Open system architectures for the ADF: opportunities and challenges

Dr Shane Dunn, Defence Science and Technology Group
Wing Commander Jesse Laroche, Royal Australian Air Force
Group Captain Pete Mitchell, DSC, OAM, Royal Australian Air Force

Introduction

Increasing uncertainty in our strategic environment, coupled with high rates of change of technology and the wider availability of sophisticated military technologies to state and non-state actors, have been identified as contextual trends in the *2016 Defence White Paper*.[1] The need for the ADF to adapt to these trends will pose challenges for the development, acquisition and sustainment of our military capabilities.

To manage the risks and opportunities posed by the above trends, the *2016 Defence White Paper* and the *2016 Defence Industry Policy Statement* have identified the following needs for the ADF:

- Systems with increasing operational agility, supported by technical flexibility;
- To be a smart buyer of increasingly technologically complex systems, maximising operational capability and value for money; and
- Systems with through-life agility enabled through partnership with a sustainable defence industry sector and academia.[2]

The *2016 Defence White Paper* also recognised that addressing these needs will require a highly capable Defence workforce with a more diverse range of skills. Air Force's Plan JERICHO's key themes of improving joint force integration; developing an innovative and empowered workforce; and improved acquisition and sustainment of capability are directly related to the above strategic needs.[3]

This article reports on a study carried out for Plan JERICHO which examined the potential of exploiting a design concept known as 'open system architectures'. An overview of the principles of open system architectures is presented, describing the effects of degrees of modularity and openness of an architecture. Some examples are then identified where these concepts are being exploited in military systems,

principally by the US Department of Defense. The article concludes by exploring some of the opportunities and challenges that might present if the ADF were to more widely exploit such system architectures.

Open system architectures

Open system architectures have been proposed by defence-related acquisition agencies (principally the US Department of Defense) for many years as offering potential for timely, agile and improved capabilities that are less expensive to acquire and maintain. There are many definitions for open system architectures. An ideal for Defence's purposes would be a model that enables hardware and/or software modules to be competitively sourced and integrated by a range of developers of Defence's choosing without being constrained by intellectual property considerations.

Practicalities typically compromise this ideal, with competing considerations arising from issues such as security, intellectual property, performance, safety, etc. These considerations will be evident in the system design through trade-offs in the degree of modularisation and the level of openness of the interfaces between modules.

The implementation of open system architecture concepts has been policy in the US Department of Defense for over 20 years, and more recently in the UK Ministry of Defence.[4] Strategic guidance for its application in the US Department of Defense can be found in the 'Better Buying Power' initiatives that describe the need for improved value for money in acquisition and for systems that can be adapted quickly to address new threats and technology developments.[5] In underpinning the development of a competitive buying environment, Better Buying Power 'emphasize[s] competition strategies [that] create and maintain competitive environments … [and] enforce open system architectures and effectively manage data rights'.

> While Australia does not mandate the use of open system architectures, needs expressed in the *2016 Defence White Paper* can be directly related to opportunities offered through the use of these design concepts.

Modular architectures

Open system architectures arise at the intersection of modular architectures and open standards. The design of a system from the perspective of how its various sub-systems are interconnected is described in its system architecture. A high-level definition for a system's architecture is:

> The fundamental organisation of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution.[6]

Hence, the architectural design of a system is key to addressing force needs by defining the system's development process, complexity, evolvability and its relationship and interoperability with its environment and other systems.

A well-architected modular system manages complexity by creating modules, in hardware and software, such that the capability delivered by these modules can be developed, maintained and upgraded with minimal risk to the technical performance of other modules in the system. The level of impact one module has on another defines how tightly coupled that module is.

Modules that are loosely coupled and able to deliver a scalable and/or extendable system that can be upgraded or have modules added with minimal testing is desirable for system flexibility.[7] Older, monolithic systems did not partition or modularise the design, such that interdependencies between systems were not clear and any change could present a significant risk through accidental influences on unrelated sub-systems that could only be mitigated through extensive testing.[8]

How modules are defined within a system will be decided through trade-offs, considering the range of competing technical and business requirements and related constraints inherent in any complex design process. The modularity of a system can conceptually sit on a continuum that ranges from every part/line of code being able to be changed without recourse to regression testing to a purely monolithic system where no change can be made without full system regression testing.

Technical constraints constraining the degree of modularity may include compromises to size, weight and power considerations, meaning that systems with tighter constraints on these issues can expect a higher cost from increasing modularity.[9] A business factor leading to constraints could be from intellectual property considerations or that management of too many interfaces may be prohibitively expensive relative to the expected gain.[10]

Open standards

Fundamentally, an 'open standard' provides sufficient information for physical and data interfaces to enable a module to be modified without recourse to an original vendor or other intellectual property restrictions. The following is a definition for an open-standard that has been synthesised from a range of definitions available in the literature:

> 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.[11]

Given the range of requirements in the above definition, and that many of the requirements are inherently subjective, it is not surprising that the practical application of such definitions has been described as being 'hazy at best', and that openness of a system is best considered as being 'not black and white but rather a matter of degree'.[12] The result is that the degree of openness of a standard sits on a continuum depending on the degree to which it meets each of the criteria in the above definition.

Modularity and open standards present opportunities to achieve the White Paper goals of increasing system agility through partnership with Australian defence industry, as well as helping to manage complexity and deliver improved value for money. A key to achieving Defence's aims from the application of open system architectures will be managing the spectrum of modularity and openness of the interface standards to ensure the required level of access to best meet the ADF's strategic needs.

The range of open system architectures

There are numerous open system architecture concepts that have been designed for use in different domains and for different intended applications. For example, a 2014 RAND report outlined nine open architecture concepts in various stages of development for uninhabited systems across air, land and maritime domains and with varying mission roles.[13] Based on the range of technical drivers, and given the different performance targets of the various concepts, the report concluded that the US Department of Defence should not attempt to develop a single architecture model for its uninhabited systems.

Indeed, for example in two large-scale projects, the US Navy and US Army are collaborating in the development of the 'Future Airborne Capability Environment', and the US Air Force is developing 'Open Mission Systems', with each using quite different architectural models, which are largely incompatible, despite being designed to meet similar goals.[14]

To ensure that the design and maintenance of an open system architecture remains manageable, rather than trying to be all-encompassing, each should be designed to meet the operational requirements of the environment in which it will operate. In addition, its design—with its architectural topology, identification of key interfaces, the standards used and their degree of openness—needs to consider the business and technical drivers and consequent cost-benefit trade-offs in the overall system design.

These trade-offs need to be assessed through broad stakeholder engagement, providing traceable, defensible decisions supported by a rigorous assessment process. This will also be required for system maintenance and development.[15]

Opportunities provided by open system architectures

A design based around modularity helps to mitigate risks arising from uncertainties about future requirements by enabling a system to be brought into service without meeting all its envisaged requirements. With an extensible

architecture, modules can be developed and added with relative ease after a capability has entered service, facilitating an evolutionary spiral acquisition process. Operators can bring their experience with the use of the system to the design and test process to help ensure that subsequent iterations deliver real operational improvements.[16]

Beyond design, development and acquisition, open system architectures enable improved obsolescence management through the life of a capability. Not being tied to an original equipment manufacturer (either the prime system integrator or module developers) for through-life support should enable competitively sourced alternatives for maintenance and upgrades, will provide Defence with choice in how systems are evolved, and will offer potential for greater innovation through competition.

Rapid development of technologies is a growing driver of obsolescence risk. Such obsolescence may simply present as missed opportunities for performance improvement through to sustainment challenges arising from diminishing manufacturing sources and material shortages where parts can become prohibitively costly or unobtainable. These obsolescence issues have been particularly evident in electronic hardware, driven by the rapid development of microprocessors, and are increasingly being seen in software.

These risks can be exacerbated by increasing use of commercial-off-the-shelf components, particularly given reducing commercial product life-cycles.[17] For example, the US Navy found that during the development process of a surface ship sonar system, from 1996 through to its first installation in 2002, over 70 per cent of the off-the-shelf parts became 'out of production (un-procurable)' before the first system had been installed.[18]

With capabilities being increasingly delivered through software functionality, open system architecture principles address some of these obsolescence risks by providing 'wrappers' that enable software to be easily hosted on a range of hardware platforms. In this way, hardware and software upgrades can be applied independently.[19]

An exemplar application of this is the US Navy's 'Acoustic – Rapid COTS [commercial off-the-shelf] Insertion' program. This program implements what the US Defense Science Board has called an 'incremental, iterative acquisition process' employing a continual spiral development approach that has shortened the technology insertion cycle for these types of systems from 12 years to two for software, and four years for hardware.[20] This process has helped US Navy anti-submarine warfare capabilities address increasingly quiet adversary submarines by exploiting up-to-date hardware and software developments that are competitively sourced and able to be continually improved through operator feedback.

As of 2011, this program had been in progress for more than 15 years and has been considered a great success from cost, performance and timeliness perspectives. Similar processes for processor and software upgrades are now being implemented for the US Navy's 'AN/BYG-1 Submarine Combat Control System' and for the Aegis combat mission system.[21]

Hardware and software module re-use across defence systems offers additional opportunities for the application of open system architecture principles across the ADF. There are many examples where sub-system components and algorithms fulfil similar or identical requirements across platforms and domains: a few generic examples are sensors and sensor pods; data processing/data fusion; communication system hardware and software; and human-machine interfaces.

A specific example of such re-use has been the development of an open architecture track manager in collaboration between General Dynamics and Lockheed Martin for the US Navy for its Aegis combat system and for the 'Ship Self Defense System' used on its large deck ships.[22] This development has led to a single system track manager and track server being used on both combat system types.

Such re-use of modules across the ADF, and with coalition partners, offers considerable potential for improved efficiencies in joint force capability management, as well as potential training benefits through increased commonality of functions and human machine interfaces. It would also enable smoother transition for personnel working across multiple systems.

Mission modularity occurs where systems are designed to operate with hardware and/or software modules that are easily swapped in and out for tailoring to specific mission requirements (for example, an operator may be able to choose between a range of intelligence, surveillance and reconnaissance sensors, communications packages and/or electronic warfare systems). Such modularity is a typical design feature in new unmanned aerial systems, emphasising the multi-role utility of many of these systems.[23]

Modular systems have the potential for improved force-level integration through the application of open system architecture principles by enabling sensors and communications systems to be adaptable to mission requirements. However, the benefits are typically focused on individual combat systems, and broad interoperability requires a joint system-of-systems architecture that goes beyond what is typically considered in open system architecture designs.[24]

Implications of open system architecture-enabled systems for the ADF

Many of the platforms and associated systems the ADF acquires are sourced from other nations. While Australian applications will be similar to those of the host nation, it is to be expected that Australia will have other requirements for these military capabilities, which may also include a greater number of roles than the system's original design purpose.

Carrying out indigenous modifications to military systems for Australian-specific requirements without original manufacturer support has proven to be challenging and expensive, particularly due to a lack of Australian knowledge base and intellectual property restrictions. Modularity can be expected to assist in providing a greater degree of multi-role applications through improved ability to tailor a system for specific missions, while the application of an open system architecture should enable module development by Australian industry tailored to Australian needs.

With a growing impetus towards the use of open system architectures in military capabilities, systems acquired from other nations will potentially offer increasing degrees of access to parts of the system for Australian-developed modifications. To get the required access, Australia will need to influence the development of projects to ensure sufficient access to the interface specifications required to exploit opportunities for Australian-sourced hardware and software modules.

By way of example, using the AIR 7000 maritime patrol aircraft replacement program, the P-8 Poseidon aircraft is expected to have elements of its mission system modularised with open interfaces by increment three of its development, while the Triton unmanned aircraft system is to have open system hardware and software modularity, enabling the integration of payloads without affecting the rest of the system.[25] However, it should be noted that these architectures are designed for the benefit of US operators and it is not yet clear if the ADF will have sufficient access to exploit these concepts. The F-35 joint strike fighter is also reported to have some level of open system architecture-enabled modularity such that the Israeli Air Force is reported to be able to add its own command, control, communications and computing system.[26]

Provided these systems are being architected to enable modular upgrades, they should not require full system regression testing to demonstrate that there are no safety implications or other significant performance risks.[27] The Collins submarine combat mission system is an example where Defence has access to system interfaces to enable Australian-developed modules/applications for improved functions, such as tracking algorithms and human-machine interface, to be submitted to the certifying authority (US Navy in this case) for inclusion in the next block upgrade.[28] This process has proven to be very successful with regards to addressing Australian requirements and enabling Australian innovation.

The 'Evolutionary Layered ISR [intelligence, surveillance reconnaissance] Integration eXemplar ARchitecture' (ELIIXAR), developed by Australia's Defence Science and Technology Group, is an exemplar enterprise architecture, comprising hardware and software built using open-systems principles designed to enable integration across diverse systems/sub-systems.[29] ELIIXAR

is currently being trialled within Army. However, being an Internet protocol-based enterprise architecture, ELIIXAR is not a real-time system, meaning it is not a suitable backbone for real-time, tightly integrated systems.

The 'Layered Approach to Service Architectures for a Global Network Environment' (LASAGNE) is a distributed embedded open system architecture framework, also developed by Defence Science and Technology Group, that spans real-time tactical to enterprise environments and can support real-time integration requirements.[30] In addition to being open system architecture frameworks for Australian designed systems, models such as ELIIXAR and LASAGNE offer potential as Defence-managed middleware that can be built on to foreign-sourced systems that may come with their own open system architectures.

Use of such indigenous architectures involve additional system overheads and Defence would then have the responsibility of maintaining that interface. However, the potential benefit in having an Australian outward-facing open system architecture to provide a more controlled interface for Australian industry may outweigh the cost implications.

Key requirements for the success of the Australian programs that have exploited open system architecture principles have been high-fidelity test beds for the development and testing of upgrades. These test beds have fully representative operator interfaces enabling direct involvement by operators in setting the requirements and performing evaluations of these proposed modifications for operational utility.

Communication systems are an area of rapidly improving technology in the civilian world but are relatively slow to progress in military systems due to considerations related to security, robustness and interoperability. An aim of open system architecture-enabled systems is to provide greater flexibility in hardware and software for communications, delivering improved integration and interoperability.[31]

Facilitation of interoperability across joint and coalition forces is expected with the growing application of open system architectures across the three Services. Chief of Army has asserted that Army's future vehicle fleets, including Land 400, should exploit common vehicle architectures and integration standards, and that effective partnership with industry will be enabled through more federated and open C4I [command, control, communications, computers and intelligence] architectures. Chief of Army also contended that:

> Open hardware and software architectures, shared integrations and more modular systems will be central to the manner in which our Army will train and fight as a digitised, joint force into the future.[32]

The application of open system architectures in Defence systems can be expected to have a strategic impact through supporting the White Paper goals to develop and maintain an indigenous, technologically advanced defence industry capability. Through enabling the more direct involvement of Australian industry in the development of modules for Defence systems, industry can expect greater export opportunities and Australia will have a workforce that is better prepared to respond to Defence's needs.[33] The prospects offered by increasing commonality and system flexibility across the Services should also facilitate joint force integration and interoperability.

Challenges arising from the implementation of open system architectures on ADF systems

Open system architectures promise better delivery and maintainability of Defence capabilities, and have been promising this for many years, noting that their use in systems acquired by the US Department of Defense has been mandated in various forms since 1994. Certainly, there have been many hurdles to the implementation of open system architectures—and the promise is still a long way from being realised.

The US Government Accountability Office has described two key challenges as being culture and investment in the defence acquisition community, and a lack of adaptation by industry to an open system architecture model that enables competition—noting that the development of a suitable model for compensating industry for its

intellectual property to enable the ideal application of open system architecture principles is an ongoing challenge.[34]

A case study from the commercial sector is the development of the IBM personal computer, which employed an open system architecture to develop a system based on widely available components and standards. These principles enabled third-party developers to create additional hardware and software accessories that contributed to systems based on this architecture gaining the dominant personal computer market share.[35]

The IBM personal computer is also an example of the challenges that can be faced by original manufacturers in embracing open system architecture principles. IBM's design became the market leader but, because of the openness of its standards and with no licensing constraints on its component suppliers, IBM lost control of its design, enabling compatible machines to take the dominant market share. Defence will have to be cognisant of the concerns of original manufacturers that similar outcomes could potentially threaten their business models.

The patchy and relatively slow progress with the US Department of Defense's implementation of open system architectures is instructive for Australia's application of these concepts. A report by the US Government Accountability Office on the use of open system architectures in unmanned aircraft systems across the Army, Navy and Air Force highlighted that the US Navy is the only Service prioritising its use, albeit in three of its four unmanned aircraft system programs.[36] None of the three Army and three Air Force programs examined in the report included open system architectures at the design stage.

Increased upfront costs can be expected with the design of a well architected system, with the payoff coming with reduced through-life management costs and improved system flexibility. However, project managers' incentives are typically more directly related to minimising acquisition costs, leading to 'brittle or unscaleable architectures that significantly increase life-cycle costs'.[37]

Also, the US Air Force and US Army have not had the expertise required to assess and manage a system employing an open system architecture. A key factor in the US Navy's uptake of these concepts has been a cultural willingness in its acquisition community to embrace the concepts, underpinned by a cadre of personnel skilled in the application of open system architectures. It was noted by the Government Accountability Office that stronger leadership is required across the US Department of Defense to enforce the application of open system architectures, and that this must be resourced by the organisation, including the provision of skilled personnel to support it.[38]

The trend of increasingly long in-service life of military systems has resulted in long times between new acquisitions. In this context, industry seems supportive of a model that enables continuous technology insertion as a means to maintain industry capability between large programs. Supporting continuous improvement, however, does not necessarily translate to supporting the concept of open competition. This has led to a range of proprietary modular architectures for which the complete interface definitions will not be fully disclosed, and original manufacturer support for integration will be required.[39]

In this way, the original manufacturer reaps the integration efficiency benefits of a modular architecture without having to submit to open competition. This could be considered a partial win for Defence, as it should reduce schedule and cost risks in upgrade programs, although the other benefits of a truly open system, such as widely sourcing innovative concepts and Defence-wide module re-use would not be realised.

Exploiting the opportunities offered by open system architectures for the ADF

There will be some military systems for which Defence will have ultimate design and certification authority. However, some other systems will be acquired, and likely maintained, in partnership with a foreign agency. For these systems, Defence may be able to influence the architecture and standards to ensure they meet Australian requirements through partnership in the development process. Where Defence does not have influence in the development process, modern systems will likely come with some

degree of modular design that may be exploited if the appropriate access rights can be negotiated.

Given this range of acquisition models, Defence will need the ability to work with a wide range of open system architecture concepts to exploit the opportunities that will enable Australian-sourced innovation and agile system development. For foreign-sourced systems, it is to be expected that a foreign agency will be the system integrator with final certification authority. In these cases, there is the risk that Australian integration requirements may not have high priority, leading to slower than anticipated introduction into service.

A risk to accessing the requisite rights to these open system architectures for foreign-sourced systems and components is that they may be subject to export restrictions, such as those that may arise from the *International Traffic in Arms Regulations*, which may limit Defence's ability to engage with Australian industry. Ensuring opportunities for Australian industry to develop innovative modifications involving systems subject to such restrictions will require careful management by Defence.

If the ADF requires a truly agile capability for modular development of its capabilities that is not constrained by foreign defence and industry priorities, an Australian-controlled organisation, infrastructure and personnel base will be required to enable design and test through to certified integration. The degree of testing required to mitigate integration risks would be dictated largely by the system architecture relating to the component being modified, particularly with regards to any safety risks that may arise. To enable indigenous integration, the ADF would also need a robust certification process, enabled by flexible developmental, acceptance and operational test and evaluation processes for open system architecture-enabled new modules or upgrades.

An aspect in defining where module boundaries lie will be the anticipated rate of change of technologies that deliver that function. Technology and capability road-mapping (or forecasting) is an important requirement when designing and maintaining defence capabilities that utilise modular architectures.[40] Such road-mapping will look at future capability requirements framed around potential future threats and opportunities that future technologies may provide.

If a functional role is anticipated to be subject to rapid technological development, then that function should be encapsulated by key interfaces enabling ease of upgrade of such technologically volatile components of the system. At the architecture design phase, this would help prioritise where the boundaries for these key interfaces should be. The openness of the standards employed at these interfaces defines the degree to which these modules can be competitively replaced or upgraded.

Reasons for interfaces not being open may include that the overhead associated with enforcing and maintaining an open interface is too high compared to having a proprietary, or no, standard; conformance to a standard may unacceptably decrease system performance; or there may be security concerns raised through conforming to a particular standard.[41]

For all systems where the ADF is reliant on open system architectures for a capability's through-life management, Defence will need access to the expertise required to ensure that the system architecture and the nature of 'openness' of the interfaces is appropriate and that the standards for these interfaces are maintained through the life of the capability.

It is important to note that there needs to be confidence and resourcing to ensure that standards will be maintained and keep pace with technology developments. Standards enable innovation by having a broad range of developers compete for the design of new components.[42] However, being consensus-based and typically having broad application, standards are not inherently agile and, if too constraining or not adequately maintained, may actually stifle innovation.

Defence will need the capability to assess an open system's attributes, influence the development of standards, and manage the risks that may arise from adopted standards not being maintained within useful timeframes. As noted earlier, the road-mapping of technology and capability needs is a requirement that Defence will have to instigate with the explicit aim of planning for and prioritising module-based upgrade opportunities. This capability will also ensure

that interface standards anticipate rather than lag Defence's requirements.

The US Air Force's 'Mission Systems Open Architecture Science & Technology' program has a requirement that the 'open architecture solutions accommodate "built-in" cybersecurity features'.[43] There is, however, the risk that the implementation of open system architectures in military systems could enable vectors for cyber threats, which will need careful management.[44]

One of the proposed benefits of open system architectures in Defence is that they will enable the leveraging of rapid technological development in the civilian sector for use in military systems leading to potential greater use of off-the-shelf components.[45] Software and hardware in such components will be an attractive target for potential adversaries that will be very challenging to avoid.[46]

Considering the security of the interface standards, it has been claimed that an open system architecture based on completely open specifications would be more secure than a proprietary, or otherwise closed, interface because there is effective crowd-sourcing to mitigate the risk of vulnerabilities.[47] The security considerations of open interface standards are related to the issues of security within the open-source software community, where it is still an open question as to how much reliance can be placed on open-sourcing to improve security and how the overall risks around these issues will be managed.[48]

Open system architecture concepts offer the potential to reduce the training burden because of increased commonality of sub-systems across capabilities. However, the pace and nature of system change must be managed to ensure that training does not fall behind upgrades and that force integration issues are considered. If the pace of change is too high, training will not be able to keep up.

A significant potential benefit from the application of open system architectures arises from portability and re-usability of modules, particularly software modules across different systems. This benefit will be best realised across the joint force and will require the development and maintenance of a repository of modules that are available for use across projects.

Broader considerations of a whole-of-mission system arise when considering integrated operations involving other joint and coalition systems. Regression testing of upgrades by systems integrators is currently largely considered at the platform level, and not at the broader system-of-systems level. An overall 'system architect' role will be required to manage risks at the wider system-of-systems level, which would obviously require a high level of understanding of what and how different platforms contribute to a mission.[49]

Where the aspects of the overall mission package are loosely integrated, modular change in one platform should present little risk to the mission package performance. If the mission is dependent on aspects of the overall system requiring tight integration between platforms, then regression testing of modifications will need to consider these larger systemic risks, noting the challenges to test and evaluation that arise when validating systems of systems.[50]

Conclusion

A growing aspect of the capability management of Defence systems will involve exploiting the opportunities offered by open system architectures while managing the risks that this will pose. The main opportunities will be increased system flexibility through modularity; improved ability to keep pace with threats and technological developments; and strategic benefit through increased Australian defence industry capabilities in design and integration of hardware and software modules for Defence. These opportunities contribute to addressing Australia's strategic requirements as articulated in the *2016 Defence White Paper* and *2016 Defence Industry Policy Statement.*

Enabling the successful exploitation of open system architectures by Defence underscores the identified need for a Defence workforce with the requisite skills to manage new technologies with greater agility. Defence will need access to a workforce with the technical and business skills to negotiate system architectures that meet Australia's strategic requirements around delivering operational capability, value for money, and offering opportunities for Australian innovation while also supporting the needs of original

manufacturers for a viable business model. To help achieve these outcomes, Defence needs to learn from US and UK defence projects that have successfully implemented these principles.

Capability managers will need assurance that the risks and opportunities offered by open system architecture-enabled systems are appropriately managed. This will require an acquisition culture and skills base to develop appropriate requirements for Defence and to support projects through their acquisition phase to ensure these requirements are met. These skills could reside within Defence or be sourced from industry, and the development and maintenance of this skills base could be shareable across the whole of Defence. Sharing this resource will assist with ensuring the consideration of mission and force level integration and interoperability.

The benefits of open system architectures will be best realised in an environment where operators and developers can work closely to realise systemic improvements that are grounded in operational needs. Exploiting the opportunities through the life of a capability will place responsibilities on capability managers for providing this development environment, as well as the need for appropriate test and evaluation infrastructure, organisation and personnel to manage the risks of development and/or integration of modular upgrades. This can evolve as different systems become available, with the scale to be matched to the level of complexity or risk that the capability manager is willing to accept.

Dr Shane Dunn completed his Bachelor's degree in Aeronautical Engineering from the Royal Melbourne Institute of Technology in 1986 and was awarded a PhD from the University of Melbourne in 1992. Shane has over 30 years' experience in Defence Science and Technology Group in air platforms and systems, and air power-related research. He is currently the Science Team Lead for Air Power Future Concepts in the Joint and Operations Analysis Division.

Wing Commander Jesse Laroche completed his Bachelor's degree in Science at the Australian Defence Force Academy in 1996 and completed a Master of Military Operational Art and Science in 2015 and a Master of Philosophy in Military Strategy in 2016 at the US Air Force's Air University. Jesse has served in numerous positions throughout his 24 years in the Royal Australian Air Force, primarily as a pilot flying both air lift and maritime patrol aircraft. He is currently posted to Air Force Headquarters, closely involved in the implementation of Plan JERICHO.

Group Captain Pete Mitchell joined the Royal Australian Air Force in 1993 and graduated as a pilot in 1995 before qualifying on the F/A-18A and serving with No. 75 and No. 77 Squadrons. He served on exchange with the US Marine Corps, again flying F/A-18A aircraft before his command tours with Forward Air Control Development Unit, Joint Electronic Warfare Operational Support Unit and No. 75 Squadron. He has deployed to the Middle East twice, in 2003 and again in 2015. He is currently the Director of Plan JERICHO in Air Force Headquarters.

Acknowledgements

The authors would like to gratefully acknowledge the assistance and support of the following during the study that led to this paper: Air Commodore Andrew Campbell and Air Commodore Robert Chipman for initiating the study and helping to guide it through its early stages; subject-matter experts from the Maritime Electronic Warfare Systems Program Office, and Aerospace, Maritime, Land, Joint Operations and Analysis and Cyber and Electronic Warfare Divisions of the Defence Science and Technology Group.

The time and assistance offered by the LASAGNE and ELIIXAR development teams of Weapons and Combat Systems and National Security and ISR Divisions respectively was of particular value. It is the insights developed through practical experience from the subject-matter experts from all of the above areas that has been key to shaping this paper.

Notes

1 Department of Defence, *2016 Defence White Paper*, Commonwealth of Australia: Canberra, 2016.

2 Department of Defence, *2016 Defence Industry Policy Statement*, Commonwealth of Australia: Canberra, 2016, available at <http://www.defence.gov.au/WhitePaper/Docs/2016-Defence-Industry-Policy-Statement.pdf> accessed 23 January 2018.

3 Royal Australian Air Force, 'Plan JERICHO', *Air Force* [website], available at <https://www.airforce.gov.au/our-mission/plan-jericho> accessed 23 January 2018.

4 Under Secretary of Defense for Acquisition, Technology and Logistics, 'Memo amplifying DoDD 5000.1: guidance regarding modular open systems approach implementation', *Office of the Assistant Secretary of Defense for Logistics & Materiel Readiness* [website], available at <http://www.acq.osd.mil/log//mpp/ats_

opensystems.html> accessed 23 January 2018; also UK Ministry of Defence, *Defence Standard 23-09 - generic vehicle architecture*, UK Ministry of Defence: London, 2010.

5 N. Guertin and T. Hurt, *DoD Open Systems Architecture Contract Guidebook for Program Managers: a tool for effective competition*, Defense Acquisition University: Fort Belvoir, September-October 2013.

6 International Organization for Standardization (ISO), 'Systems and software engineering – architecture description', *ISO* [website], 2011, available at <http://www.iso-architecture.org/ieee-1471/defining-architecture.html> accessed 23 January 2018.

7 MITRE Corporation, *Systems engineering guide – collected wisdom from MITRE's systems engineering experts*, MITRE Corporation, Bedford, 2014.

8 For example, integrating a new camera on the Northrop Grumman Triton unmanned aircraft system required 'as much as 66 per cent' less software regression testing than would have been required for an architecture that was not modularised: US Government Accountability Office, 'Defense acquisitions – DoD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly', *US Government Accountability Office* [website], July 2013, available at <https://www.gao.gov/products/GAO-13-651> accessed 23 January 2018.

9 Katja Hölttä, Eun Suk Suh and Olivier de Weck, 'Tradeoff between modularity and performance for engineered systems and products', *CiteSeer*^{x} [website], abstract available at <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.116.4138> accessed 23 January 2018.

10 D. Firesmith, 'Open system architectures: when and where to be closed', *Software Engineering Institute* [blog], available at <https://insights.sei.cmu.edu/sei_blog/2015/10/opensystemarchitecturewhenandwheretobeclosed> accessed 23 January 2018.

11 B. Sims, 'Approaches to open technology systems specification', *Defence Science and Technology Organisation* [website], May 2012, available at <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DSTO-TN-1087%20PR.pdf> accessed 23 January 2018.

12 R. Black and M. Fletcher, 'Open systems architecture - both boon and bane', *Academia* [website], 2006, available at <http://www.academia.edu/20896448/Open_systems_architecture_-_Both_boon_and_bane> accessed 23 January 2018; also Firesmith, 'Open system architectures'.

13 D. Gonzales and S. Harting, *Designing unmanned systems with greater autonomy: using a federated, partially open systems architecture approach*, RAND Corporation: Santa Monica, 2014.

14 J. Cernezia, 'Introduction to The Open Group and the FACE™ Consortium', *The Open Group* [website], 4 August 2015, available at <https://www.opengroup.us/face/documents/17354/SOSA_FACE_Overview_Industry_Day_2.pptx> accessed 23 January 2018; US Air Force Research Laboratory, 'Mission systems open architecture science & technology (MOAST)', unpublished paper by Avionics Vulnerability Mitigation Branch, Sensors Directorate, Air Force Research Laboratory, 12 Aug 2015; and J.L. Tokar, 'A comparison of avionics open system architectures', *Sigada* [website], January 2017, available at <http://sigada.org/conf/hilt2016/paper-Tokar.pdf> accessed 23 January 2018.

15 See, for example, J. Tyree and A. Akerman, 'Architecture decisions: demystifying architecture, *IEEE Software*, March/April 2005, pp. 19-27, available at <https://www.utdallas.edu/~chung/SA/zz-Impreso-architecture_decisions-tyree-05.pdf> accessed 23 January 2018.

16 MITRE Corporation, 'Systems engineering guide'.

17 US Department of Defense, *Diminishing manufacturing sources and material shortages – a guidebook of best practices for implementing a robust DMSMS Management Program*, Defense Standardization Program Office, US Department of Defense: Washington DC, August 2012.

18 P. Singh and P. Sandborn, 'Obsolescence-driven design refresh planning for sustainment-dominated systems', *The Engineering Economist*, Vol. 51, No. 2, April-June 2006, pp. 115-39.

19 The concept of 'wrappers' is embodied in the open system architectures-related software development concept known as 'service oriented architectures'.

20 Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, *Report of the Defense Science Board 2010 Summer Study on Enhancing Adaptability of US military forces – Part A. Main Report*, Department of Defense: Washington DC, January 2011.

21 US Department of Defense, 'AN/BYG-1 Combat Control System' (under 'Navy Programs in FY 2012'), in *Director of Operational Test and Evaluation (DOT&E) Annual Report*, US Department of Defense: Washington DC, December 2012; P. DeLuca *et al.*, *Assessing Aegis Program transition to an open-architecture model*, RAND Corporation: Santa Monica, 2013.

22 G. Fein, 'Navy developing path forward for open architecture implementation', *Defense Daily*, 21 August 2008.

23 For example, the US Navy's small tactical unmanned aerial system program anticipates having at least 32 different payloads from 24 different manufacturers: US Government Accountability Office, 'Defense acquisitions – DoD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly'; and Gonzales and Harting, *Designing unmanned systems with greater autonomy.*

24 S. Sommerer *et al*., 'Systems-of-systems engineering in air and missile defense', *Johns Hopkins APL Technical Digest*, Vol. 31, No. 1, 2012.

25 US Government Accountability Office, 'Defense acquisitions – DoD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly'.

26 E. Tegler, 'Israel's F-35 app and its implications', *Aviation Week & Space Technology*, 22 April 2016.

27 An important consideration of open system architecture implementations is that systems should be loosely coupled as much as possible and tightly integrated only where required: MITRE Corporation, 'Systems engineering guide'.

28 See <https://www.dst.defence.gov.au/projects/collins-class-submarine-replacement-combat-system>

29 See <https://www.dst.defence.gov.au/projects/

evolutionary-layered-isr-integration-exemplar-architecture-eliixar>

30 Defence and Science Technology Group (DST), 'Layered Approach to Service Architectures for a Global Network Environment (LASAGNE)', *DST* [website], available at <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DSC%201753%20Avalon%20Air%20Show%20LASGNE%20.pdf> accessed 23 January 2018.

31 Sims, 'Approaches to open technology systems specification'.

32 Lieutenant General Angus Campbell, 'Chief of Army address to the Defence Magazine Conference', *Army* [website], 9 February 2016, available at <https://www.army.gov.au/our-work/speeches-and-transcripts/chief-of-army-address-to-the-defence-magazine-conference> accessed 23 January 2018.

33 From a UK perspective, one of the key aims of adopting open system architectures is the opportunity for improved local science and technology involvement in Ministry of Defence systems development and the strategic and export opportunities this creates: UK Ministry of Defence, *National security through technology: technology, equipment, and support for UK defence and security*, Ministry of Defence: London, February 2012.

34 US Government Accountability Office, *Defense acquisitions: review of private industry and Department of Defense open systems experiences*, US Government Accountability Office: Washington DC, 26 June 2014; and S.I. Erwin, 'DoD clashes with suppliers over data rights', *National Defense*, January 2014.

35 H.W. Chesbrough and D.J. Teece, 'When is virtual virtuous? Organizing for innovation", *Harvard Business Review*, January-February 1996.

36 US Government Accountability Office, 'Defense acquisitions – DoD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly'. 'Fire Scout' is the only US Navy unmanned aircraft system program considered that did not consider this.

37 J. Doyle, *B2PCOE Open Systems Architecture – Final Report*, ACI Technologies Inc.: Philadelphia, 2011; also B. Boehm, *Tradespace and affordability – Phase 1*, Systems Engineering Research Center, Stevens Institute of Technology, Hoboken, 9 July 2013.

38 US Government Accountability Office, 'Defense acquisitions – DoD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly'.

39 National Research Council, *Responding to capability surprise: a strategy for US naval forces*, The National Academy Press: Washington DC, 2013; Doyle, *B2PCOE Open Systems Architecture – Final Report*.

40 Sims, 'Approaches to open technology systems specification'.

41 Firesmith, 'Open system architectures'.

42 R. H. Allen and R.D. Sriram, 'The role of standards in innovation', *Technological Forecasting and Social Change*, Issue 64, 2000, pp. 171-80.

43 US Air Force Research Laboratory, 'Mission systems open architecture science & technology'.

44 US Air Force, 'Global horizons, final report', *Homeland Security Digital Library* [website], 21 June 2013, available at <https://www.hsdl.org/?abstract&did=741377> accessed 23 January 2018; C. Sledge and D.C. Schmidt, 'A discussion on open-systems architecture', *Software Engineering Institute* [blog], 23 November 2015, available at <https://insights.sei.cmu.edu/sei_blog/2015/11/a-discussion-on-open-systems-architecture.html> accessed 23 January 2018; B. Meyer, '4 best practices for open software ecosystems', *Software Engineering Institute* [blog], 17 November 2015, available at <https://insights.sei.cmu.edu/sei_blog/2015/11/osa-4-best-practices-for-open-software-ecosystems.html> accessed 23 January 2018.

45 Leveraging off-the-shelf developments is an explicit aspect of some military open system architecture programs, particularly with regards to processor upgrades: see, for example, M. Boudreau, *Acoustic rapid COTS insertion: a case study in spiral development*, Naval Postgraduate School: Monterey, 30 October 2006.

46 Defence Science and Technology Group, *Future cyber security landscape – a perspective on the future*, Cyber and Electronic Warfare Division, Defence Science and Technology Organisation, May 2014, available at <https://www.dst.defence.gov.au/publication/future-cyber-security-landscape-perspective-future> accessed 23 January 2018.

47 Sledge and Schmidt, 'A discussion on open-systems architecture'.

48 G. Schryen, 'Is open source security a myth?', *Communications of the ACM*, Vol. 54, No. 5, May 2011, pp. 130-9.

49 N.H. Guertin, R. Sweeney and D. Schmidt, *How the Navy is using open systems architecture to revolutionize capability acquisition*, Naval Postgraduate School: Monterey, May 2015.

50 J.D. Dahmann, K.J. Baldwin and G. Rebovich, 'System of systems and net-centric enterprise system', *MITRE* [website], 2009, available at <https://www.mitre.org/publications/technical-papers/systems-of-systems-and-netcentric-enterprise-systems> accessed 23 January 2018.