JSP 602 Instruction	1006	**Applicability**	Infrastructure, Network/Communications
Configuration Identity	Version: 03.00 Reviewed: 2006-11-26	**Epoch Applicability**	2005 - 2009

JSP 602: 1006 - Data Link Services

Outline

Description: This policy leaflet mandates the standards, protocols and procedures necessary to ensure interoperability amongst Data Link (DL) equipment. DL provide near real time exchange of digital information utilising standard message formats among Air, Land and Maritime units. This leaflet covers Tactical DL (TDL), Common and other wide band DL are the subject of an additional leaflet.

Reasons for Implementation: TDLs are the principal bearers of 'tactical picture' information within the tactical environment. They are widely used within MOD and by its allies and coalition partners and:

- provide an effective and interoperable set of TDLs that meet operational capability requirements
- provide an effective means of sharing tactical information with allies and coalition partners
- support effective Command and Control
- support efficient mission execution
- help reduce incidents of 'blue-on-blue'.

Issues: The DLs considered in this leaflet are all controlled through the use of NATO or US standards documentation. However, due to the wide capabilities offered by DLs individual platform implementation reflect their individual needs. Different implementations have in the most part been undertaken with little consideration for their potential impact on the wider network and as a result Interoperability (IO) issues have been created. Also, the standards are living documents which evolve over time to meet new operational requirements. As a result of this evolution, all platforms need to evolve their platform implementations to ensure IO with future platforms.

Guidance: The Data Link Network Acquisition Authority (DLNAA) is a federation of the Sponsors, Chaired by EC CCII-JDN; the Users are represented by the Joint Data Link Management Organisation (JDLMO), CBMJ6, the Integration Authority (IA) and the TDL IPT acts under the auspices of the CBMJ6 - MOD Policy on DLs and answers to the 1*NEC Steering Committee.

The DL IO and Network Integration Policy and Process have been developed to provide IPTs with a structure for the achievement of DL IO and Network Integration.

All MOD projects implementing a DL are mandated to follow the DLNAA DL IO and Network Integration Policy and Process. This policy is endorsed by the DL Network Acquisition Authority (DLNAA) as the UK process for bringing coherence to the MoD acquisition of DLs. The process contains 4-Key assurance points throughout the complete lifecycle of a programme:

- Assessment 0 - Incorporates the detailed assurance of projects at the Concept Phase, between breakthrough and Initial Gate, across all DLoD. The DLNAA assurance process is an integral part of the IA IOCA process.
- Assessment 1 - Incorporates the detailed scrutiny of projects at the Assessment and Demonstration Phases, between Initial Gate and Main Gate, across all DLoD. The DLNAA assurance process is an integral part of the IA IOCA process.
- Assessment 2 - Incorporates the detailed assurance of projects during Demonstration, Manufacture and Implementation Phases and prior to Contractual Acceptance and In-Service Date (ISD). This shall be in the form of an assurance process focusing on a programme's test and evaluation plan and results. Following Completion of Assessment 3 the DLNAA shall issue a Certificate of Clearance for Use (CCU) for the programme. The CCU shall outline any issues with the operation of the system and any performance constraints and limitations and a recommendation for the Commander on the risks of deploying the equipment for either training or operational purposes. It shall also outline the actions that need to be taken to overcome the stated issues. A DLNAA nominated independent IO assessor shall authorise the final content of the CCU and make the final recommendation for signature to the Chairman of the DLNAA. A CCU is signed by DEC CCII as Core DEC for Command, Control, Computers, Communication and Information (C4I).
- Assessment 3 - Incorporates the continual monitoring of platforms and systems and ongoing test and trials post ISD and throughout the In-service Phase. This shall take the form of operational network monitoring but shall also be used to recertify a platform after any updates to its DL system.

The final decisions on any assessments made shall lie with the Chairman of the DLNAA; however, no decision shall be made without relevant consultation with stakeholders.

The following MOD Data Link policies apply:

- MOD Policy for Data Link IO and Network Integration - 1-Star Core DEC for C4 endorsed.
- MOD Policy for Data Links (DGINFO/DCBM J6/Data_Links_Policy/10/01/1 dated Nov 04) - 2-Star CBM Executive Steering Group endorsed.

- Tactical Data Link Core DEC Policy and Architecture Ed 3 - 1-Star Core DEC for C4 endorsed.
- DL Recording and Analysis Policy V1.0 - awaiting 1-Star Core DEC for C4 endorsed.
- MOD/CAA Frequency Clearance Agreement (FCA) MIDS/JTIDS V6.4 - 2-Star DGINFO Endorsed.
- Defence Tactical Data Link Standards Policy (DCISB 9/94 dated 21 Sep 94)
- Application of the UK Defence Technical Data Interoperability Requirements Specification (DTDL-IOR) is mandatory.
- Application of the UK Defence Tactical Data Link Interface Requirements Specification (DTDL-IRS) is mandatory.
- Integration of the platform with the TDL Multi-Link Test Facility is highly recommended.

Policy

Strategic

1006.01: Through-Life Interoperability Management

1006.01.01 It is mandatory for all platforms procuring, supporting or maintaining UK TDL applications to instigate a Through-Life Interoperability Management Process.

Through life IO

Comment: iSMART is the current MOD best practice Through Life IO process for Data Links.

1006.02: J-Series Family

1006.02.01 All UK TDL-fitted platforms shall fulfil their near real-time data exchange requirements using one of the J-Series Family TDLs as defined by their individual IERs or through approved Gateways. The J-Series Family of messages are defined as Link 16, Link 22, VMF, IBS

1006.02.02 Link 16 - MIDS/JTIDS

1006.02.02.01 Link 16 is a high capacity, ECM-resistant communications link designed for all services (air, surface and land) and all platform types, i.e. for C2 and non-C2 units.

1006.02.02.02 The message Transaction rules for all pre-Main Gate Platforms and for all-Platforms by 2015 for Tactical Data Exchange - Link 16 are contained within:

1006.02.02.02.01 MIL-STD 6016 (C) in parallel with the UK MIL-STD 6016 National Difference Document. Link 16 Network Management implementations should reference DTDL-IRS Part II (Single Link) - Link 16.

1006.02.02.03 Platforms implementing Link 16 on MIDS terminals shall do so using:

1006.02.02.03.01 STANAG 4175: Technical Characteristics of the Multifunctional Information Distribution System (MIDS).

1006.02.02.04 Platforms providing Link 16 messages over Satellite communications shall do so using the UK-STDL Standard.

1006.02.03 Tactical Network Design Suite

1006.02.03.01 Link 16 requires that all participating platforms are initialised prior to operation with a discrete set of data parameters that define each platform's interaction on the Link. These Initialisation Data sets are normally pre-defined and grouped in a Link 16 Network Design. All UK Link 16 Network Designs are produced by the Network Design Centre, which forms part of the JDLMO. All new (pre-Main Gate) platforms or systems implementing Link 16 must conform to the MOD Tactical Network Design Suite (TNDS) Policy contained in this JSP 602

1006.02.03.02 For all systems and/or projects developing new Link 16-equipped platforms, a single Common File Format (CFF) ID Set is produced by the TNDS and distributed by the JDLMO NDC via the JDLMO internet website. The following are also mandated:

1006.02.03.02.01 The CFF shall be supplied by the TDL IPT as GFE and implemented by each platform Initialisation Data Preparation Facility (IDPF).

Strategic (continued)

1006.02.03.02.02 New Link 16 platform programmes shall develop their IDPF equipment to accept the CFF.

1006.02.03.02.03 existing non-CFF conforming load file formats and IDPFs shall be maintained but not amended. Where amendment to an existing format is required, Platforms shall implement the CFF.

1006.02.04 MOD/CAA Frequency Clearance Agreement (FCA) for JTIDS/MIDS

1006.02.04.01 All platforms planning to operate JTIDS/MIDS Link 16 within the UK Flight Information Region (FIR) shall produced an approved MOD/CAA FCA Safety Case for JTIDS/MIDS before they shall be permitted to operate.

VMF

Comment: VMF is defined in the UK VMF documentation set, containing the UK SLIRS and UK BDD.

1006.02.05 Variable Message Format (VMF)

1006.02.05.01 VMF is a US bit-orientated, bearer-independent message set. Platforms required to implement VMF shall do so using the following:

1006.02.05.01.01 UK VMF Single Link Interface Requirements Specification (SLIRS).

1006.02.05.02 Platforms providing VMF messages over Tactical IP shall use:

1006.02.05.02.01 UK Bearer Definition Document (BDD).

1006.02.06 Link 22

1006.02.06.01 Platforms required to interface with Link 22 shall do so using the following standards:

Link 22

Comment: Data Link 22 is an ECM resistant, BLOS tactical data communication system utilising Fixed Frequency or Frequency hopping techniques.

1006.02.06.01.01 STANAG 5522 Ed 1 (Draft): Tactical Data Link - Link 22.

1006.02.06.01.02 STANAG 4372 Saturn - Ed 2 dated 26 Nov 02:

1006.02.06.01.03 STANAG 4444 (HF Comms)

1006.02.07 IBS

1006.02.07.01 The Integrated Broadcast System (IBS) is not included within this JSP 602 Leaflet.

1006.02.08 Joint Range Extension Application Protocol (JREAP)

Strategic (continued)

1006.02.08.01 JREAP is a US standard that enables the wrapping of Link 16 J-Series messages for transmission over non-TDL mediums. JREAP is not a DL in its own right and requires an independent transmission medium i.e. Satcom provision. The JRE Application Protocols are defined in:

1006.02.08.01.01 Mil-Std 3011 and associated annexes.

1006.03: NON-J-SERIES FAMILY

1006.03.01 Non-J-Series family of TDLs shall not be used by new platforms or during upgrades unless unavoidable to provide IO. A waiver against this JSP leaflet should be sought by any platform wishing to implement a non-J-Series Family TDL.

1006.03.02 Link 1

1006.03.02.01 Link 1 mainly provides for exchange of air surveillance data between Control and Reporting Centres (CRCs) and Combined Air Operation Centres (CAOCs)/Sector Operation Centres (SOCs). The standard is as follows:

1006.03.02.01.01 STANAG 5501: Tactical Data Exchange - Link 1 (Point-to-Point).

1006.03.03 Link 11

1006.03.03.01 Link 11 supports the exchange of air, surface and subsurface tracks, EW data and limited command data among C2 units, but does not support aircraft control or other warfare areas. The standard is as follows:

1006.03.03.01.01 STANAG 5511: Tactical Data Exchange - Link 11/Link 11B

1006.04: DATA FORWARDING AND GATEWAYS

1006.04.01 Systems and/or projects providing gateways between Link11/11B and Link 16 shall do so using:

1006.04.01.01 STANAG 5616 - Standards for Data Forwarding between Tactical Data Systems employing Link-11/11B and Link-16.

1006.04.01.02 Mil-Std 6020 - For the forwarding of Link 16 and VMF

1006.05: RECORDING AND ANALYSIS POLICY

1006.05.01 The TDL Recording and Analysis Policy defines the requirements for the recording and analysis of TDL data at multiple points within a programmes TDL System for the purpose of UK-MOD/CAA Frequency Clearance Agreement (FCA) within the UK FIR monitoring and platform and network fault finding.

1006.05.02 All pre-Main Gate programmes implementing a TDL are required to adhere to this policy

1006.06: STANDARDS EDITIONS

1006.06.01 Advice on which standards edition to implement shall be sought by each IPT from IA6

Deployed
As for Strategic domain.

Tactical
As for Strategic domain.

Remote
Not applicable.

Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all MOD projects/IPTs providing Data Link services and/or equipment within the GII and including any NATO or international systems procured as part of a NATO or international collaborative arrangements. MOD Policy for DL Interoperability and Network Integration and Process shall be applied to all UK DL platforms, both in-service and in-development.

Procedure

The principal authority for this policy is IA6 - Data Networks. They must be contacted by projects implementing this policy.

Relevant Links

A glossary of terms and abbreviations used within this document is available here.

Instructions on how to read a JSP602 leaflet are available here.

Compliance

Stage	Compliance Requirements
Initial Gate/DP1	MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s) as required. Where it is deemed that the policy, or parts thereof, will apply to the system, equipment or application being procured or updated, reference to this policy leaflet shall be made in the URD (and MODAF technical views where appropriate).
Main Gate/DP2	MOD Projects shall reference in their SRD (and MODAF technical views where appropriate) the specific policy elements contained within this leaflet that are applicable to the system, equipment or application they are procuring or updating.
Release Authority/DP5	MOD Projects (supported by their equipment suppliers) shall provide evidence of their compliance with the elements of this policy defined within the SRD (and MODAF technical views where appropriate). Evidence of conformance with standards shall be presented; appropriate sources of evidence include: conformance/compliance certificates provided by equipment suppliers (e.g. under type approval or other assessment regimes), demonstrations, inspection, analysis, tests carried out by suppliers (e.g. Factory Acceptance Tests) and tests carried out at appropriate Defence Test and Reference Facilities. All projects procuring UK TDL platforms shall produce a Platform Implementation Difference Document (PIDD) and an associated Interoperability Matrix (IOM). These are to be updated annually or whenever a significant change is implemented. They are to be produced against the appropriate Defence Tactical Data Link Interface Requirements Specifications (DTDL-IRS).