Australian Government
Department of Defence
Defence Science and
Technology Organisation

Approaches to Open Technology Systems Specification

Brendan Sims

Land Operations Division
Defence Science and Technology Organisation

DSTO-TN-1087

ABSTRACT

Open system considerations are important for future military systems to permit ease of integration, reconfiguration and upgrade, and to reduce the total cost of ownership of a system. This document provides guidance on the specification of open systems for acquisition.

RELEASE LIMITATION

Approved for Public Release

Published by

Land Operations Division
DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 7389 5555
Fax: (08) 7389 6567

AR-015-307
May 2012

APPROVED FOR PUBLIC RELEASE

Approaches to Open Technology Systems Specification

Executive Summary

Open systems considerations for military information and technology systems are gaining increased attention in the Defence environment. A major contributing factor is the difficulties and high costs associated with the inability of stove-piped legacy systems to integrate and interoperate with other systems and be easily upgraded or modified. These issues have highlighted the importance of open systems considerations during the development and/or acquisition of military information and technology systems.

The information presented in this document was gathered through internet searches of open literature relating to open systems and discussions with relevant expertise within DSTO. It was examined to develop a common definition for open systems and to determine how other militaries and Defence organisations are specifying openness for system acquisition and/or development. Approaches and resources that may be particularly useful to Australian Defence have been documented and discussed.

An open system makes use of open standards to specify its key interfaces. It is characterised by modular design to support its modification, upgrade or integration and is capable of being verified and validated to ensure open systems goals have been achieved. Open systems support interoperability with other systems and may offer many other benefits, such as portability of users and reduced cost of ownership, through vendor independence for through-life support.

The specification of open systems for systems acquisition should be undertaken by stakeholders with significant domain knowledge. It first requires identification of capabilities that would benefit from the implementation of open systems and market research to determine the availability of open standards and technologies. If an open system is feasible for a particular application, it is necessary to establish an enabling environment to promote the use of open systems through system requirements and specifications. To achieve a modular, open system design, the system must be decomposed into modular elements and a capability roadmap must be developed for the system life-cycle. This information is used to identify the key interfaces of a system and open standards must be determined for specification of these interfaces. Verification and validation of the system is then required to ensure openness objectives have been achieved.

This page is intentionally blank

Author

Brendan Sims
Land Operations Division

Brendan Sims graduated from the University of Adelaide with a BEng (Mechx) (Hons) in 2008. He has been employed at DSTO Edinburgh (Land Operations Division) since October 2009. In that time, he has worked in the Vehicle Electronics and Architectures team.

This page is intentionally blank

Contents

This page is intentionally blank

List of Acronyms and Abbreviations

ADF	Australian Defence Force
AEW&C MST	Airborne Early Warning and Control Mission System Testbed
ANSI	American National Standards Institute
API	Application Programming Interface
AUTOSAR	Automotive Open System Architecture
C4ISR/EW	Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance and Electronic Warfare
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-The-Shelf
DoD	Department of Defense (USA)
DSTO	Defence Science and Technology Organisation
FPS	Function and Performance Specification
GVA	Generic Vehicle Architecture
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IEC	International Electrotechnical Commission
IP	Intellectual Property
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union
KOSS	Key Open Sub-Systems
MAIS	Major Automated Information Systems
MDAPS	Mandatory Procedures for Major Defense Acquisition Programs
MIMOSA	Machinery Information Management Open Systems Alliance
MoD	Ministry of Defence (UK)
MOSA	Modular Open Systems Approach
MOTS	Military Off-The-Shelf
NAVAIR	US Navy Naval Air Systems Command
NDI	Non-Development Item
OA	Open Architecture
OAAT	Open Architecture Assessment Tool
OACE	Open Architecture Computing Environment
OCD	Operational Concept Document
OMG	Object Management Group
POSIX	Portable Operating System Interface for Unix
ROI	Return On Investment
SAE	Society of Automotive Engineers
SME	Subject Matter Expert
SOSCOE	System of Systems Common Operating Environment
SRD	Systems Requirement Document
SWaP	Size, Weight and Power
TIA	Telecommunications Industry Association

UK	United Kingdom
US	United States (of America)
V&V	Verification and Validation
VICTORY	Vehicular Integration for C4ISR/EW Interoperability
VSG	Vetronics Standards and Guidelines
WSC	World Standards Cooperation

1. Introduction

The current landscape of information and technology systems in the Australian Defence Force (ADF) consists of many monolithic or stove-piped sub-systems with inefficient and awkward integration into the larger infrastructure. This situation could continue under the ADF's focus on procuring Commercial Off-The-Shelf (COTS) and Military Off-The-Shelf (MOTS) products, which are often encumbered by proprietary technologies and arms traffic restrictions, resulting in vendor lock-in for through life support.

Defence forces globally are recognising the disadvantages and costs of this scenario, and are attempting to address the integration issue through awareness programs and legislation. The most widely accepted approach is to depart from the monolithic stove-pipe model, and build systems from modular components with Defence-mandated, open, non-proprietary interfaces. Examples of such efforts include the Generic Vehicle Architecture (GVA) [1][1], the Vehicular Integration for Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance and Electronic Warfare (C4ISR/EW) Interoperability (VICTORY) architecture [2], the System of Systems Common Operating Environment (SOSCOE) [3], and the Airborne Early Warning and Control Mission System Testbed (AEW&C MST) [4].

In the context of this document, the term "system" primarily refers to technologies used in the military environment that satisfy vehicle platform, propulsion, protection and control, and related functions, such as C4ISR/EW capabilities. A system may provide external interfaces to other systems and internal interfaces between its component subsystems. These interfaces may be used to exchange data, information or other services. Systems can range in scale from a component, such as a sensor or computer, to a functional collection, such as a vehicular power management system or local communication system, to a distributed capability, such as an entire battlefield information network.

The aim of this document is to provide insight on specifying open systems, to improve system interoperability and flexibility in Defence information and technology systems. The information presented in this document was gathered through discussions with relevant expertise within the Defence Science and Technology Organisation (DSTO) and through internet searches of open literature relating to open systems. The information was examined to develop a common definition for open systems and to determine how other militaries and Defence organisations outside of Australia are specifying openness for system acquisition and/or development. Approaches that may be particularly useful to Australian Defence have been documented and discussed. This document does not necessarily capture the complete range of information available regarding open systems specification, and other approaches may exist for open system specification that are not presented here.

The motivation for Defence to develop or acquire open systems stems from the range of benefits that these systems offer compared to existing monolithic or stove-piped systems within Defence, which do not tend to support modular decomposition of the system or

[1] See Section 0.2 of Defence Standard 23-09 – Generic Vehicle Architecture for information regarding application of the standard.

externally accessible interfaces for integration and interoperation of the system. As core principles, open systems are designed to support clean and efficient integration and interoperability with other systems through well defined interfaces [5]. This facilitates insertion of new technology, as it evolves, to address rapidly evolving threats and requirements. From a project management perspective, open systems can reduce the total cost of ownership of a system [5, 6] through their ability to use materiel from multiple competing vendors. This creates vendor independence, increasing the range of system upgrade options and reducing the risk of obsolescence for system components [5]. Open systems also allow trained personnel to conduct activities across a range of systems without re-training [6] due to the utilisation of common, defined interfaces.

This document first provides a definition of open systems, focussing on the functional properties and capabilities of such systems. This is followed by a description of a methodology for defining open systems in system specifications based on the Modular Open Systems Approach (MOSA), developed by the United States (US) Department of Defense (DoD). Further guidance on open systems specification and open systems information sources is provided in the appendices.

2. Open Systems Definition

Although there appears to be no single, common definition of an open system in the open literature, a number of common open system characteristics exist. They are used to form the following definition:

> In the context of military information and technology systems, an open system may be defined as a system of modular composition with its key interfaces between functional components defined according to open standards. Such a system must be capable of being verified and validated to ensure open system goals have been achieved.

This definition explicitly and implicitly defines common characteristics of an open system:

- The use of modular design;
- The identification of key interfaces;
- The use of open standards to specify the key interfaces of a system, where appropriate;
- Full accessibility to relevant documentation; and
- The ability to be verified and validated to ensure open system goals are achieved.

Each of the major characteristics of an open system are now discussed.

2.1 Use of Modular Design

A modular system uses discrete, self-contained, reusable modules with well-defined interfaces to partition the functionality of a system [5]. Although the modules are independently operable of one another, they can be combined for a cohesive purpose, with system developers able to synthesise a system using an inventory of pre-implemented modular elements. This allows elements to be swapped out and replaced with other elements of superior capability.

The use of modular design in an open system supports efficient integration and rapid upgrade of the system, a key objective for open systems. By decomposing a system into modular, functional elements, distinct interfaces between these elements exist and key interfaces (see Section 2.2) are more easily identified. Open standards (see Section 2.3) applied to these key interfaces ensure appropriate interface definition to support the integration and upgrade of the system. Modular design is also important since it promotes reuse of functional components, which creates commonality in systems and mitigates the risk of obsolescence [7].

2.2 Identification of Key Interfaces

A key interface is a boundary between modules or systems through which critical data, information or other services are passed [5]. Such interfaces may be considered to be key interfaces due to the rapid technological change, high rate of failure or costliness of systems connected by these interfaces [5]. The identification of key interfaces is of great importance to the design of open systems, as key interfaces become candidates for Defence-mandated standards.

Key interfaces can be defined through various processes including roadmapping activities with consideration given to estimated sub-system rate of change and obsolescence. It is not necessary to mandate that all interfaces within and between systems achieve a high level of openness since this would be very costly and impractical to manage [5]. However, it is important to identify the key interfaces for which open standards should be applied to achieve the associated benefits of an open system. This is discussed further in Section 3.4.

2.3 Use of Open Standards

A common characteristic of open systems defined in the open literature is the designation of open standards to define the key interfaces of an open system. Open standards provide common guidance for the design, function, development, maintenance and modification of a system. However, the definition of an open standard is subject to conjecture, for example, recent statements from the United Kingdom (UK) Government indicated that their definition of an open standard remains up for consultation [8]. The following definition attempts to take into consideration the range of definitions in open literature for an open standard.

> An open standard is a well-defined, consensus-based and non-proprietary standard of sufficient maturity to be widely accepted and used by competing vendors and system developers. For a standard to be open, it should be developed collaboratively, open to change through collaboration, and be readily, if not freely, available with no barriers to implementation by a third party.

Care must be taken when specifying the use of open standards to ensure they are fit for purpose, in addition to being suitably open. In a military environment, situations may arise that require proprietary solutions instead of those guided by open standards, for example, to meet strict security or performance requirements. Hence, open standards should only be used where appropriate. Other types of standards are discussed in Appendix D.

2.4 Full Accessibility to Relevant Documentation

For a system to be able to be verified that it is sufficiently open for its intended application, it requires full accessibility, for all relevant organisations, to relevant documentation, namely a fully populated Interface Control Document (ICD) [9]. An ICD is a document describing all the interfaces of a system and is necessary to ensure a consistent approach to interface definition. Access to the ICD gives visibility of the system interfaces, allowing a system to be modified or upgraded by third parties in the future.

2.5 Verifiable and Validatable

An open system must be subjected to successful verification and validation (V&V) to ensure its key interfaces are sufficiently open [5], functionally valid and relevant since the interpretation of a standard may vary. The ability of a system's openness to be verified and validated is a key characteristic of an open system. Verification is conducted to verify that the openness requirements in the system specifications have been met. It involves a combination of reviews, analysis and tests [1]. A system that meets its requirements does not necessarily perform according to its intended use: user requirements may be incomplete or there may be emergent, unintended effects that prevent the system from operating as intended. Hence, validation is required to confirm that a system functions as intended.

Verification of an open system requires documentation of system design and standards used, in addition to published policies for system upgrade. Open system verification is enabled early in a project, by developing system requirements with sufficient detail to provide verification criteria [7].

Verification and validation of open standards conformance may be assisted through a reference implementation. A reference implementation is an implementation of a standard that is conformant to that standard [10]. It demonstrates that a standard can be implemented and provides a reference against which other implementations of the standard are evaluated. Further information on the verification and validation of open systems is provided in Section 3.6.

3. Open Systems Specification

There are many useful resources for specifying open systems. The information presented in this section is a combination of information from the following resources:

- The GVA, from the UK Ministry of Defence (MoD), specifies the mandatory standards for common interfaces for use in all future land platform procurements by UK Defence [1].

- The Key Open Sub-Systems (KOSS) tool, from the US Navy Naval Air Systems Command (NAVAIR), is used to identify key interfaces for which open standards should apply [11].
- The MOSA, developed by the US DoD, describes an approach to implement open systems in Defence [5].
- The Naval Open Architecture (OA) Contract Guidebook, from the US Navy, provides guidance to industry on the incorporation of open systems principles into relevant system acquisitions [12].
- The Open Architecture Assessment Tool (OAAT), from the US Navy, is a tool to assess compliance with the MOSA, in addition to the technical and programmatic openness of programs [13].
- The Open Architecture Computing Environment (OACE), from the US Navy, is a standards-based set of computing resources designated for use in US Naval warfighting systems [6].
- The VICTORY architecture, developed by the US Army is an effort to develop and validate a set of open standards (in cooperation with industry) for the integration of C4ISR and related items of equipment on Army platforms [2].
- The Vetronics Standards and Guidelines (VSG), from Qinetiq in the UK, presents standards and guidelines for Vetronic infrastructures [14].

These resources are specifically discussed further in Appendix C. Further useful guidance is provided by the US DoD in DoD 5000.2-R – Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs [7].

The process of specifying open systems follows a number of steps, which are depicted in Figure 1 and discussed further in the following sections. These steps are based on the process described by the MOSA. They should be conducted by a team of stakeholders, with significant domain knowledge, who are involved in the acquisition, deployment and employment of the proposed system [5]. Although the MOSA does not necessarily reflect the Australian Defence capability development process [15], it is an example of an approach that could be adapted to improve open system specification in Defence acquisition and development.

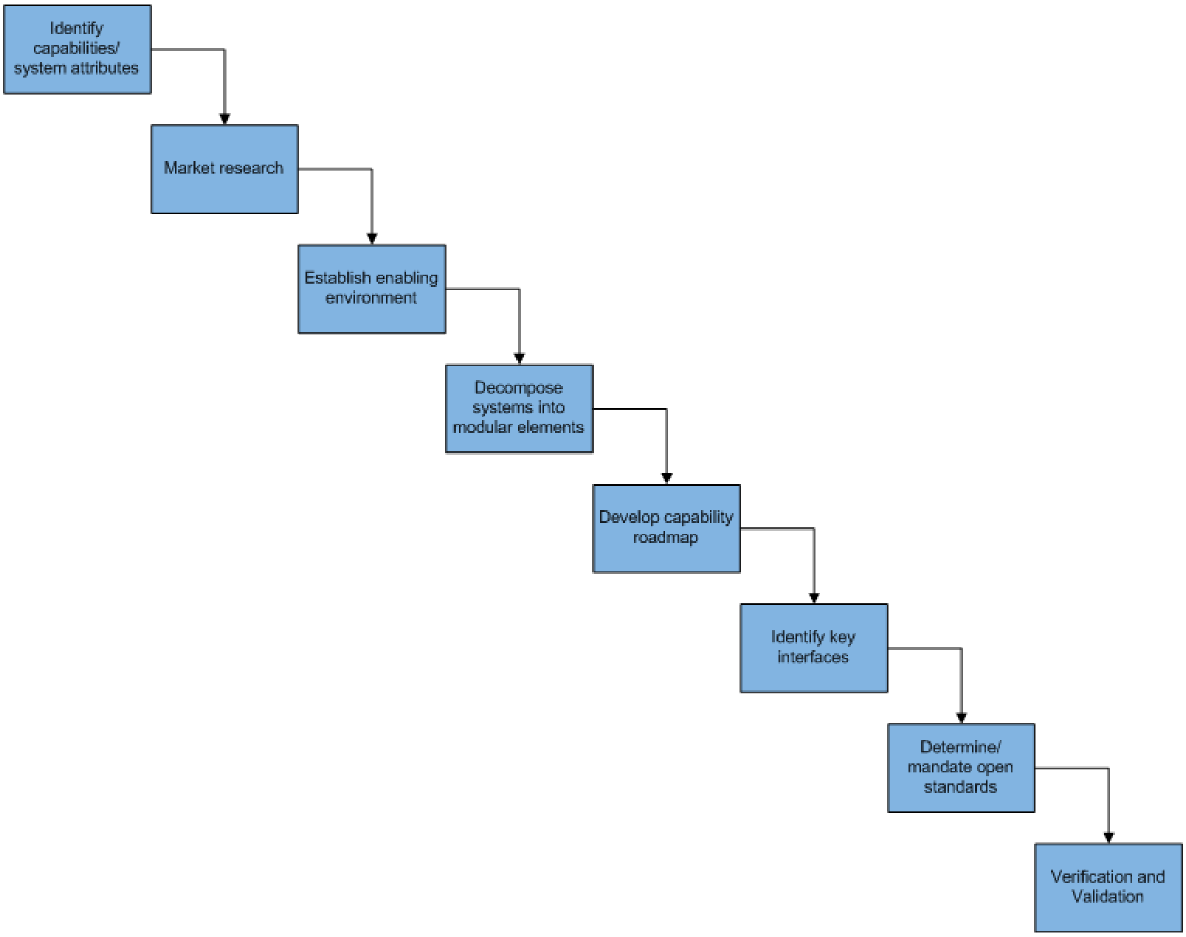
Identify capabilities/ system attributes
Market research
Establish enabling environment
Decompose systems into modular elements
Develop capability roadmap
Identify key interfaces
Determine/ mandate open standards
Verification and Validation

Figure 1 Overview of the process for open systems specification. The diagram has been adapted from information presented in [5] and [11].

The first step in open system specification is to identify the specific desirable capabilities or system attributes that will be enabled by the implementation of open systems [5]. For example, a system may be subject to incrementally specified operational requirements and will require multiple upgrades throughout its life cycle. Such a system would benefit from open system considerations.

The next step involves market research to assess whether it is feasible to implement an open system to enhance the required capability [5]. The purpose of this research is to identify technologies, standards and compliant products that can address capabilities requiring open systems. It should also identify any risk areas that may impact the operation or sustainment of a system over its life cycle.

Once it has been determined that a capability exists that can be enhanced by an open system approach, and sufficient technologies, standards and compliant products exist to ensure an open system solution is feasible for the capability, it is necessary to specify such a system. The specification of an open system for acquisition should roughly follow the following steps, which have been adapted from the MOSA principles for open systems [5]:

- Establish an environment that enables open systems.
- Decompose proposed systems into modular elements.
- Develop a capability roadmap for the system lifecycle.
- Identify key interfaces.
- Determine open standards for key interfaces.
- Implement strategies to enable verification and validation of open system conformance.

3.1 Establish an Environment that Enables Open Systems

For the acquisition of open systems, it is first necessary to establish an environment that promotes the use of open systems [5]. This is achieved through corporate culture, legislation, policy, or statements in the initial project documentation. The aim should be to create non-functional requirements that promote growth of the system capability [16] by encouraging open system acquisition and not imposing design specific solutions. Defence's processes should ensure that sub-systems provide correct implementations, the ability to change and appropriate obsolescence management. Where capability evolution is expected, the underlying system should be specified to support change through design for change.

It is important that the Operational Concept Document (OCD) describes the evolution of the operational context over the capability's lifecycle. This involves assessing technologies and developing roadmaps to estimate the expected rate of change of the capability's major equipment components. The components that are expected to have a faster rate of change, such as computers, software and communication equipment, require good interface definition and interface control specification, while those expected to change at a slower rate should be designated for obsolescence management. In conjunction, configuration management processes should be established to encompass any changes to key interfaces and corresponding standards over the system lifecycle [5]. The development of capability roadmaps is discussed further in Section 3.3.

The Function and Performance Specification (FPS) should address a number of issues to enable open systems. It is important to state requirements for extensibility of the system via defined interfaces. The FPS should also specify demonstration of interoperability with other projects. Further requirements should be included to allow the project to obtain and manage Intellectual Property (IP), including relevant documentation, associated with systems and their interfaces. This will enhance V&V and risk assessment, and will facilitate maintenance, future system upgrades and development. Mandating backwards compatibility with legacy systems to promote interoperability is another important consideration.

Market research should be used as a primary means to determine the applicability of available and emerging interface standards for open system specification [7]. This market research should also identify the breadth of open and de facto[2] standard-compliant products to determine whether suppliers will continue to produce or support selected standards [5]. Market research should continue throughout the acquisition process and during post-production support [7].

[2] See Appendix D for definition.

3.2 Decompose Proposed Systems into Modular Elements

Prior to identifying the key interfaces of a system, it is necessary to decompose the proposed system into modular elements [11], for example a Work Breakdown Structure or technical reference model [5], to provide a high level view of system modularity and the interfaces between these modules. This decomposition should produce a set of the major components, grouped by hardware, software, middleware and operating systems. It is this set of components that is analysed to determine the key interfaces.

For legacy or acquired systems, information must be gathered on the system design to enable modular partitioning of the system and mapping of services and interfaces to known functions and capabilities [5]. This requires design specifications, ICDs, functional specifications, and known standards profiles [5]. The output of this process is assessed to determine the suitability of an open system approach for the proposed system.

3.3 Develop a Capability Roadmap for the System Lifecycle

Following the system decomposition, a capability roadmap should be developed to identify system components expected to add capability during the system lifecycle [11]. In addition, consolidation of the expected changes to existing system components should be conducted, including an estimation of their rate of obsolescence [11]. These changes may be continuous in nature, such as crew turnover and the availability of information, or may be associated with technology refresh cycles [16]. The capability roadmap is determined from capability requirements [11] and is important in planning for the life of a platform.

For each of the components identified in the system decomposition, a qualitative estimate of the expected rate of obsolescence over the roadmapped period should be produced [11]. This, along with the capability roadmap, enables the relative rate of change of system components to be determined and volatile interfaces to be identified. Any rapidly changing components that are not targeted during upgrade cycles will require strict obsolescence management[3].

3.4 Identify Key Interfaces

The identification of key interfaces is an important task in realising open systems. The MOSA specifies that programs must determine the level of implementation at and above which control over key interfaces is required and open standards should be applied [5]. This requires market research to determine the availability of open standards for key interfaces (as discussed in Section 3.1) [5]. The results of market research are also used to assess the impact of the chosen level of interface control on long-term viability and affordability [5]. Care must be taken in specifying the level of interface control since defining it too low may limit efficient technology insertion, while defining it too high may cause proprietary system interfaces to be used for major system components [5].

A number of tools exist to provide guidance for the identification of the key interfaces of a system, such as the KOSS tool [11]. This tool makes use of system requirements and Subject

[3] Refer to the Defence Policy on Obsolescence Management for further information [17].

Matter Expert (SME), sponsor and warfighter knowledge to identify the system components expected to have a high volatility over a long period of time. The KOSS tool specifies the key interfaces as those either side of volatile components. The process used by the KOSS tool to identify key interfaces is depicted in Figure 2.

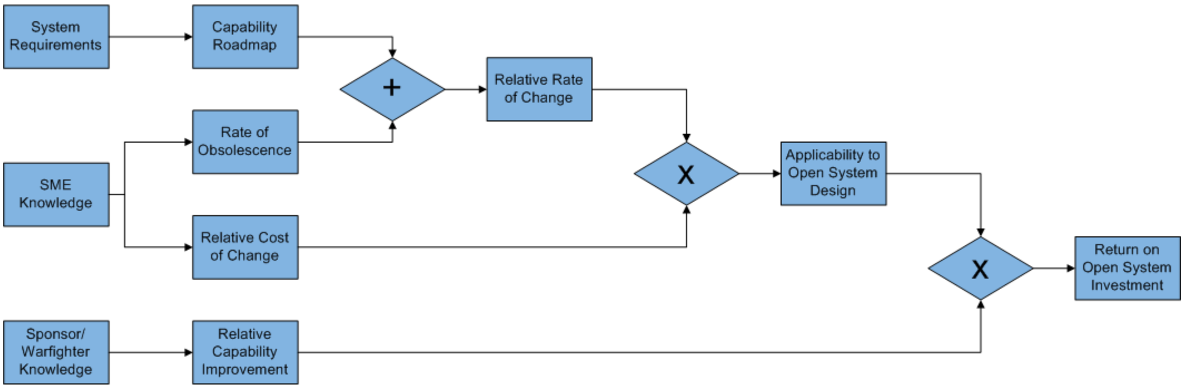
System Requirements
Capability Roadmap
+
Relative Rate of Change
Rate of Obsolescence
SME Knowledge
X
Applicability to Open System Design
Relative Cost of Change
X
Return on Open System Investment
Sponsor/ Warfighter Knowledge
Relative Capability Improvement

Figure 2 Process used by the KOSS tool to identify key interfaces. The process is repeated for each relevant system component. This diagram has been adapted from [11].

The tool first requires a system decomposition, to determine major system components, and development of a capability roadmap, to determine the relative rate of change of system components, as described in Section 3.2 and Section 3.3. The relative rate of change information is then combined with relative cost of change estimates for the system components to determine their applicability to open system design. The components with the highest rate and cost of change are most applicable.

Next, sponsor and/or warfighter knowledge should be used to estimate the relative capability improvement that each component provides to the warfighter. This is combined with the open system applicability to determine each component's return on open system investment. Interfaces to those components that are most applicable to open system design and provide the highest return on investment should be designated as key interfaces.

The process defined for the KOSS tool should be conducted recursively to designate all key interfaces from the top-level system down to component level. This process should also be repeated each time the capability roadmap is updated [11]. The KOSS tool does not specifically consider interfaces between more frequently failing components, or those that pass vital interoperability information. These aspects should also be factored when identifying key interfaces.

Once the key interfaces of a system have been identified, it is necessary to establish configuration management processes to manage these interfaces over the system lifecycle [5]. These configuration management processes include identification and documentation of the functional and physical characteristics of all relevant interfaces, recording interface configuration, and controlling changes to an interface and its documentation [7]. The configuration management process should ensure that all interface requirements changes are properly recorded and communicated [7]. A further process should be conducted to define the roles and ownership of all key interfaces and their dependencies. This ensures all key interfaces are well defined and managed, and responsibility is assigned for all key interfaces over the system lifecycle.

3.5 Determine and Mandate Open Standards for Key Interfaces

Once the key interfaces have been identified, it is necessary to determine the open standards to define these interfaces. This is achieved through an analysis of the market to determine the availability of relevant open standards for the identified key interfaces [5]. It allows the feasibility of using open standards for each key interface to be assessed. The MOSA recognises that there are instances where it may not be sensible to use open standards for key interfaces [5]. Stakeholders should carefully examine the key interfaces to ensure the use of open standards for these interfaces is appropriate, based on business and performance objectives [5].

In Defence systems, some key interfaces are likely to have particularly strict performance, security or functionality requirements. Additionally, the utilisation environment for military systems may impose modification of commercial products to meet military requirements. In these cases, it may not be feasible to use open standards to specify the interface, or there may not be an appropriate standard available. Hence, open standards should only be used where appropriate. Should a vendor want to use proprietary interface standards or modify existing open interface standards to meet these requirements, they must provide sufficient justification and evidence that their system can be evolved. However, the preferred implementation of a key interface should employ a formal open interface standard.

If it is determined that there are available open standards for the specification of a system's key interfaces, the appropriate open standards for key interfaces should then be selected by those stakeholders with significant domain knowledge [11]. The selection of open standards is assisted by market research and enabled by the correct wording of project documentation. The MOSA [5] and the OA Guidebook [12] provide guidance on language to use in a Request for Proposal to encourage the use of open standards. Examples are included in Appendix A.

3.6 Verification and Validation (V&V) of Open Systems

The final principle of the MOSA concerns the V&V of open systems to ensure openness objectives for the system have been met [5]. The verification of an open system involves verifying that the requirements relevant to openness have been met, and validation of an open system is conducted to ensure the system performs according to its intended use. The MOSA suggests that the program manager and user should coordinate to develop V&V mechanisms, such as conformance certification and test plans to ensure the key internal and external interfaces of a system conform to open system goals [5]. The V&V processes should also ensure that the system components and commercial products implemented do not make use of vendor-unique extensions to interface standards to avoid vendor lock-in.

To achieve an open system, and the subsequent benefits, it is important to establish business and technical indicators or attributes early in a project for the assessment of system openness [5]. These attributes allow the level of openness to be monitored during development, prior to acquisition, or during the V&V process of a system to ensure open system objectives are ultimately achieved. The MOSA suggests using specific performance measures to gauge the progress of implementing an open system approach [5]. For example, the degree of system openness could be measured by the percentage of key interfaces defined by open standards [5]. Other performance measure examples provided in MOSA documentation are the percentage of modules that can change without major system redesign and the percentage of total life cycle cost savings attributable to compliance with MOSA principles [5]. The business attributes should be established to assess the procurement approach for acquisition of the system to ensure the process encourages and implements open system acquisition.

The OAAT, from the US Navy, provides an example of a method for assessing the openness of systems. The OAAT is a Microsoft Excel-based tool consisting of a standard question set designed to assess the business and technical characteristics of a program that are relevant to openness [13]. The business characteristics refer to the processes and documentation used by programs to employ and manage systems, while the technical characteristics refer to the technical features of a system. These characteristics are discussed further in Appendix C. Prescribed criteria are used to answer the OAAT question set on a scale from one to five with the OAAT calculating a total score to form a rating of the openness of a program. It is encouraged to provide an explanation for each answer and evidence or supporting documentation. The OAAT helps to identify areas for improving openness and it allows the impact of proposed upgrades to be analysed.

4. Summary

The acquisition of monolithic, stove-piped systems by Defence continues to contribute to difficulties associated with the integration and interoperation of military systems. Such systems are often encumbered by the use of proprietary technologies, resulting in vendor lock-in for through-life support of the system, significantly constraining maintenance and upgrade of the system. Integration and interoperation issues are encountered with these systems since their interfaces are not externally accessible to Defence.

Systems developed or acquired based on a modular, open systems approach aim to improve the integrability and interoperability of military capability systems. Open systems make use of modular design and open standards to define their key interfaces. This supports efficient integration and upgrade of the system, allows vendor independence and improves interoperability between military systems. In turn, the total cost of system ownership may be reduced and users can be trained across a range of systems.

Many sources in open literature provide guidance on the specification and acquisition of open systems. It first requires identification of capabilities that would benefit from the implementation of open systems, and market research to determine whether sufficient technologies and standards exist for an open system to be feasible. Once it has been determined that an open system can be pursued, it is necessary to establish an enabling environment to promote the use of open systems through system requirements and specifications. To achieve a modular, open system design, the system must be decomposed into modular elements and a capability roadmap must be developed for the system life-cycle. This information is used to identify the key interfaces of a system. Open standards must then be determined for specification of these interfaces, which is assisted by market research. Finally, verification and validation should be conducted to ensure an open system has been achieved.

5. References

[1] Defence Standard 23-09 - Generic Vehicle Architecture. UK Ministry of Defence, 2010.

[2] VICTORY Standards Public Site, n.d. Last viewed 31 October 2011, <http://www.victory-standards.org/>.

[3] Boeing Defence, Space and Security. System of Systems Common Operating Environment (SOSCOE), 2010. Last viewed 3 February 2012, <http://www.boeing.com/bds/soscoe/SOSCOE_overview.pdf>.

[4] Foster, K, et al. Exploring a Net Centric Architecture using the Net Warrior Airborne Early Warning Control Node, DSTO-TN-2093. Edinburgh, Australia: Air Operations Division, Defence Science and Technology Organisation, 2007.

[5] A Modular Open Systems Approach to Acquisition. Open Systems Joint Task Force, US Department of Defence, 2004.

[6] Open Architecture (OA) Computing Environment Design Guidance. Program Executive Office, Integrated Warfare Systems, US Department of the Navy, 2004.

[7] DoD Regulation 5000.2-R - Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs. US Department of Defense, 2002.

[8] Moody, G. UK Government: Open Standards Must be RF, not FRAND, 2011. Last viewed 13 September 2011, <http://blogs.computerworlduk.com/open-enterprise/2011/09/uk-government-open-standards-must-be-rf-not-frand/index.htm/>.

[9] Press, S. Annex to Vetronics Standards and Guidelines: VSI Metrics for Electronic Architecture Assessment. Farnborough, UK: Qinetiq, 2009.

[10] Carnahan, L. Conformance Testing, 2010. Last viewed 10 February 2012, <http://www.nist.gov/itl/ssd/is/conformancetesting.cfm>.

[11] Naval Air Systems Command. Key Open Subsystems (KOSS) Tool: KOSS Description and Application, 2009. Last viewed 10 August 2011, <https://acc.dau.mil/adl/en-US/317012/file/46502/KOSS%20Overview_FINAL_5Aug09.pdf/>.

[12] Naval Open Architecture Contract Guidebook. Program Executive Office, Integrated Warfare Systems, US Department of the Navy, 2006.

[13] Zimmerman, M. US Navy Open Architecture and the OA Assessment Tool, in Automation and Controls Symposium, Milwaukee, USA, 2010.

[14] Connor, R. Vetronics Standards and Guidelines. Farnborough, UK: Qinetiq, 2009.

[15] Defence Capability Development Manual. Australian Department of Defence, 2006.

[16] Kott, K, Adams, K, Dove, R. Agility and the Combat System. Naval Engineers Journal 2008; 120(4): 67-78.

[17] DEFLOGMAN Part 2, Volume 5, Chapter 7 - Defence Policy on Obsolescence Management. Australian Department of Defence, 2010.

[18] Belson, C. Open Systems: State of the Practice, in NDIA Simulation-Based Acquisition/Advanced Systems Engineering Environment Conference, Washington DC, USA, 2002.

[19] Common Object Request Broker Architecture, 2011. Last viewed 2 September 2011, <http://en.wikipedia.org/wiki/Common_Object_Request_Broker_Architecture>.

[20] POSIX, 2011. Last viewed 2 September 2011, <http://en.wikipedia.org/wiki/POSIX>.

[21] Wilson, C. Open, De Jure, De Facto and Proprietary: Standards and Microsoft, 2006. Last viewed 23 September 2011, <http://www.scribd.com/doc/13586799/Open-De-Jure-De-Facto-and-Proprietary-Standards-and-Microsoft/>.

Appendix A: Examples of Language

An important programmatic characteristic of an open system is the inclusion of open systems language in project documentation and contracts. The MOSA [5] and the OA Guidebook [12] provide examples of the language to use in project documentation to enable open system acquisition. Note that both of these references discuss project documentation for projects in the US. A snapshot of language examples is included here and the referenced documents should be referred to for further information.

In the Statement of Work (or Statement of Objectives), the OA Guidebook suggests a number of design approach characteristics should be utilised, including implementation of a modular, open design, adherence to MOSA objectives and the use of standards [12]:

> *(a) Modular, Open Design – The contractor shall develop an architecture that is layered and modular and uses COTS/Non-Development Item (NDI) hardware, operating systems, and middleware that utilise non-proprietary or non-vendor unique, key Application Programming Interfaces (API). As part of its open system management plan, the Contractor, will be required, at a minimum, to describe how the proposed system architecture meets these goals, including the steps taken to use non-proprietary or non-vendor unique COTS or reusable NDI components wherever practicable.*
>
> *(b) The Contractor shall specify how it plans to use MOSA to enable the system to adapt to evolving requirements and threats; accelerate transition from science and technology into technology and deployment; facilitate systems reconfiguration and integration; reduce the development cycle time and total life cycle cost; maintain continued access to cutting edge technologies and products from multiple suppliers; and mitigate the risks associated with technology obsolescence, being locked into proprietary or vendor-unique technology, and reliance on a single source of supply over the life of the system.*
>
> *(c) In designing the system(s), the Contractor shall use the following standards in descending order of importance:*
>
> - *Standards as specified within this contract*
> - *Commercial standards*
>   - *Standards developed by international or national industry standard bodies that have been widely adopted by industry.*
>   - *Standards adopted by industry consensus-based standards bodies and widely adopted in the market place.*
>   - *De facto standards*[4]*.*
>
> *Note: Standards that are not specified within this contract or that are modified by adding must be submitted and approved by the government project manager prior to use.*

[4] See Appendix D for definition.

The MOSA recognises that vendors are more likely to adopt an open systems strategy for their systems when modular open systems attributes are embedded in operational requirements. The following paragraphs are examples of requirements specified by the MOSA [5]:

> *The Offeror shall use a modular open systems approach to evaluate the appropriateness of implementing a modular design strategy for building systems. A primary consideration in selection of equipment to meet the design functionality shall be the impact to the overall modular open systems architecture. A modular open systems approach and analysis of long term supportability, interoperability, and growth for future modifications shall be major factors in the Offeror's final selection of equipment and integration approach. All the systems components shall facilitate future upgrades and permit incremental technology insertion to allow for incorporation of additional or higher performance elements with minimal impact on the existing systems.*
>
> *The architectural approach shall provide a viable technology insertion methodology and refresh strategy that supports application of a modular open systems approach and is responsive to changes driven by mission requirements and new technologies.*
>
> *The Offeror's modular design and integration shall preclude long term dependence on closed or proprietary interface standards, technologies, products, or architectures. Secure or classified data systems shall also conform to the modular design approach as much as practical. The design shall provide sufficient growth and open interface standards to allow future reconfiguration and addition of new capabilities without large-scale redesign of the system.*

Proper V&V of open systems requires indicators to assess the level of openness a system has achieved. The following is an example, from the MOSA, of indicators to judge the implementation of key interfaces and open standards [5]:

Key Interface Indicators

- *Proactive management of system interfaces.*
- *Identification of key system interfaces based on module characteristics (e.g. criticality of function, ease of integration, change frequency, etc.).*
- *Appropriate designation of open standards for key system interfaces.*

Open Standards Indicators

- *Feasibility studies to assess the use of open standards for key interfaces.*
- *Application of a standards selection process that gives preference to open standards.*
- *Standards selection for key interfaces is based on application of specific criteria (e.g., DoD mandate, industry consensus, market support, prime contractor recommendation, etc.).*

These examples, and many others in the referenced documents, provide an indication of the language to use to develop an open systems approach to meet the business and technical aims of an acquisition program.

Appendix B: Open Systems Sources

B.1 GVA (Generic Vehicle Architecture)

The GVA, from the UK MoD, specifies a set of mandatory standards for the common interfaces of a system. Application of the GVA is mandatory for all future land platform procurements by Defence in the UK[5] [1]. All information on the GVA has been taken from Defence Standard 23-09 [1].

The GVA is an approach undertaken by industry and the MoD to ensure the proper physical, electrical and electronic integration of sub-systems on land platforms. It intends to allow required sub-system interoperability, whilst allowing innovative solutions to be proposed by vendors. According to Def Stan 23-09, the GVA should be used in conjunction with a Systems Requirements Document (SRD) for a platform. The use of Def Stan 23-09 should be mandated in the SRD for platform acquisitions, upgrades or refreshes. Note that the GVA does not mandate a specific design, but it emphasises the need to use open standards for key interfaces.

B.2 KOSS (Key Open Sub-Systems)

The KOSS tool, from NAVAIR in the US, is used to identify the key interfaces of a system, for which open standards should be applied. The KOSS tool was developed to comply with the third MOSA principle: designate key interfaces, see Section 3.4. It supports Program Managers to identify volatile sub-systems and components that benefit most from open systems consideration in terms of lifecycle affordability. All information on the KOSS tool has been taken from a presentation given by NAVAIR in 2009 [11].

The inputs required for the KOSS tool are derived from the system requirements and SME and sponsor or warfighter knowledge. The inputs are:

- A major component set, including hardware, software, middleware and operating systems;
- Capability roadmaps, highlighting components expected to add capability to the system in the future;
- Qualitative obsolescence measures within the roadmapped period;
- Estimates for the relative cost of change of system components; and
- The relative capability improvement offered by components.

The process followed by the KOSS tool is discussed in Section 3.4, and is summarised below:

1. Conduct System Decomposition.
2. Develop Capability Roadmap.
3. Determine Rate of Obsolescence.
4. Calculate Relative Rate of Change. Calculated from 2 and 3.
5. Determine Cost of Change.

[5] See Def Stan 23-09, Section 0.2 – Application of the Standard.

6. Calculate Open System Applicability. Calculated from 4 and 5.
7. Determine System Capability Improvement.
8. Calculate Warfighting Return On Investment (ROI) of an Open System. Calculated from 6 and 7.

The components that have the highest open system applicability are those with the highest rate and cost of change, and the components with the highest warfighting ROI are those that are most open system applicable and offer the greatest capability improvement. The open system applicability and the ROI of an open system to the warfighter are used to designate the key interfaces of a system.

B.3 MOSA (Modular Open Systems Approach)

The MOSA, established by the US DoD, is an approach for the acquisition or upgrade of open systems. It is a means to assess and implement widely supported commercial interface standards in developing systems using modular design concepts. Section 3 describes a general process derived from the MOSA. It incorporates the five key MOSA principles [5]:

- Establish an enabling environment.
- Employ modular design.
- Designate key interfaces.
- Use open standards.
- Certify conformance.

These principles are incorporated into the process for implementing a MOSA, which, at a minimum, should incorporate the following tasks [5]:

- Identify and analyse MOSA enabled capabilities and strategies.
- Assess the feasibility of open systems design solutions.
- Establish metrics to assess MOSA implementation progress.
- Use MOSA principles to develop an open architecture.
- Identify and resolve MOSA implementation issues and report the unresolved issues.

Implementation of the MOSA by the US DoD aims to achieve the many benefits associated with open systems, such as the ability to adapt to evolving requirements and a reduction of total life-cycle costs, and it is dependent on continuous market research [5].

B.4 OAAT (Open Architecture Assessment Tool)

The OAAT, from the US Navy, is used to assess compliance with the MOSA, but also the technical and programmatic openness of programs. As discussed in Section 3.6, the OAAT uses a standard set of questions, addressing various business and technical indicators, to elicit the level of openness of a system. These indicators are tied to the five MOSA principles, with the key technical and business indicators (taken from [13]) summarised as follows:

Key technical indicators:

- Interoperability – The use of standardised data and functional models is essential for the exchange of information between readily separate systems.
- Services – A service is a software component described by metadata, which can be understood by a program. These metadata are published to enable re-use of the service by remote entities that require no knowledge of the service implementation beyond the published metadata.
- Maintainability – The ability to keep a system operable for a long period of time. This is facilitated by COTS components and the use of open standards.
- Extensibility – The ease with which changes can be made to the system.
- Composability – The extent to which components can be selected and assembled in various ways to meet user requirements.

Key business indicators:

- Is open systems language included in the project documentation?
- Have program personnel been trained in open systems?
- Has an individual been designated as being responsible for open system implementation?
- Is there a plan for implementing an open system with metrics defined to measure progress?
- Does the government own the controlling performance and interface specifications?

The OAAT question set is formulated around these indicators, with questions answered based on prescribed criteria on a scale from 1 to 5. The OAAT uses the answers to calculate a total score for the openness of a system. Users of the tool are encouraged to give explanations for theirs answers and provide evidence or supporting documentation.

B.5 OACE (Open Architecture Computing Environment)

The OACE, from the US Navy, is a standards-based set of computing resources designated for use in US Naval warfighting systems. The OACE Design Guidance document [6] provides guidance concerning OACE technologies and application design using these technologies. It forms one of five volumes that comprise the Open Architecture Documentation Set:

- Volume 1 – An overview of Open Architecture.
- Volume 2 – Description of Open Architecture Engineering process.
- Volume 3 – Open Architecture Functional Architecture Definition Document.
- Volume 4 – The OACE Technologies and Standards document.
- Volume 5 – OACE Design Guidance.

The OACE Technologies and Standards document accompanies the OACE Design Guidance document and outlines a set of standards and product selection criteria that apply to the OACE technology base. Generally, the families of standards invoked for the OACE include [6]:

- Telecommunications Industry Association (TIA) physical media standards
- Internet Engineering Task Force (IETF) network standards
- Portable Operating System Interface for Unix (POSIX) operating system standards
- Object Management Group (OMG) middleware standards

B.6 VICTORY (Vehicular Integration for C4ISR/EW Interoperability)

The VICTORY architecture, from the US Army, is an effort to develop and validate a set of open standards (in cooperation with industry) for the integration of C4ISR and related items of equipment on Army platforms [2]. This effort aims to reduce Size, Weight and Power (SWaP) requirements of platforms, and accommodate system modification and upgrades. Access to VICTORY documentation is currently restricted to US citizens.

B.7 VSG (Vetronics Standards and Guidelines)

The VSG is a product of the Vehicle Systems Integration program, funded by the UK MoD and conducted by QinetiQ. This document presents standards and guidelines for vetronic infrastructures for legacy and future land platforms. The standards are based on existing, industry wide, open standards, while the guidelines demonstrate examples of employment of these standards. Standards and guidelines are presented for a number of vetronic sub-areas, including Command and Control, Video, Software and Power, which can be seen in the VSG document [14].

B.8 DoD 5000.2-R

DoD 5000.2-R (Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs) [7] provides some useful guidance on business and technical indicators for V&V of open systems. According to the Regulation, these indicators should be introduced during the acquisition process. This enables acquisition of open systems to be encouraged and assessed.

To achieve acquisition of an open system, several business indicators are required [18]:

- The feasibility of using widely supported interface standards must be assessed.
- Market research should be conducted to determine industry support for interface standards.
- The order of preference for various types of interface standards (e.g. open, de facto, proprietary[6]) to be used for key interfaces should be documented.
- Priority should be given to most cost effective solution over the system life cycle.

[6] See Appendix D for definitions.

- A business case analysis should be conducted to assess the economic impacts of not using open standards for key interfaces.
- A support strategy must be formulated to address technology insertion and refreshment.

A number of technical indicators are also required [18]:

- The use of commercial or non-developmental items should be facilitated.
- Early commitment to system-specific solutions should be avoided.
- Risk associated with technology obsolescence and dependence on single source of supply should be mitigated.
- Key interfaces of the system architecture to the desired level must be identified.
- Open standards must be designated for appropriate key interfaces.
- A standards selection process must be used, which gives preference to widely supported open interface standards.
- System interfaces should be managed as part of the overall configuration management process.
- A modular standards-based architecture must be employed for the system design.

Appendix C: Standards Bodies

In analysing the open standards market, it is necessary to keep abreast of the major standards organisations from around the world. These organisations are responsible for the majority of open standards on the commercial market. For land vehicle programs that aim to achieve open vehicle systems, the most relevant standards bodies include:

- International Organisation for Standardisation (ISO)
- International Electrotechnical Commission (IEC)
- International Telecommunication Union (ITU)
- American National Standards Institute (ANSI)
- Automotive Open System Architecture (AUTOSAR)
- Institute of Electrical and Electronics Engineers (IEEE)
- Internet Engineering Task Force (IETF)
- Machinery Information Management Open Systems Alliance (MIMOSA)
- Object Management Group (OMG)
- Society of Automotive Engineers International (SAE)

The World Standards Cooperation (WSC) is an alliance of the three largest and most well-established standards organisations, ISO, IEC and ITU.

Examples of open standards defined by bodies in the above list include:

- CORBA (Common Object Request Broker Architecture) – Defined by OMG and enables software components written in multiple computer languages and running on multiple computers to work together [19].
- POSIX – Specified by IEEE and defines the Application Programming Interface, and shell and utility interfaces, for software compatible with variants of the Unix operating system [20].

Appendix D: Types of Standard

The standards used to develop an open system should be open (as defined in Section 2.3), and preference should be given to these standards over de facto, de jure or proprietary standards. The following points describe each of these other standards.

- De facto standard
    - Standards that are widely accepted and used, but lack formal approval by a recognised standards organisation [5].
    - De facto standards are often proprietary standards that have grown to become adopted as standards.
- De jure standard
    - Standards that have been declared as a standard, by a consortium or a government [21], but they may not necessarily be commonly used.
    - De jure standards are not strictly open standards, but they are often open.
- Proprietary standard
    - May be developed privately, owned by an individual or organisation, and may require a license or fee to implement [5, 21].

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION DOCUMENT CONTROL DATA	1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE Approaches to Open Technology Systems Specification	3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION) Document (U) Title (U) Abstract (U)
4. AUTHOR(S) Brendan Sims	5. CORPORATE AUTHOR DSTO Defence Science and Technology Organisation PO Box 1500 Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER DSTO-TN-1087	6b. AR NUMBER AR-015-307	6c. TYPE OF REPORT Technical Note	7. DOCUMENT DATE May 2012

8. FILE NUMBER 2011/1250523/1	9. TASK NUMBER CDG 07/357	10. TASK SPONSOR CDG	11. NO. OF PAGES 22	12. NO. OF REFERENCES 21

13. DSTO Publications Repository http://dspace.dsto.defence.gov.au/dspace/	14. RELEASE AUTHORITY Chief, Land Operations Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for Public Release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DSTO RESEARCH LIBRARY THESAURUS

Open architecture, Open systems, Standards, Validation, Verification

19. ABSTRACT

Open system considerations are important for future military systems to permit ease of integration, reconfigurability and upgrade, and to reduce the total cost of ownership of a system. This document provides guidance on the specification of open systems for acquisition.