choices from a set of possible answers can apply: all relevant choices are to be marked.

c. Each item is identified by a Item Reference in the first column; the second column contains the question to be answered; the third column contains the reference or references to the material that specifies the item in the main body of the STANAG or in other STANAGs. The remaining columns record the status of the item - whether support is mandatory, optional, prohibited or conditional - and provide space for the answers: see also 3.4 below.

d. A nation may also provide - or be required to provide - further information, categorised as either Additional Information or Exception Information. When present, each kind of further information is to be provided in a further subclause of items labelled A<i> or X<i> respectively for cross-referencing purposes, where <i> is any unambiguous identification for the item (eg simply a numeral): there are no other restrictions on its format and presentation.

Note:

Where an implementation is capable of being configured in more than one way, a single NPICS may be able to describe all such configurations. However, the nation has the choice of providing more than one NPICS, each covering some subset of the implementations's configuration capabilities, in case that makes for easier and clearer presentation of the information.

3.2 Additional Information. Items of Additional Information allow a nation to provide additional information intended to assist the interpretation of the NPCIS. It is not intended or expected that a large quantity will be supplied, and an NPICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations; or a brief rationale - based perhaps upon specific application needs - for the exclusion of features which, although optional, are nonetheless commonly present in implementations of this protocol. References to items of Additional Information may be entered next to any answer in the questionnaire and may be included in items of Exception Information.

3.3 Exception Information. It may occasionally happen that a nation will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No pre-printed answer will be found in the Support column for this: instead, the nation shall write the missing answer into the Support column, together with an X<i> reference to an item of Exception Information, and shall provide the appropriate rationale in the Exception item itself.

Note:

A possible reason for the situation described above is that a defect in the STANAG has been reported, a correction for which is expected to change the requirement not met by the implementation.

3.4 Conditional Status

3.4.1 Conditional Items.

a. The NPICS proforma contains a number of conditional items. These are items for which the status - mandatory, optional or prohibited - that applies is dependent upon whether or not certain other items are supported, or upon values supported for other items.

b. In many cases, whether or not the item applies at all is conditional in this way, as well as the status when the item does not apply.

c. When a group of items is subject to the same condition for applicability, a separate preliminary question about the condition appears at the head of the group, with an instruction to skip to a later point in the questionnaire if the "Not Applicable" answer is selected. Otherwise, individual conditional items are indicated by one or more conditional symbols (on separate lines) in the Status column.

d. A conditional symbol is of the form "<pred>:<x>" where "<pred>" is a predicate as described in 3.4.2 below, and "<x>" is one of the status symbols M, O, O.<n> or X.

e. If the value of the predicate in any line of a conditional item is true (see 3.4.2), the conditional item is applicable, and its status is that indicated by the status symbol following the predicate; the Support column is to be marked in the usual way. If the value of a predicate is false, the Not Applicable (N/A) answer is to be marked in the relevant line. Each line in a multi-line conditional item should be marked.

3.4.2 Predicates

a. A predicate is one of the following:

(1) An item-reference for an item in the NPICS proforma: the value of the predicate is true if the item is marked as supported and is false otherwise: or

(2) A predicate name, for a predicate defined elsewhere in the NPICS proforma item: see below; or

(3) The logical negation symbol "   " prefixed to an item-reference or predicate name; the value of the predicate is true if the value of the predicate formed by omitting the "   " is false, and vice versa.

b. The definition of a predicate name is a Boolean expression constructed by combining simple predicates, as at (1) or (2) above, using the Boolean operators AND, OR and NOT, and parentheses, in the usual way. The value of such a predicate is true if the Boolean expression evaluates to true when the item-references are interpreted as at (1) above.

c. Each item whose reference is used in a predicate or predicate definition is indicated by an asterisk in the Item column.

4 Identification

4.1 Implementation Identification

Nation	
Contact point for queries about the NPICS	
Implementation Name(s) and Version(s)	

4.2 Protocol Summary

Identification of standard	STANAG 4211
Identification of amendments and corrigenda to this PICS proforma which have been completed as part of this PICS	Am: Corr: Am: Corr: Am: Corr: Am: Corr:
Have any exception items been required? (The answer Yes means that the implementation does not conform to STANAG 4211)	No [ ] Yes [ ]
Date of statement	

5 Protocol Implementation

References in the questionnaire refer to the the text of STANAG 4211, unless otherwise indicated.

5.1 Communications Planning Information

Item	Protocol Feature	Refs	Status	Support
	Do system managers have records of the following information:			
CP1	Identities of formations below and to the right in accordance with STANAG 5048	A/2a	M	Yes [ ]
CP2	Deployment locations of gateway facilities	A/2b	M	Yes [ ]
CP3	The types of gateway or interface available	A/2c	M	Yes [ ]
CP4	The types of links available	A/2d	M	Yes [ ]
CP5	The formations reached through gateways and the NIACs in their area of control	A/2e	M	Yes [ ]
	The security status for available links			
CP6	A list of limiting factors	A/2f	M	Yes [ ]
CP7		A/2g	M	Yes [ ]

5.2 Means of Exchanging Information

Item	Protocol Feature	Refs	Status	Support
	Are system managers able to exchange information by:			
IE1	Voice	E/1	M	Yes [ ]
IE2	Telegraph, ACP127	E/1	O.1	Yes [ ] No [ ]
IE3	Data, ADatP3	E/1	O.1	Yes [ ] No [ ]
IE4	Facsimile, STANAG 5000	E/1	O.1	Yes [ ] No [ ]

5.3 Gateway Messages

Item	Protocol Feature	Refs	Status	Support
	Do system managers have the facilities to format messages to use the means of exchanging information in Section 5.2			
GM1	Request Message	E1	M	Yes [ ]
GM2	Acceptance Message	E2	M	Yes [ ]
GM3	Warning Order/Executive Order	E3	M	Yes [ ]
GM4	Gateway Status	E9	M	Yes [ ]

5.4 Gateway Links

Item	Protocol Feature	Refs	Status	Support
	Indicate the types of link available for gateways:			
GL1	Electrical cable	ST4210	M	Yes [ ]
*GL2	Optical cable	ST4290	O	Yes [ ] No [ ]
*GL3	Radio relay	ST4212	O	Yes [ ] No [ ]
*GL4	SATCOM	ST4484	O	Yes [ ] No [ ]
*GL5	Permanent Connections	ST4206	O	Yes [ ] No [ ]

*Predicate usage: GL2-5 are used in Sections 5.5.1 and 5.5.2.

5.5 Gateway Engineering

5.5.1 Facilities for Link Quality Monitoring and Fault Detection

Item	Protocol Feature	Refs	Status	Support
	Indicate the availability of facilities for monitoring of link quality and for fault detection by looping on: Electrical cable links			
GE1e		E3.1,	M	Yes [ ]
	Optical cable links	E3.2		
GE1o		E3.1,	GL2:M	N/A [ ]
	Radio relay links	E3.2		Yes [ ]
GE1r		E3.1,	GL3:M	N/A [ ]
	SATCOM links	E3.2		Yes [ ]
GE1s		E3.1, E3.2	GL4:M	N/A [ ] Yes [ ]

5.5.2 Opening of Links

Item	Protocol Feature	Refs	Status	Support
	Indicate the availability of facilities and operating procedures for opening the following types of link:			
	Electrical cable links			
GE2e	Optical cable links	E5	M	Yes [ ]
GE2o		E5	GL2:M	N/A [ ] Yes [ ]
	Radio relay links			
				N/A [ ] Yes [ ]
GE2r		E4	GL3:M	
	SATCOM links			N/A [ ] Yes [ ]
GE2s		E6	GL4:M	N/A [ ] Yes [ ]
	Permanent Connections			
GE2p		E8	GL5:M	

5.5.3 General Processes

Item	Protocol Feature	Refs	Status	Support
	Indicate the availability of facilities and operating procedures for the following general processes:			
	Opening switch-switch traffic			
GE3	Monitoring switch-switch traffic	E7	M	Yes [ ]
	Closing a gateway			
GE4		E9	M	Yes [ ]
GE5		E10	M	Yes [ ]

5.5.4 Engineering Order Wire

Item	Protocol Feature	Refs	Status	Support
EOW	Is a secure Engineering Order Wire available for gateway links?	G	M	Yes [ ]

5.6 COMSEC Management

Item	Protocol Feature	Refs	Status	Support
CM	Are facilities and procedures available for COMSEC management?	MCM-SYP-104-92	M	Yes [ ]

5.7 Directory Numbers

Item	Protocol Feature	Refs	Status	Support
	Does the network respond to calls to reserved addresses for Special Facilities, as defined in STANAG 4214, C3?			
DNa	Subscriber Assistance, 7999990	5.2	M	Yes [ ]
DNm	System Management, 7999991	5.3	M	Yes [ ]

5.8 Facilities of Subscriber Assistance

Item	Protocol Feature	Refs	Status	Support
	Are procedures available to provide the following subscriber assistance facilities?			
SA1	Set up assistance	H/1	M	Yes [ ]
SA2	Information on modes	H/2	M	Yes [ ]
SA3	Information on subscriber numbers	H/3	M	Yes [ ]