A Socio-Technical Perspective on SoSE

Prof. Michael Henshaw
Loughborough University, LE11 3TU
UNITED KINGDOM

m.j.d.henshaw@lboro.ac.uk

ABSTRACT

Through some illustrative case studies, it is shown that effective development and operation of Systems of Systems (SoS) can only be achieved if the owners and operators of constituent systems can understand the effect of their decisions on the wider SoS. It is shown that appreciating the role of human beings in SoS is essential for successful operation of SoS. The role of human beings must be understood in an organisational sense to be useful in understanding SoS. A socio-technical perspective and approach is needed to manage SoS; two aspects of this, governance and situation awareness, are considered to be the most important human-related considerations for effective operation of SoS. These can be addressed by taking an open approach to information sharing in SoS.

1.0 INTRODUCTION

It is generally understood that Systems Engineering must proceed by taking account of the involvement of people in systems; however, in Systems of Systems (SoS) that involvement happens at several different levels and in different forms. In this paper, we shall consider the nature of SoS and show that the operation and engineering of such systems requires the human, or social, aspects to be a foremost consideration.

We begin with clarification of the meaning of 'socio-technical' before illustrating the issues that will be discussed through three case studies in Section 2. In Section 3 we examine the characteristics and ambiguities of SoS, from which we demonstrate the significance of a socio-technical perspective for SoS engineering. Two main themes emerge from this discussion: governance (Section 4) and situational awareness (Section 5). Some concluding remarks are given in Section 6.

1.1 The Meaning of Socio-Technical

The term, socio-technical, is used rather loosely to refer to the involvement of people in technical systems and is almost inevitably imprecise in its meaning. Klein[1] asserts that the term was first used in the context of industrial democracy, by which she meant the ability of workers to organise themselves to work within a technologically constructed system. She views its application to technology design to be either the way in which the design affects human behaviours, or the way in which anticipated human behaviours affect the way the system is designed. She believes that these two perspectives are largely held by two different communities that approach the task of design from opposite ends, rather that recognising that the way in which people affect the working of technology and that technology affects the way people work, should be considered as interdependent from the outset.

Klein[2] draws attention to the main difference between the two perspectives (system affects people – people affect system) is where the system boundary is drawn. The system boundary defines what is included in

[1] Klein, L., 2014. What do we actually mean by 'sociotechnical'? On values, boundaries and the problems of language. App. Erg., Volume 45, pp. 137-142.

[2] Ibid.

consideration of the system; generally this is called the System of Interest (SOI)[3]. She comments that this difference in where communities would draw the system boundary can be viewed as a difference in values.

Atkinson, et al.[4] made a distinction between socio-technical systems, in which intelligibility and influence of the system are the key variables, and techno-socio systems, in which predictability and control of the system are the key variables. In the first case, many aspects of the system's behaviour are not apparent to the human immersed in (or interacting with) the system. This is frequently the case for SoS, as will be discussed further below.

Maguire[5] has identified four main elements that constitute socio-technical systems:

- There are collective operational tasks;
- They contain social and technical sub-systems;
- They are open systems (i.e. strongly interacting with their environments); and
- The concept of the system being an unfinished system.

This last implies adaptivity to deal with a changing environment and the need to meet new requirements. A key characteristic of SoS is that they evolve[6] (Maier, 1998); this constant adaptation generally requires significant human intervention and may also change the way that humans behave with respect to the system.

So, for the purposes of this paper, we choose to imply that socio-technical means that the humans (their individual and organisational behaviour) are wholly included within the system of interest; that is to say: they are as much a part of the system as the hardware and software components. We shall then go on to consider how such a perspective will help with designing systems for inclusion in SoS and for operating SoS (which includes adaptation in the form of ongoing design).

2.0 EMERGENT BEHAVIOURS

In Section 3, we shall consider the causes of problems in SoS; to provide background to this discussion, three case studies are briefly reported. The reader is encouraged to read the reference sources for these case studies to understand in greater detail the various complexities of each. The three cases concern a fatal accident, a catastrophic services failure and, from the military, consideration of how to overcome complexity. In each case, one can point to both design and operational causes of difficulty; in every case, both the cause and opportunity for success are firmly in the human rather than technological space, although one can speculate that changes in technology would make the problems that arise less likely.

2.1 Accidents

The term, *normal accident,* was introduced by Perrow[7] in the 1980s to describe accidents that occur in systems which are so complex that all the failure modes cannot realistically be identified. Such accidents are rare and require the unlikely alignment of many contributing factors. In many cases, such as the loss of Air

[3] Flood, R. L. & Carson, E. R., 1988. Dealing with Complexity: An Introduction to the Theory and Application of Systems Science. Plenum Press.

[4] Atkinson, S. R., Goodger, A., Caldwell, N. H. M. & Hossain, L., 2012. How lean the machine: how agile the mind. The Learning, 19(3), p. 183 – 206.

[5] Maguire, M., 2014. Socio-technical systems and interaction design - 21st century relevance. App. Erg., Volume 45, pp. 162-170.

[6] Maier, M. W., 1998. Architecting Principles for Systems-of-Systems. Systems Engineering , Winter, 1(4), pp. 267-284.

[7] Perrow, C., 1999. Normal Accidents - living with high-risk technologies. Reprint from 1984 ed. New Jersey: Princeton UP.

Alaska flight 261 in January 2000 as Dekker[8] described it, it would seem that all the people involved were making appropriate decisions regarding their local environment, but that collectively these decisions resulted in a disaster. There were failures in training, maintenance, regulation and safety culture. These are all socio-technical systems that must work together co-operatively to ensure safe aviation. Of note, in this particular disaster, was a radio conversation that took place between the pilot and a dispatcher when the pilot had alerted him to a problem with the horizontal stabiliser on the aeroplane. The pilot wanted to land at the nearest suitable airpot (Los Angeles), but the dispatcher urged him to go on to San Franscico, on the basis that once landed at Los Angeles, it would be difficult to get an early take-off slot after repairs. The focus of the pilot was, naturally, the aircraft as a system within the SoS; the dispatcher was focused on the workflow system (within that SoS) that manages the scheduling and dispatch of aircraft. There are many similar examples – see for instance the famous failures paper of Bahill & Henderson[9] in which they present a morbid list of failures in complex systems resulting, mainly, from misunderstandings between various parts of the development system. The cause of the loss of pitch control (horizontal stabilizer) was eventually traced to insufficient lubrication of a jackscrew assembly; this had resulted from changes made over time to the maintenance schedules. The significance of such changes had not been appreciated by any involved in the maintenance.

2.2 Failures

On 8th September 2011, millions of people along the US West Coast were left without power for up to 12 hours when the power grid failed. A relatively minor local failure, due to a mistake by a technician in failing to isolate a capacitor bank on a Coachella Valley Transformer, cascaded into transformers being tripped all over the place. But it was not the tripping of transformers individually that caused the problem; it was an unexpected emergent behaviour of these cumulative failures. There were eleven major energy companies responsible for the delivery of power from Northern Mexico to Southern Canada, along the Western seaboard. They had overlapping responsibilities for real-time operations, long-term planning, transmission planning, reliability co-ordination, and balancing of resources in real-time. Different organisations had different levels of authority in different geographical areas. There are three main corridors for high voltage transmission running North-South in Arizona and Southern California. As different transformers were tripped (by excessive loads) each energy company sought to maintain their own service by diverting power along other transmission paths, and one path (path 44) reached such a high load that a safety process was activated, which separated the San Onofre Nuclear Power station from the network; at which point power was lost across the entire network and a blackout resulted[10].

The black-out was effectively caused by individual systems owners (the energy companies) taking actions to maintain their own service without considering the effect such action would have on the SoS (i.e. whole network). The blackout also had a knock-on effect on an even larger SoS. The loss of power meant that millions of people were without air conditioning on one of the hottest days of the year; schools and businesses closed early leading to massive traffic jams, with people being stuck in their cars for hours. Flights and public transport stopped, due to lack of power. The sewage pumping stations lost power and the spillage that resulted meant that beaches had to be closed. Many other services were affected or closed down.

The full report[11] of the outage is of great interest to SoS engineers; it exemplifies how relatively insignificant events can combine to cause a massive emergent impact. With the exception of the technician's error in servicing a transformer in Coachella Valley (against which the systems should have been robust), the

---

8 Dekker, S., 2011. Drift into Failure. Fareham: Ashgate.

9 Bahill, A. T. & Henderson, S. J., 2005. Requirements Development, Verification, and Validation Exhibited in Famous Failures. INCOSE Systems Eng., 8(1), pp. 1-14.

10 FERC/NERC Staff Report on Arizona-Southern California Outages on September 8th, 2011, Causes and Recommendations. Published April 2012. http://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf.

11 Ibid.

decisions taken by the various operators involved in managing the systems were locally sensible. However, a combination of different control practices in each area, different operating practices, misunderstood information, and the lack of a view of the whole network for any single entity, resulted in a catastrophic system failure. The principal findings of the report[12] highlight the problems of SoS:

- There was inadequate situational awareness among operators:
  - They did not know what the impact of neighbouring suppliers' failures would be on their own systems.
  - They did not know what the impact of their internal failures and changes to operations would have on the systems of neighbouring suppliers.
  - They did not have any accurate real time models to allow them to understand the developing situation.
- There was inadequate planning for contingencies.
- There was a failure to recognise interconnection reliability operation limits – there was a variation in trip limit settings from one organisation to another.
- Each operation was managed differently.
- Each operator optimised their own system by calling on neighbours to backfill their lack of generation capacity (but everyone was doing this).
- Localised predictions did not predict the overall emergent behaviour.
- Operators were unaware of what was happening in the wider system and this resulted in misinformation between neighbouring operators.

2.3 … and Overcoming Complexity

Maj. Gen. (Rtd) Andrew Stewart commanded in Bosnia and Iraq; he has written of the complexity of working within a multi-national command[13]. In Multi-National Division South-East, he had forces from nine different countries under his command; even within these various national forces there was a mixture of different types of force, including military police. All forces had different rules of engagement and Stewart remarks that multi-nationality is "a political necessity, but in some ways a military nonsense". Each force is constrained in the way that it can deploy and use its military systems, so that in constructing a battle group, for instance, some systems could be used and others could not, which reduced the agility of the Multi-National Division. The different rules for different forces create a C2 nightmare. Nevertheless, the Multi-National Division functioned well, and Stewart remarks that this was as a result of getting to know the strengths and weaknesses of each nation's deployment. His advice is: "good electronic communications is important, but face-to-face communication is far more effective." You have to get both the socio and the technical right!

3.0 THE PROBLEM WITH SYSTEMS OF SYSTEMS

3.1 Local Interests, Global Outcomes

The Maier characteristics[14] of SoS have been presented and discussed by Dahmann[15]; in fact, the characteristics of evolutionary development, geographical distribution, and emergence could be equally true

[12] Ibid.

[13] Stewart, A., 2013. Southern Iraq 2003-2004: Multi-National Command. In: J. Bailey, R. Iron & H. Strachan, eds. British Generals in Blair's Wars. Fareham: Ashgate, pp. 79-88.

[14] Op. cit.

[15] Dahmann, J. S., 2015. Systems of Systems Characterization and Types. In: SCI-276 Lecture Series. CSO.

of a single system as of a SoS, but those of managerial and operational independence are particular to the SoS concept. It is worthwhile appreciating the full implication of these two chracteristics.

Operational independence means that the constituent systems can operate (and achieve useful outcomes) separately from the SoS. That is to say, if the SoS were taken apart, the individual systems could be operated in a useful way.

Managerial independence of constituent systems implies that choices about the development of the systems, their functionality and procedures for operation are determined by their owners or managers, rather than by a centralised owner of the whole SoS. Of course, the level of authority that managers of constituent sytems can exercise in this respect is determined by the type of SoS[16]. But the implication is that the architecture of the SoS, for all except the 'directed' type, may change because of localised decisions. This means that the constituent systems may have different funding lines and independently developed sets of requirements. In terms of operations, the systems may interoperate within the SoS, but under separate controls.

The implications of operational and managerial independence have been neatly summarised by Rebovich[17]:

> *From the single-system community's perspective, its part of the SoS capability represents additional obligations, constraints and complexities. Rarely is participation in an [sic] SoS seen as a net gain from the viewpoint of single-system stakeholders.*

The focus of a particular constituent system owner/operator on maximising the performance of his/her system is, of course, entirely understandable. Within a commercial environment, for instance, it is hardly likely that one company will compromise (i.e. reduce) their own profits to accommodate more effective interoperation with systems from another company. The power outage case study (Section 2.2) illustrates this very well; each company endeavoured to maintain the performance of their own power distribution system, but this was at the expense of the overall SoS performance and, eventually, it ended up with all losing performance. An important consideration, though, is that if individual companies had better understood the impact of their actions on other parts of the SoS, and could have understood (predicted) the overall outcome, their behaviour would have likely been different. Situational Awareness of individual system owners with respect to the SoS in which they participate is a significant concern, to which we shall return later.

3.2 Characterisation of SoS and the System of Interest

Although the Maier characteristics[18] give a general characterisation of SoS, they are not sufficient to give a means of distinguishing one SoS from another; a further level of detail is required in the characterisation. Kinder et al.[19] considered an approach to characterisation of particular SoS based on the concept of the System of Interest (SOI). In general, there are two approaches to defining the SOI in Systems Engineering[20]: the structured approach, in which it is assumed the elements of the system are known in advance, and the behavioural approach suitable for more complex (sometimes called "messy") systems. The latter focuses on the interactions between elements of the system, rather than the elements themselves. If the SoS is of the directed type, then the structured approach may afford some benefit, but for all other types, quite clearly the need to know all the elements (in this case component systems) *a priori* invalidates the structured approach. It is unusual for either approach to be used in isolation; for instance, one might start with the structured

---

16 Ibid.

17 Rebovich, G., 2009. Enterprise Systems of Systems. In: M. Jamshidi, ed. *Systems of Systems Engineering - principles and applications.* Boca Raton: CRC, pp. 165-190.

18 Op. cit.

19 Kinder, A., Barot, V., Henshaw, M. & Siemieniuch, C., 2012. Systems of Systems: Defining the System of Interest. Genova, IEEE, pp. 463-468.

20 Flood & Carson, op. cit.

approach and then use the results to begin to discover the behaviours of the system in question. Kinder et al.[21] proposed a set of dimensions through which a SoS could be characterised and these were used as the basis for classification of case study SoSs in the European Support Action T-AREA-SoS (Trans-Atlantic Research and Education Agenda in Systems of Systems)[22]. These dimensions cannot be considered exhaustive and it is anticipated that they will be further elaborated in the future. The dimensions are as follows.

3.2.1 Component Systems

These are the individual, independent systems comprised within the SoS. The ability to establish this depends to some extent on the level of abstraction with which one regards the SoS. For some military SoS, identification of the component systems (e.g. aircraft, satellites, HQ, etc.) is straightforward, but may be insufficient to provide confident prediction of behaviour. For other SoS, it may not be possible to identify accurately the participating systems; for instance, a particular system owner may provide a service without exposing the system through which it is delivered. Another possibility for this dimension is to specify the types of constituent systems included, rather than the specific systems.

3.2.2 Interactions

The SoS exists because there are interactions between constituent systems; if there were not, then there would be no emergent behaviour. Interactions in a SoS are exchanges of information, mass, or energy between the constituent systems; in general for SoS, the interactions of concern are mostly information exchanges. To specify all interactions logically requires that all component systems are known, or can be discovered. This may not be the case. However, interaction types may be used to classify the SoS. In fact, for a SoS it makes sense to speak of interoperability. The component systems must be able to interoperate with each other and there is a spectrum of interoperability that can help define the SoS. One in common use, and rooted in the Network Enabled Capability (NEC) initiative, is the NCOIC Interoperability Framework[23] which is depicted in Figure 1; this shows that interoperability occurs at various levels from the physical level through to the strategic level of business objectives. A number of the levels at the top of the spectrum involve intrinsically human attributes. If the effectiveness of interoperability is a means of assessing the SoS, then for the systems involved appropriate interoperability at all levels is required.

[21] Op. cit.

[22] https://www.tareasos.eu/.

[23] NCOIC Interoperability Framework, 2007. https://www.ncoic.org/home.

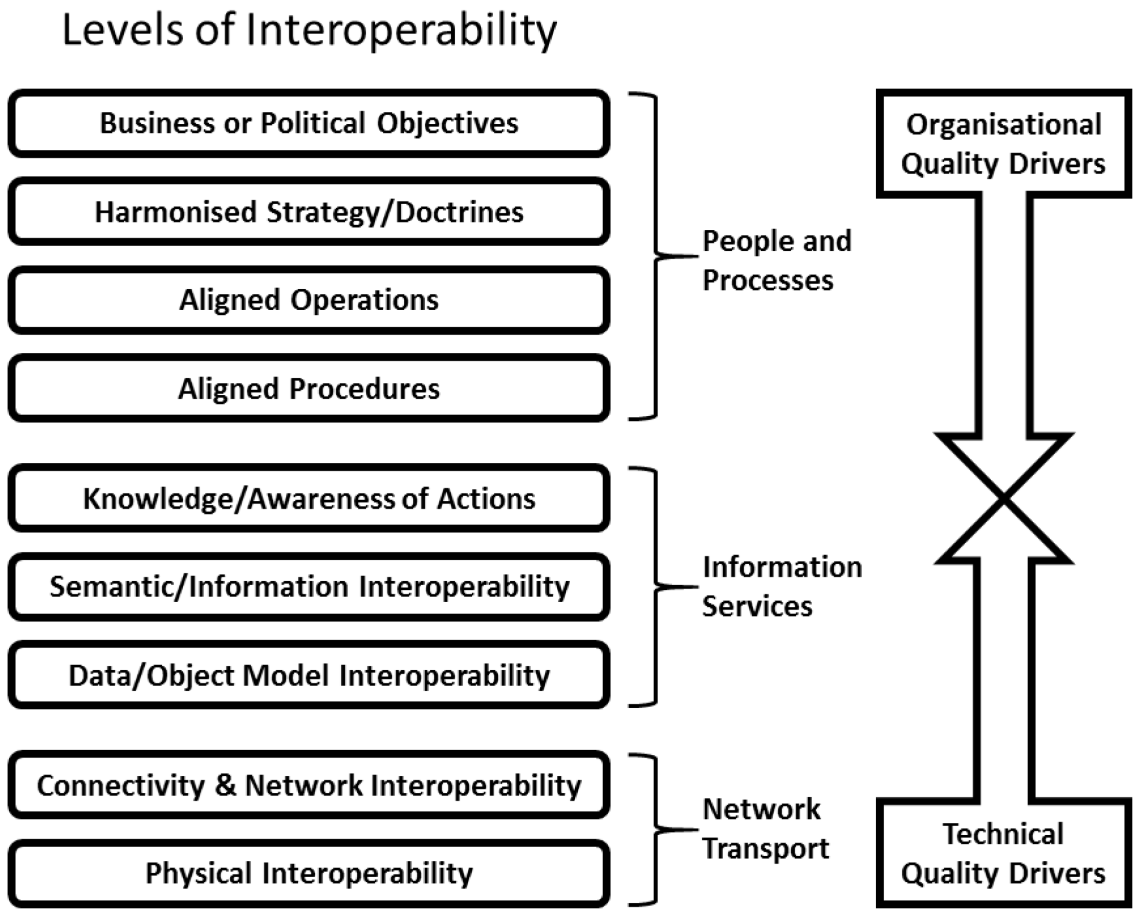

Figure 1: The NCOIC Interoperability Framework (NIF)[24].

3.2.3 Functions

Functions are accomplished by component systems and combinations of component systems. A means of classification is to identify the various functions executed within the SoS. This has proved useful in an architectural view of SoS, described by Liu et. al.[25] (Figure 2) in which the SoS delivers capability through the aggregation of functions into services which are then composed to realise certain capabilities. The various services are considered to be built from the functions delivered by people, process, products (equipment), and infrastructure. In Figure 2, the systems could be platforms, but some of the functions could be purely human-delivered as part of the overall system's offering. As an example, for System A, function F4 might be data acquisition and function F5 interpretation of the data by a human operator "eyeballing" it, to provide the information service SB.

---

[24] Ibid.

[25] Liu, L., Russell, D., Webster, D., Luo, Z., Venters, C., Xu, J., Davies, J.K., 2009, Delivering sustainable capability on evolutionary service-oriented architecture, ISORC'09. IEEE Int. Symp. Object/Component/Service-Oriented Real-Time Distributed Computing.

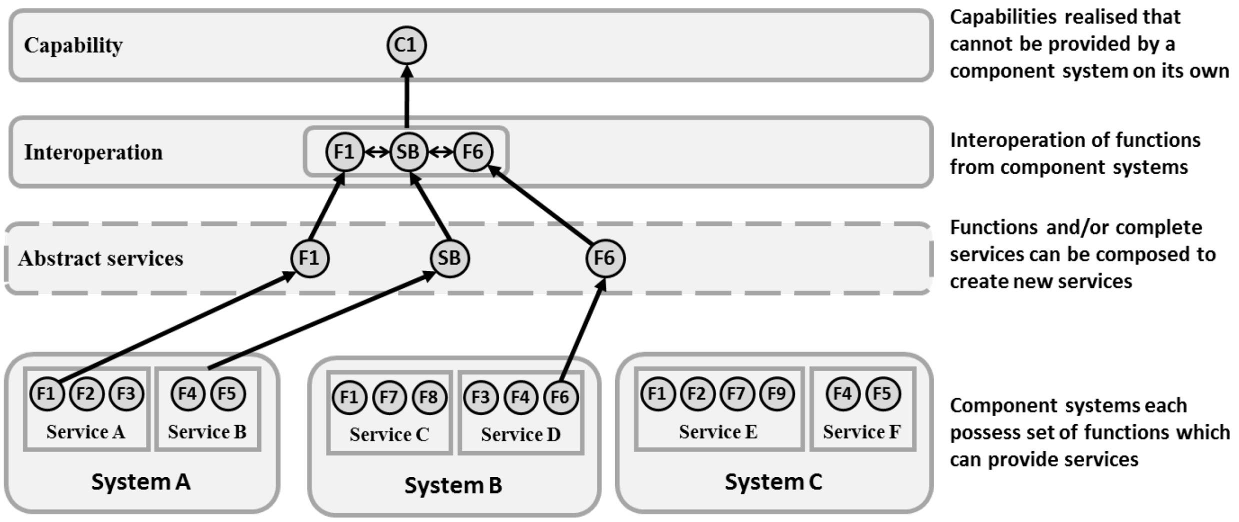

Figure 2: Conceptual Composition of Contributing Services or Contributing Functions into Capabilities; Diagram Based on Liu, et al.[26].

3.2.4 Nature of Relationships

This dimension is used to define the category of relationship between component systems, such as peer-to-peer, hierarchical control or distributed control. This is related to the SoS type[27] but is also concerned with the exchanges that take place between systems, as well as the authority mapping between systems.

3.2.5 Lifecycle

SoS lifecycle is discussed in detail by Dahmann[28]; this is a troublesome dimension, because there are various lifecycles that can be considered. But even just the identification of the most appropriate lifecycle model for a particular SoS may be a means of distinguishing it from others.

3.2.6 Classification

This dimension basically refers to the SoS type[29] (directed, acknowledged, collaborative, virtual) but, as has been observed, a SoS may be composed simultaneously of several types and so a means of describing how the various types are combined is also required. One could speculate that the combination of SoS types within a SoS could be related to the significance of the socio-technical considerations, but such a relationship has not yet been established.

3.2.7 Variability

This is related to lifecycle, but considers the rapidity with which the SoS changes (reconfigures). Some SoS are comparatively static; they are composed of different systems that stand in a more or less consistent relationship to each other. Other SoS may exist only for a short time when a number of systems are called upon to interoperate to achieve a specific goal, and then decouple. A particular feature of relevance here is

[26] Ibid.

[27] Dahmann & Baldwin, op. cit.

[28] Dahmann, 2015, op. cit.

[29] Ibid.

that some constituent systems service several different SoS, either consecutively or simultaneously. Variability could be considered to be some kind of characteristic time for a SoS.

3.2.8 Systems Owners and Operators

This dimension is concerned with organisations, management and enterprise (multi-organisational) relationships. It is related to the classification type of the SoS. Even in the case of constituent systems that are autonomous, this dimension points towards a socio-technical concern as the operation of the individual systems are ultimately determined and maintained by human desires and priorities.

3.2.9 Concept of Operation or Use or Employment

The CONOPs, CONU, or CONEP is included in most Systems Engineering plans and is a means through which requirements for new systems are defined. For certain types of SoS, and certainly for military applications, the CONOPs etc. should be well defined and available for use in classification.

3.3 Socio-Technical Relevance of Characterising Dimensions

Several of the dimensions (interactions, relationships, classification, owners and operators) cannot be described except with reference to societal and/or sociological considerations. In terms of the human aspects of SoS, it is the organisational, or managerial, aspects, more than the psychological or physiological, that is relevant. Generally with complex systems, design and operation is concerned with control, but the classification of SoS is based on the notion of diminishing central control, as the types go from directed to virtual. Sauser, et al.[30] have described, what they term, the ‘control paradox of SoS’ and develop their ideas towards the assertion that for SoS, management is replaced by governance. Thus in C2 terms, the emphasis in SoS is on command, rather than control: ‘Control is a function of rules, time, and bandwidth; whereas command is a function of trusts, influence, fidelity, and agility’[31]. Trusts, influence, and fidelity are intrinsically human qualities.

3.4 Dealing with Complexity

There are many definitions of complexity but, in the context of SoS, a definition provided by Siemieniuch and Sinclair[32] captures the essence of the challenge with which SoS engineers must deal:

> *Complexity is a behavioural characteristic of the network of agents and relationships that make up the system. It is not decomposable to individual elements of relationships.*

They draw attention[33] to a variety of organisational characteristics[34] that concern the interactions among systems operators in a SoS:

- Many agents, of different kinds.
- Some degree of behavioural autonomy for agents.

---

[30] Sauser, B., Boardman, J., and Gorod, A. 2009, System of Systems Management, in System of Systems Engineering: Innovations for the 21st Century, ed. Mo Jamshidi, Wiley.

[31] Atkinson S.R. and Moffat, J. 2005, The Agile Organization, DoD CCRP.

[32] Siemieniuch, C.E. and Sinclair, M.A., 2002. On complexity, process ownership and organisational learning in manufacturing organisations, from an ergonomists perspective. App. Ergonomics, 33(5), 449-462.

[33] Siemieniuch, C.E. and Sinclair, M.A. 2014, Extending systems ergonomics thinking to accommodate the socio-technical issues of Systems of Systems, App. Ergonomics, 45, pp. 85-98.

[34] Gregg, D. 1996, Challenges in Business and Manufacturing Decision Support, in The Science of Business Process Analysis, ESRC Business Process Resource Centre, Univ. Warwick, UK.

- Multiple steady states for agents.
- Interactions between agents in an environment.
- Lots of connections between agents.
- Communicating in parallel.
- Effects of an evolving environment.
- Effects of evolving agents.
- Interactions between different goals within an agent.
- Interactions between agents with different goals.
- Language/culture differences.

Whilst formulated in the context of manufacturing enterprises, it is clear that the same characteristics are profuse in NATO operations. In the discussion that follows, we use the term enterprise to describe an endeavour (commercial, military, etc.) in which several or many systems-owning organisations participate such that their systems interoperate. One can consider enterprise complexity to be generated in two forms: intrinsic complexity and induced complexity[35]. Intrinsic complexity is that which is inherent in the structure of the enterprise, due to the characteristics listed above. Induced complexity, though, arises because individual parts of the enterprise create structures to cope with the dynamically changing SoS endeavour. In essence, it is unnecessary complexity, but it arises because individual organisations do not have sufficient information or knowledge about the whole of the SoS and because the various organisations, whilst subscribing to the overall goal, will undoubtedly have secondary (or even primary) goals that are not shared across the SoS enterprise. Henshaw, et al.,[36] studied a major product manufacturer undertaking a transformation to become a product-service organisation. Their highly complex organisational structure could be directly attributed to the induced complexity caused by creating a service structure without significant modification to the existing product structure. Viewed through a SoS lens, one set of systems were operated to prioritise product manufacturing outcomes, the other set to prioritise service business outcomes.

Command and Control approaches are designed to cope with complex situations. To some extent, the results of SAS-085[37], point to a conclusion that the type of C2 that is required to be agile depends on the type of complexity that needs to be confronted. In consideration of C2, Alberts has commented[38]:

> *If it is local interactions that give rise to the outcomes that occur, we can no longer think about organizing activities solely from a top-down perspective. The simple fact is that complex systems or situations cannot be predicted or controlled. The best that one can hope for is to exert some influence to keep behaviors within acceptable bounds.*
>
> *As a result, there is virtually nothing left in our traditional tool kit to deal with the degree of difficulty that attends complex endeavors.*

There is, thus, a need to consider different decision making constructs for complex endeavours such as those characterised by SoS. Most importantly, there is a need to consider the structure (including rules governing decision making) of the enterprises that build, and the enterprises that operate, SoS. There is also a need to ensure that decision making at the local level is cognisant of the effect at the SoS level. These enterprise

[35] Siemieniuch, C.E. and Sinclair, M.A. 2014, op. cit.

[36] Henshaw, M.J.d., Morcos, M.S., Siemieniuch, C., and Sinclair, M.A. 2011. Identification of induced complexity in Product Service System Enterprise, J. Ent. Trans. 1(4) pp 269-289.

[37] NATO, Command and Control (C2) Agility, 2014, Final Report: STO-TR-SAS-085 AC/323(SAS-085)TP/549.

[38] Alberts, D.S., 2011. The Agility Advantage, US DoD Command & Control Research Program.

considerations need to be developed hand-in-hand with the technical systems that are deployed within the SoS.

3.5 The Main Socio-Technical Issues in SoS

The discussions hitherto have identified various characteristics of SoS with which designers, engineers, operators, and systems' owners must deal. The motivations and complexities of SoS cause two main issues for operations, which, in the case of SoS, are somewhat related. The first is the need for appropriate governance, given that top-down direction is compromised by the characteristics of managerial and operational independence. The second is lack of situational awareness, such that the managers or operators of constituent systems lack the necessary information to understand the effect of their decisions on the wider SoS.

4.0 SoS GOVERNANCE

Governance is normally considered in the context of corporate behaviour, and refers to the proper running of an organisation and, particularly, how it manages risk[39]. One of the difficulties with SoS operation is the understanding the allocation of risk; referring to the power outage case study of Section 2.2, each organisation probably believed it was managing the risk of failure by the various actions it took to re-route transmission. Local risks were, supposedly, dealt with by these actions, but an un-identified risk eventually caused failure at the national network level, that then affected all the local networks.

In general, governance can be summed up by three connected questions[40]:

- Are we doing the right things? (Leadership)
- Are we doing those things right? (Management)
- How do we know this? (Metrics and measurement processes)

A general framework for addressing these questions in a SoS context is a question for future research. However, Henshaw et al.[41] have considered the implications for Technical and Engineering Governance (TEG); the conclusions focus strongly on architectures. For SoS, the architecture and TEG is about the interfaces between the constituent systems, rather than the systems themselves. This is not meant to imply that governance of individual systems can be neglected, but rather that these are already covered by existing TEG, but need some alignment though governance protocols and processes at the interfaces. Henshaw et al.[42] postulate that a SoS can be regarded as a set of trust and contract relationships between systems; this, to some extent, covers informal and formal relationships (in a business sense). The systems architect of a constituent system must, therefore, address trust issues for each participating organisation in the overall enterprise with which his/her system must interoperate. For SoS, TEG is concerned with defining and ensuring compliance with trust at the interface between constituent systems. Describing this as an aspect of architecting suggests that the concerns are purely technical, but this is far from the case. Consider the interoperability framework presented in Figure 1. TEG must address every level of the interoperability framework, and the upper levels are largely non-technical. Delivering the requisite quality of service at the interface across the interoperability spectrum is not a simple matter; it requires attention to the following[43]:

[39] Weir, C. and Laing, D. 2001, Governance structures, director independence and corporate performance in the UK, European Business Review,. 13(2), pp. 86 - 95.

[40] Siemieniuch, C.E. and Sinclair, M.A. 2014, op. cit.

[41] Henshaw M.J.d., Siemieniuch, C.E. and Sinclair, M.A. 2013. Technical and Engineering Governance in the Context of Systems of Systems, Paper 9, NATO SCI Symp. Architecture Assessment for NEC (STO-MP-SCI-254), Tallinn, Estonia.

[42] Ibid.

[43] Ibid.

- 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 organisation, 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.

These objectives can be more readily approached in the defence procurement world if an open architectures approach is taken. An open architecture is defined as[44]:

> *Open system architecture is an open specification of the architecture of a system or systems of systems for the purpose of acquiring specified capabilities. As a general feature of good design (for a system or system of systems), an open system architecture should allow for easy improvement and update of system capabilities by adding or changing components.*

Open architectures carry with them their own set of issues regarding Intellectual Property and commercial prowess, but enable better sharing of information across a SoS, thus reinforcing trust and providing participants with greater awareness of other parts of the SoS, which are not under their direct purview.

5.0 SITUATIONAL AWARENESS IN SoS

Situational awareness is basically a decision maker's understanding of the environment in which he/she takes a decision; it concerns information, awareness, perception, and cognition. Endsley[45] emphasises that situational awareness is a state of knowledge. In the three case studies, it is evident that shared knowledge and information are critical issues. In the case of the Air Alaska accident (Section 2.1), advice from staff on the ground was inadequate in various ways because they did not properly understand the situation with which the pilot was trying to deal. In the power outage case (Section 2.2) the wider implications of their local decisions were not understood by operators, so that a developing failure at the SoS level was not appreciated until the failure occurred. In the third case (Multi-National forces, Section 2.3), Stewart[46] highlights the importance of face-to-face communications; i.e. the most effective way of sharing knowledge (and accommodating, if not circumventing, constraints).

Of course, the motivation for NEC (Network Enabled Capability) is better use of information to achieve military objectives, and there is more written about this from both the technical and social perspectives that can be sensibly reviewed in the space available here. It is worth noting, though, that the NEC benefits chain, as depicted by Court[47] is concerned with the quality of decision making, which relies on the quality of shared awareness, which relies, in turn, on networks and information quality. As with the question of governance (Section 4), a crucial element is the sharing of information, knowledge, and understanding. NEC is

---

44 Henshaw, M.J.d., et al. 2011, Assessment of open architectures within defence procurement Iss. 1, Systems of systems approach community forum working group 1 – open systems and architectures, London, Crown owned copyright. https://dspace.lboro.ac.uk/dspace-jspui/handle/2134/8828.

45 Endsley, M.R. 1995. Toward a theory of situation awareness in dynamic systems. Human Factors 37(1), 32–64.

46 Stewart, A., 2013. Op. cit.

47 Court, G., Validating the NEC Benefits Chain, 11th ICCRTS, Cambridge, 2005, http://www.dodccrp.org/events/11th_ICCRTS/html/papers/155.pdf, p.8.

predicated on the ability to share useful information effectively among the stakeholders that need it. We can conclude, then, that improving situational awareness will improve SoS performance, or at least reduce the risk of failures at the SoS level. Therefore, the principles which govern the organisation of the SoS should support sharing information effectively across the network; in essence, ensuring that every level of the interoperability spectrum (Figure 1) is adequately serviced.

Another aspect of situational awareness is to be able to understand how a system, or environment, is changing. Operators need insight into the effect that their own local decisions may have on the changing SoS or environment; similarly they need to understand how external changes will affect the systems that they own.

6.0 CONCLUSIONS

Through consideration of case studies, of which three representative ones have been presented, it has been concluded that the managerial and operational independence of constituent systems in a SoS are the most significant aspects because locally sensible decisions can give rise to unanticipated emergent behaviour at the SoS level. The problem of SoS is that individual systems owners/operators will tend to maximise the performance of their own system at the expense of the overall SoS performance. There are two areas of concern that must be addressed if SoS are to be operated successfully. The first is governance which, if not addressed, can lead to unexpected changes in the SoS performance either because of operational decisions or because of independent development of a constituent systems such that its interoperation is inadequate with existing member systems of the SoS. The second issue is situational awareness. In an operations environment, governance, and the architectures that support it, should ensure that the trusts and contracts that exist between systems are designed appropriately and operated with integrity. The second issue is situational awareness of operators and, as it happens, of developers as well. It is essential that operators have appropriate knowledge about the SoS in order to make effective decisions at the local level, such that the SoS behaviour remains appropriate.

It is concluded that an open approach is required to architecting for SoS development, and to the process of management within a SoS for operations. Open approaches present commercial challenges for organisations, however, these can be overcome with the correct business model. Therefore, the main conclusion is that there is a need to develop appropriate business models, or NATO processes, that incentivises good SoS behaviour which, we conclude, has effective information and knowledge sharing at its heart.

7.0 ACKNOWLEDGEMENTS

The author is grateful to Prof. Carys Siemieniuch and Dr. Murray Sinclair for many helpful insights and ideas concerning the socio-technical considerations of SoS, and to the whole ESoS group for research contributions that have informed this paper.