SAE Aerospace
An SAE International Group

AEROSPACE INFORMATION REPORT

SAE AIR5720

Issued 2008-01

Technical Architecture for Aircraft, Launcher, and Weapon Interoperability (ALWI TA)

RATIONALE

This document was developed in response to a request from NATO to define a technical architecture (including an associated standards framework) that would support a future interoperable plug-and-play integration capability for aircraft, launchers, and weapons across NATO air platforms.

FOREWORD

This report presents a recommended technical architecture for interoperable plug-and-play integration of aircraft, launchers, and weapons across NATO air forces. It was developed under the Aircraft, Launcher, and Weapon Interoperability - Common Interface (ALWI-CI) study performed over the period from October 2005 to November 2006. This study was authorized by the Conference of National Armament Directors (CNAD) at the request of Aerospace Capability Group 2 of the NATO Air Force Armament Group (NAFAG). It followed two previous studies on aircraft, launcher, and weapon interoperability (ALWI-1 and ALWI-2) that addressed all aspects of interoperability including the physical and electrical interfaces, environmental compatibility, and data/software. The focus of ALWI-CI was to build upon the recommendations of those two studies in the area of data/software.

The technical architecture described in this document was defined by a team within Subgroup 97 of the NATO Industrial Advisory Group (NIAG), which conducted the ALWI-CI study in collaboration with the SAE Aerospace AS-1 Committee. The Technical Architecture team was required by the NATO sponsor to address the following items in performing its role in the study:

- Analyze the applicable results of the previous ALWI-1 and ALWI-2 studies
- Take compatibility with legacy weapons into account, as well as compatibility with both airplanes and helicopters, and all types of unmanned combat air vehicle (UCAV)
- Harmonize the technical architecture with the Integrated Modular Avionics (IMA) standards of the Allied Standard Avionics Architecture Council (ASAAC) and with NATO Air Force Armament Group (NAFAG) Air Group 5 (Avionics and Landing Systems)
- Harmonize the technical architecture with the requirements of the Generic Open Architecture (GOA) and other applicable definitions/specifications of the Society of Automotive Engineers (SAE)
- Coordinate with other relevant NATO agencies as applicable
- Develop a Technical Architecture Document with interface descriptions for use within NATO

The developed Technical Architecture Document is the underlying basis of this report.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

TABLE OF CONTENTS

1. SCOPE

The technical architecture defined in this document outlines mandatory, emerging, and needed standards to provide interoperability at key interfaces in the aircraft/store system (including an associated NATO Network Enabled Capability environment), as required to support a future plug-and-play aircraft/store integration capability. These standards relate to services and protocols associated with the subject interfaces. Modeling standards to facilitate the Model Driven Architecture® (MDA®) approach to system definition and implementation are also included. Note that the status of referenced standards as reflected in this document is as of August 2007, and document users should check to see if there has been a subsequent change of status relative to applicable standards.

1.1 Purpose

The purpose of this document is to define the technical architecture for the NATO Aircraft, Launcher, and Weapon Interoperability - Common Interface (ALWI-CI) environment for aircraft/weapon integration. It was developed by NATO Industrial Advisory Group (NIAG) Subgroup 97 in response to direction from the NAFAG Air Group 2, with technical support from the Society of Automotive Engineers (SAE) Aerospace Avionic Systems Division, to facilitate an interoperable plug-and-play integration capability for aircraft, launchers, and weapons across NATO airpower.

1.2 Field of Application

The field of application for the ALWI Technical Architecture is NATO aircraft, carriage devices (launchers, carriage devices, etc.), stores (weapons, pods, etc.), and other systems/subsystems which support store employment (communication networks, mission planning systems, etc.).

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supercedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or 724-776-4970 (outside USA), www.sae.org.

AS4893 Generic Open Architecture (GOA) Framework

AS5506 Architecture Analysis and Design Language (AADL)

AIR5532 Generic Aircraft-Store Interface Framework (GASIF)

AS5652 10 Megabit/Sec Network Configuration Digital Time Division Command/Response Multiplex Data Bus

ARD5668 1760 Routing Protocol Requirements

AIR5682 Common Launch Acceptability Region Approach Interface Control Document (CLARA ICD)

2.1.2 ANSI Publications

Available from American National Standards Institute, 25 West 43rd Street, New York, NY 10036-8002, Tel: 212-642-4900, www.ansi.org.

ISO 8648 Information Processing Systems - Open Systems Interconnection - Internal Organization of the Network Layer

2.1.3 IEEE Publications

Available from Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854-1331, Tel: 732-981-0060, www.ieee.org.

IEEE 1003 Series Portable Operating System Interface

2.1.4 NATO Documents

Requests regarding availability of NATO documents may be made via e-mail at nsa@hq.nato.int.

ALWI-CI Team 2 API Methodology Report

ADatP-34 NATO 3C Technical Architecture

STANAG 4586 Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability

STANAG 5516 Tactical Data Exchange – LINK 16

2.1.5 OMG™ Publications

Available from Object Management Group™, 140 Kendrick Street, Building A, Suite 300, Needham, MA 02494, Tel: 781-444-0404, www.omg.com.

UML 2.0 Unified Modeling Language Version 2.0

XMI 2.1 XML Metadata Interchange Version 2.1

2.1.6 TIA Publications

Available from Telecommunications Industry Association, Standards and Technology Department, 2500 Wilson Boulevard, Arlington, VA 22201, www.tiaonline.com.

TIA-485-A Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems

2.1.7 U.S. Government Publications

U.S. Government standards documents are generally available from Document Automation and Production Service (DAPS), Building 4/D, 700 Robbins Avenue, Philadelphia, PA 1911-5094, Tel: 215-697-6257, http://assist.daps.dla.mil/quicksearch/.

MIL-STD-1553B Notice 4 Department of Defense Interface Standard for Digital Time Division Command/Response Multiplex Data Bus

MIL-STD-1760 Department of Defense Interface Standard for Aircraft-Store Electrical Interconnection System

MIL-STD-3014 Department of Defense Interface Standard for Mission Data Exchange Format (MiDEF)

2.2 Acronyms and Abbreviations

AADL: Architecture Analysis and Design Language

AIR: Aerospace Information Report

ALWI: Aircraft, Launcher, and Weapon Interoperability

API: Application Program Interface

ARD: Aerospace Resource Document

AS: Aerospace Standard

ASAAC: Allied Standard Avionics Architecture Council

BC: Bus Controller

BoP: Basket of Products

CASE: Computer-Aided Software Engineering

CC: Common Component

CDF: Configuration Data File

CI: Common Interface

CLARA: Common Launch Acceptability Region Approach

C2: Command and Control

C3: Consultation, Command, and Control

DBMS: Data Base Management System

DCE: Distributed Computing Environment

D-L: Data Link

DoDAF: Department of Defense Architectural Framework

EBR-1553: Enhanced Bit Rate 1553

EEI: External Environment Interface (EEI)

FC: Functional Configuration

GASIF: Generic Aircraft-Store Interface Framework

GIG JTEN: Global Information Grid – Joint Tactical Edge Network

GOA: Generic Open Architecture

HB: High Bandwidth

HTTP: Hypertext Transfer Protocol

ICD: Interface Control Document

IEEE: Institute of Electrical and Electronics Engineers

IMA: Integrated Modular Avionics

IMM: Interface for Micro Munitions

JAUS: Joint Architecture for Unmanned Systems

JMPS: Joint Mission Planning System

JTA: Joint Technical Architecture

LAN: Local Area Network

LAR: Launch Acceptability Region

MDA®: Model Driven Architecture®

MIDS: Multifunctional Information Distribution System

MMSI: Miniature Mission Store Interface

MP ICD: Mission Planning ICD

NAFAG: NATO Air Force Armament Group

NATO: North Atlantic Treaty Organization

NCM: NCOE Component Model

NCOE: NATO Common Operating Environment

NCSP: NATO Common Standards Profile

NC3: NATO Consultation, Command, and Control

NC3TA: NATO C3 Technical Architecture

NE: Network Environment

NEW: Network Enabled Weapons

NIAG: NATO Industrial Advisory Group

NID: NATO Interoperability Directive

NNEC: NATO Network Enabled Capability

NTRM: NATO Technical Reference Model

OA: Operational Architecture

OCU: Operator Control Unit

OFP: Operational Flight Program

OMG™: Object Management Group

ORB: Object Request Brokers

OS: Operating System

OSE: Open System Environment

OSI: Open Systems Interconnection

OSIE: Open System Interconnection Environment

OTM: Object Transaction Monitors

PnP: Plug and Play

POSIX®: Portable Operating System Interface

PS ICD: Platform/Store ICD

RPC: Remote Procedure Calls

RSE: Real System Environment

RT: Remote Terminal

SA: Systems Architecture

SAE: Society of Automotive Engineers

S&RE: Suspension and Release Equipment

SNAcP: Subnetwork Access Protocol

SNDC: Subnetwork Dependent Convergence

SNDCP: Subnetwork Dependent Convergence Protocol

SNIC: Subnetwork Independent Convergence

SNICP: Subnetwork Independent Convergence Protocol

SOA: Service Oriented Architecture

SOAP: Simple Object Access Protocol

STANAG: Standardization Agreement

TCP/IP: Transmission Control Protocol/Internet Protocol

TA: Technical Architecture

TRM: Technical Reference Model

TV: Technical View

UAI: Universal Armament Interface

UAV: Unmanned Air Vehicle

UCAV: Unmanned Combat Air Vehicle

UML: Unified Modeling Language

WAN: Wide Area Network

WDM: Wavelength Division Multiplexing

WSA: Web Services Architecture

WSDL: Web Services Description Language

WS-I: Web Services Interoperability Organization

W3C: World Wide Web Consortium

XMI: XML Metadata Interchange

XML: Extensible Markup Language

XOS: Extended Operating System

xUML: Executable UML

3. BACKGROUND

3.1 Architecture Views

This document represents the technical view (standards and technologies framework) of the aircraft/store system architecture, in accordance with the system architectural views defined in the U.S. DoD Architectural Framework (DoDAF) and Joint Technical Architecture (JTA) Version 4. The DoDAF and JTA define a structured approach for documenting the architectures of military systems and the associated standards and technologies frameworks for implementing those systems. The term architecture is defined by the JTA as "the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time." The JTA and DoDAF define three architectural views: operational, system, and technical. These three views and their relationships are illustrated in Figure 1, and their definitions (as excerpted from the JTA) are subsequently described.

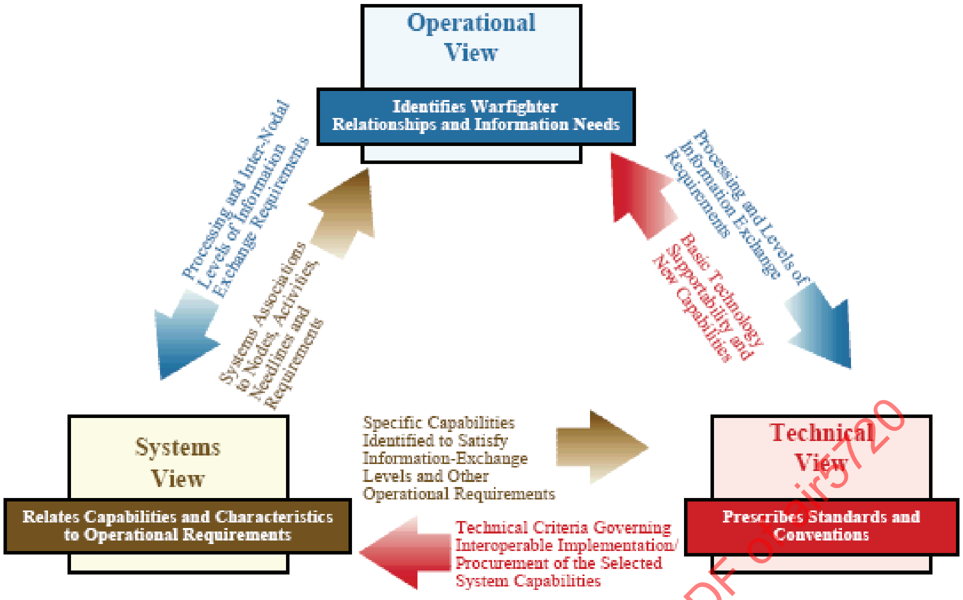

FIGURE 1 - ARCHITECTURE VIEWS

Operational Architecture View – The operational architecture (OA) view is a description of the tasks and activities, operational elements, and information flows required to accomplish or support a military operation. It contains descriptions (often graphical) of the operational elements, assigned tasks and activities, and information flows required to support the warfighter. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges in detail sufficient to ascertain specific interoperability requirements.

Technical Architecture View – The technical architecture (TA) view is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The technical architecture view provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The technical architecture view includes a collection of the technical standards, conventions, rules, and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular systems-architecture views that relate to particular operational views.

Systems Architecture View – The systems architecture (SA) view is a description, including graphics, of systems and interconnections providing for, or supporting, warfighting functions. For a domain, the systems architecture view shows how multiple systems link and operate, and may describe the internal construction and operations of particular systems within the architecture. For the individual system, the systems architecture view includes the physical connection, location, and identification of key nodes (including materiel-item nodes), circuits, networks, warfighting platforms, etc., and it specifies system and component performance parameters (e.g., mean time between failure, maintainability, availability). The systems architecture view associates physical resources and their performance attributes to the operational view and its requirements following standards defined in the technical architecture.

3.2 ALWI Technical Reference Models

Within the context of information systems, a Technical Reference Model (TRM) is a generally accepted construct that provides a basic set of concepts and a conceptual framework for identifying and resolving standards issues. The ALWI TRM provides the structure for standards in the ALWI Technical Architecture (ALWI TA), and allows coordination between different NATO (and national) standardization activities, including those within the NATO C3 Technical Architecture (NC3TA).

The ALWI TA differs from the NC3TA in that it relates to the Weapon Systems Domain as defined in the US Department of Defense Joint Technical Architecture (JTA). In contrast, the NC3TA addresses NATO C3 Systems, which more closely relate to the JTA C4ISR Domain. The Weapon Systems Domain applies to those systems whose primary function is to support attack and/or defence against an adversary. It is typically characterized by embedded computers that have hard quality of service requirements (such as safety, real-time performance and dependability) that must be implemented with challenging resource constraints (such as space, weight and power).

Specifically within the JTA Weapon Systems Domain, the ALWI TA falls within the Aviation Subdomain and Missile Systems Subdomain.

The ALWI TA is intended to promote interoperability with other systems within the Weapon Systems Domain, and with systems external to the Weapon Systems Domain such as NATO C3 Systems. To support the NATO Interoperability Directive, the relationship between the ALWI TA and the NC3TA is defined in 3.2.1 through 3.2.5. Further definition of the NC3TA is to be found in ADatP-34.

3.2.1 NATO Technical Reference Model

The NC3TA is based on the NATO Technical Reference Model (NTRM). The main purpose of the NTRM is to structure the standards listed in the NATO Common Standards Profile (NCSP).

The basic elements of the NTRM are those identified in the Institute of Electrical and Electronics Engineers (IEEE) Portable Operating System Interface (POSIX®) Open System Environment (OSE) Reference Model. This model includes three classes of entity and two types of interface (illustrated in Figure 2):

- Application Software Entity
- Application Program Interface (API)
- Application Platform Entity
- External Environment Interface (EEI)
- External Environment Entity

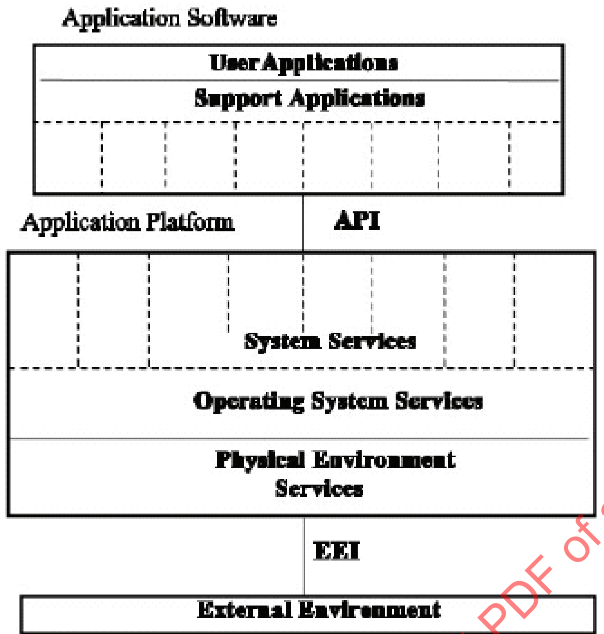

FIGURE 2 - NTRM SERVICES VIEW

The Application Software Entity includes both User Applications and Support Applications. In NATO C3 Systems, User Applications implement specific user (mission) requirements using the services of readily available Support Applications.

The Application Software Entity is supported by System Services, Operating System Services and Physical Environment Services within the Application Platform Entity. These services are accessed directly or indirectly via the API.

The External Environment Entity comprises external services that interact with the Physical Environment Services of the Application Platform Entity. In NATO C3 Systems, these services are classified into User Services (e.g., display, keyboard), Information Exchange Services (removable data storage) and Communications Services (e.g., local area or wide area networks).

3.2.2 NATO Common Standards Profile

In the NATO Common Standards Profile (NCSP), twelve Application Platform service areas are identified:

User Interface Services – graphical windows APIs, toolkits and style guides;

Data Management Services – data dictionary/directory services, object-oriented and relational database services, distributed data services, database replication, and NATO Common Schema;

Data Interchange Services – graphics data interchange services, video and audio interchange services, tactical data link message formats, NATO text formats, technical/business data interchange services, file compression and archiving, military symbology, and data encoding;

Graphics Services – computer graphics interfaces, and printer/plotter interfaces;

Communication Services – communication protocols based on the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite and/or the OSI Basic Reference Model;

Operating System Services – either POSIX® services or Windows 32 bit (Win32) APIs;

Internationalisation Services – interfaces to national systems, languages and conventions (this is a cross-service area);

System Management Services – Wide area network (WAN) and local area network (LAN) management;

Security Services – data object encapsulation services, data confidentiality services provided by network layer, data storage management infrastructures, defence against cyber attacks, OS security services;

Distributed Computing Services – remote data access, remote procedure calls (RPC), distributed computing environment (DCE), message oriented middleware, distributed transaction processing monitors, object request brokers (ORB), object transaction monitors (OTM), and message brokers;

Software Engineering Services – languages and bindings, Computer-Aided Software Engineering (CASE) environments and tools, software development methods,

Common C2 Applications Services – none specified.

It is expected that enhancement to the NCSP will be required to support a high degree of interoperability between NC3 Systems and the ALWI domain within a Service Oriented Architecture (SOA). These additional service areas are identified in 3.2.6.

3.2.3 NATO Common Operating Environment Component Model

The NTRM provides the structural basis for the NATO Common Operating Environment (NCOE) Component Model (NCM), illustrated in Figure 3. The principal components of the NCM are:

- Common Support Application Services
- Infrastructure Services
- Kernel Services
- Network Services
- APIs
- Data Component Definitions
- Support Services (methods and tools, information repository, training, system management and security)

Each Functional Configuration (FC) within an NC3 System is expected to comply with the NCOE and the NCSP, and is encouraged to utilize software from the NCOE Basket of Products (BoP). Functional Configurations include user terminals/devices, user workstations, administration workstations, network servers, messaging and communication servers, document management servers, web portal/application servers, database servers, directory servers and imagery servers.

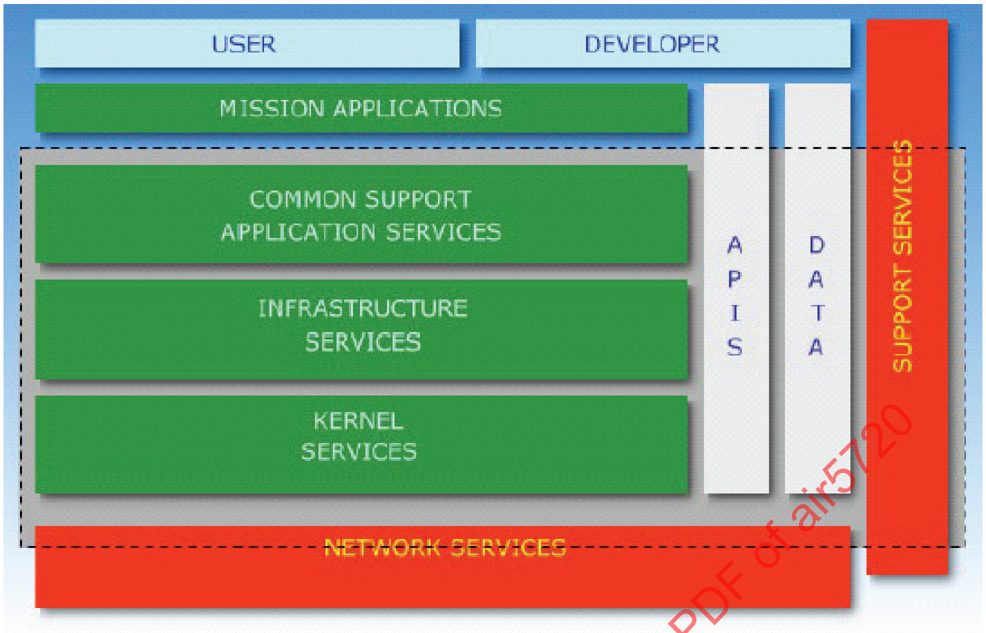

FIGURE 3 - NCOE COMPONENT MODEL

3.2.4 NCOE Basket of Products

The NCOE Basket of Products covers these software categories with mappings, where applicable, to the NCSP and/or to APIs.

Common Support Application Services – remote data access (e.g., Data Base Management System, or DBMS), tactical message data, office automation (e.g., Microsoft Office™, Adobe® Acrobat®), web browser (e.g., Netscape), document management client, message client (e.g., Microsoft Outlook™), document management server, message transfer agent (e.g., Microsoft Exchange™);

Infrastructure Services – DBMS middleware, file and print services, circuit-switched data exchange services, secure facsimile terminal services, tactical digital information links (e.g., Multifunctional Information Distribution System, or MIDS), LAN management, virus protection;

Kernel Services – Real-time/embedded or non real-time kernels.

3.2.5 Interoperability Degrees within NATO

The NATO Interoperability Directive (NID) defines five degrees of interoperability for NC3 Systems:

Degree 0 – **Isolated interoperability in a manual environment** (e.g., voice/fax);

Degree 1 – **Connected interoperability in a peer-to-peer environment** (in which physical connectivity is provided using Network Services);

Degree 2 – **Functional interoperability in a distributed environment** (in which independent applications exchange and use independent data components in a direct or distributed manner among systems);

Degree 3 – **Domain interoperability in an integrated environment** (in which domain data components are shared among independent applications using domain procedures);

Degree 4 – **Enterprise interoperability in a universal environment** (which enterprise data components are seamlessly shared among applications that work together using enterprise procedures).

The ALWI-CI Technical Architecture is intended to support degree 3 or 4, depending on the level of adoption in the NC3TA of data models and procedures. This is achieved through a Service Oriented Architecture that allows NC3 Systems to discover and use ALWI services.

3.2.6 ALWI Service Oriented Architecture

The ALWI Service Oriented Architecture is intended to support the interoperability of Aviation Systems and Missile Systems with NC3 Systems in accordance with the non-normative model shown in Figure 4.

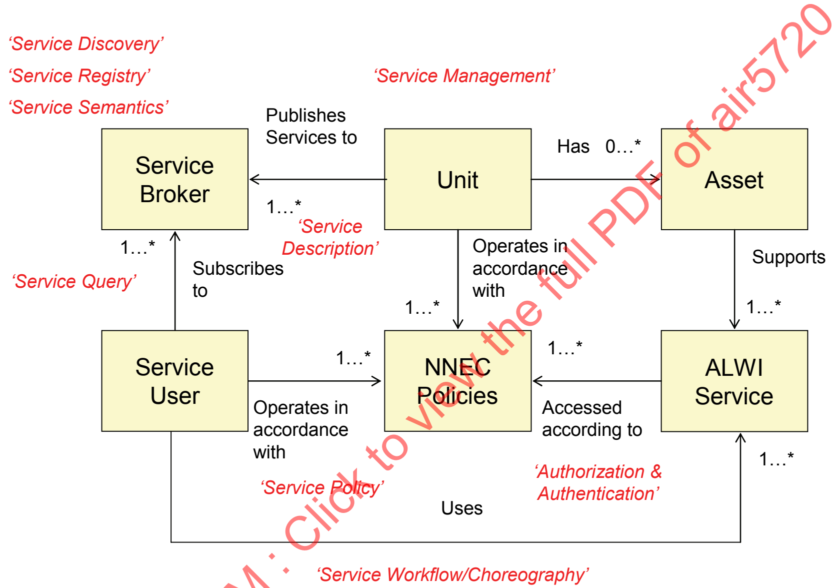

FIGURE 4 - ALWI SERVICE MODEL (NON-NORMATIVE)

The principal objects in the ALWI Service Model are:

Unit – the aircraft (manned or unmanned) that has Assets (including weapons). Upon discovery of its Assets, the Unit publishes its services to a Server Broker. The unit operates in accordance with NATO Network Enabled Capability (NNEC) Policies, including how its services may be used by a remote Service User.

Asset – the weapon. One or multiple weapons (and other assets) may support an ALWI Service.

ALWI Service – The collection of service facilities offered to a remote Service User. Facilities may be public or private (i.e., accessed only by the Unit) depending on its NNEC Policies.

Service User – The Weapon System or NC3 System that requires the ALWI Service to complete its mission. The Service User may request and utilize the ALWI Service only in accordance with its NNEC policies (and operational doctrine). To discover and gain access to the ALWI Service, the Service User must subscribe to a Service Broker.

Service Broker – The NC3 System that associates and prioritises published ALWI Services with Service User requirements in accordance with its policies and NATO operational doctrine.

To support the ALWI Service Model, the Infrastructure Services component of the NCOE (and NCSP) provides these additional service classes (or subclasses):

Service Registry;

Service Discovery;

Service Description;

Service Query;

Service Policy;

Service Management;

Service Workflow/Choreography;

Service Semantics;

Authorization & Authentication.

All of these service areas are supported by existing (domain independent) standards, including the Web Services of the World Wide Web Consortium (W3C), although this is a fast moving technology. However data models and procedures shall require standardization at the domain level or enterprise level within NATO for full interoperability to occur.

3.2.7 Weapon Systems Domain TRMs

Up to this point, the focus has been on NC3 Systems and the management of ALWI Services within NC3 Systems. The focus will now shift to the JTA Weapon Systems Domain, and specific TRMs that support the development of an ALWI Service and aircraft-weapon interoperability. Two TRMs are introduced: Generic Open Architecture (GOA) for 'real open systems' (corresponding to the NTRM) and Generic Aircraft-Store Interface Framework (GASIF) for 'open systems' (corresponding to the OSI Basic Reference Model). The GASIF is more useful for structuring standards that are based on peer-to-peer ICDs that are independent of the internal system implementation behind the ICD. Examples are MIL-STD-1760 and the Universal Armament Interface (UAI) Platform/Store ICD.

3.2.8 GOA Framework

In common with the NTRM, the JTA Weapon Systems Domain TRM is traceable to the POSIX® OSE Reference Model. The Service View extends the POSIX® model by decomposing its entities into the applications and services required by weapon system computing systems. The Interface View is based on the GOA Framework (SAE AS4893). The interface view is more applicable to real-time systems and is therefore the primary TRM for the ALWI TA.

The GOA Framework Interface View is shown in Figure 5 for two peer systems. The GOA Framework divides the components of a computing system into four conceptual layers. Together the three lower layers broadly correspond with the Application Platform Entity of the POSIX® OSE Reference Model. The fourth and highest GOA layer is the Application Software Layer.

The GOA Framework has both logical and direct interfaces. A logical interface defines the abstract protocol for the peer-to-peer exchange of data between Applications (4L interface), System Services (3L interface), Resource Access Services (2L interface) or Physical Resources (1L interface) in different systems. To implement a logical interface it is necessary to invoke the services of the layer below it using a direct interface. The Application Program Interface (API) of the POSIX® OSE Reference Model is broadly synonymous with the GOA 4D interface. For NC3 Systems, the GOA 4D interface would therefore support the twelve service areas identified in the NCSP (see 3.2.2), and perhaps some higher level services.

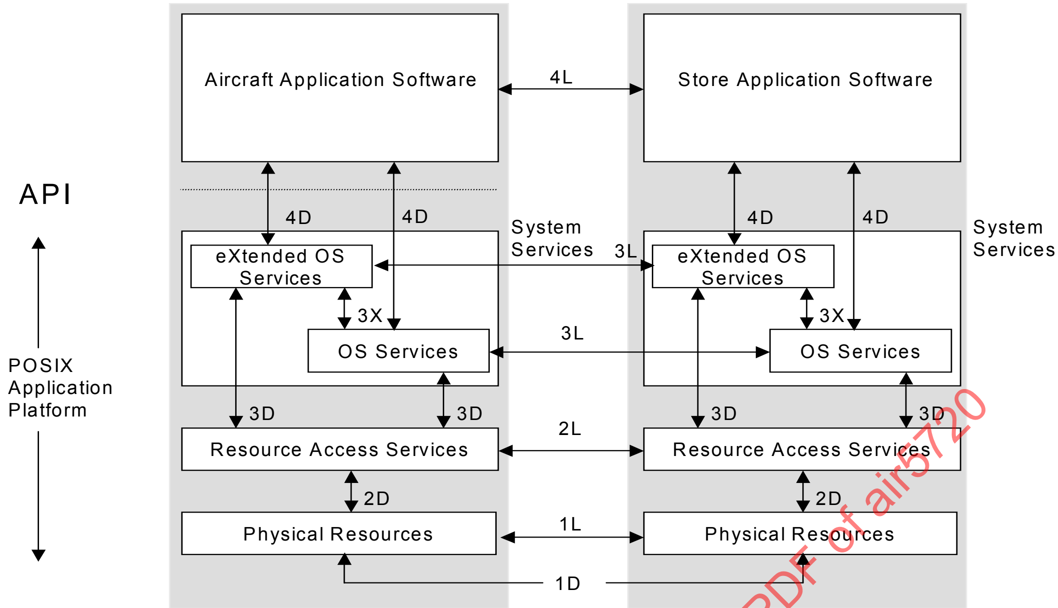

FIGURE 5 - GOA FRAMEWORK APPLIED TO PEER SYSTEMS

Within the System Services Layer there are two secondary layers. These are the Operating System (OS) Services and the Extended Operating System (XOS) Services. The OS Services correspond with the real-time/embedded Kernel Services of the NCOE. The XOS Services consist of modular extensions to the OS Services as well as higher-level functions that are shared by multiple Applications. These correspond with the NCOE Infrastructure Services and some Common Support Applications if considered part of the core services of the system.

3.2.9 Generic Aircraft Store Interface Framework

The SAE Generic Aircraft-Store Interface Framework is a reference model for an 'open system' as defined in the OSI Basic Reference Model. This model describes only the external behaviour of systems (through their peer-to-peer interfaces) and makes no assertions about the internal component architecture within each system. Many aircraft-weapon integration standards map more readily to GASIF than to GOA.

GASIF organizes the aircraft-weapon ICD into three nested environments (illustrated in Figure 6). The Real System Environment (RSE) encompasses the complete logical interface. Within the RSE, the aircraft and store application processes exchange data using a shared abstract syntax using the services of the Open System Interconnection Environment (OSIE). The OSIE complies with the OSI Basic Reference Model in that it describes operations and mechanisms that are assignable to its seven layers.

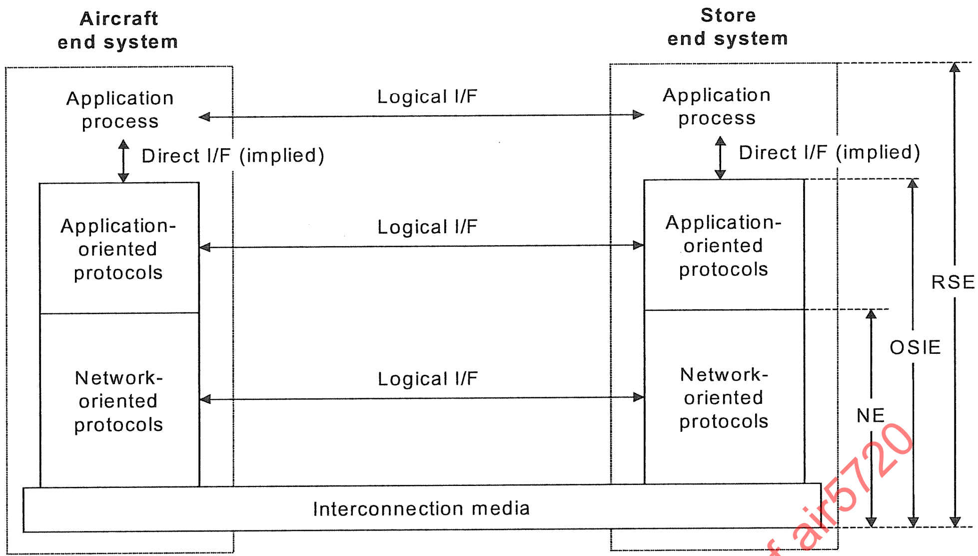

FIGURE 6 - LAYERED AIRCRAFT-WEAPON ICD

Within the OSIE, application-oriented protocols exchange data using a shared transfer syntax using the services of the Network Environment (NE). The application-oriented protocols map to the Application, Presentation and Session Layers in the OSI Basic Reference Model. Within the NE, network-oriented protocols exchange data using the physical interconnection media. The network-oriented protocols map to the Transport, Network, Data-Link and Physical Layers in the OSI Basic Reference Model. In GASIF, the Network Layer is sub-layered in accordance with ISO 8648 (OSI Internal Organization of the Network Layer). This is necessary to correctly model MIL-STD-1760 and UAI based ICDs.

3.2.10 ALWI GOA Profile

The GOA Framework is applied to the aircraft only (because the ALWI TA is not concerned with the internal implementation of the weapon or launcher system). The ALWI profile of the GOA Framework (illustrated in Figure 7) results in secondary layers within the Application Software. These are Mission Area Applications and Support Application Services, which broadly correspond with the peer layers in the NTRM. Mission Area Applications may provide ALWI Services to remote Service Users per the ALWI Service Model. The internal interfaces are denoted as 4X.

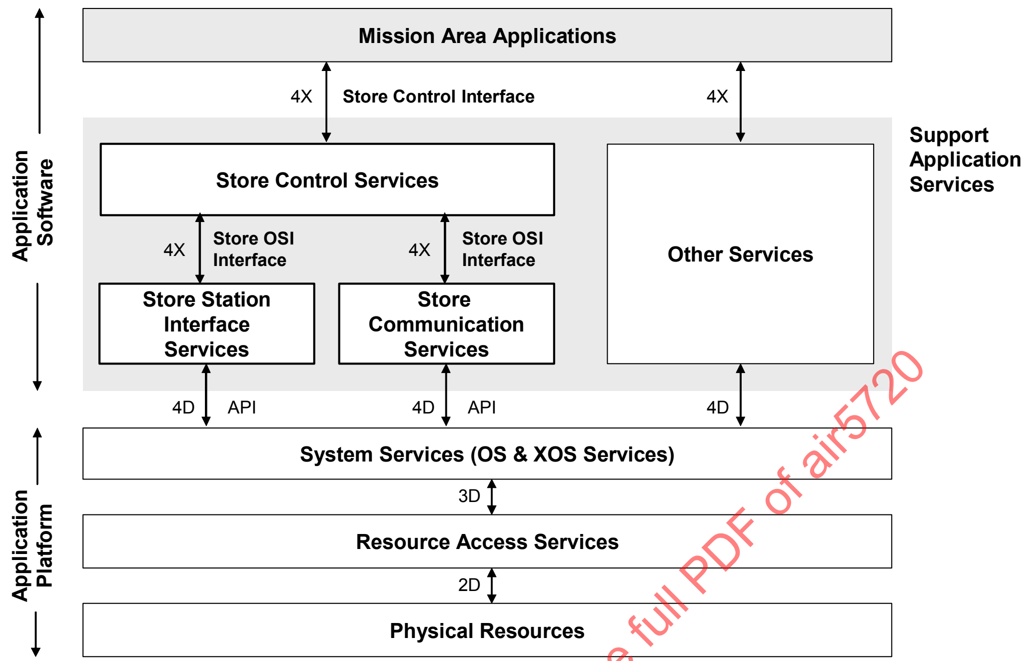

FIGURE 7 - ALWI PROFILE OF GOA APPLICATION SOFTWARE

The Support Application Services include Store Control Services, which are made available to the Mission Area Applications, and may also be made public to remote Service Users (depending on the type of aircraft). The Store Control Interface provides access to the Real System Environment (RSE) of the aircraft-weapon interface as defined in GASIF.

Underneath the Store Control Services are the Store Communication Services and Store Station Interface Services. The 4X interface provided to these services is the Store OSI Interface, which provides access to the OSIE of the aircraft-weapon interface as defined in GASIF, and provides generic S&RE functions for weapon release, arming and jettison. These services are supported by the underlying communication services provided by the GOA System Services.

Aircraft XOS Services may provide underlying facilities for ALWI Service Description, ALWI Service Management, ALWI Service Policies and ALWI Service Authorization & Authentication for advanced interoperability with NC3 Systems.

3.2.11 GASIF Profile

GASIF applies to the aircraft-weapon ICD. A complete description of GASIF is provided in AIR5532, along with various interconnection scenarios. Figure 8 shows a communication scenario involving an intervening carriage system and indicates the sub-layering of the Network Layer necessary to support MIL-STD-1760 based ICDs.

The mapping between GASIF and the ALWI GOA Profile is not intrinsic, but is suggested in Figure 9. It shall be noted that the GOA System Services are assumed to provide only a subnetwork service (SNDC Protocol). The Network Environment is completed by domain specific routing/relaying protocols and file transfer services that are implemented in the Support Application Services for ALWI.

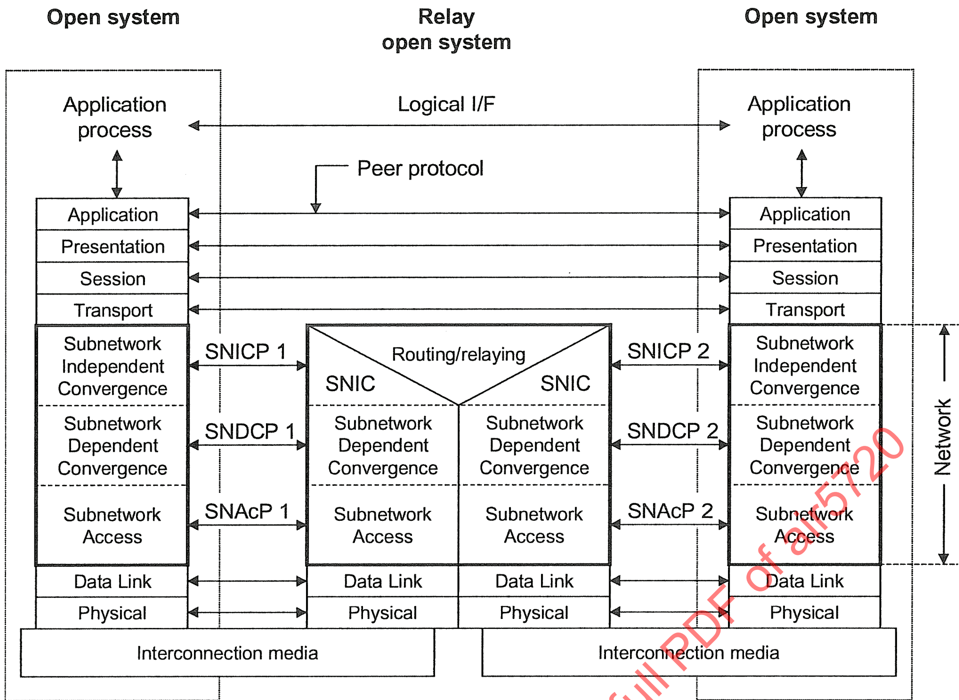

FIGURE 8 - NETWORK SUB-LAYERS

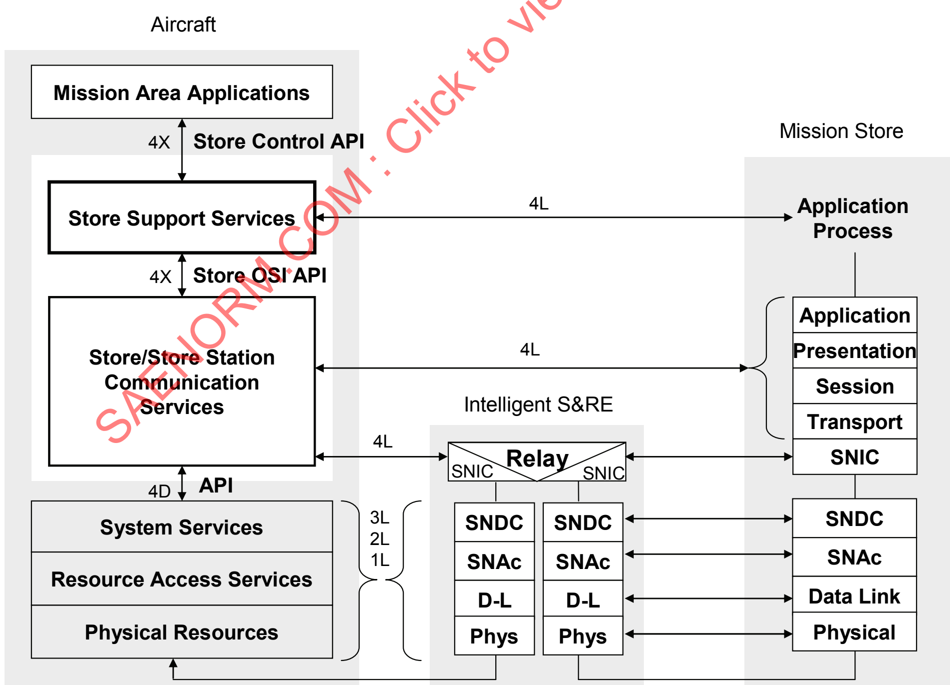

FIGURE 9 - MAPPING OF GOA STACK TO GASIF STACK

3.3 Standards Selection Criteria

The ALWI-CI Technical Architecture reflects only those standards necessary to maintain interoperability at interfaces within the aircraft/store system that are key to supporting a plug-and-play integration capability for aircraft and stores. Mandated standards were selected in accordance with the following criteria:

- Enhance aircraft/store interoperability across programs, services, and nations
- Are technically mature and stable and are supported in the commercial market place (where applicable)
- Are technically implementable
- Are non-proprietary and available to all qualified NATO aircraft/store integration organizations and personnel, and are not oriented toward any vendor-specific approach
- Have no fee for usage, other than charges for the standards documents (and any supporting application guidance) by publishing organizations
- Are consistent with all applicable law, regulation, policy, and guidance documents

4. SERVICES

This section identifies the mandated standards, emerging standards, and recommended additional standards that are required to support the ALWI Service Oriented Architecture.

4.1 Mission Area Applications

The aircraft Mission Area Applications Entity may provide various services to NATO C3 Systems including weapon-oriented services.

4.1.1 Mandated Standards

STANAG 4586

STANAG 4586 defines the architectures, interfaces, communication protocols, data elements and message formats that are required for interoperability of UAV systems in a NATO Combined/Joint Service Environment. In the ALWI TRM, STANAG 4586 messages are exchanged between the UAV Mission Area Applications Entity and NATO C3 Systems.

At present, STANAG 4586 provides basic payload/weapon control and status message formats for basic types of weapon (identified simply as air-to-air, air-to-ground, or air-to-surface). These message formats include:

- Message #4: Payload Configuration and Status
- Message #27: Stores Release System Status
- Message #28: Stores Release System Control

It is recommended that the STANAG 4586 message set be extended to provide additional control and status capabilities for stores that support the Universal Armament Interface Initiative and MIL-STD-3014. (See 5.1.)

In the longer term, it is recommended that the STANAG 4586 message set be harmonized with the application software domains proposed in Volume 2 of the ALWI-CI Final Report.

Additionally, it is recommended that the content of applicable Link 16 messages be incorporated into the STANAG 4586 message set. STANAG 5516 (MIL-STD-6016) defines the logical interface for the commonly adopted Link16. Link 16 is used to exchange all tactical data information within a theatre. The organization is hierarchical: the Link 16 network is split in subnets, which can be established amongst and between formations. Some messages are specified and only applicable for control units, while some messages can be used between MIDS units.

Currently a weapon data link interface is not addressed, but it is an expected development as is the transfer of imagery information through the network. (Refer to the Network Enabled Weapons Message Set discussion in 5.1.2.) However, the transfer is limited due to available bandwidth, since real-time capability is required for a weapon data link.

Relevant Link 16 J-Messages include (excerpt):

- J2 PPLI Word - e.g., J2.2 Air PPLI (Precise Participant Location and Identification also available for maritime and land/ ground based systems in J2.3-J2.5)
- J3 Surveillance Word - e.g., J3.2 Air Track (also available for Ground/ Point Track in J3.5)
- J7 Track Management (issued by Reporting Responsibilities only)
- J9 Weapons Coordination and Management (specific applicability for threat warning, ECCM coordination etc.)
- J10 Weapons Coordination and Management (J10.2: Engagement Status, issued by controlling C2 units only, J10.3 Handover)
- J12 Control Word - e.g., J12.0 Mission Assignment, J12.5 Target/ Track Correlation, J12.6 Target Sorting
- J13 Platform and System Status - e.g., J13.2 Air Platform and System Status (includes store status)

In addition to these LINK-16 messages, the United States is considering an interface change proposal to add messages specific to post-release weapon control, proposed to be assigned as the J11 series. If and when the United States has an approved position on this proposal, a corresponding change proposal will be submitted to the NATO Data Link Working Group (DLWG) for review and adjudication.

AIR5682

An SAE task group is working to define a Common Launch Acceptability Region Approach for supporting the LAR function in future aircraft/store systems. An ICD for the interfaces associated with major functions within the defined approach has been generated and published as AIR5682.

4.1.2 Emerging Standards

JAUS

The Joint Architecture for Unmanned Systems (JAUS) defines the architecture, interfaces, communication protocols, data elements and message formats that are required for interoperability of all types of unmanned systems. In the ALWI TRM, JAUS messages would be exchanged between the UAV Mission Area Applications and an external entity such as a JAUS Operator Control Unit (OCU).

Ownership of the JAUS standards transitioned in 2004 from the US DoD JAUS Working Group to the SAE Aerospace AS-4 Committee. The AS-4 committee plans to migrate the JAUS standards toward a service oriented architecture and define common service specifications for effects.

The future harmonization of JAUS and STANAG 4586 is being considered.

SOA Infrastructure Services

Service Oriented Architecture Infrastructure Services provide the interoperable means by which service requesters are dynamically connected with service providers in a network centric environment. Non-government SOA standards are primarily focussed on business/enterprise systems. The principal exponents of non-government SOA standards are the World Wide Web Consortium (W3C) and the Web Services Interoperability Organisation (WS-I).

The W3C Web Services Activity (http://www.w3.org) is designing the infrastructure, defining the architecture and creating the core technologies for Web services. A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format, specifically the Web Services Description Language (WSDL). Other systems interact with the Web service in a manner prescribed by its description using Simple Object Access Protocol (SOAP) messages, typically conveyed using Hypertext Transfer Protocol (HTTP) with an Extensible Markup Language (XML) serialization in conjunction with other Web-related standards.

The W3C published the Web Services Architecture (WSA) in 2004. The Web Services Activity is presently refining standards for WSDL, Web Services Addressing, Web Services Choreography, Web Services Policy, XML Protocols (such as SOAP) and XML Schema Patterns for Databinding.

The WS-I (http://www.ws-i.org) is an open industry organisation chartered to promote Web services interoperability by providing profiles, software and tools for web-related standards.

Adoption of standards for military Network Enabled Capability is new and is being managed by a variety of interrelated and sometimes competing initiatives within the NATO nations. While many of these initiatives have potential applicability to NC3 Systems, fewer are applicable for the Weapon Systems Domain and the ALWI TA. The principal constraint is the low and variable quality of service of mobile tactical networks versus the bandwidth requirements of XML based messaging. Recent initiatives to resolve this include the Global Information Grid - Joint Tactical Edge Network (GIG JTEN) in the United States. It is recommended that initiatives such as GIG JTEN are followed closely for ALWI applicability.

UAI Common Launch Acceptability Region (LAR) Approach

The UAI initiative includes a common approach for generating LAR-related information. This approach should be considered for incorporation into the ALWI-CI standards framework if detailed UAI information is released to NATO in the future.

4.1.3 Recommended Additional Standards

None.

4.2 Support Application Services

The aircraft Support Application Services Entity may provide various services to NATO aircraft application level programs for controlling and interfacing with stores and associated equipment in support of store employment operations.

4.2.1 Mandated Standards

None.

4.2.2 Emerging Standards

ALWI-CI API Methodology

Team 2 of NIAG Subgroup 97 developed a concept for a Model Driven Architecture approach to definition of a common API for store control and related services, which is documented in Volume 2 (API Methodology) of the NIAG Subgroup 97 study report. An MDA® based API definition which supports plug-and-play aircraft/store integration should result assuming this concept is carried forward, and should ultimately be standardized for application across NATO platforms.

4.2.3 Recommended Additional Standards

Additional standards relating to specific service areas reflected in the Team 2 API methodology and the ALWI GOA profile discussed in 3.2.10 are also recommended as subsequently described.

Store Control Services

A common superset of services required for a platform to initiate and control the functions and processes associated with employment of store types of interest should be standardized and documented.

Store Communication Services

A common superset of communication services for transferring information to and from stores to support the control functions/processes of the defined store control services should also be standardized and documented. These services should be compatible with relevant UAI communication provisions, if UAI is eventually adopted for NATO usage.

Store Station Interface Services

A common set of services for controlling and monitoring store station functions (suspension and release equipment control, store present switch monitoring, etc.) required for store employment should also be standardized and documented.

5. PROTOCOLS

This section identifies the mandated standards, emerging standards, and recommended additional standards for protocol elements required to support signal and information transfer across key interfaces within the ALWI TA, in general accordance with the GASIF layered protocol structure.

5.1 Presentation Layer Protocols

5.1.1 Mandated Standards

MIL-STD-1760 (STANAG 3837AA) Standard Messages/Data Entities

MIL-STD-1760 Appendix B (Digital Data Bus Communication Rules and Message Requirements) specifies certain standard messages for aircraft/store communications over the MIL-STD-1553 multiplex data bus, as well as a framework for other user-defined messages. It additionally specifies common formats for a number of data entities applicable to aircraft/store information transfers within the referenced messages. The MIL-STD-1760 Appendix B requirements for message and data entity formats are also referenced by the evolving Miniature Mission Store Interface (MMSI) standard for the electrical interface between miniature munitions/stores and their carriage systems.

Some near term updates to the Appendix B message/data entities will likely be made to accommodate additional functions that have recently been identified as common requirements. Longer term, there is ongoing consideration within the aircraft/store integration community toward separating the Appendix B logical requirements from the basic standard as a separate stand-alone document. It could then be independently referenced by other interface standards such as the MMSI.

MIL-STD-3014

MIL-STD-3014 defines a generic file structure for transferring mission data to stores, using existing communication paths and transport protocols (data bus, radio frequency, etc.). Provisions are included for definition of the specific file structure and content within a file header. A registry of standard data elements for use in MIL-STD-3014 mission data files is maintained on a website associated with the standard. New data elements can be registered for applications which cannot be adequately supported by the existing set of registered data elements.

5.1.2 Emerging Standards

UAI Platform to Store ICD (PSICD) Type Standard Messages

The UAI PS ICD defines a common consolidated set of MIL-STD-1553 messages for communication between platforms and air-to-ground precision-guided stores via a MIL-STD-1760 electrical interface. Messages from this set are to be used as applicable for a given aircraft/store combination. If the UAI detailed technical data is released to NATO for general usage, the UAI PS ICD message set should be largely applicable to NATO stores of the subject class, though some augmentation for additional NATO requirements might be necessary.

Network Enabled Weapons (NEW) Message Set

An ongoing U.S. program sponsored by the Air Armament Center at Eglin Air Force Base, Florida entitled Network Enabled Weapons is developing a common set of messages for communicating directly with stores via existing tactical radio frequency data links (Link 16, UHF, etc.). The messages make use of MIL-STD-3014 data file format provisions for transmission of mission data to weapons. Work is underway to incorporate the subject messages into the existing standards for these data links (MIL-STD-6016, MIL-STD-6020, MIL-STD-188-220, etc.) and the corresponding NATO STANAGs. A new stand-alone standard for the message formats is not planned. The defined messages incorporated into the existing standards should be applicable to both pre- and post-release direct communications with stores from off-platform sources in a network-enabled store employment environment.

5.1.3 Recommended Additional Standards

Standard message sets for aircraft/store communications will need to be developed for store classes of interest if the existing UAI PS ICD for precision-guided MIL-STD-1760 air-to-ground stores and any future extensions to other store classes are not eventually released to NATO. As indicated in 3.1.2, some augmentation of the UAI message set(s) may still be necessary to address additional NATO requirements, even if the UAI documents are released to NATO.

5.2 Session/Transport Layer Protocols

5.2.1 Mandated Standards

MIL-STD-1760 Mass Data Transfer Protocol

MIL-STD-1760 Appendix B specifies a protocol for mass data transfer of information files between aircraft and stores using a sequence of MIL-STD-1553 data bus messages. File allocation to messages and the associated message protocol for setup, transfer, and verification of files are addressed.

5.2.2 Emerging Standards

None.

5.2.3 Recommended Additional Standards

None.

5.3 Routing Protocols

Store carriage configurations for many of the platforms of interest include devices which support carriage of multiple smart stores at a single platform store station. These devices may consist of carriage stores for carriage of multiple MIL-STD-1760 stores, miniature store carriage systems for carriage of multiple miniature stores, or a combination of the two. Up to two hierarchical levels of carriage devices are considered potentially relevant for the time frames of interest. Figure 10 illustrates envisioned store carriage configurations from a data bus architecture perspective.