ATKINS

Member of the SNC-Lavalin Group

The Future of Open Systems in Defence Procurement

About us

SNC-Lavalin's Atkins business is one of the world's most respected design, engineering and project management consultancies. Together, SNC-Lavalin, a global fully integrated professional services and project management company, and Atkins help our clients plan, design and enable major capital projects, and provide expert consultancy that covers the full lifecycle of projects.

Working across the entire Defence lifecycle we work with our clients to help them maximise the value of their investment in vital infrastructure and equipment, offering expert advice and support and cutting edge digital solutions. We are proud to have worked for over three decades with the UK MOD on some of the most critical systems and infrastructure projects, covering the maritime, land, air and cyber domains.

Introduction

Open standards are becoming the norm. Instead of designing systems that are heavily regulated by the controller of the hardware or software, businesses are choosing to make their platforms open for their supply chain to access, to understand and to propose upgrades. The benefits to this method are clear. It leads to easier integration, speedier upgrades, improved flexibility and – crucially – long-term value for money. But how do organisations decide how open their platforms should be?

For the Defence sector, adopting open standards is no longer just a preference; it has become a central driver in system design.

This paper considers:

- The various aspects of openness and the benefits offered
- Its growing application to Defence
- Thoughts on strategic decisions, both technically and commercially.

The nature of openness

The concept of 'openness' emerged in the 1980s and generally refers to hardware, software or interfaces where components and protocols conform to standards independent of a particular supplier. A familiar everyday example is the mobile phone operating systems, although levels of openness vary between Google's Android and Apple's iOS.

Openness allows systems to be flexible and adaptable, facilitating ease of growth and evolution – often rapidly, in contrast to closed systems with a rigid design that can be harder to change. This property arises from the fundamental system design that employs architecture to layer and disaggregate the system so that certain parts can be interchanged and upgraded with relative ease.

Security is a vital aspect that might seem intuitively at odds with openness. Whilst opening up software can introduce vulnerabilities, with careful design it is possible to overcome this problem through architectures that balance open and closed aspects. System partitioning – both for security and commercial purposes – is one such approach, as is being 'open at the interface'; for example, the USB adapter is an interface standard that uses agreed hardware and software protocols to enable different devices to communicate on a 'plug and play' basis.

Openness manifests in various properties, such as modularity, interoperability, standardisation, adaptability and validity. Traditional system design has often focussed on one or two of these properties but a more holistic 'open architecture' approach can bring to bear many more of these qualities to give a range of benefits to the taxpayer and warfighter. For example, improved validation of software can occur with 'open source' software, where software code is made publicly available. This allows others access to use and upgrade it with few restrictions, offering public benefit and, for the owner of the original software, a route to wider adoption and growth.

The benefits of openness

Openness offers a range of benefits, including:

- Easier integration – through delayered architectures, modularity and standard interfaces
- Rapid upgrades, exploiting the ease of integration through 'spiral' development - bringing a speed advantage in 'time to market' (or the battlefield!)
- Better opportunities for innovation – through opening up parts of future system development to a broad range of suppliers
- Improved adaptability and flexibility, allowing reconfiguration to different roles – whether via rapid short-term flexibility for smaller changes or through longer term evolution as circumstances change
- Inter-operability – through co-operation with other assets, again facilitated by common architectures and hardware/software interfaces
- And crucially, better long-term value for money through increased competition to drive down cost, and through better and more flexible performance.

The exact nature and mix of benefits in any one situation depends on the system in question and the strategy and degree of openness adopted, which creates challenges for system designers to consider early in the lifecycle.

Applications in Defence

So how can Defence define and access these benefits across the full range of capabilities and future procurements?

In fact, UK MOD has made a very good start, through various projects over many years, culminating in April 2018 with the introduction of a mandatory Open Architecture Key User Requirement (KUR) for all future equipment purchases, to ensure that consideration be given at the outset of an acquisition. The requirement was kept purposefully broad to ensure its applicability across all defence domains.

Commercial Openness

For UK Defence, while architecture may be open technically, the MOD is often subject to 'vendor lock-in' which limits the commercial freedoms to publish and compete for upgrades to the architecture. Solving this could mean designing commercial openness into a system from the outset to create 'freedom of action' for future upgrade bids, across all levels of the supply chain. So Prime and Tier 1 level suppliers could change, while the MOD still retains control of the underlying architecture. It may not cost more to design a system to be open, but MOD participation costs may be higher as it must influence the design approach at the outset and potentially buy Intellectual Property to retain control. Whilst the upfront cost may be greater, an open system would result in significant cost savings over the life of the system, through reduced integration costs and competition. Trade-off studies balancing affordability drivers with long term payback may be needed.

Deciding just how open a system should be is imperative not just for finding the right degree of technical openness, but also from a commercial perspective to ensure the system can be managed, upgraded and maintained efficiently and affordably. So, how easy is it to determine how open a system should be?

For many completely new systems, being technically open has become the norm. However, where there are portfolio transition issues and perhaps legacy commercial lock-in, the argument for openness requires significantly more consideration.

Portfolio transition

As the British Army has developed new armoured vehicles, open architectures have been adopted. However, to achieve capability level benefits and through life cost savings, there is an aspiration to back fit openness to elements of the legacy fleet. To this end, a detailed analysis of options was undertaken to measure the range of through-life benefits to the fleet against the upfront investment required and taking into account the likely downstream cost savings. This was greatly supported by the UK Land sector's long-standing Land Open Systems Architecture (LOSA)[1] initiative; a detailed, evolving set of Generic Architecture Defence Standards created by working closely with industry.

[1] Defence Standard 23-09, 23-12 & 23-13 (MOD, 2019)

Legacy commercial lock-in

A further example is with Land tactical communications, where it was recognised that the original legacy system (Bowman) had limited capability with little interoperability and was difficult to upgrade because of the inflexible software development model and Intellectual Property 'lock in'. And so project MORPHEUS was conceived, which has adopted an 'Evolve to Open' approach, employing a strategic phased transition from the current closed system towards a more open approach. MOD in partnership with Industry is intending to eliminate vendor lock-in with a modular system strategy, as part of an open system architecture approach, thereby enabling evolutionary capability development using a wider equipment supplier base.

Three challenges for Defence

Against this promising start, particularly in the Land domain, and the new Key User Requirement – what further must UK MOD do to realise the full potential of openness?

Strategy and setting the dial – how much is enough?

The mandatory KUR poses a question that requires due consideration, and an answer in the form of a strategy for both technical and commercial openness.

Setting the optimal strategy at the outset requires not only selecting the right nature and degree of openness to be adopted, but also setting the correct role for MOD in relation to the over-arching architecture. Whilst there are many technical considerations, the biggest decision may relate to the acquisition strategy in terms of the degree of technical involvement and risk that MOD would wish to take on. A further factor may be the need to acquire rights to Intellectual Property upfront so that MOD can retain long term control and hence choices; doing so would be investing for better performance and lower cost over the life of the system, through the opportunity of competition.

Defence policy is to be 'international by design'[2] and international collaboration is increasingly common, driven by the need both to inter-operate across nations with different systems as part of coalitions, and as a means to share development costs and pool markets to lower unit costs. Here too openness plays a part, facilitating different countries and suppliers both to inter-operate and to collaborate in acquisition. The approach to the UK Future Combat Air System Team, Tempest, reflects this, as does the Type 26 frigate with its recent Australian and Canadian success. As we have seen, this can be more problematic where new systems are being added to existing fleets or transforming a capability with legacy vendor lock-in (as in the case of Land Armoured Vehicles or MORPHEUS respectively).

Outside of Defence there have been efforts to quantify levels of integration using a sliding scale of semantic, syntactic and pragmatic indicators to clarify and thus differentiate interfaces, interactions and overall compatibility[3]. This thinking has again been applied with some success within an open architecture context, however, this now needs to be expanded to fully include the other factors that support/enable openness particularly in a commercial context.

Whilst there are many views on the definitions, language and taxonomy of openness, there are no single universally accepted standards by which to categorise and measure it. NASA developed Technology Readiness Levels in the 1970s as a standard index to measure technology maturity, and the concept has since been extended to integration, manufacturing and system readiness levels. Perhaps the time has come to apply this approach here too in the form 'Openness Readiness Levels', comprising a set of metrics to capture the various dimensions of openness, including the split between technical and commercial factors.

[2] Strategic Defence and Security Review 2015
[3] Integration Readiness Levels (Gove, Sauser, and Ramirez-Marquez, 2007)

The new paradigm – owning the Architecture and MOD as a 'Quasi-Prime'

In the last 30 years, UK MOD has deliberately moved from its erstwhile role as Design Authority, transferring this to industry as part of an aspiration to transfer delivery risk to Prime Contractors. This ended badly in some cases for a variety of reasons, including the de facto abdication of the need for MOD's involvement in key decisions, resulting in well-publicised cost escalations and delays.

Recently, we have seen a more engaged MOD giving careful consideration to its exact fit, for example with submarines, where the MOD now retains Design Authority (DA), playing a role alongside industry, as set out in 'Design Management Arrangements'.

Furthermore, the issue of openness is also driving the MOD back towards the centre stage as a DA, or indeed a 'Quasi-Prime', where the MOD assumes a leading role in shaping and owning architecture and the associated IP and the ability to effect and sustain this role. This places the MOD in control of the capability through life, as per the aspiration with MORPHEUS and also MODnet Evolve.

This leads to the important question of whether the MOD can perform this role. Is there sufficient guidance to support the implications of the KUR, and the skills and experience to bring this to fruition?

Guidance and skills

Creating the KUR is a big step forwards, requiring capability planners and procurement staff to comprehensively consider the approach to openness at the early stages of a new acquisition.

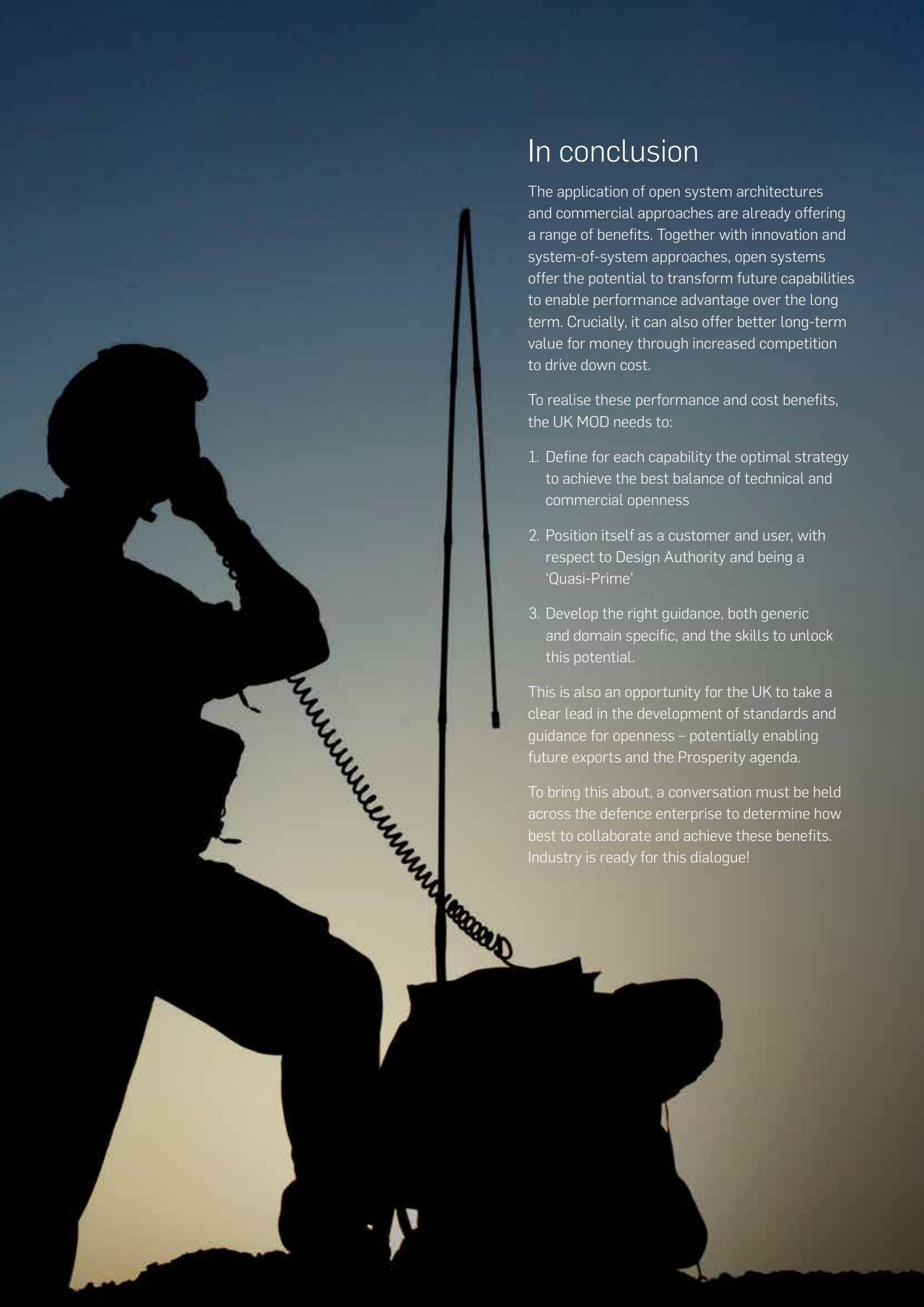
Whilst MOD's overall aspiration to repossess the role of Design Authority and act as a 'Quasi-Prime' is laudable, this will take time and inevitably require assistance and partnerships with key OEMs and support chain specialists, and trusted third parties to achieve.

Looking at the successes enjoyed by the Land sector thanks to its hands-on approach to openness, it is vital that all domains have access to authoritative guidance. The Land sector has LOSA with its associated Vehicle, Solider and Base Generic Architectures, but where are the Air and Maritime equivalents? And is specific guidance on the new Key User Requirement needed?

Clearly, a balance needs to be struck between standard broad guidance for all sectors and a more tailored guidance bespoke to each. Outside Defence, the Generic Open Architecture Framework[4] was developed by the SAE to be used to classify airborne avionics systems. However, it was realised that other domains would benefit from this open approach. Regardless of domain, the evolution of common ground via shared open standard(s) is fundamental. It is encouraging, therefore, to note that the Defence Industrial Policy[5] commits MOD "…to promote the use of open systems… building on successes such as the Land Open Systems Architecture." A further consideration is to avoid making standards too prescriptive, thereby limiting design space and innovation; so a careful balance needs to be struck.

However the Defence sector chooses to upgrade its existing guidance, collaboration must play a central role. Industry input was a key consideration when creating LOSA and played a central role in its success. Now, we must bring together the thoughts and expertise from across the Defence enterprise to more clearly define openness for the other domains.

[4] Generic Open Architecture (GOA) Framework family AIR5314 (SAE International, 2011)
[5] Industry for Defence and a Prosperous Britain: Refreshing Defence Industrial Policy (MOD, 2017)



In conclusion

The application of open system architectures and commercial approaches are already offering a range of benefits. Together with innovation and system-of-system approaches, open systems offer the potential to transform future capabilities to enable performance advantage over the long term. Crucially, it can also offer better long-term value for money through increased competition to drive down cost.

To realise these performance and cost benefits, the UK MOD needs to:

1. Define for each capability the optimal strategy to achieve the best balance of technical and commercial openness
2. Position itself as a customer and user, with respect to Design Authority and being a 'Quasi-Prime'
3. Develop the right guidance, both generic and domain specific, and the skills to unlock this potential.

This is also an opportunity for the UK to take a clear lead in the development of standards and guidance for openness – potentially enabling future exports and the Prosperity agenda.

To bring this about, a conversation must be held across the defence enterprise to determine how best to collaborate and achieve these benefits. Industry is ready for this dialogue!

About the author

ATKINS
Member of the SNC-Lavalin Gr

David Clark
Aerospace & Defence Market Director

With over 30 years' experience in leadership roles in Defence and Security, David has spent his career at the forefront of innovation. He spent 12 years with the Defence Science and Technology Laboratory, where he pioneered new technologies and enjoyed success delivering user-centric design and agile procurement – before they became buzzwords.

Joining Atkins in 2002, when innovation was becoming an integral part of business models, service delivery and value engineering, David saw himself involved in major programme delivery, operational management and latterly, business leadership. He is passionate about diversity, agility and value as the drivers of innovation, and ultimately of business success.

A graduate of the Universities of Bath and Nottingham, David is a Chartered Engineer as well as a Fellow of the Institute of Engineering and Technology (IET) and the Royal Institute of Navigation.