# Modelling and analysing standard use within system of systems

# Modelling and Analysing Standard Use within System of Systems

Russell Lock
Department of Computer Science
Loughborough University
Loughborough, United Kingdom
r.lock@lboro.ac.uk

*Abstract*— **Despite increasing interest by organisations in deploying SoS (Systems of Systems) to manage complexity, and promote agility within their businesses, there are a number of research areas that are currently underdeveloped. One of these is the role of standards within organisations which develop, operate and share systems within SoS. The paper is not about what standards should be chosen, or indeed developed. Instead, it explores the information that needs to be elicited and modelled, to reason about the standards that member systems of a SoS adhere to; and to provide a structure within which to promote discussion of the incompatibilities that inevitably arise within large SoS. The paper evaluates the approach taken using a running example based on the supply chain SoS for RAF Nimrod aircraft, in light of the recent investigations into the explosion of an aircraft in 2006. The paper concludes that the interaction of standards within SoS is a complex issue, but that a methodology to discover, model and analyse problems can be developed to further best practice in this area.**

***Keywords: Information Modelling, SoS, Standards, Risk***

## I. INTRODUCTION

The term SoS (System of Systems) has been widely used in literature, but a general definition remains elusive [1]. Some, including [2] define a separate term, system portfolio, to describe a SoS where software components are rapidly assembled using envisioned development platforms, the precursors of which are available today in the form of tools such as Google App Engine. The term FoS (Family of Systems) may also be encountered, denoting systems that are related in terms of background or type [3]. FOS (Federation of Systems) is another related term used by some authors [4][5] to discuss decentralised SoS. This paper does not overly restrict what should be termed a SoS, defining the term broadly as follows:

*A collection of member systems, comprised from technical components, people, processes and environmental considerations, working together to accomplish common goals.*

Despite being a recent term, many existing systems can be categorised as SoS, including major telecommunication networks, the internet, financial systems, multi organisational supply chains etc. SoS may develop in response to temporary conditions, for example in response to an emergency, or they may be more permanent arrangements of systems.

The term SoS is socio-technical at its core. The concept of socio-technical systems has roots in psychological theories [6] originally designed to explore the interaction of people, machines and processes in coal mining. However, it has become a popular term within computer science [7] to help understand the interactions that influence the dependability of complex systems. The impact on dependability and agility made by the management and interaction of human work processes, in combination with technical systems, is a significant challenge which is further complicated by the characteristics of SoS, including those of decentralisation [8] and organisational boundaries.

Maier argued that interface and communications standards become more important within SoS [9], given that control over other aspects of the system would be devolved to the largely autonomous member systems of a SoS. The importance of standards within system evolution and re-development as a whole has been recognised for some time [10]. Standards could take many forms within SoS and have multiple overlapping levels within organisations as shown in fig 1.

The term standard does not refer exclusively to international and national agreements. Standards may be developed within an organisation, and remain exclusively in internal use for commercial & competitive reasons, rather than through lack of applicability outside a given organisation.

A table outlining some of the differences between standards in a System, and standards in a System of Systems management context is provided in Table 1.

This paper argues that SoS can face significant difficulties


Figure 1: Levels of Standard

in achieving standard homogenisation, making standard integration crucial within SoS. The potential lack of centralised control makes discursive techniques aimed at bringing together the potentially disparate management of different member systems valuable. Information needs to be gathered from stakeholders within a SoS, but much of the information that would be needed is likely to be scattered across existing systems and process documentation, making it difficult to discuss and analyse.

A methodology is proposed to allow those involved in SoS management to explore what standards are in use within a given SoS, and to understand the effect the integration of different standards across organisations / systems has on shared work processes. In order to promote critical analysis of the available data a risk analysis technique is put forward to aid in the development of future strategy.

The paper uses a running example based on the supply chain SoS for RAF (Royal Air Force) Nimrod aircraft. Nimrod aircraft are used for surveillance operations, often over hostile territory, and have been in service since 1969. The aircraft design predates the modified version constructed for the RAF, and is based on the original civilian De Havilland Comet design dating back to the late 1940s. A SoS is in place to cover maintenance, part manufacturing, management and ongoing operation of the aircraft which has evolved over 60 or so years. Nimrod XV230 exploded in mid air during an operation over Afghanistan in 2006, killing all 14 members of the crew.

At the time a number of different scenarios were put forward as to the cause of the explosion. This part of the debate is not covered directly by this case study, which instead focuses on the SoS standard issues that. Further information regarding the explosion itself can be found in the independent Nimrod review, published in 2009 [11]

The structure of the paper is as follows. Section II explores the background of standard use within systems and SoS. Section III outlines the methodology proposed to model standard use, and promote discussion of the risks relating to standard configurations. Finally, section IV explores future work within the area and provides conclusions.

Table 1: Characteristics of standards

| Characteristic | System | SoS |
|---|---|---|
| Homogeneity of Standards | Active movement towards homogeneity for efficiency | May not be plausible due to political, commercial, resource and time restrictions. |
| Management | Most likely centralised | Unlikely to be centralised |
| Goals | Common purpose | Potentially conflicting, shared for limited time. |
| Development | Typically top down | Typically bottom up |

## II. BACKGROUND

Much of the research into standards has focussed on development practices for new standards, a significant amount of this for the telecommunications domain [12] [13]. There has also been significant work into the mechanics of how standards form from a games theoretic perspective [14]. However, this aspect of research is outside the scope of this paper. Standards can be logically categorised from the perspective of who proposes them. Stango [15] outlined four main types:

- Un-sponsored (developed internally)
- Sponsored (by a standards organisation)
- De-facto (through market competition)
- De-jure (emerging through consensus within an industry).

Within a given SoS any / all of these could be observed. A given sponsored / de-facto standard may already exist within multiple member systems of a SoS, allowing greater economies of scale, however, further homogenisation may prove difficult for political and commercial reasons.

The development of de-jure standards within a SoS, though appealing, may also prove difficult given the instability and limited lifespan of many SoS. Markus's [16] exploration of Collective Action Theory examines this area with reference to standardisation within the US property market, concluding that within disparate, competitive groups of companies, heterogeneity of interest can greatly inhibit the success of standard collaboration.

Therefore, instead of arguing for standard homogenisation, this paper focuses on providing techniques for those attempting the integration of different standards within the shared work processes of SoS.

The nature of potentially competing organisations within a temporary organisational construct such as a SoS makes modelling standards only part of the solution. Ensuring compliance with standards is also a significant issue. In order to work together, organisations need to be able to trust that standards are upheld.

### *A. Standards and Trust*

Assurance that a given organisation adheres to product and process standards that are approved of, is a driver for trust [17]. SoS cannot operate without trust, which in these circumstances cannot be built through recommendation to the extent that interactions between individuals can. This can partly be attributed to the lifespan of SoS, and the fact that organisations may choose not to trust the opinion of other potentially competing organisations.

Trust can be built through a number of methods. Standards can be used for compliance purposes (a given party stating that they follow a given set of standards), certification where a third party attempts to prove an organisation follows a set of standards, and finally accreditation which allows an organisation to certify others. When considering

who certifies accreditation bodies, hierarchies exist, but often only in a national setting. This makes trust through certification complicated in a SoS setting, where organisations and systems may be geographically spread across multiple countries. Discursive techniques are best applied in such situations where clear guidance is not available.

For example:

- X certifies Y
- X is accredited to do so by Z
- Z is the accreditation body, X is the certification body and Y has been certified

When dealing with internally developed standards, the organisation that developed the standard is likely to behave as the accreditation body. Whether the resources and personnel are in place in order to certify others to use that standard within a SoS, is a matter which requires further investigation, an area which is explored further in section 3a.

### *B. Evolving Standards*

In addition to considering the changing use of standards within a SoS, change within standards themselves also needs to be considered. Changes to a standard within a single system or organisation will affect those concerned. The lack of centralised control and transparency common to SoS, has the potential to cause additional problems relating to a lack of communication, and potential breakdown to work processes. An example of this was seen in the development of the Airbus A380. Airbus can be considered a SoS, as the organisation contains many autonomous member organisations, working across Europe, whilst also maintaining their own competitive businesses in parallel. The A380 launch was significantly delayed by wiring problems caused by engineers in Spain and Germany using different versions of the same design software [18].
Standards can take more effort to overhaul than the original effort expended [19], for example, technical standards such as HTML, and organisational standards such as ISO 9000 have changed considerably over their lifetimes. As with any change, people will need to be informed, and the risks associated with compatibility between standards, and compatibility of versions within standards will need to be re-assessed on an ongoing basis.

### *C. Standards and Risk*

Risk analysis is useful to ascertain the impact of deviation from the norm within the socio-technical structures of a given SoS [20]. For standard management, risk analysis is useful to structure discussions on how changes to standards in use affect SoS, and to help formulate actions that can be taken to avoid, minimise and mitigate such risks in future.

HAZOPS [21] is one approach to risk analysis originally developed for ICI (Imperial Chemical Industries) in the 1970s, which has been applied to wider domains, including work on socio-technical systems [22]. HAZOPS focuses on the identification of potential hazards using keywords which then have risk assessments attached, with a focus on technical operability and efficiency. HAZOPS keywords are used to construct tables, examining the effect of deviation from the norm for a given process. For example:

Given a specific deviation for a given process, (something occurring early, late, never, in reverse, too much etc)

- What are the consequences?
- What actions could be taken to mitigate the consequences?
- What safeguards could be put in place?
- What are the risks of occurrence etc?

Section 3b applies an adapted HAZOPs approach designed to explore the risks associated with standard configurations.

## III. METHODOLOGY

This section addresses the following three points:

- What questions need to be asked regarding individual standard use, in order to manage the wider SoS?
- How do you graphically model standards?
- How do you manage standards evolution through risk analysis?

Given the focus of the methodology on promoting discussions between those managing SoS a graphical technique is proposed. It has been argued [23] that graphical techniques are a better way to understand the complex inter-relations between different organisations / systems. A visual notation could be constructed using existing diagram types from for example, UML or SysML, utilising object diagrams, sequence diagrams etc. However, developing diagrams in this manner requires at least cursory knowledge of UML, and requires the user to adapt the basic diagram types to fit the needs of standard modelling. In particular with reference to outlining the meta information gathered for each standard. As such this paper puts forward a simple proprietary format, geared towards the needs of standard analysis, supported by a tool to collate and analyse the data gathered.

### *A. SoS Standard Modelling*

The methodology proposed allows stakeholders to construct diagrams to explore a number of different types of standard interaction within a SoS. Consistency of view between stakeholders within an organisation, or across organisations, is a goal to aim towards through discussion, and is unlikely to emerge immediately.

The most abstract view proposed for SoS modelling outlines the organisations involved and the standards they adhere to. At this level the intricacies of those interactions with regard to specific systems are not examined, instead focusing on the examination of standards that cover entire organisations. Some of the standards seen at this level of abstraction may affect multiple organisations within the SoS, or shape the environment of the SoS in whole or part (for example, in the case of laws). Within a SoS that inhabited a single country such as the United Kingdom it is probable that laws such as FOI (Freedom of Information) or DPA (Data protection Act) would apply. Certification standards such as the ISO 9000 family can also be applied to entire organisations. In this instance there are interesting consequences for organisations engaged in SoS interactions, in that systems engaged, even in a temporary manner must meet the same standards as other ISO 9000 family certified processes within an organisation.

Once issues relating to standards covering entire organisations have been discussed, the SoS can be decomposed to explore more complex interactions at different levels of abstraction. The following list shows the decomposition diagrams that have proven useful so far during discussions:

- Decomposition by system to explore the interactions between organisational standards, and the standards applied within systems shared between multiple organisations. This aspect is not explored within this paper, as the Nimrod example contained largely 'siloed' systems which operated almost entirely independently of one another.
- Further decomposition of SoS member organisations by hierarchy (into departments / divisions such as Finance, Marketing etc)
- Decomposition by area of concern across the SoS (Manufacturing, Customer relations etc). This may show conflicting use of standards within shared activities across a SoS
- Decomposition by geographic location. By decomposing by geographic location aspects relating to the effect of national laws, regulations formed by regulatory bodies etc can be explored.

The visual modelling notation proposed contains only organisations, systems, links (which can be annotated with meta information regarding type) and standards. Dependent on the area being modelled however, it may be useful to visually annotate the modelling notation with additional information to guide discussions. For example, to indicate which systems interact directly, whether there are common interests / goals, the flow of products or information between systems etc. Rather than constrain the end users of the methodology such additions are not currently standardised within the graphical notation, this area will be explored as part of future work in the area in consultation with industrial end users. In order to make best use of the diagrams produced, tool support has been designed to monitor the consistency of diagrams.

The following list outlines the meta information attached to the graphical representation of an individual standard:

- **Type of Standard**
  As outlined in section II: Sponsored, unsponsored, de-jure, de-facto.
- **Enforcement processes in place**
  Standards are only useful when followed with rigor, evidence that an organisation performs periodic tests / reviews is an important consideration.
- **Party responsible for adherence**
  Is the organisation responsible for checking its own compliance, or is that in the hands of another organisation, regulator or independent third party?
- **Evidence of adherence to the standard**
  An important consideration in the building of trust.
- **Support systems in place**
  To facilitate communication, documentation, training etc.
- **Training provided**
  The use of both internal and external standards is weakened through poor training. Although 'on the job' training in situ has an important role in experiential learning, there has to be support in place to recover from problems caused by lack of experience [24].
- **Coverage of a system**
  Standards could cover countries, industries, companies, departments, areas of concern or individuals. By exploring where standards abut in a SoS, and analysing the system for risks associated with gaps in standard coverage across a SoS, a more dependable SoS configuration can be maintained.
- **Responsibility for maintaining and updating standards**
  With reference to external national and international standards, the role of maintainer could be held within the organisation that originally developed the standard, or in the case of standards embodied as laws it could rest with a national government / regulatory body.
- **Process in place to support the evolution of individual standards, and the evolving use of standards within a given system?**
  The role of maintainer within an organisation is necessary in the case of external international standards in order to ensure that the organisations processes adapt to changes within the standards themselves. In the case of standards embodied by laws such as the DPA there could be a legal imperative to roll out changes rather than a mere business / economic one.
- **What applicable standards are not in place, and for what reasons?**
  Many standards overlap; many have near duplicates, even within the same standards organisations. For example, differences between ISO 12207 and IEEE 12207[25]. Standards should be followed or not

followed for justifiable reasons (even if this is that a given standard has been embedded within an organisation for a long time).

Fig 2 outlines an example based on the organisations operating within the Nimrod SoS. As with many SoS, the organisations included are not wholly contained within the SoS, having significant work outside the SoS. This shows the implausibility of standard homogenisation at the organisational level. The SoS diagram has been annotated with additional data to show the links between organisations, in this case the flow of communication and contractual obligation between them. In particular it shows part procurement flow between the MOD and Cellular, and the role of BAE systems in fitting the parts supplied. A number of important points can be noted, some of which appear clear when represented graphically.

- Cellular were not CAA (Civil Aircraft Airworthiness) accredited to manufacture parts for aircraft.
- Upon further investigation it was determined that contractor B provided Taunton Aerospace with only a subset of the requirements mandated by MOD quality standards, and that in turn Taunton Aerospace only mandated ISO9002 compliance in Cellular.
- By sub contracting to organisations that were not ISO9000 series compliant, the MOD took a risk that the work processes followed by those sub-contractors would be of a sufficient standard. The limited disclosure of information within the inquiry report may have obscured whether the other contractors were in fact compliant with ISO9000, however, the fact remains that the MOD had little of knowing whether this was the case, depending on the next sub contractor down the line to check the standards of those they were sub-contracting to.
- It was reported that although contractors A & B were certified to manufacture parts, they did not take on the role of testing parts they had sub-contracted, relying on the sub contractors own internal testing. This raises an interesting point regarding how sub contracted work is checked against the standards of its contractor.

Although incomplete, the information here is typical of the type of data that is likely to be available at this level when dealing with a decentralised control structure. It highlights questions that need to be asked, many of which may, on further examination reassure rather than highlight the need for change. However, where answers cannot be provided it shows the need for further investigation.

Fig 3 provides an example of an organisational breakdown of the MOD with regard to Nimrod part procurement. Within the diagram the term IPT refers to Integrated Project Teams, socio-technical systems containing personnel, processes and capabilities tasked with specific operations within the MOD.

The convoluted nature of interactions within the MOD is believed to have weakened the awareness of those involved. The parts were contracted through Medical & General stores IPT for Nimrod IPT, however, Medical and General were non specialists who relied on the Air Commodities IPT to deal with technical matters pertaining to quality control with regard to contracting.

A decision was made to test samples of parts a number of years before the explosion by Nimrod IPT & Air Commodities (who asked BAE to look into the matter). BAE reported they did not have the facilities to perform the required tests in full, but that the limited tests they could do did not indicate a problem. Interestingly, this statement halted further testing. It is plausible that by having two different IPTs responsible for ensuring safety standards were adhered to, neither was clear on their responsibilities. It was reported that Nimrod IPT staff were undertrained, and placed significant blind trust in BAE. In doing so they

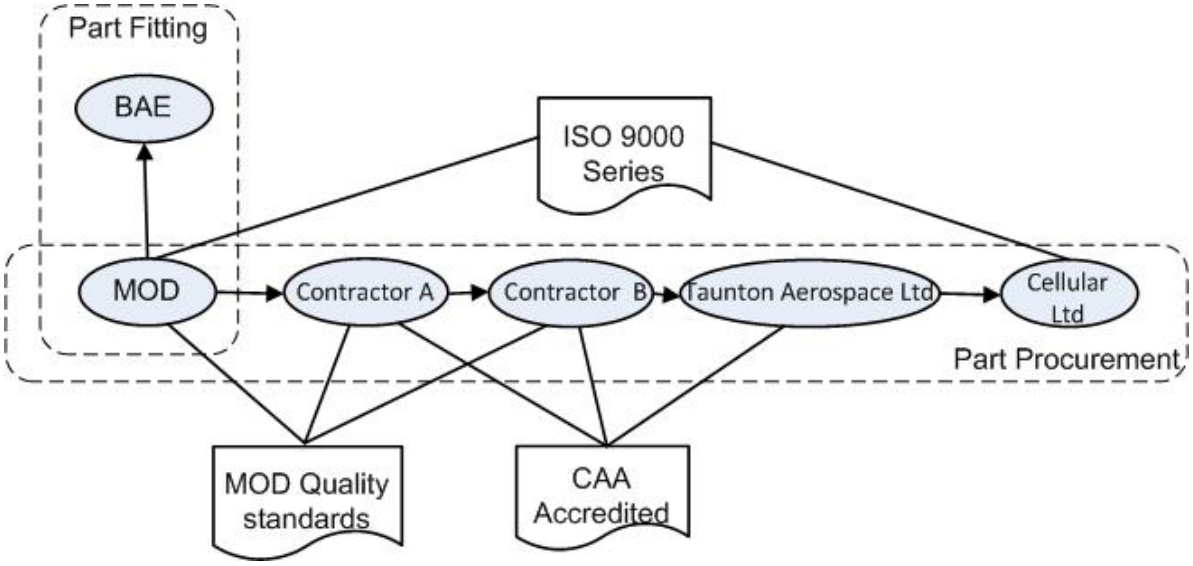


Figure 2: SoS Standard Modelling within Nimrod

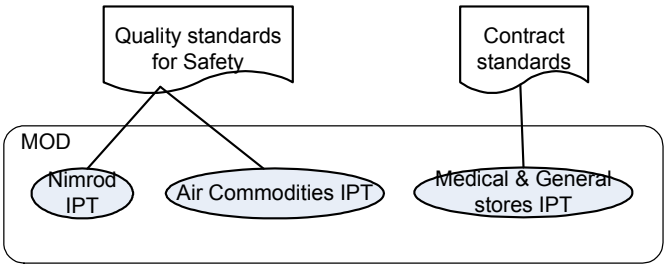


Figure 3: Breakdown of MOD

actually broke their own internal standards, in particular by not assigning an independent safety advisor. Throughout the Nimrod report there are indications that although in theory significant quality controls were in place, they were not followed, nor was adherence checked in others, and that many of the organisations involved within the supply chain did not follow their own internal procedures.

Fig 4 illustrates a subset of the standards to which Nimrod operation was supposed to adhere. In this instance the socio-technical system in question included the aircraft themselves, aircrew and maintenance staff responsible for keeping the aircraft operational, and the procedures they followed.

Changes to the makeup of the SoS responsible for keeping Nimrod operational compounded standard adherence issues. It is clear that the original design for Nimrod breached design regulations at that time; in particular AvP (Aviation Publication) 970, the military version of BCARs (British Civil Aircraft Requirement), to which the commercial airliner was originally certified. However, continued improvement and change to the design over the next 40 years did not rectify this, partly because the risks associated with changes did not take into account the wider picture of the state of the design, effectively assuming the design must have met earlier standards without further investigation. A change considered and analysed in isolation without considering the wider environment can be a dangerous move.

The Falklands war gives a prime example of how sudden evolution can affect standard adherence. During the war Nimrod aircraft were modified for in-flight refuelling, despite the fact that this modification involved breaking Defstan (Defence Standard) 00-970. After the war modifications were made permanent, however the report criticized BAE for not recognising during this remedial work that the original modifications breached Defstan 00-970. The evolution of systems, and their retro-fitting with current standards is also a significant issue which in Nimrod led to a number of breaches, which at first glance appeared to comply with the relevant standards.

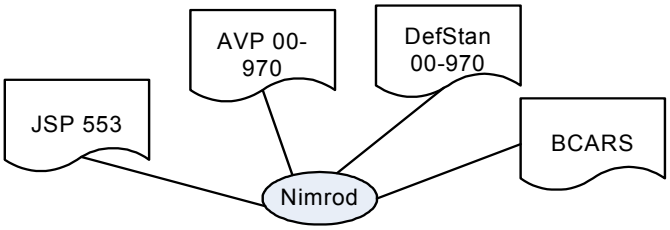


Figure 4: Nimrod operating & design standards

MOD standards dictated the use of Safety Cases in analysing the risks associated with aircraft operation within JSP (Joint Service Publication) 553. However, the Safety Case developed contained a number of serious mistakes which were at the time overlooked. The inquiry report stated the Safety Case was "riddled with errors". Part of the reason for this was the relative inaccessibility of the information system (CASSANDRA) in which the safety case was stored. The information stored within CASSANDRA was not considered portable, and was stored statically at one location (a site in Chadderton). The proprietary format, and licensing issues caused some degree of difficulty for the investigation even during the inquiry. The Safety Case itself was rushed, and those who depended on it had no way of knowing this. This example illustrates the difference between following the correct procedures and following the procedures correctly, and shows the importance of ensuring sufficient checks are in place. In this instance the poor quality of the JSP553 standard itself in prescribing the processes that needed to be followed, was partly to blame for this.

This paper argues that many of these issues would have been picked up if the questions posed within the previous sections had been asked at the time.

### *B. Risk Analysis*

In addition to the discussion format of graphical notation with accompanying questions, a risk analysis method is put forward which draws on the information gathered. Risks associated with the use and proposed use of standards within organisations can be categorised as follows:

- Risks relating to the potential use of standards in the future (proactive)
- Adequacy of adherence (quality of use in terms of training, disciplinary action etc)
- Risks related to transfer (handover) between standards during work processes (both proactive and during operation)

HAZOPS tables are constructed by bringing together a number of HAZOPs clauses which each explore one particular area of concern. A HAZOPS clause has the following structure:

**Standard**: The standard being analysed
**Category**: Potential use / adequacy of adherence / transfer Risk
**Keyword**: Early / Late / Never / Insufficient / Incompatibility

Table 2: Risk analysis of subset of problems identified

| Standard (s) | Category & System | Keyword | Risk (severity-probability | Consequences | Actions |
|---|---|---|---|---|---|
| DefStan 00-970 | Adequacy of adherence, Nimrod operations | Insufficient | Severe, Medium | Issues related to assumptions made by others, potential safety breaches | Re-evaluation |
| JSP553 | Adequacy of adherence, Nimrod operations | Insufficient | Severe, Medium | Safety case may be invalid | Examine Safety Case |
| ISO9000 | Adequacy of adherence | Never | Severe, High | If MOD procedures do not check, they cannot know if sub-contracting breaks this | Monitor sub-traction process more tightly |
| BCARS to AvP 00-970 | Transfer risk | Incompatibility | Severe, High | BCARS civilian standard and military AvP 00-970 contradict | Investigate issues and rectify where necessary |

**Risk**: The severity & probability of occurrence (if applicable)
**Consequences**: What would or could this situation lead to
**Actions**: How could this be avoided in future, and what actions would be taken if this did occur

Table 2 highlights a few of the issues that have been explored within this paper showing how, through methodical investigation, the problems could have been highlighted and dealt with through suitable risk analysis.

## IV. FUTURE WORK AND CONCLUSIONS

In the future this research will be further developed through the extension of the current tool prototypes developed within Visio, to allow integration with other systems modelling tools including UML, SysML, Responsibility modelling etc. This area is important as the methodology currently calls for the re-modelling of information that may already exist within given organisations. The research will be extended through an upcoming EPSRC grant application, designed to further develop and test the methodology put forward within real world organisations.

In conclusion, the area of standard use within SoS is complicated by the inherently decentralised and competitive nature of many SoS. However, although it remains a challenge for those who manage SoS, the application of best practice, in combination with suitable modelling and analysis, can offset much of the risk associated with standard use in this context. The paper has put forward a workable methodology for discursive analysis of standards specifically within SoS; and through the use of a real world running example has grounded the concepts discussed to show how they could discover and prevent real world problems.

## REFERENCES


[1] Brian Sauser and John Boardman, "System-of-Systems Engineering Management: A review of Modern History and a Path Forward," *IEEE Systems*, vol. 2, no. 4, pp. 484-499, 2008.

[2] Stephen C. Cook, "On The Acquisition of SoS," in *INCOSE 2001 Annual Symposium*, Melbourne, Australia, 2001, p. 9,

[3] (2010) The Defense Acquisition Handbook. [Online].

[4] Annette J Krygiel, *Behind the Wizard's Curtain*.: National Defense University Press, 1999.

[5] Abd-El-Kader Sahraoui, Dennis M Buede, and Andrew P Sage, "Systems Engineering Research," *Journal of Systems Science and Systems Engineering*, pp. 319-333, September 2008.

[6] E L Trist, "The Relations of Social and Technical Systems in Coal-Mining," in *British Psychological Society*, 1950.

[7] Enid Mumford, *Sociotechnical Systems Design: Evolving Theory and Practice*. Manchester: Manchester Business School and Centre for Business Research, 1985.

[8] Tom Boyle and John Cook, "Towards a Pedagogically Sound Basis for Learning Object Portability and Re-use," in *18th Annual Conference of the Australian Society for Computers in Learning in Tertiary Education*, Melbourne, 2001, pp. 101-110.

[9] Mark W Maier, "Architecting principles for System-of-Systems," *System Engineering*, vol. 1, no. 4, pp. 267-284, 1999.

[10] D Clausing, "Reusability in product development," in *Engineering Design Conference '98*, London, 1998, pp. 57-66.

[11] Charles Haddon-Cave QC, "THE NIMROD REVIEW," 2009.

[12] Stanley M Besen, "The European Telecommunications Standards Institute: A preliminary Analysis," *Telecommunications Policy*, pp.

521-530, 1990.

[13] Jane K Winn, "US & EU Regulatory Competition in ICT Standardization Law & Policy," in *4th International Conference on Standardization and Innovation in Information Technology*, 2005, pp. 281-291.

[14] Robert Axelrod, Will Mitchell, Robert E Thomas, Scott D Bennett, and Erhard Bruderer, "Coalition Formation in Standard-Setting Alliances," *Management Science*, pp. 1493-1508, 1995.

[15] Stango, Victor. Federal Reserve bank of Chicago., "The economics of standard wars," *Review of Network Economics*, vol. Volume 3, no. 1, 2004.

[16] Lynne Markus, Charles W Steinfield, Rolf T Wigand, and Gabe Minton, "Industry-Wide Information Systems Standardization as Collective Action: The Case of the U.S. Residential Mortgage Industry," *MIS Quarterly Special Issue*, vol. 30, pp. 439-465, August 2006.

[17] Onora O'Neil, *A question of trust*. Cambridge: Cambridge University Press, 2002.

[18] Alexander Hellemans, "Manufacturing Mayday," *IEEE Spectrum*, pp. 10-14, January 2007.

[19] Tineke M Egyedi and Petra Heijnen, "Scale of Standard Dynamics in JTC1," *The 4th Conference on Standardization and Innovation in Information Technology* , pp. 71-93, 2005.

[20] Russell Lock and Ian Sommerville, "Modelling and Analysis of Socio-Technical System of Systems," in *ICECCS*, Oxford, 2010, p. 9.

[21] Trevor A Kletz, *HAZOP and HAZAN, Identifying and Assessing Process Industry Hazards*, 4th ed.: The Institution of Chemical Engineers, 2006.

[22] Russell Lock, Tim Storer, Ian Sommerville, and Gordon Baxter, "Responsibility modelling for Risk Analysis," in *ESREL*, 2009, pp. 1103-1109.

[23] Edward R Tufte, *Visual Explanations: Images and Quantities, Evidence and Narrative*. Cheshire, Conneticut: Graphics Press, 1997.

[24] Paul R Sparrow and D R Davies, "Effects of Age, Tenure, Training, and Job Complexity on Technical Performance," *Psychology and Aging*, vol. 3, no. 3, pp. 307-314, September 1988.

[25] Mark De Chazal, *PhD Thesis: The development and use of a toolset for industrial IT portfolio management*. Loughborough: Loughborough University, 2004.