The Impact of Technical Regulation on the Technical Integrity of Complex Engineered Systems

Michael Edwards
Defence and Systems Institute, University of South Australia / Raytheon Australia
Michael.Edwards@postgrads.unisa.edu.au / medwards@raytheon.com.au

Abstract. The explicit aim of the application of technical regulation is to ensure that the requisite Technical Integrity of the developed system is achieved. Technical Integrity encompasses fitness for service, system safety and minimised environmental impact. The beginnings of a program of research to test the hypothesis that "The application of technical regulation yields improved technical integrity of the complex engineered system" are established. It is shown that only the intended emergent properties of a complex engineered system and its unintended hazards are directly addressed by technical regulation. A candidate set of measures to assess technical integrity is proposed. The methods that may enhance technical integrity of complex systems are reviewed. The degrees to which technical regulatory frameworks actually enforce methods known to have a contribution to technical integrity are also reviewed resulting in a list of corollary questions to be considered by future research.

Introduction

"Technical Integrity" is the term used to encompass the concepts of a system's fitness for service, safety and compliance with regulations for environmental protection, i.e. its compliance with technical standards and the minimisation of unintended consequences. The explicit aim of the application of technical regulation is to ensure that the requisite technical integrity of the system being developed is achieved. The implicit assumption is that in the absence of any technical regulation the requisite technical integrity may not be achieved.

Current and future technological systems are steadily increasing in complexity, both in terms of technology employed and the interactions they have with users and other stakeholders. Defence systems in particular are increasingly required to not only introduce higher organic capabilities within the system itself, but also to integrate into systems of systems to enable capabilities with higher performance across a wider spectrum of domains and environments. At the same time, the need for these systems to achieve ever increasing levels of technical integrity is paramount. Systems are expensive to develop and sustain, therefore there are less of them and each one that is realised must achieve higher and higher levels of availability and dependability. The stakeholders of the system, not least the general public (and consequently the political leaders of the nation) are less and less willing to accept mishaps – be they accidents to personnel, loss or damage of equipment or impacts to the natural environment.

Technical regulation seeks to provide more assurance to the acquirers and ultimately the users of engineered systems than just a reliance on system developers to unilaterally apply the "best" engineering and management processes. "Best" for a developer does not necessarily lead to a set of practices that will yield the required technical integrity. Engineering practices, like Systems

Engineering for instance, do not alone assure technical integrity goals are a primary focus or that the processes will be executed by competent professionals with explicit responsibility for their design decisions and the system outcomes. Technical regulation therefore generally attempts to assure that development is conducted to approved standards, by competent individuals in an organisation that is authorised to do so. There is also an explicit process to achieve certification; at a minimum by the developer formally attesting to the completeness and quality of its own work, but usually also encompassing some independent validation of the developer's claims of compliance with technical standards and processes.

It would be expected then, in some average sense at least, that the technical integrity of systems developed by an organisation outside an explicit technical regulatory system would be less than that developed inside a technical regulatory system. Indeed, this is accepted as a truism in the context of complex engineered systems for the Australian Defence Force (ADF) where acquisition and development under a Technical Regulatory Framework is now mandated for all procurements of defence materiel (ADF 2002).

The author is undertaking a program of research to test the hypothesis that "The application of technical regulation yields improved technical integrity of the complex engineered system". In particular the research intends to primarily consider the acquisition and development of complex engineered systems in the ADF context.

This paper defines a framework in which this research is intended to be conducted. It outlines the scope of technical regulation to be examined; it defines technical integrity and to establish limits to the research, defines the range of complex engineered systems of interest and current considerations in the development of these in the ADF context. Some initial research questions are posed and explored including the relationship of the emergent properties of complex engineered systems with technical regulation, it considers what set of measures may be appropriate for determining the technical integrity of a complex engineered system.. It also examines what engineering methods and related factors have been shown to or at least accepted as contributing to enhanced technical integrity of complex engineered systems. Finally it begins to establish the extent to which technical regulation enforces these methods.

Background

What is Technical Regulation?

In the ADF context, Technical Regulation is the means employed to assure technical integrity of materiel. The principles of technical integrity embodied in DI(G) LOG 08-15 (ADF 2002) are illustrated in Figure 1.

As a point of comparison, the development of civil aircraft and their systems are also governed by technical regulation. Airworthiness certification, as it is called by most national regulatory bodies is "the systematic process, during the design of an aircraft or airborne system of demonstrating conformance to a set of specific and predetermined airworthiness regulations (eg FAR 25) for a specific type and category of aircraft." (Kritzinger 2006).

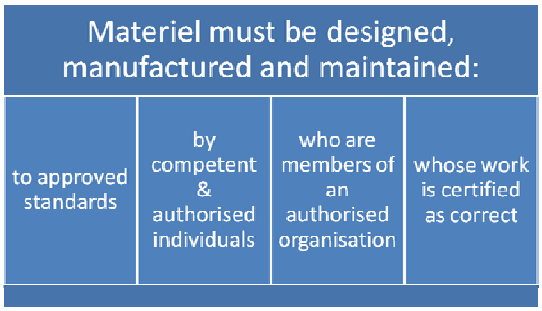

Figure 1. Principles of ADF Technical Regulation

What is technical integrity?

Technical Integrity is "An item's fitness for service, safety and compliance with regulations for environmental protection" (ADF 2002). The elements of technical integrity are shown in Figure 2 and are defined as:

- Fitness for service. "The materiel's ability to satisfy operational requirements. Hence it is a subset of technical integrity" (ADF 2002).
- Safety: "Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment". (DoD 2000, MIL-STD-882D)
- Environment Protection: Poses no hazard to the environment.

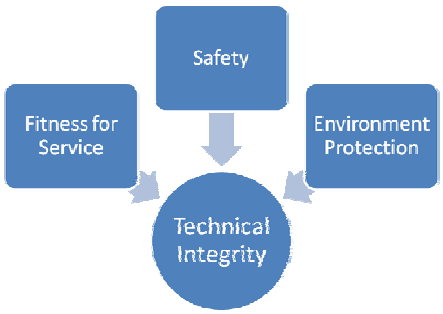

Figure 2. The elements of technical integrity.

Influence of Technical Regulation on Technical Integrity

Technical Regulation is established as a means to assure technical integrity of developed systems and materiel. Figure 3 provides an influence diagram that summarises the key concepts. A technical integrity gap exists where the technical integrity being achieved by systems is less than that desired. It may be that extant systems have some performance or effectiveness (fitness for service) shortfalls, or have incurred accidents or environmental impacts that are beyond what can be tolerated by the users and stakeholders of the system. This gap influences the adoption of technical regulation as a means of achieving the requisite technical integrity. Technical regulation in an ADF context, requires that approved specifications and standards be in place for development, that development be conducted by competent individuals, working in authorized

organizations and that all work is certified to be correct

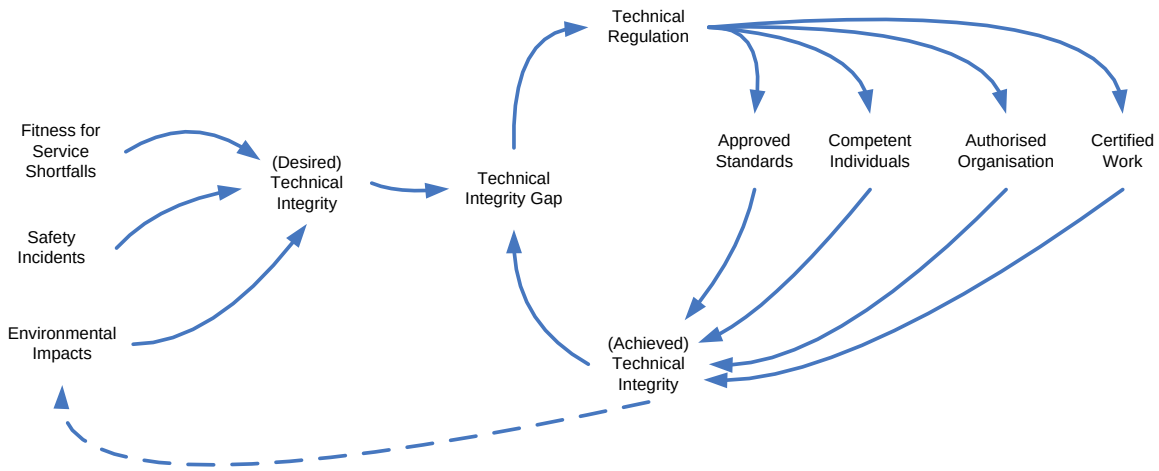

Figure 3. The influence of technical regulation on technical integrity.

Technical regulation is actualised by certifications which attest to the implementation of the regulations:

- The specifications developed to define the acquisition project must be certified as complying with the required standards (the list of required standards is usual maintained by a regulatory body). This certification is normally provided by the regulator (e.g. by endorsement of the specification and the plan for certification of the system).
- Secondly, the supplier must be certified as being competent to undertake the design, development and production of the system being acquired.
- Thirdly, the supplier certifies that delivered system has achieved the entire technical integrity requirement embodied in the specification.
- For significant mission and/or safety critical systems where the risks to technical integrity are reasonably high, a certification is generally required, usually by a party independent of the supplier, that the compliance claimed by the supplier has been verified (ie to provide assurance that the supplier's claim of compliance is valid).

Complex Engineered System Defined

The work of (Magee and de Weck 2002) attempts to classify a complex system as "a system with numerous components and interconnections, interactions or interdependencies that are difficult to describe, understand predict, manage, design and/or change." They also define an engineering system as "a system designed by humans having some purpose". Engineering systems are further classified as those with designed function that can transform, transport, store, exchange or control operands including matter, energy, information and value.

(DeRosa et al. 2008) assert that the essence of a complexity in engineering of complex systems is interdependence. Interdependence is where a reduction of components into a system's constituent parts is not alone sufficient to understand its behaviour. Behaviour is an emergent

property which changes as elements of the system are added, removed or rearranged. A system can be designed for intended emergent properties, but it is very likely that some unintended properties will also be created.

Of particular interest, is the definition of complex engineered systems that are part technology and part human – termed composite-information/decision/action (Composite-IDA) systems by (Hitchins 2003): “such systems operate at high stress levels, making great demands on operators and technologies not only for performance, but also for integrity and reliability in decision making”. In an ADF context, most Command and Control and weapons systems, which are of primary interest to the current research, fit well into this definition.

For the purpose of this paper then, a complex engineered system is defined to be a system that has been intentionally engineered from numerous components (technological (hardware and software) as well as human), each of which has several interconnections and is interdependent, yielding a system with both intended and unintended emergent behaviour. The primary interest therefore will be to determine measures for these emergent properties which can be considered to contribute to the technical integrity of the complex engineered system.

Complex Engineered Systems - Considerations in the ADF Context

The types of complex engineered systems of interest to this research include examples in the ADF like warship Combat Systems, airborne command and control, sensor and weapon systems, and ground based command and control systems for single service and joint operations. These may be compared and contrasted to similar systems in other services and complex systems like aviation systems, space systems and nuclear power systems in the civil sector.

As systems become bigger and more complex it is less feasible to design them from scratch. Rather, the current approach in the ADF context is to build and integrate systems from COTS/MOTS components in order to meet the objectives for the system. The system solution is therefore constrained by the MOTS components – not all initial objectives for the system may be met. But this is contrasted to a developmental solution where the attainment of system objectives may be constrained by the development cost and risk. Integration of a system from MOTS/COTS then, should be done with customer willing to be flexible in the requirements of the overall system - the vendors of the MOTS/COTS components are really driving a large fraction of the function, performance and technical integrity characteristics of the system.

Difficulties with designing and integrating the emergent behaviour and integrity of this type of system need to be addressed. These include the OTS design being relatively unknown and therefore difficult to establish its behaviour, faults and failure modes; addressing incompatibilities between interfacing products; products evolving over the systems lifecycle which may be beneficial or may become prematurely unsupportable.

How well does the technical regulatory system deal with these current trends in the development of more complex systems and systems of systems which increasingly are constrained by a philosophy of procuring MOTS components to reduce development risk?

Initial Questions and Concepts

What is the Relationship of Complex Engineered System Emergent Properties and Technical Integrity?

(Honour 2007) nominated a categorisation of emergent properties in two dimensions. Firstly "Designed" (ie intended emergent properties of the system) and "Surprise" (the potentially unintended emergent properties of the system). The second dimension encompasses "Useful" (desirable emergent properties), "Neutral" (neither desired nor undesired properties of the system) and "destructive" (undesirable properties of the system).emergent properties.

This framework has been extended in Table 1 to examine the relationship of each of the six categories of emergent properties with the extent to which technical regulation address the property.

Table 1. Categorisation of system emergent properties and the degree to which they are addressed by technical regulation.

EMERGENT PROPERTIES	**Useful**	**Neutral**	**Destructive**
Designed (ie intended)	Capability	Facts of Design	Accepted Trade-Off
Addressed by Technical Regulation	*Compliance – assuring that all desired capabilities are achieved.*	*Design is documented, understood and managed.*	*Risks to technical integrity are explicitly identified, minimised and residual risk accepted.*
Surprise (ie unintended)	Exploitable Feature	Facts of Existence	Fearful features (unanticipated hazards)
Addressed by Technical Regulation	*Not addressed*	*Not addressed.*	*Intent is that these are minimised or at least moved into an Accepted Trade-Off.*

Technical regulation clearly address the "Designed" range of emergent properties that a complex engineered system can exhibit. Capability is directly assured by efforts to assure compliance with requirements. Facts of Design: a focus on controlled engineering efforts, in particular configuration management and the adoption of systems engineering paradigms ensure the design is documented, understood and managed. Accepted Trade-Off: a technical risk management approach and in particular a focus on system safety engineering ensure that potential compromises to technical integrity are identified and made explicitly known to users and stakeholders of the system.

The "Surprise" ranges of emergent properties of the complex engineered system are not

addressed so comprehensively by technical regulation. Unanticipated hazards and other unwanted features are intended to be identified by system safety engineering efforts; these efforts, to the extent they are successful, really move identified unintended hazards of the system into the "Accepted Trade-off" category. The categories of Exploitable features and Facts of Existence are not really addressed by technical regulation. For instance, technical regulation does not explicitly seek to enforce methods or other means to identify, let alone promote the generation of exploitable features which may create a system of much higher value to stakeholders of the system.

In summary, technical regulation would seem to be focussed on ensuring the intended features are achieved, the design is documented and controlled, risks are accepted and that to the maximum extent possible, detrimental unintended behaviours are mitigated. There is no focus on measuring or maximising the beneficial, yet unintended, exploitable features of a complex engineered system. It would seem that there is great value in systems that have more beneficial features than were originally specified and these would be the features that would lend a complex engineered system to be evolved over its lifecycle. The lifecycle value of a system with more of these beneficial exploitable features should clearly be of more value to stakeholders than one with less. Such a system could be said to have a higher technical integrity than one that does not, all other factors being equal. Should technical regulation seek to operate in this space? Is it possible to mandate engineering methods that would seek this as a goal?

What can we measure to determine the Technical Integrity of Complex Engineered System?

It has long been accepted that there is no single overall measure for the quality or integrity of a complex engineered system (see for example (Boehm 1978)). "System Effectiveness" for a complex system, to the extent that it can be thought of as a partial proxy for Technical Integrity, most often appears to be a combination of capability, reliability and availability in a value hierarchy (Parnell, Driscoll, and Henderson 2008). A system effectiveness measure is usually constructed for supporting selection decisions between alternate systems. There is little in the way of comparative measures available to compare the utility of disparate systems.

In order to test the hypothesis of this research, it is necessary to settle on a set of measures that directly indicate the technical integrity of the emergent properties of the system. The measures need to be general enough so that they are applicable to across the class of systems of interest and be able to be supported by quantitative or qualitative data that can be practically obtained for those systems.

(Hitchins 2003) nominates a set of common candidates for measuring the value of a system. His candidates include: life cycle cost; efficiency; effectiveness; performance; availability; survivability; process (e.g. simplicity, resource consumption, ..); product ((e.g. utility, quality, fitness for purpose, …); entropy (the degree of disorder in the system).

(Barbacci et al. 1995) provide a useful set of software quality attributes encompassing performance, dependability, security, and safety. The subsequent methodology for determining the required quality attributes for a development, Quality Attribute Workshops (Barbacci et al. 2002), allows for the attributes to be developed for each system.

Table 2 presents an initial list of candidate measures to indicate the level of technical integrity achieved by a system. Potential sources of data to evaluate these measures are also included. It is

intended to mature these measures over the course of the research.

Table 2. Measures for Assessing the Technical Integrity of a Complex Engineered System.

Technical Integrity components	Candidate measures	Sources of Data
Fitness for Service The materiel's ability to satisfy operational requirements	Meeting operational requirements: • Compliance • Latent defects • Achieved performance • Other characteristics of the system: o Availability o Dependability o Robustness	Project verification records Project latent defect claims Results of operational evaluations In service RMA data
	Other attributes of a system that could be direct or indirect measures of technical integrity: • System operator satisfaction levels • Other stakeholder satisfaction levels • Public perceptions • Rate of problem reports discovered after acceptance	Operator surveys Stakeholder surveys Government committee reports. Press articles. In service trouble report records; warranty and latent defect records.
Safety Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property	Freedom from hazards: • Accident rates • Accident severity • Incident (near miss) rates	Accident and incident databases. Accident and incident investigation reports.
Environment Poses no hazard to the environment	Compliance with environmental standard Freedom from environmental impact • Environment incident rates • Environment incident severity	Environment incident databases. Environment incident investigation reports.

A gap in the available literature is the lack of a theory for developing a composite measure of technical integrity of a complex engineered system. Such a theory would, as a minimum, provide a ranking scale of technical integrity for a particular class of complex systems. Ideally the theory could provide a ratio scale for a composite technical integrity measure and this measure could be

used to compare and relate the technical integrity over a broad range of complex engineered systems. Value modelling (Parnell, Driscoll, and Henderson 2008) and conjoint measurement (Anon. 2009) are possible bases for the development of such a theory. Conjoint analysis techniques, in particular techniques for establishing preference functions and for conducting surveys of stakeholders (Gustafsson, Herrmann, and Huber 2007), also require examination.

What do research findings and heuristics point to as being the best methods for achieving Technical Integrity of a Complex Engineered System?

(ISO/IEC 26702 IEEE Std 1220-2005ISO/IEC 26702 IEEE Std 1220-2005 2007) is the current standard concerning the development of man-made systems that include one or more of hardware, software, human processes, procedures, facilities and entities in the environment. It forms the current accepted practice for the engineering of all such systems including the complex engineered systems of interest to this research. While the defined systems engineering processes (requirements analysis and validation, functional analysis and verification, synthesis, design verification, systems analysis and control) are not in dispute as being required for a successful system implementation project, there is no indication in the standard as to their relative priority or the contribution each process may have to the technical integrity of a complex system.

(Elm 2008) has conducted research that indicates which systems engineering processes have the strongest positive relationship to program performance. Technical Integrity is at least partly a subset of Program Performance (includes customer satisfaction, budget performance and schedule performance) as defined in Elm's research. The systems engineering processes that have a higher positive relationship with project performance than the SE capability as a whole are "Architecture", Trade Studies", "IPT Capability" and "Requirements Development and Management". (Boehm, Valerdi, and Honour 2008) also report evidence that the right level of systems engineering applied to a project, increase the likelihood of the project running to cost and schedule budgets, but generally treats technical performance or integrity outcomes as invariant (ie implicitly assumes they are achieved at completion of the project). However, this is rarely the case in practice. Many projects are deemed to be "complete" not having achieved all technical requirements and having to have accepted unresolved risks to technical integrity.

(McDermid 2001) suggests that rigour in engineering process is perhaps not the dominant contribution to the production of complex systems with the requisite technical integrity, but that relevant experience and competence of the designer is: "For airborne software developed to DO-178B, there seems little evidence that the more rigorous processes applied in software development for software of higher required Software Integrity Levels (SILs) actually yield a lower hazardous failure rate. The limited data does suggest that the most significant correlated factor in producing software with lower hazardous failure rates is domain experience. This is most linked to the consequent reduction in initial requirements errors that domain experience would bring."

(McDermid 2001) also casts doubt on the ability of some of the engineering standards to directly contribute to the assurance of technical integrity: "Do the software safety standards actually address safety issues? They seem to be mostly focused on quality and repeatability. You would think they would aim directly at potentially hazardous failure modes of the software. An evidence-based approach is proposed – eg provide analysis to show that data structures can never

be corrupted; that a scheduled function can always run on time." It would seem that this criticism could be readily extended to systems engineering standards and even to the technical regulations and their supporting manuals – quality and the repeatability of process seem to be a primary focus rather than the imposition of particular management and engineering measures to attain technical integrity.

The prevalent view in the Australian defence industry at present remains that technical integrity can be assured through the use of systems engineering methodologies but "The Systems Engineering discipline remains intrinsically tied to the individual skill, competence and notably the availability of senior systems engineers on projects" (Irving 2008). This accepted thinking places a focus on experience and competence both at an organisational and an individual level.

(Sheard and Mostashari 2008) posit a set of 26 principles for complex systems engineering. They include the categories of Systems architecting-type principles, Systems analysis principles, Problem-space-relevant-principles, Configuration management principles, Coordination principles, and Management-related principles. While these principles are generally known or thought to be valid heuristics for the development of complex systems and would be expected to have a positive effect on the technical integrity of a complex system, there is currently little research evidence to confirm such a conclusion.

How well do the technical regulation frameworks in place in the ADF enforce these methods?

The main elements of the ADF's technical regulation is to enforces the development of systems to approved standards, the work is to be undertaken by competent and authorised individuals, who are acting as members of an authorised organisation and whose work is certified as correct (ADF 2002). As an example, Figure 3 shows the main elements of the Navy Technical Regulatory Framework (NTRF). This distils the main elements that must be implemented in the acquisition and development of maritime materiel for the ADF.

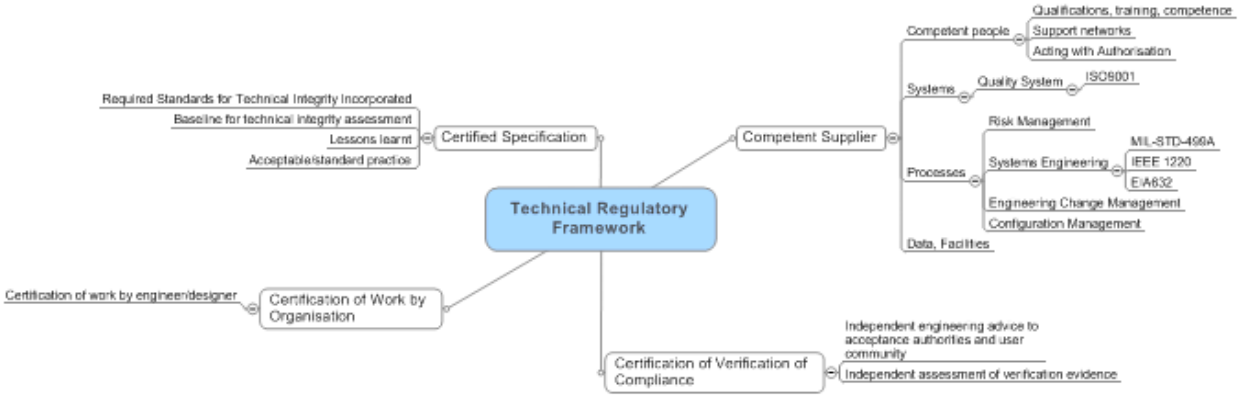

Figure 3. The main elements of the ADF's Navy Technical Regulatory Framework.

Table 3 takes the elements of the Technical Regulatory Framework highlighted in Figure 3 and provides an indication as to the extent that element is actually known (either through reported research evidence or compiled professional knowledge (e.g. standards)) to contribute to enhanced technical integrity outcomes for complex engineered systems.

Table 3. Elements of Technical Regulatory Framework and the Known Support for their contribution to Technical Integrity.

Technical Regulatory Framework	Support for Contribution to Technical Integrity
Competent Supplier	
• Competent people	Competency certifications assure minimum competency in place for significant design decisions. Certainly there are numerous case studies where the lack of competency has been directly linked to lack of required competency (eg HMAS Westralia). Also anecdotal evidence that the competence and domain experience of key designers is a determinant of project success. Not known if there is evidence that technical integrity is positively related to competent people.
• Systems (e.g. Quality System)	Standards like ISO 9001 capture industry wide knowledge. Certainly focuses on repeatability of processes to produce consistent products. Doe not focus specifically on technical integrity. Not known if there is direct evidence that technical integrity is positively related to quality systems.
• Processes	
Risk Management	The explicit consideration of risks to technical integrity embodied in the ADF Technical regulations does it would seem have to impose a mind set on the designers involved to minimise these risks. Not known if there is direct evidence that technical integrity is positively related to technical integrity risk management systems.
Systems Engineering	Standards like ISO/IEC 26702 capture industry wide knowledge for current projects. Research is beginning to provide evidence that the application of systems engineering process do contribute positively to project success and are worth the cost. Other research is indicating that the current processes requiring extension to cater for increasingly complex systems. The evidence for the relationship between these systems engineering processes and the technical integrity of complex systems is not yet established.
Configuration Management	Heuristics for complex system point out that CM must prepare for and accommodate design changes and design alternatives. The evidence for the relationship between the configuration management and the technical integrity of complex systems is not yet established.

Technical Regulatory Framework	Support for Contribution to Technical Integrity
• Data, Facilities	Research indicates that good decisions in complex situations are made on data (rather than instinct). It is therefore reasonable to extrapolate that data – correct and readily accessible to the designer – will allow good design decisions to be made. Not known if there is evidence that technical integrity is positively related to data, facilities and other supporting resource.
Certification of Verification of Compliance	
• Independent engineering advice to acceptance authorities and user community	Not known if there is support for this contributing to technical integrity.
• Independent assessment of verification evidence	Independent assessment is standard practice for high risk engineering work. Research indicates peer and expert review are effective means of eliminating defects in design.
Certification of Work by Organisation	
• Certification of work by engineer/designer	Not known if there is support for this contributing to technical integrity.
Certified Specification	
• Required Standards for Technical Integrity Incorporated • Baseline for technical integrity assessment • Lessons learnt • Acceptable/standard practice	Prescriptive regulatory regimes impose the list of standards that must be met to assure technical integrity. There are known issues (eg standards not able to keep up with pace of technology advances) and known benefits (available standards can embody previous lessons learnt) with the prescriptive approach. Not known if there is support to determine if there is any contribution to the technical integrity of complex engineered systems, which are typically unprecedented by requiring the use of extant standards.

Overall, it appears that there is a high level of experiential knowledge that the components of the technical regulatory framework support the attainment of technical integrity. They certainly seem necessary, but supporting evidence is generally scant in the literature. There is also no consideration is this analysis as to if they framework is a sufficient basis for technical integrity.

As mentioned previously in this paper, the technical regulatory framework does not address at all the attainment of emergent behaviour that may not have been intended but which is of benefit and value to the system. This is at best a nascent area of research.

Other considerations and questions that arise from this analysis that will need to be addressed by the intended research include:

Is certifying the specification any different from what standard SE standards require in terms of defining stakeholder requirements and formalising them before committing to development?

Is a supplier, as assessed as being competent under a technical regulatory framework, demonstrably better than one who isn't? Don't all suppliers of complex systems operate under an

ISO 9000 or equivalent quality system accreditation? Don't all suppliers of complex systems seek to hire, train and retain competent staff to maintain their effectiveness and therefore there commercial advantage? Don't they all assure their staffs are qualified in order to mitigate liabilities for errors in design and to minimise things like insurance costs?

Don't all suppliers of complex systems strive to improve their processes and methods to achieve competitive advantage (eg most high technologies are strongly committed to seek best practice under schemes like CMMI for competitive advantage more so than because it was an imperative established by technical regulation)?

Don't all suppliers of complex systems assure they have access to and control all requisite information? Indeed don't they assiduously guard this data to protect their trade secrets and other elements of competitive advantage?

What does the explicit certification of compliance by the supplier achieve? Is not the supplier otherwise committed to achieve compliance with the specifications embodied in a contract anyway? They are also compelled to meet legislative requirements for product safety and compliance with environmental protection standards?

Is the certification of verification of compliance really any different than the technical contract oversight that would usually be applied by an educated customer function? Is it really any different to the independent verification and validation processes that would normally be applied to systems that were clearly safety critical?

Can prescriptive standards, embodied in certified specifications, really be expected to be highly applicable to unprecedented complex engineered systems? Does this mean we may really be left with mandated standard engineering processes to try to assure the technical integrity of these systems?

Conclusion

A framework to research the hypothesis "The application of technical regulation yields improved technical integrity of the complex engineered system" has been established. Initial research questions have been raised and initial concepts developed. It has been shown that only the intended emergent properties of a complex engineered system and it unintended hazards are directly addressed by technical regulation. A candidate set of measures and sources of data to assess technical integrity have been identified and it is anticipated that these will need to mature as the research progresses. The need for a composite measure of technical integrity has been identified and future research is intended to create a theory that could provide a ratio scale for a composite technical integrity measure and this measure could be used to compare and relate the technical integrity over a broad range of complex engineered systems.

The methods that may enhance technical integrity that are available to the designers of complex systems have been reviewed. They are largely heuristic at this time. Where primary methods like systems engineering have been quantitatively assessed in the literature, their impact on the overall project's performance is assessed rather than the level of technical integrity achieved on the resultant system. The degrees to which technical regulatory frameworks actually enforce methods known to have a positive contribution to technical integrity have also been reviewed. This review has resulted in a list of corollary questions to be considered by future research.

References

ADF. 2002. Defence Instruction (General) LOG 08-15. . In *Regulation of Technical Integrity of Australian Defence Force Materiel*. Canberra, ACT, Australia: Department of Defence.

Anon. 2009. *Theory of conjoint measurement*. Wikipedia 2009 [cited 9 March 2009]. Available from http://en.wikipedia.org/wiki/Theory_of_conjoint_measurement.

Barbacci, Mario, Mark H. Klein, Thomas A. Longstaff, and Charles B. Weinstock. 1995. Quality Attributes. Pittsburgh, Pennsylvania: Software Engineering Institute, Carnegie Mellon University.

Barbacci, Mario R., Robert Ellison, Anthony J. Lattanze, Judith A. Stafford, Charles B. Weinstock, and William G. Wood. 2002. Quality Attribute Workshops. In *Architecture Tradeoff Analysis Initiative*. Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.

Boehm, Barry. 1978. *Characteristics of Software Quality*, *TRW Series of Software Technology*. New York: American Elsevier.

Boehm, Barry, Ricardo Valerdi, and Eric Honour. 2008. The ROI of Systems Engineering: Some Quantitative Results for Software-Intensive Systems. *Systems Engineering* 11 (3):14.

DeRosa, Joseph K., Anne-Marie Grisogono, Alex J. Ryan, and Douglas 0. Norman. 2008. A Research Agenda for the Engineering of Complex Systems. Paper read at IEEE International Systems Conference, April 7-10, 2008, at Montreal, Canada,.

DoD. 2000. MIL-STD-882D. In *Standard Practice for System Safety*: Department of Defense, USA.

Elm, J.P. 2008. A Study of Systems Engineering Effectiveness - Initial Results. Paper read at Systems Conference, 2008 2nd Annual IEEE, 7-10 April 2008, at Montreal, Canada.

Gustafsson, Anders, Andreas Herrmann, and Frank Huber. 2007. *Conjoint Measurement. Methods and Applications*. 4th ed. Berlin Heidelburg New York: Springer.

Hitchins, Derick K. 2003. *Advanced Systems Thinking, Engineering and Management*. Norwood, MA, USA: Artech House.

Honour, Eric C. 2007. Connecting an Architecture with its Emergent Properties. Paper read at Conference on Systems Engineering Research, 2007, March 14-16, at Hoboken, NJ , USA.

Irving, Ian. 2008. Emergent Challenges Facing Systems Engineering in the Defence Industry in Australia. *Systems Engineering Society of Australia Newsletter*.

ISO/IEC 26702 IEEE Std 1220-2005. 2007. In *Systems Engineering - Application and Management of the Systems Engineering Process*: ISO/IEC and IEEE.

Kritzinger, Duane. 2006. *Aircraft system safety. Military and civil aeronautical applications.* Cambridge, England: CRC Press, Woodhead Publishing Limited.

Magee, C. L., and O.L. de Weck. 2002. An Attempt at Complex System Classification. In *ESD Working Paper Series*: Massachusetts Institute of Technology, Engineering Systems Division.

McDermid, John A. 2001. Software Safety: Where's the Evidence? In *6th Australian Workshop on Industrial Experience with Safety Critical Systems and Software*. Brisbane, Australia: Australian Computer Society, Inc.

Parnell, Gregory S., Patrick J Driscoll, and Dale L Henderson. 2008. *Decision Making in Systems Engineering and Management*. Edited by A. P. Sage, *Wiley Series in Systems Engineering and Management*. Hoboken, New Jersey: John Wiley &Sons Inc.

Sheard, Sarah A., and Ali Mostashari. 2008. Principles of Complex Systems for Systems Engineering. *Systems Engineering*:17.

Biography

Michael Edwards holds a Bachelor of Engineering (Honours) and a Master of Engineering Science (Communications) from the University of NSW and a Master of Business Administration (Technology Management) from Deakin University. He is currently a part-time research student at the Defence and Systems Institute of the University of South Australia. He is a Fellow of the Institution of Engineers, Australia, a Chartered Professional Engineer, a member of the Systems Engineering Society of Australia, a Member of the Australian Institute of Program Management and a Master Project Director.

He is currently employed by Raytheon Australia where he is the Design Acceptance Representative for the RAN's Air Warfare Destroyer Combat System. His professional and academic interests build on an extensive experience base in the practice of engineering management and systems engineering largely in the domain of complex naval systems including applications in surface combatant and submarine combat systems, mine warfare systems, hydrographic systems and naval aviation systems.