Technical and Engineering Governance in the Context of Systems of Systems

M.J.de C. Henshaw, C.E. Siemieniuch and M.A. Sinclair
Engineering Systems of Systems Research Group,
Loughborough University, Loughborough,
UNITED KINGDOM.

M.J.d.Henshaw@lboro.ac.uk

ABSTRACT

This paper concerns the implications of governance within a defence procurement enterprise. It argues that architecting of Systems of Systems (SoS) must take governance and decision making into account and that such matters should also form part of the assessment of architectures. Through consideration of the different types of SoS, it is suggested that there may be differences in applicable architecture measures between nationally operated SoS and NATO operated SoS. The paper draws parallels with the non-defence, commercial environment, which highlights the importance of the forms of contract for SoS governance and the socio-technical implications of these. Based on an assumption that open architectures are meritorious for the operation of SoS, a framework for relating openness to decision making and SoS effectiveness is suggested.

1.0 INTRODUCTION

Systems of Systems (SoS), whether in Defence or other environments, are usually developed by complex supply chain SoS , comprising single and multi-disciplinary teams, in different organisations, often globally distributed. The distributed nature of these teams, allied to the parallel design streams, and the number of different levels of hierarchy that usually exist, make it imperative to maintain good control in order to meet contractual obligations for the delivery of a SoS.

Corporate or financial governance refers to the proper running of a commercial organisation, particularly the management of risk, for the benefit of the shareholders (Cadbury 1992; Weir and Laing 2001). Its principal aim is to assure shareholders of the financial state of a company and the level of (good) control imposed over it by the board. It has become a core topic in recent years as is illustrated by the collapse of Enron and the ensuing Sarbanes-Oxley Act of 2002. In Defence, there is the Nimrod Review (Haddon-Cave 2009) which examined the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006 and its subsequent organisational implications. More recently the on-going crises in the banking world and in European economies have also illustrated failures in corporate governance.

This paper concerns the implications of governance within a defence procurement enterprise for the architectures and assessment thereof that are used to describe the systems, and systems of systems, that are acquired by a nation and subsequently become part of NATO operational systems. It will draw parallels with the non-defence, commercial environment and will indicate how considerations of governance during the life cycle of systems may influence the degree to which open architectures can be used to achieve more effective interoperability of deployed systems.

Risk is a fundamental consideration in governance and the type and nature of risk in a defence enterprise is different between different parties (i.e. different between commercial and government participants in the enterprise). In the UK and other NATO countries the use of open architectures has been viewed as an enabler for commercial, technical, and operational agility (see Henshaw *et al.*, 2011). However, the implementation of open architectures is not without risk to commercial organisations in the defence sector and the business models that support them are under-developed. This paper focuses on one aspect of the

development of such models; governance and its part in the assessment of architectures. The paper is concerned with the open architecture construct, but views this as one approach within the general architecting challenges for systems of systems.

The risk to commercial organisations may be changed (possibly increased) when the systems they provide form part of large complex SoS; the factors that influence an increased risk include:

- Businesses that have recently been consolidated. Multiple processes from different legacy organisations will continue to be operational (both formal and informal processes) for some time within the business. Even when some degree of uniformity is brought about, the people involved will operate these from legacy cultures and viewpoints. How can this situation be governed effectively?
- Businesses that are involved in collaborative projects or extended supply chains. Increasingly, large engineering contracts are being awarded to consortia of (possibly) multinational partner organisations. How should distributed engineering activities in this type of context be governed to ensure that engineering quality and requirements are met?
- Organisations that are engaged in many different projects at the same time are working at different stages in the SoS engineering lifecycle. How is it possible to govern engineers that are (concurrently) working at multiple lifecycle stages?
- Supply chains will vary in size, content and influence over the life cycle of a SoS. How can governance be maintained throughout an entire supply chain under these circumstances?

Given this context it is evident that Corporate Governance (commonly interpreted as the maintenance of financial probity and shareholder value) needs to be complemented by Technical and Engineering Governance (TEG) activities. In essence, TEG addresses the three questions, "Are we doing the right things?"; "Are we doing those things right?" and "how do we know this?" TEG is focussed on the control that is present through the network of the supply chain SoS with respect to the engineering function. This control is an important lever for the SoS 'owners and operators' who want to assure customers, stakeholders and shareholders that a delivered SoS will meet its requirements in a safe, ethical, effective and efficient manner.

2.0 TEG WITHIN A SYSTEMS OF SYSTEMS CONTEXT

SoS are composed from a finite number of constituent systems each of which is a viable system in its own right, but the interoperation of these constituent systems leads to behaviours that are not possible for each of the constituent systems acting in isolation. (Maier 1998) has suggested that a SoS will exhibit a majority of the following five characteristics:

- Operational independence of the constituent systems (i.e. that they can act as single systems and are themselves sufficiently complex to be considered systems)
- Managerial independence of the constituent systems, which means that they not only can operate independently but do so.
- Emergent behaviour, which implies the exhibition of behaviours by the SoS that cannot be achieved by the individual systems acting alone and which usually cannot be predicted by consideration of the individual systems behaviours.
- SoS develop in an evolutionary manner. Sometimes this evolution may be slow with new systems being added to legacy systems, in other cases it may be rapid when systems not necessarily designed to work together must interoperate through short-term composition.

- In general, the constituent systems of a SoS are geographically dispersed. This is usually taken to imply that the focus is on information exchange between the constituent systems.

Complementing these, (Dahmann and Baldwin 2008) have provided a typology of SoS from a control perspective;

- Directed SoS are those in which the constituent systems are subordinated to the SoS, which has a top-level management structure.
- Acknowledged SoS have recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, and development and sustainment approaches.
- Collaborative SoS have component systems that interact more or less voluntarily to fulfil agreed central purposes. The central players collectively decide how to provide or deny service, thereby providing some means of enforcing and maintaining standards.
- Virtual SoS lack a central management authority and a centrally agreed upon purpose for the system-of-systems. Large-scale behaviour emerges—and may be desirable—but this type of SoS must rely on relatively invisible mechanisms to maintain it.

It should be noted that these types of SoS are derived very much from the perspective of the acquisition community. In general, national defence SoS are Acknowledged or (possibly) Directed, whereas NATO SoS could be considered to be of a more Collaborative nature.

Given the characteristics above, some corollaries are evident, that set the context for the TEG issues discussed in the rest of this paper:

- SoS architecture and TEG is more about the interfaces between the systems, not the systems themselves.
- The dilution of the control hierarchy implies that co-operation and collaboration between organisations owning constituent systems within the SoS must be negotiated, and then maintained by some form of service level agreements (SLAs) and contracts for the entire lifecycle of the SoS. This becomes a part of the architecting process.
- Maintenance of these inter-system and inter-organisation interfaces as they develop over the lifetime of the SoS, including, for instance, the replacement of systems and their organisations, will require continuous attention at all interoperability levels. There are many frameworks describing interoperability which typically range from technical interoperability (e.g. physical, data), through semantic which concerns correct interpretation of exchanged information, to organisational and political interoperability which is concerned with alignment of processes and policy. The authors have found the NCOIC Interoperability Framework (NCOIC 2011), to be particularly helpful, especially from a Quality of Service (QoS) perspective.
- Because each organisation may have intellectual property rights (IPRs) to protect, and may have entered confidentiality agreements with other organisations, there will be limits and delays to the information flows necessary for fully-efficient operation of the SoS. This is of greater importance for those organisations that participate in several SoS, some of which might be in competition with each other.
- Each participating organisation will have its own sustainability and growth goals, which from time to time may interfere with SoS goals as each participating organisation addresses its risks and opportunities in an evolving business environment.

Consequently, the SoS is likely to exhibit emergent behaviour from time to time. Often, this occurrence of behaviour can be anticipated within a given time period, though its nature may not; this is the 'known unknowns' problem, and is most efficiently addressed by architecting for robustness. On other occasions emergence is unexpected, and there is no warning. For these instances, architecting for resilience may provide the best answer. Since there are no accepted guidelines for architecting robust and resilient SoS simultaneously, it may be prudent to predict as best as one may those parts of the SoS that are likely to be more volatile than others, and then to architect for resilience of the volatile regions and for robustness of the less volatile regions. In this respect, it may be useful to survey the approaches of (deMeyer, Loch et al. 2002) and (Henshaw 2011).

The concept of SoS lifecycle is not well defined (Kinder, et. al., 2012), but in this paper it is supposed to imply appropriate phases of SoS development and operation either in part or as a whole.

3.0 AIMS OF TECHNICAL AND ENGINEERING GOVERNANCE (TEG) IN A SOS CONTEXT

TEG should aim to control and monitor the engineering functions in a SoS in an effective way, but with the prime aim of not stifling the innovation which is necessary to retain a competitive edge. The following are an initial proposed series of objectives that an SoS TEG framework should aim to achieve:

- Manage the engineering function along the SoS lifecycle effectively and efficiently in order to meet or comply with all requirements placed upon it from the customer/stakeholders, other internal business functions (e.g. finance) and any external usage, safety or other constraints in the SoS environment.
- Comply with any associated engineering legislation that may impact on the design or operation of the SoS. An example of this would be airworthiness requirements.
- Ensure that the engineering function is flexible and adaptive to change since SoS requirements from customers/stakeholders are likely to change over the life-cycle of the SoS, dependent on need and changes in the SoS environment.
- Ensure that the engineering function is acting in support of the overall enterprise system delivering the SoS. In some enterprise systems there is a large wall between the engineering function and the rest of the business which can breed an 'us-and-them' attitude which is counter-productive for the enterprise. Therefore the engineering function should be transparent, decisions should be traceable and clear communication links and interfaces with other key functions of the enterprise system should be established.
- The engineering function should be aware that SoSE risks can have a large impact on the enterprise as a whole. Engineering should manage and control these risks so as not to impact on the rest of the business.
- Deploy 'best practice' processes in the different engineering areas and ensure that key decision making roles are clearly identified. The engineering function should ensure that the configuration of competences among its staff is optimal, and deploy those competent staff to roles in the most effective and flexible way.

We now move on to discuss some socio-technical issues relating to TEG in an SoS context

4.0 TRUST, CONTRACT NETWORKS, RESILIENCE AND ROBUSTNESS

Trust, contract networks, resilience, and robustness form an interconnected set that is of importance for architecting SoS. Trust we define for this paper as the belief that one party has about another party in its ability and reliability to deliver what it said it would deliver, in full, and within agreed constraints, usually of time and cost. Contracts, then, can be considered as formal expressions of this belief, with standing in law. What makes the other party trustworthy is its resilience and robustness to be able to keep on delivering what it promised despite the inevitable buffeting of the business environment over time. Intuitively, one would expect longer-term relationships to exhibit greater trust and hence openness between partners would lead to increased disclosure of detail and greater compatibility between component architectures within the wider enterprise architecture. Contracts usually provide a framework for interactions between organisations and should form a protective fall-back should trust be betrayed. In the non-defence environment the need for detailed contracting can be significantly reduced; for example, in the 1990s a major supermarket chain refused to sign contracts with its suppliers, and signed only a Letter of Intent. Because of the reputation of the chain, this was enough for the supplier to obtain major loans from the banks to build factories in foreign countries with no payback until there was a flow of products. Of course, the nature of contracts has a dependency on the particular industrial sector, but it is clear that different contracting arrangements can be used to drive different behaviours in any sector.

It can be argued that resilience and robustness are a function of an organisation's risk awareness and governance; competent risk analysis can provide answers to the TEG questions above that will deliver these qualities – enough strategic foresight to provide time in which to react; re-allocatable resources (essentially time, money, knowledge, technology) to address the buffeting, and the provision and use of appropriate metrics to enable proper awareness of the various situations as they develop.

Within a SoS, there may be a diverse range of contract arrangements, including both formal and informal contracts. The systems architect, working within one organisation of a multi-organisational enterprise, must address the trust issues for each participating organisation and the systems they contribute. The architect must also take into account the SoS-wide network of contracts because the behaviours they influence may interact to create negative emergent effects, particularly at times of buffeting. The available strategies to address such issues will differ between the types of SoS (directed, acknowledged, collaborative, and virtual). The level of openness and goodwill between participating organisations will significantly affect these strategies as well.

While there has been significant interest in the notion of contract networks for some time, e.g. (Hogan 1992; Johari, Mannor et al. 2006; Goldsmith 2008), the authors are not aware of any work that has explored trust, contracts, resilience and robustness in the kind of detail and in terms that can be applied to SoS enterprises that are emerging at the present time.

A practical illustration of the blend of formal and informal contracts concerns Toyota (Sheffi 2005). In 1997, the Aisin Seiki Company made P-valves for brake systems for Toyota and supplied 99% of all Toyota models. The main factory caught fire; 506 machines were destroyed. Toyota's alternate supplier making 1% was unable to ramp up production fast enough to make up the shortfall. Toyota at this time was running at 115% of normal production, as a commercial response to impending legislation.

Toyota had only a few hours' stock of valves, with trucks on the road carrying another 2 day's capacity. Aisin salvaged some tools, replaced others and was in production in 2 weeks, making 10% of their requirements, 60% after 6 weeks, and 100% after 2 months. Both Aisin and Toyota, in their respective keiretsus, asked for short-term help. A Keiretsu is a grouping of operationally independent organisations with very strong commercial relationships; it could be considered to be similar to an acknowledged SoS. 22 organisations from the Aisin keiretsu and 36 from the Toyota keiretsu replied. Within 5 days, Aisin had made available blueprints and process expertise and production had been allocated. Notably, Denso, a major

Toyota supplier, outsourced their own production to free up tools and processes to produce these P-valves (as did others), and helped to develop alternative processes for the valves using different precision tools in other smaller suppliers. Within 2 days some valves were delivered by these alternate suppliers; within 9 days of the fire, all Toyota plants were functioning as normal again.

During this period, neither financial nor legal negotiation took place, nor was pressure applied to Aisin Seiki to prioritise Toyota over other customers. However, Aisin eventually covered the direct costs - labour, equipment, materials involved - for these suppliers, and Toyota gave their Tier 1 suppliers 1% of their respective sales to Toyota for the January-March quarter as an appreciation gesture. It is important to recognise in this example that informal trust-based contracts together with a broad view of business imperative led to success where formal contracting strictly applied might have failed.

5.0 TEG AT THE INTERFACE

The activity of architecting and the available architectural forms depend on the type of SoS in question. Clearly, whatever the form, it is necessary to address issues of performance and governance and each and every interface. In fact, this is a matter of Quality of Service (QoS). Traditionally, at each interface the requirement is for delivery of an agreed output, on time, in full (OTIF), and at an agreed cost and location, for an appropriate period of time. This is usually a bi-directional activity; product in one direction, and payment in the other, accompanied by paperwork. In SoS a similar model pertains, but if there are changes in SoS strategy to meet the demands of a changing business environment, then achievement of appropriate QoS consistently will require TEG activities at all interoperability levels of the NCOIC Interoperability Framework (NCOIC, 2011); see Fig. 1.

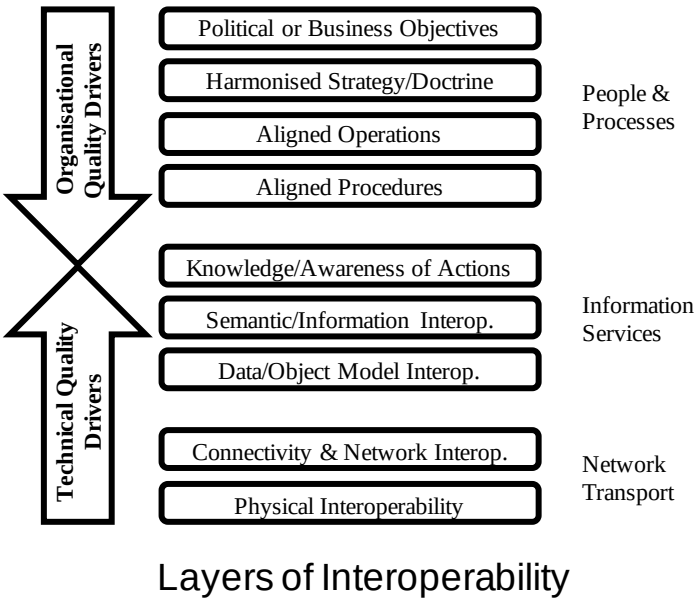

Fig. 1: The Network Centric Operations Industry Consortium (NCIOC) Interoperability Framework (NIF). The diagram shows the layers of the framework, and their function (NCOIC 2011).

For Directed and Acknowledged SoS it may be presumed that the architectural capability therein will specify the structure, protocols, and standards that will apply, though it is unlikely to specify all the NCOIC levels. For the other two types, these may have to be negotiated interface by interface. However, given managerial independence for each party to the interface (Maier 1998), whatever the type of SoS it is likely that each party will be responsible for the QoS aspects of its side of the interface. As a side issue, there may be an

added complication where two large systems providing organisations have multiple interfaces with each other, albeit for different SoS in which they jointly participate; this can lead to confused perceptions of each other and unwanted emergent behaviour from time to time that may need extra effort to maintain the status quo in QoS.

Although the architecting of the interface structures, protocols and standards may be seen as a technical issue, in general, the day-to-day operations at the interface will be socio-technical in nature, as is indicated by the uppermost levels of the NIF in Fig. 1. Consequently, the architecting of the interface interactions will also be an intra-organisational issue. Efficient and effective management to deliver the requisite QoS at the interface is not a simple matter. It requires attention to the following:

- A devolved organisational architecture that facilitates the achievement of the organisation's goals by moving decisions closer to the problems
- An architecture for the information technology and telecommunications infrastructure serving the organization, enabling decision-makers both to access timely knowledge and information and to configure the disposition of resources for current and future action
- Revised, 'current-best', business processes.
- Sound metrication for governance.
- Efficient knowledge management processes.
- The development and maintenance of a culture that supports organisational change and growth. There has been a wealth of literature written about all aspects of culture (Hofstede 1991; Hampden-Turner and Trompenaars 1994).

6.0 ENTERPRISE ASSESSMENT

An underlying assumption of the following discussion is that greater use of open architecture is beneficial to the operational effectiveness of SoS. However, the approaches to enterprise assessment suggested could be applied to other aspects of architecture improvement. Often, the organisational structure of an enterprise reflects the design of its products and/or systems, e.g. (Conway, 1968). Another way of considering this is that the structure of the enterprise may constrain the architecture of, or architecting approach to, the Systems it develops.

There are several models for enterprise assessment (e.g. Castka, et. al., 2001; Tannenbaum et. al., 1996; Curtis, et. al., 2001), but none provide measurement that explicitly identifies cause and effect between the human and organisational aspects of an organisation and its performance. It is clear, though, that success factors tend to be associated with structure of communication and decision making processes. Henshaw, et. al. (2011) recommends that an assessment of enterprise openness, as an enabler of increasing the use of open architectures in defence procurement, should focus on decision making over relevant lifecycles. The implication of Conway's Law (Conway, 1968), that the communication structure in an organisation constrains the architectural design of its products, is that open architectures will be more likely to result from organisations that are characterised by openness.

Defence systems are generally realised through the contribution of an enterprise that comprises many individual organisations. The degree of openness at the individual interfaces within such an enterprise has a direct impact on the cost of composing the capabilities that are developed over the longer term and the operational effectiveness that can be achieved. Henshaw, et. al. (2011) proposed a conceptual framework (Fig. 2) through which the (multi-organisational) enterprise can be analysed and which would inform decisions about the appropriate business models under which to procure systems for integration into existing SoS.

The underlying assumption in the model of Fig. 2 is that decision making within an enterprise is significantly affected by the degree of openness that exists. Different organisations within the enterprise provide different systems and/or sub-systems to the SoS which are provided with a broadly defined level of openness. The levels concern open architecture (whole system), open interface specification (modular systems), or completely restricted information. Notice that these definitions concern commercial constructs applied to technical information.

Fig. 2 considers three main levels of openness: the top level indicates almost complete openness across interfaces. In practice, this means that participating organisations (and possibly those currently outside the SoS in question) would have access to detailed architecture of the constituent systems. The next level represents openness at the interfaces, but not within individual constituent systems. The lowest level represents tightly closed systems in the sense that only the original equipment manufacturer has access to systems and interface architecture design. The level of openness of each participating organisation must be measured at a particular stage in the lifecycle; this can be achieved through assessing the contractually defined openness of the systems or sub-systems. It is know that such openness may change as the lifecycle of the systems progresses and the lifecycle illustrated is the CADMID cycle, well-known in UK defence acquisition. The classification for different systems/organisations should be plotted at defined times in the lifecycle; there is a subcategory for specifications available to restricted groups that measures the proportion of groups within the overall SoS. The spread of system openness provides a guide to the nature of decision making, although it is important to keep in mind that different systems may have different impacts according their role within the SoS. In some cases measurements might be real, in others they may be predicted (depending on the current lifecycle stage). It is understood (Garvin and Roberto, 2001), (Noble, 2004), (Swanson, et. al., 2004) that openness is positively associated with organisational health, such a measure, therefore, can be related to the quality of enterprise architecture for a SoS.

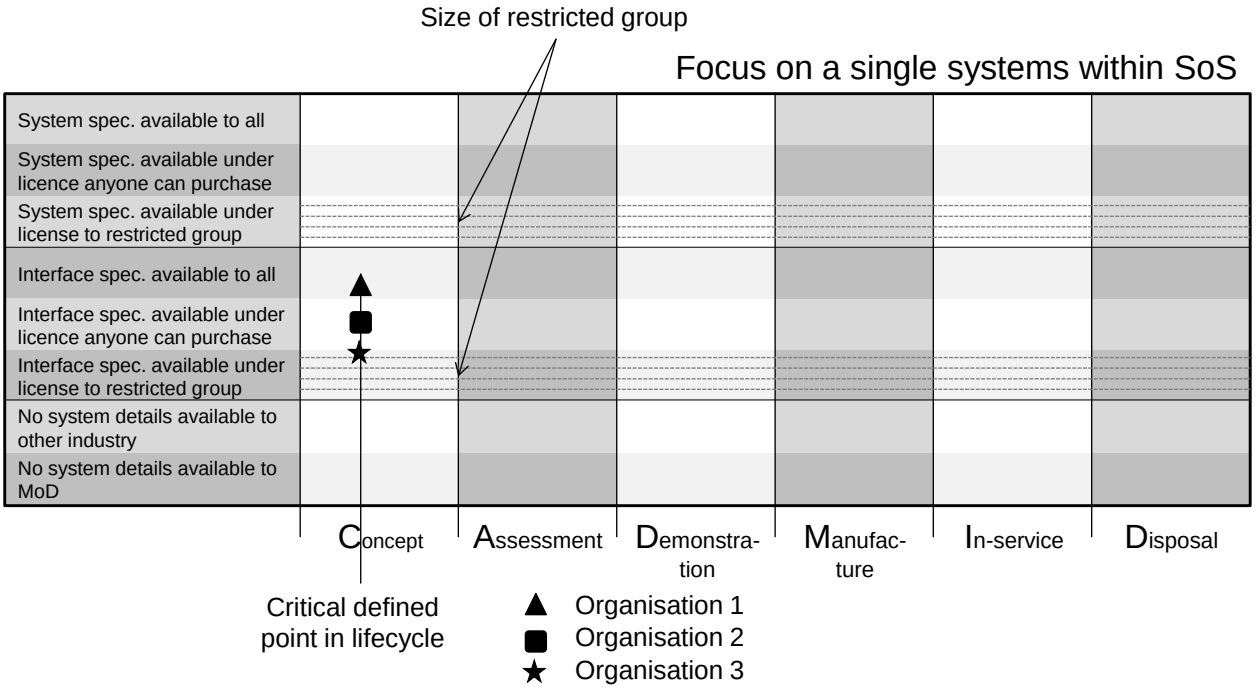

Figure 2: Approach to measuring openness of decision making in an acquisition enterprise system of systems (from Henshaw, et. al., 2011)

Such an approach would provide early warning of interoperability issues that could then be overcome through appropriate contracting and architecting.

7.0 CONCLUSION

Technical and Engineering Governance is a critical issue and in a SoS situation it can be extremely challenging to correctly define it. This paper has provided examples of SoS-related failures that were caused, at least in part, by failures in governance. A SoS can be viewed as a network of contracts (formal and informal) that determine the interactions between the constituent systems and it has been suggested that the different types of SoS (as defined by Dahmann and Baldwin, 2008) to some extent represent different arrangements of such contracts. The contracts define the nature of interoperability between systems and the governance arrangements, but it is noted that formal contracts may not fully define all the levels of interoperability; indeed ambiguities may contribute to failures. Furthermore, the contracts establish the nature of the trust relationships between systems. Taken together, this description indicates that decision making within, and by corollary performance of, a SoS is a significantly determined by the network of contracts and the TEG that they imply. From this argument, it is concluded that TEG must be considered when architecting (i.e. creating) SoS and in the analysis and assessment of architectures that describe instantiated SoS.

8.0 ACKNOWLEDGEMENTS

The contribution of the Systems of Systems Approach Community Forum Working Group 1 (Open Architectures): Sean Baker, Jeff Carter, Simon Colby, Robert Cooper, Charles Dickerson, Neville Drawbridge, Carl Evans, John Fagg, Simon Hart, Rachel Haywood-Evans, Jeremy Hobbs, David Huggett, Andrew Kinder, Mike Morua, David Pearce, Tim Rabbets, Kirsten Sinclair, John Spencer, Steve Tutt to section 6 is acknowledged.

9.0 REFERENCES

[1] Cadbury, A. (1992). The financial aspects of corporate governance, London Stock Exchange.

[2] Conway, M. E. (1968), "How do Committees Invent?" Datamation **14** (5): 28–31

[3] Dahmann, J. and K. Baldwin (2008). Understanding the Current State of US Defense Systems of Systems and the Implications for Systems Engineering. . 2nd Annual IEEE Systems Conference. Montreal.

[4] deMeyer, A., C. H. Loch, et al. (2002). "Managing project uncertainty: from variation to chaos." Sloan Management Review **43**(2): 60-67.

[5] Garvin, D. A. and M. A. Roberto (2001). "What you don't know about making decisions." Harvard Business Review **79**(8): 108-116.

[6] Goldsmith, S. (2008). Governing by network, National Governors Association Centre for Best Practices, USA.

[7] Haddon-Cave, C. (2009). The Nimrod review: An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006. London, The Stationery Office.

[8] Hampden-Turner, C. and A. Trompenaars (1994). The seven cultures of capitalism. London, Piatkus.

[9] Henshaw, M. J. C. (2011). Assessment of open architectures within defence procurement. Bristol, UK, UK Ministry of Defence.

[10] Hofstede, G. (1991). Cultures and organisations. London, McGraw-Hill.

[11] Hogan, W. W. (1992). "Contract networks for electric power transmission." Journal of Regulatory Economics **4**: 211-242.

[12] Johari, R., S. Mannor, et al. (2006). "A contract-based model for directed network formation." Games and Economic Behaviour **56**: 201-224.

[13] Kinder, A., Barot, V., Henshaw, M., and Siemieniuch, C. (2012) System of Systems: "Defining the System of Interest", ieee 7th Int. Conf. SoSE, Genova, Italy, 16-19 Jul

[14] Maier, M. W. (1998). "Architecting principles for systems-of-systems." Systems Engineering **1**(4): 267-284.

[15] NCOIC (2011). NCOIC Interoperability Framework 2.1. Washington, DC, Network Centric Operations Industry Consortium.

[16] Noble, D. (2004). Knowledge foundations of effective collaboration. 9th International Command and Control Research and Technology Symposium, Copenhagen, Denmark, US DoD.

[17] Sheffi, Y. (2005). The resilient enterprise: overcoming vulnerability for competitive advantage. Boston, MA, MIT Press.

[18] Swanson, K., J. Drury and R. Lewis (2004). A study of collaborative work practices in a joint military setting. 9th International Command and Control Research and Technology Symposium. Copenhagen, US DoD.

[19] Weir, C. and D. Laing (2001). "Governance structures, director independence and corporate performance in the UK." European Business Review **13**(2): 86-94.