Realising

System of Systems Interoperability

ABSTRACT

The transformation of the Singapore Armed Forces into a fully networked force operating with network-centric system of systems (SoS) capability is a strategic imperative for the Third Generation Singapore Armed Forces. Such SoS capability depends critically on interoperable systems. Any shortfalls in interoperability between the system elements may degrade the performance or capabilities demanded of the whole SoS architecture.

This paper presents a working understanding of SoS interoperability and proposes a systematic approach to realise the required SoS interoperability.

Sim Kok Wah
Foo Kok Jin
Daniel Chia Kim Boon

Realising System of Systems Interoperability

INTRODUCTION

The systems that the Singapore Armed Forces (SAF) needs for its transformation into a Third Generation armed forces will be increasingly complex, versatile and intertwined. Looking at the various systems in a holistic manner using a System of Systems (SoS) approach will allow many of the non-obvious compatibility and interoperability problems to be identified at an early stage. The Integrated Air Defence network as illustrated in Figure 1 is a good example of a system of (complex) systems, comprising advanced fighter jets, early warning aircraft, either standalone or platform-mounted advanced radars and surface-air missile systems, anti-aircraft artillery and C2 networks.

With effective and coherent SoS architectures that can evolve over time, a new generation of capabilities can be built for the Third Generation SAF transformation, and these capabilities will be adaptable, flexible, sustainable, scalable, responsive and robust. It is the synergy achieved from integrating different platforms, sensors and weapons at the SoS level, guided by robust operational concepts, that will give the SAF greater potency on the battlefield (Tan, Yeoh, Pang, Sim, 2006).

The ability of the system elements to function together effectively in an SoS architecture depends on the extent of interoperability achieved between the system elements. Any shortfalls in interoperability may degrade the performance or capabilities of the whole SoS. Indeed, network-centric warfare depends critically on interoperable systems.

WHAT IS SYSTEM OF SYSTEMS INTEROPERABILITY?

Let us consider a typical soccer team as depicted in Figure 2 as an example of an SoS. The players are assumed to be of different nationalities or cultures, speak different native languages, and play with different styles. Each individual player can be considered as a system element. As such, to achieve interoperability, they must be able to adopt the same technical means of communication, such as using a common language and a common set of body signs and hand signals. Otherwise, they will not be able to play as a team.

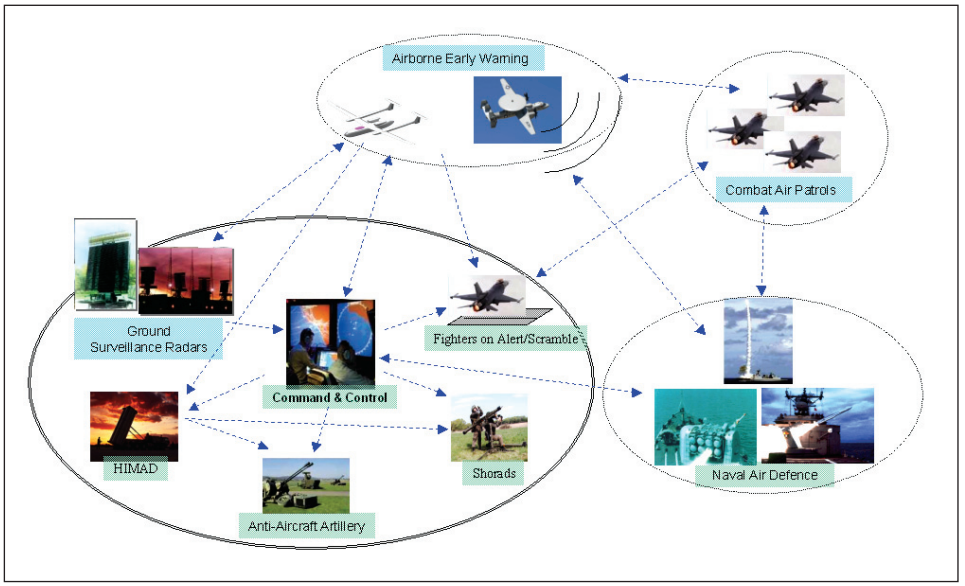

Figure 1. Integrated Air Defence network – a system of (complex) systems

Figure 2. Interoperability in a soccer team

Operational factors that drive interoperability may include the team's game strategy and tactics, operating norms and culture. The coach is akin to both the systems architect as well as the operations manager who leads his team in deriving the concept of operations that would enhance the team's effectiveness. The coach sets the operating norms within the team and influences the team's culture. This may determine the level of operational interoperability that needs to be achieved among the players. The coach and the team's captain are the SoS Integrators (SSI) who facilitate integration among team players. The technical means to achieve interoperability within the team include the use of spoken language, body language such as eye contact and hand signals, and auto-synchronisation through rehearsed moves. Training is critical to harmonising and ironing out any interoperability issues, analogous to improving the teamwork among the players. Operational validation of interoperability occurs when the team plays against other opposing teams.

In the SoS context, interoperability may be understood as the ability of the system elements to work seamlessly with one another to realise the operational capability enabled by the SoS architecture. The level of interoperability in the SoS architecture is driven by the operational interoperability or capabilities demanded of the SoS architecture, as envisaged in the SoS concept of operations (CONOPS). Operational interoperability refers to the ability of systems, units, or forces to use the services or information exchanged to operate together effectively (DACS, 2004).

Technical interoperability provides the means to realise the operational interoperability demanded of the SoS architecture. Technical interoperability refers to the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces in the SoS architecture (DACS, 2004). It addresses issues of connectivity among systems, data and file exchange, networking, and other communications related scenarios. One key attribute of technical interoperability architecture design is robustness, i.e. the ability to adapt to changing operational environments or requirements, handle new technology insertion, and manage legacy systems while incorporating new systems. One common challenge is to identify the best way to evolve the interoperability architecture for sustained and cumulative capability development in terms of ease in new capability integration. This can be done by either defining reasonable and achievable intermediate interoperability state(s) within the capability development roadmap, or by identifying basic interoperability architecture, standards and guidelines that are more enduring to changes in operational requirements and technology. The ideal state of "plug and play" may be challenging to achieve in an SoS context.

FACTORS OF INFLUENCE

There are four key factors that may influence the level of operational interoperability. They are organisation, people / processes, technology and cost.

Organisational factors such as culture, norms may influence the methods and the level of co-operation among the operators of various system elements. For example, facilitated by an integrated data link network at the SoS level, the effectiveness of the ground armoured forces may be significantly enhanced by the asymmetric anti-armour capabilities of the attack helicopters. Greater effectiveness made possible at the SoS level may mean a smaller formation size of the ground armoured forces. There is also the question of funding for the necessary efforts in SoS interoperability

architecting, implementation, testing, evaluation and certification. Strong leadership, commitment and support from the top management are necessary in arbitrating organisational differences and overcoming organisational barriers to achieve operational interoperability. However, operational security considerations such as the desire to guard against network failures or attacks may drive the need for certain system elements to function independently.

People and processes also have a bearing on the level of operational interoperability to be achieved. The stakeholders will need to reach a consensus on the party or entity that will decide on the level of interoperability required. There is also a need for consensus on how the evaluation or analytical and decision process should take place. The system elements as well as the desired level of interoperability among the elements will have to be determined during the Systems Architecting (SA) process. One major challenge lies in determining and understanding the consequences or trade-offs, particularly in a quantifiable manner, among possible options for an informed decision on the optimal levels of interoperability. The degree of buy-in from stakeholders during the SA process may determine their level of support during the implementation and exploitation of the interoperability. However, the challenge lies in identifying all the stakeholders.

Advances in technologies, in particular communication and information technologies, change the way people work together, and thus change the expectations of the users on the level of operational interoperability as well as create new ways of enhancing collaboration among operators of different systems. For example, during Operation Iraqi Freedom, an integration of data link technologies enabled precise communication and close collaboration between Joint Tactical Air Controllers operating on the ground and fighter aircraft for time-critical strikes. The interoperability of data linked systems was critical for the joint operations.

Cost is another factor that determines the level of operational interoperability to be achieved. It is influenced by the maturity of the technologies necessary to meet the operational interoperability requirements. Cost-effectiveness is a value judgement by users on whether the capability offered by the technology is worth the dollar investment. Budget availability may influence the cost appetite of the decision-makers, in terms of what is deemed to be affordable.

LEVELS OF SYSTEM OF SYSTEMS INTEROPERABILITY

One reference model of SoS interoperability is the Layers of Coalition Interoperability Framework (Tolk, 2003) as depicted in Figure 3. This model was first proposed to address interoperability challenges at the coalition level. The lower levels deal with the layers of technical interoperability, i.e. the ability to collect, manipulate, distribute, and disseminate data and information.

The physical layer (key attributes include operating frequencies, waveform, bandwidth or capacity) is an important enabler.

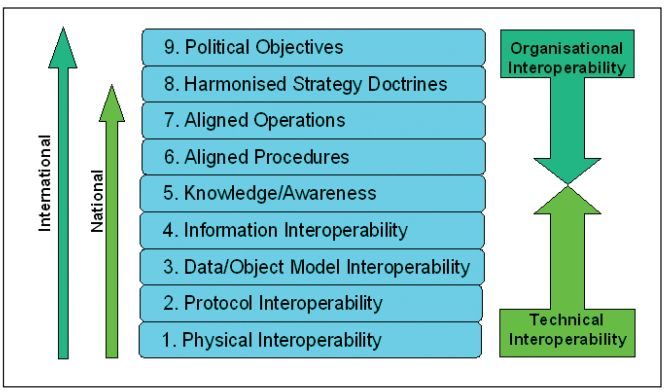

Figure 3. Layers of Coalition Interoperability Framework (Tolk, 2003)

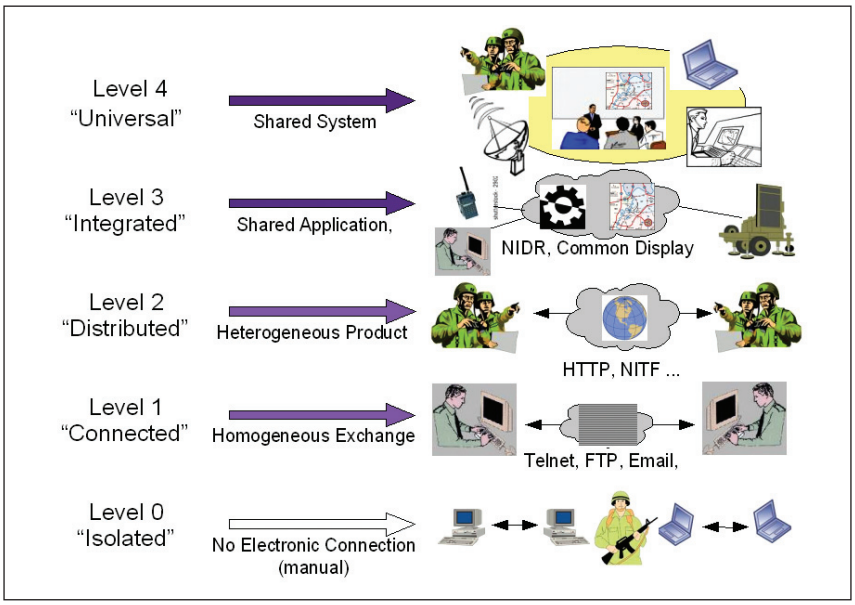

Figure 4. Levels of Information System Interoperability – LISI (Tolk, 2003)

Data / object model interoperability refers to the standardisation of data elements for data / information exchange, as well as the use of self-explaining meta data for the mapping of exchanged data elements to data elements used in the participating systems. The ability of system elements to provide the required services / data (key attributes include semantics, syntax, resolution, accuracy, update rate, format and encryption) and common references (geo-spatial, time clock, etc) will be crucial. At the information interoperability level, we should aim to harmonise the procedure and models used to represent the dynamic information in the various systems.

The knowledge / awareness level of interoperability requires the systems in an SoS to share a common understanding and awareness of the situation. The knowledge / awareness layer provides the transition from technical interoperability layers, which are supported by physical systems, to organisational interoperability layers, which deal with the harmonisation and co-ordination of related network-centric warfare operations. One may note that Layers 1 to 5 address mainly technical interoperability, Layers 6 and 7 address mainly operational interoperability, while Layers 8 and 9 may only be applicable for coalition SoS operations.

Another possible reference model is the Level of Information System Interoperability (LISI) model established by the US Department of Defense, Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). In its Framework Architecture, LISI identifies four domain categories of interoperability, namely: procedures and policies, applications, infrastructure and data (PAID). Each of these PAID domains has an impact on information exchange. In other words, the resulting technical interoperability depends on the lowest level of interoperability existing in any of the PAID domains and is measured in five categories as depicted in Figure 4. At the lowest extreme is Level 0 where the system elements are not connected at all, and information transfer takes place through the use of removable media such as thumb drives and diskettes. Level 4 is the highest level of technical interoperability, where data is electronically delivered to the military user regardless of the access method he uses, handheld devices or workstations, and the location where he uses his device. He can just plug his device into the infosphere. The US Global Information Grid is one good example of an enterprise information system that aims to achieve this technical vision.

OUTCOMES OF SYSTEM OF SYSTEMS INTEROPERABILITY

Achieving operational interoperability among the system elements means that they will be able to work together to achieve the operational capabilities demanded of the SoS architecture. The outcome of SoS operational interoperability can be broadly categorised as co-existence, co-operation or collaboration. The desired outcome applicable for each set of system elements depends on the SoS concept of operations.

In an SoS context, the system elements have to co-exist in order to operate in the same environment or locality. Co-existence is a pre-requisite for both co-operation and collaboration. There are situations where for technical or cost reasons, co-existence in an SoS architecture can only be achieved in a co-ordinated way through time-space arrangements. Such co-ordinated manoeuvres or behaviours can be considered as lower level types of co-operation. For example, during co-ordinated ground strikes, different groups of airborne shooters may co-exist in the SoS architecture by co-ordinating their manoeuvres to attack different sets of targets in the same area of operation within very short time intervals.

There are two types of co-existence, namely static co-existence and motion co-existence. Static co-existence refers to the ability of a system element to operate seamlessly with the specified physical environment in which other system elements exist or operate. Natural factors include rain, lightning, wind, humidity, temperature, salt fog, sea-state, air / water pressure and solar radiation. Other factors include ambient noise and physical access. Motion co-existence refers to the ability of a system element to operate seamlessly with other moving system elements in the specified area of operation. Factors include traffic control mechanisms such as voice communications, anti-collision devices and fratricide avoidance. For example, to operate an unmanned aerial vehicle (UAV) in civilian airspace, interoperability must be achieved between the UAV and other civilian traffic. If co-existence cannot be achieved in a cost-effective manner on a permanent basis, prior or dynamic co-ordination through time-space arrangements may be necessary and may at times post limitations on the SoS capabilities.

Co-operation can be understood as the process of each system element doing different task(s) which will, either sequentially or concurrently, contribute to a shared outcome. In many cases, work is partitioned into independent subtasks and carried out by the system elements for greater efficiency in terms of cost or time, with each system element responsible for its portion of work. Co-ordination is only required when assembling partial results. One example is co-operative engagement, where Unmanned Combat Aerial Vehicles (UCAVs) decide among themselves and execute the most efficient way of attacking a group of targets. A single UCAV, if given sufficient time, would be able to attack all the targets over a number of sorties, but it would not be as efficient and effective, especially if the targets were capable of going into hiding. Another example is co-operative sensing, where several tactical UAVs provide surveillance in different parts of an area of operation (AO), thereby providing a timely overall surveillance picture of the AO. Figure 5 shows a group of UAVs performing co-operative flights during a laboratory demonstration at the Massachusetts Institute of Technology (MIT).

Collaboration refers to the process where the system elements work together to achieve a desired outcome, with each system element being incapable of achieving it alone, even when given sufficient time. Collaboration is a co-ordinated, synchronous activity that is the result of a continued attempt to construct and maintain a shared conception of a problem, and where cognitive processes may be divided into intertwined layers (Dillenboug, 1995). A common situation awareness is often necessary for mutual engagement of system elements in a co-ordinated effort to solve the problem. The system elements typically possess

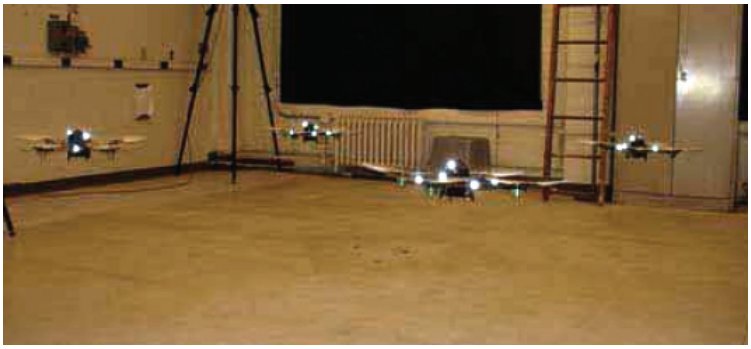

Figure 5. Laboratory demonstration of UAV co-operative flight at MIT

complementary skills or knowledge. The ability of the system elements to work closely together to achieve the desired outcome is a result of the SoS architectural design. One example is the integrated air defence architecture, where various sensor systems provide real-time surveillance and cues to the shooter systems for a comprehensive air defence umbrella. As shown in Figure 6, another example can be found in nature, where honeybees mob an invader wasp and raise their body heat until the intruder insect dies. In both examples, each system element is unable to achieve the outcome alone.

APPLICABILITY OF SYSTEM OF SYSTEMS INTEROPERABILITY OUTCOMES

The requirement for co-existence may be applicable to systems that are stand-alones by design for operational or legacy reasons, or among major sub systems in large-scale complex systems (LSCS). There is also a need for co-existence among system elements belonging to different SoS, such as the Integrated Air Defence and Maritime Security. Examples of such systems include radar sensors and ground data link terminals at high points, while examples of LSCS include F-15s equipped with radar, electronic warfare suite and weapons.

While the requirement for co-operation is more applicable within an SoS architecture, the requirement for collaboration may also be applicable among major subsystems of an LSCS. For example, collaboration is needed among different subsystem elements of an air defence weapon system on board a frigate.

The SoS CONOPS, which includes the scheme of co-operation or collaboration and the C2 structure (central versus self-synchronised, man-in-the-loop versus autonomous execution), will determine the type or minimum level of services that need to be provided, such as information (e.g. type, format, accuracy, update rate). On the other hand, technology and costs may limit the degree of co-operation or collaboration possible. Defining the technical interoperability requirements is therefore an iterative process during the SA phase, which at times may require reviews of the SoS architecture.

Figure 6. Honeybees mob an invader wasp

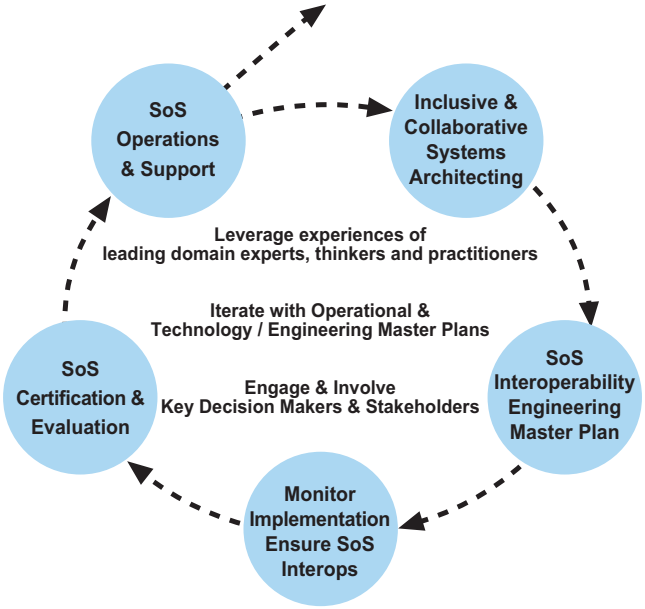

Figure 7. Realising SoS interoperability

REALISING SYSTEM OF SYSTEMS INTEROPERABILITY

Figure 7 presents a systematic approach for realising SoS interoperability, comprising the SA phase, the Engineering Masterplanning phase, the Implementation phase, the Certification and Evaluation phase and the Operations & Support phase.

1. Systems Architecting. SA is employed to visualise, conceptualise, plan, create and build a system of (complex) systems. It aims to bring various system elements together with the purpose of achieving operational capability greater than the sum of what each individual system could provide. SA can be carried out based on heuristic principles. It can also be an analytical exercise to determine the optimum combination of resources (people, organisation, equipment, weapon), systems (hardware, software, network) and their interactions to achieve the desired outcome.

SA is an art because people are an important but not necessarily predictable factor. More often than not, it is not possible to arrive at the SoS architectural solution purely through analytical or concrete mathematical derivations. Indeed, the solution is often derived through intellectual discussions and engagements with key decision-makers and stakeholders, and by leveraging holistic experiences of leading domain experts and thinkers, senior commanders, as well as other established large-scale systems engineering practitioners. It is through such an inclusive and collaborative SA process (Tan, Yeoh, Pang, Sim, 2006) that the desired robust, enduring and coherent SoS architecture will be identified. The various operational, system and technical views of the SoS architecture will enable the SoS interoperability requirements to be better and more clearly understood.

2. Engineering Masterplanning. To realise the SoS interoperability as required by the SoS architecture, it is necessary to understand the services to be exchanged among the system elements that will define the level of interoperability required. This means taking reference points from the SoS architecture. Where possible, the common or minimum interoperability requirement across the system elements should be identified to facilitate technical solutioning. Policies, conventions and standards that are useful in attaining the required levels of interoperability would be identified early. Factors such as cost-

effectiveness, supportability, security and insertion of new technologies would be considered in the interoperability solution. It is necessary to adhere to the Technology Master Plans that may have been formulated for each interoperability domain for coherent architecture as well as commonality of technical subsystems. This is to enhance interoperability and reuse so as to create systems that are interoperable from the onset. Various possible and achievable intermediate states of SoS interoperability with the respective timeframe and costs can be identified to manage the transition of existing systems into the SoS architecture.

The possible solutions could be partially evaluated through modelling and simulation experiments or analysis. Actual live experiments, where possible, should be carried out for better understanding of the issues. The impact on the SoS capability and effectiveness will need to be understood and the solution(s) refined where necessary and possible. The evaluation may also facilitate an understanding of the extent of SoS capabilities realised at each intermediate state of SoS interoperability.

The key deliverable of this phase is the SoS Engineering Master Plan (EMP), which will also address SoS interoperability. The SoS EMP will require formal endorsement and buy-in by the key stakeholders to facilitate its subsequent implementation. As the SA and EMP processes are iterative and mutually influential, it is possible that the EMP is formulated as the SoS architecture takes shape. In this case, the EMP can be endorsed together with the SoS architecture by the appropriate forums. The SoS EMP will be a document to guide SoS implementation.

The EMP should define the interoperability requirements of the SoS architecture and the intermediate stages in the implementation of SoS interoperability. It also includes possible risk mitigation measures to ensure a smooth implementation to meet SoS interoperability requirements. One example is an SoS Integration Lab that will facilitate SoS integration. Where necessary, interoperability test sets simulating classified system elements may also be identified to facilitate SoS interoperability tests as part of the factory acceptance test of relevant system elements. The EMP may present a broad approach in verifying and validating the SoS architecture upon successful implementation.

3. Implementation. Taking reference from the endorsed SoS architecture and SoS EMP, the specific operational requirements (SOR) for each system element in the SoS will need to include SoS interoperability requirements (SIRs). The required budget for meeting the SIRs will need to be catered for. Where possible, relevant aspects of the SoS architecture should be shared with the Programme / Project Managers (PMs). With a good understanding of the larger SoS picture shared in common with the armed forces' counterparts, the PMs would be better placed to achieve the desired interoperability and networking for their system elements in the SoS architecture.

An SoS Integrated Programme Management Team (IPMT) led by a Lead PM or Programme Director can be formed to spearhead the SoS implementation. Where necessary, a Programme Steering Committee may be formed. As part of the SoS IPMT, SSI may be appointed to work with PMs of different participating systems to ensure technical interoperability in specific domains. At times, additional trade-offs may be required during SoS implementation. For example, more stringent requirements may be imposed on a particular system at the Approval of Requirements stage so as to mitigate the shortfall encountered in the implementation of other capability systems. In the event that such trade-offs result in a major impact on the SoS capabilities and / or architecture, it will be necessary to review and refine the SoS architecture. Formal endorsement should be sought for such an adjustment to the SoS architecture.

For visibility, continuity and systematic implementation in the achievement of SoS-level interoperability, the PM of key capability systems may prepare a SIRs Compliance Plan

(SCP) or its equivalent. The SCP captures a common understanding of the SoS-level interoperability and networking requirements as stipulated in the SOR to assimilate the capability system into the overall SoS architecture, as well as the programme team's approach and specific measures to be implemented to meet these requirements. The SCP will also highlight any shortfalls in complying with the SoS interoperability requirements in the SoS EMP. Early identification of such shortfalls may help to trigger a timely review of the SoS capability architecture. The outcome of the review may lead to either subsequent system upgrades to close those gaps, or a conscious decision to live with those gaps or to adjust the SoS architecture as well as some of the interoperability requirements to mitigate the impact of these gaps. The SCP should be updated throughout the project life cycle.

It is possible that a new technology or capability system may become available for insertion / integration into the SoS architecture in the midst of SoS implementation. It will be necessary to understand the unique value of the new capability in the SoS context so as to refine the SoS concept of operations. As the niche role of the new capability is identified and presented in the various updated views of the SoS architecture, the Layers of Coalition Interoperability Framework as depicted in Figure 3 provides a good reference point for the identification of the SoS interoperability requirements. The SoS Architecture and EMP may need to be reviewed and updated for coherent implementation.

4. Certification and Evaluation. The PMs will need to verify and test their system's compliance with the stipulated SoS interoperability requirements and standards via the appropriate system-level conformance tests during either the Factory Acceptance or On-site Acceptance phase of the programme to achieve "Yes SIRs" status. Successful completion of the conformance tests for one system element will enhance the probability of success in achieving interoperability with other system elements that have also been successfully tested for conformance. For monitoring purposes, the SSI may define different levels of compliance (e.g. pass, marginal, fail) and the corresponding thresholds to be applied across all system elements for consistency.

The SoS interoperability test and verification approach as well as implementation plan as envisaged in the SoS EMP may need to be reviewed at each stage of implementation of the SoS architecture, given potential delays and shortfalls in the actual programmes. One typical approach is to focus on the delta interoperability requirements at each stage of implementation so as to save time and costs in the verification tests.

Prior to any operational evaluation or validation, technical SoS interoperability tests can be carried out to verify the ability of a system to exchange usable electronic information with other systems. Interoperability test sets will be required. Ideally, such tests should be carried out at the Factory Acceptance phase to save time and effort downstream. Figure 8 shows a typical matrix presentation of the results of SoS interoperability pair-wise tests among the elements in a particular interoperability domain (Kasunic, 2003). Colour codes and letter symbols are used to indicate the different levels of SoS interoperability requirements for any pair of elements and the degree of compliance as verified. The thresholds should be clearly defined prior to

	S1	S2	S3	S4	S5	---	Sn
S1							
S2	G						
S3	Y	R					
S4	Y	G	N/A				
S5	G	G	R	Y			
:	:	:	:	:	:		
Sn	G	Y	N/A	G	G		

Figure 8. Matrix presentation of SoS interoperability test results

the tests. As the scope and complexity of the pair-wise test increase with the number of systems and system life cycles, it may be necessary to focus on the critical links in a complex SoS architecture so as to make it more manageable. On the other hand, such matrix presentation may not be necessary if the interoperability requirement in a particular domain involves only two participating systems.

SoS operational tests typically require the deployment of the system elements in an operational context. Therefore, they are often carried out during operational exercises. SoS operational tests aim to evaluate the effectiveness of the SoS capabilities enabled by the SoS interoperability achieved. Modelling and simulation experiments may be performed either as a precursor to the actual operational tests or to augment the actual tests by helping to narrow the evaluation focus. There may also be situations where operational security limits the deployment of certain classified capabilities in such SoS operational tests.

Mission settings such as the environment may affect the actual interoperability performance. The SoS operational effectiveness is usually dependent on a sequence of events performed by the interoperable systems before the desired outcome is achieved. Some failures may not matter if a redundancy path exists, as illustrated in Figure 9 (Kasunic, 2003) where there are alternative paths to complete the required information flow. Failure points along a critical path will deserve priority for remedial action.

Together with the SoS IPMT, the systems architect will evaluate the outcome of the SoS interoperability and operational tests and certify the SoS architecture as having achieved a specific state of SoS interoperability. Where necessary, PMs will need to provide technical consultation on their system's design, engineering and performance so as to support the interoperability tests and operational evaluation. The outcome of these tests will serve as feedback and may trigger a review of the overall SoS architecture to address the impact of any shortfalls or to identify any further enhancements required.

5. Operations and Support. As the SoS architecture takes shape in the process of implementation and evolves over time, configuration management will be necessary for coherence. It may be necessary to form an SoS Integrated System Management Team (ISMT) to manage operations and support (O&S) at the SoS level. Besides configuration management, the ISMT will need to ensure that depot-level maintenance activities do not significantly affect the overall SoS capabilities. The ISMT will need early exposure to the SoS architecture and implementation to ensure a smooth transition to the O&S stage. One option is to have key members of the ISMT as part of the SoS IPMT during SoS implementation. The

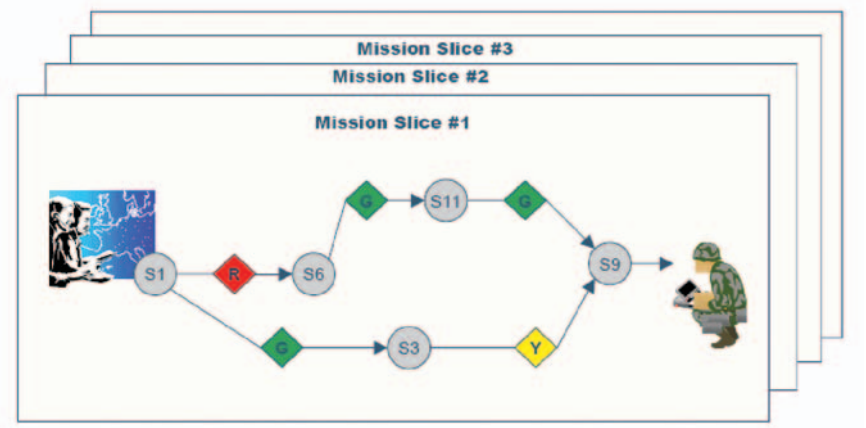

Figure 9. Information flow in an operation value chain

other option is for the SoS IPMT to continue to function as an ISMT.

Due to resource constraints or operational security reasons, it may not be possible to subject the entire SoS capability architecture to operational evaluation. A combination of operational validation as well as modelling and simulation means is more likely. It may therefore be necessary for the SoS IPMT and / or the systems architect to continue to monitor the SoS operations and identify further evaluation opportunities even after the SoS capability architecture has been certified. The continued involvement may also enable the systems architect to identify emergent behaviour and properties of the SoS that may lead to a review of the SoS architecture or an enhancement of the overall experience and learning in SoS SA.

CONCLUSION

The network-centric SoS capabilities that will give the SAF greater potency on the battlefield depend critically on fully interoperable systems. The levels of SoS interoperability required depend on the integrated network-centric warfare that may require the system elements to co-exist, co-operate or collaborate. A systematic approach is necessary to ensure success in realising the required SoS interoperability.

ACKNOWLEDGEMENTS

The authors would like to thank the following people for their guidance and sharing of experience, expertise and perspectives on the topic of SoS interoperability: Director (Systems Architecting) Tan Yang How; Director (Air Systems) Pang Chung Khiang and Director (C4I Development) Yeoh Leng Weng, who are concurrently Systems Architects; and Assistant Director (C4I Development) Teo Tiat Leng. The authors would also like to thank Engineer (Aeronautical Systems) Daniel Tan Tai Leng for his assistance in the research for this article.

REFERENCES

Carnegie Mellon Software Engineering Institute. (2004). System of Systems Interoperability Final Report.

DACS Gold Practice Document Series. (2004). Ensure Interoperability. Retrieved on 1 Apr 2007 fromhttp://www.goldpractices.com/practices/ei/index.php

Dillenboug et al. (1995). The Evolution of Research on Collaborative Learning.

Kasunic, Mark. (2003). Presentation at Software Acquisition Conference.

Tan Y. H., Yeoh L. W., Pang C. K., Sim K. W. (2006). Systems Architecting For 3G SAF Transformation, DSTA Horizon 2006, pp 36-49.

Tolk, Andreas. (2003). Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability. Old Dominion University.

US Department of Defense. (2001). DoD Dictionary of Military and Associated Terms, Joint Pub 1-02. Retrieved on 1 Apr 2007 from http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

BIOGRAPHY

Sim Kok Wah is Principal Engineer and Programme Manager (Air Systems) and concurrently Programme Manager (DSTA Masterplanning and Systems Architecting). He also holds a concurrent appointment as General Manager, Cap Vista Private Limited, which is the strategic venture investment arm of DSTA. He has extensive experience in UAV-related projects as well as modelling and simulation experiments. He was also involved in the evaluation work in the Next Fighter Replacement Programme. A recipient of the PSC – Japanese Monbusho Scholarship, he graduated from Osaka University in 1996 with a Bachelor degree in Electrical Engineering. He was the first foreigner to receive the prestigious Kusumoto Award for being the top student in his EEE department. He further graduated with MSc (MOT) and MBA degrees from the National University of Singapore (NUS) in 2000 and 2003 respectively.

Foo Kok Jin is Senior Principal Engineer and Programme Manager (Networked Systems Programme Centre), and concurrently Programme Manager (DSTA Masterplanning and Systems Architecting). He has 19 years of experience in the development of a wide range of C2I projects. A recipient of the PSC – French Government Scholarship, he graduated from Ecole Nationale Supérieure d'Electronique et de Radioélectricité de Grenoble in 1986 with a Diplome D'Ingenieur in Electronic Engineering. He further graduated with MSc (EE), MBA degrees from NUS in 1991 and 1996 respectively and with a MSc (Computer Engineering) from the University of Southern California in 1998.

Daniel Chia Kim Boon is Principal Engineer and Programme Manager (DSTA Masterplanning and Systems Architecting). He has been involved in the acquisition and R&D planning of communications and data link systems. He is currently responsible for data link system of systems architecting. He has a Master of Engineering and a Bachelor of Engineering in Electrical Engineering from NUS. He obtained a Master of Science (Electrical Engineering), specialising in communications, from the Naval Postgraduate School in 2006.