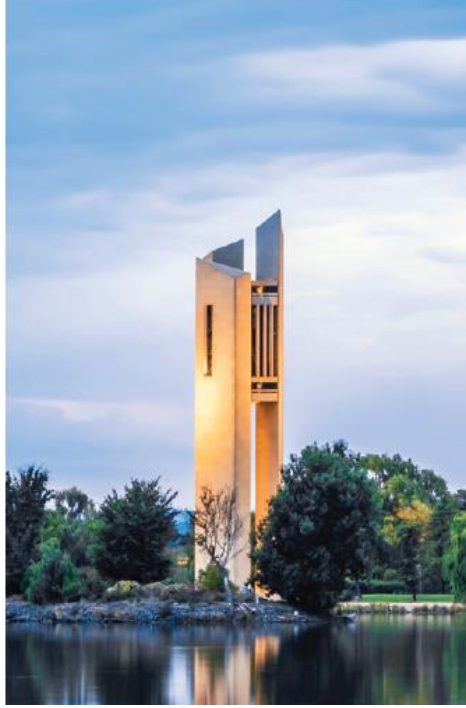
SETE
SYSTEMS ENGINEERING TEST AND EVALUATION CONFERENCE 2019
QT Canberra | Australia
29 April – 1 May 2019



SYSTEMS SCIENCE & ENGINEERING FOR A BETTER AUSTRALIA SETE2019.COM.AU

# Design Assurance based upon Goal Validation – How to Assure Designs without following the V

Scott Simmonds

# Introduction

- Classic Systems Engineering philosophy requires the verification of a design against its specification.
- However, what if there is no defined specification for a system ?
  - How is it possible to argue the assurance of a design that does not have a formally defined specification for its behaviour ?

# Introduction

- Particularly true of systems comprised of off the shelf components,
  - E.g. ICT systems
- We know we want a computer system or network, and it is comprised of off the shelf components
- It is possible to develop a specification for a such a system
- However frequently there are two principal constraints on doing this:
  - Being off the shelf components, often the customer is not understanding of the need to spend extra time and money on developing a specification for a (set of) products that already exist
  - Because it is comprised of products that already exist - why reinvent the wheel?
- Counter arguments to these constraints are usually overshadowed by the third constraint
  - the customer is spending their money and therefore is always right

# Systems Engineering

- Cornerstone of Systems Engineering philosophy –
  - Verification of a design against its specification and
  - Validation of the system against its articulated need

- AKA
  - “have you built it right” and
  - “have you built the right thing” (INCOSE 2014)

- “have you built it right” criteria frequently quoted in Technical Regulatory Frameworks
  - E.g. (former) Australian Defence Force Technical Airworthiness Regulations required an endorsed specification as one of the criteria for acceptance of a system in to service. (DGTA 2015)

# Problem

- Often when building systems comprised of COTS equipment, the need for a detailed system specification is considered a luxury in cost and schedule
  - after all, the system is COTS, right ?
- This view is surprisingly prevalent
  - Systems engineers will argue about perversion of the systems engineering process, and insist that the job *will* be done properly next time,
  - However, reality is that while financial considerations dominate the acquisition process – by which is meant – controlling the money – this situation will continue to occur no matter how many promises there are to "do it right next time“
- Usually followed by long discussions with the Group Technical Authority on how to provide a design certificate for a system with no formally agreed statement of need or system specification
  - (And promises to do it the "right way' next time)

# Question

- How can an appropriate amount of rigour be applied to the system development process so an “accepting authority” can reasonably accept the view the system being acquired suits their needs

- The question we are attempting answer, is
  - What can be done to minimize the risk of not providing a suitable system
  - Is simultaneously simple enough to perform within the available budget, and
  - Allows at least a claim of compliance with system technical integrity requirements

- Issue is particularly true in the sustainment phase of a system's lifecycle
  - In many cases, enabling systems are comprised of obsolete off the shelf ICT equipment

- We describe one means to support an assurance argument for system designs based upon presenting a goal validation argument

# Needs

- Many advanced mission systems utilized across Government, Defence and Industry are comprised of Off the Shelf ICT hardware, networks and storage systems
  - Increasingly large consumer of capital expenditure across these sector (Gardiner 2015; Jenkin 2018)
- Development of a detailed specification is not seen as necessary in the acquisition and deployment of these systems
- Does not mean some thought cannot be given to the capability needs the system is intended to address
  - Need to address the needs of the users, maintainers, designers and acquirers of the systems

# Requirements Failures

- There is a wealth of research and published material regarding failure of projects that don't generate a decent set of requirements
- Chaos Report by the Standish Group is considered a classic review of the effect of poor requirements on project success (The Standish Group 1994)
- Supplemented over the years by other research –
  - (Honour 2013) examines return on investment for systems engineering including the requirements phase;
  - Petrobras 36 is a shining example of a project with poor quality standards (NASA Safety Center 2008)

# Method

- Five principal steps in the process for producing a goal validation argument:
  - Identifying stakeholders and their concerns,
  - Goal determination,
  - Design/design rationale capture,
  - System development and
  - Generation of an accomplishment summary
    - articulates how the system satisfies the goals

- These steps are described in more detail in the following slides

# Stakeholder Analysis

- Some thought as to stakeholders involved in design, construction, use, and maintenance support of the system should be undertaken
- Can be simple or fairly extensive depending on the number of stakeholders and the level of interest, responsibility or effect the system will have on their interests

- Conduct a stakeholder analysis process where stakeholder concerns are described in:
  - short sentence form for each stakeholder, and
  - level of concern is suggested (Hilliard 2011; IEEE 2000, 2011)

  - e.g. CEO is not interested in details of the backup process, only that his capability is available and protected from loss,
  - whereas the CIO or system administrator is very interested in the backup details
    - Tape Library, the Cloud, paper printouts…

# Level of Concern

| Level of Concern | Explanation |
|---|---|
| Strategic | The "Big Picture", the capability provided by what the system enables and where it fits in the overall context of capability.<br><br>At this level, the concern is not the system as such, it is the provision of the capability to users. |
| Tactical | Ensuring the capability enabled by the system continues to provide timely and optimized support to the users.<br><br>Evolution of this capability over time. |
| Operational | Day to day operation of the system to provide support to the system users. |
| Physical | Physical artefacts – Hardware, Software, Interfaces |

SETE

ENGINEERS AUSTRALIA | SESA | INCOSE | SOUTHERN CROSS ITEA CHAPTER

QT CANBERRA | AUSTRALIA

29 APRIL – 1 MAY 2019

# Example ICT Stakeholder Concerns

| Stakeholder | Level of Concern | Concerns |
|---|---|---|
| CEO | Strategic | System Capability, System Capability Continuity, System Capability Evolution |
| CIO | Strategic, Tactical | System Capability, as provided by the System, System Capability continuity, System Capability Evolution |
| Section Lead | Strategic, Tactical | System Capability, System Capability robustness and continuity, Capability Evolution, System Strategic Evolution |
| Engineering | Tactical | Technical Integrity of System, Safety of the System as a system, System Capability Needs, Fitness for purpose, Control of engineering changes, System CCB Conduct |
| Logistics Support | Tactical | Supportability of the System through life, Obsolescence management, Spares, and Component repair/replacement, Warranty provisions, System refresh/replacement, Commonality with existing preferred equipment |
| IT Security | Operational | Security of systems and data from unauthorized access, Physical Security, Protection of systems and data from malicious attack (virus protection), User Account Management, Network Interconnection, Network Isolation, System Isolation, Network and System Logging, Intrusion Detection, Control of changes and change traceability, Compliance with security requirements, System Accreditation |
| System Users | Operational, Physical | Data Storage, Data Access (as required), Network Communications, Network Drive Mapping, User Authentication, Printing Services, Hardware Obsolescence, Hardware Performance, Software Obsolescence, Software Licensing, Software Configuration, Hardware Interfacing, Obsolete Hardware Failure |
| Administrators | Operational, Physical | Day to Day system operation, System Backup, Data Backup, Data Recovery, System Recovery, System Power Up, System Startup, System Shutdown, System Power Down, System Repair, System Maintenance, User Administration, Software Installation, Software Configuration, System Configuration, Network Configuration, System Performance, Network Performance, VM Creation, VM Management, VM Performance, Storage Space utilization, User Environment, Software Configuration, Hardware Interfacing, Obsolete Hardware Failure. |

# Concerns

- Concerns are  collected and like concerns are combined
- Concern is then re-expressed in question form,
  - additional questions added as required to clarify the actual concern of the stakeholder
- Questions are written (largely) in Who/What/Where/How form
  - E.g. who is performing backups, what hardware is required to perform backups, how will backups be performed, etc.
- For each concern question, a goal is stated. When the goal is achieved, it will satisfy the concern
- For example:
  - Concern: What hardware is required to perform backups ?
  - Goal: There is a need to supply hardware that can perform backups

- With goals identified, agents who are involved in providing the function that satisfies the goal can be identified
  - The goal can be further decomposed if required, and allocated to a particular views or viewpoints

# Concern to Goal Mapping

| Concern | Concern Type | Category | Goal | Stakeholder |
|---|---|---|---|---|
| Is there sufficient storage space available ? | Data Storage | Architecture | The system will need to provide sufficient storage space for user needs. | System Users |
| Is the amount of space available able to be expanded ? | Data Storage | Architecture | The system will need to have the capability to be expanded to add additional storage space as user needs for storage grow. | Administrators,<br>CIO |
| How are the drives mapped to the storage array ? | Drive Mapping | Architecture | The system will need to provide a means to map the logical drive structure to the storage array system, so that a regular hierarchy of drives, directories and data files can be implemented. | System Users,<br>Administrators |
| Is the hardware performance adequate to undertake the user tasks ? | Hardware Performance | Architecture | The system will need to provide adequate performance to the user, for them to undertake their computing tasks. | CIO<br>Section Lead<br>Administrators<br>System Users |
| Is the System able to maintain continuity of capability in the event of unforeseen circumstance ? | System Capability continuity | Architecture | The system needs to provide internally consistent protection against loss of capability due to external damage, or internal failure. | CIO<br>Administrators |

# Goals

- Goals of the system should be documented up front, even informally
- Even without a formal specification, capturing the high level goals sets the scene for eventual system acceptance

- Goal list might be comprised of attributes as follows:
  - The goal statement
  - The principal stakeholder and stakeholders who have an interest in the goal being achieved
  - Goal rationale – why do we need that goal

# Goal Analysis Methods

- There are a number of goal based requirements engineering approaches that can also be used
- For example:
  - Goal Oriented Requirements Language (Amyot et al. 2009),
  - i* (Yu 2009) and
  - KAOS (van Lamsweerde 2007)
- All provide a means to describe user and system goals

# System Design, Implementation

- While the requirements specification may be omitted from the list of deliverables, often there is an understanding that the system design needs to be captured
  - Often in a System Design Description or similar artefact

- Key questions that need to be answered in this context are:
  - What is the overall architecture of the system ?
  - What elements is the system composed of ?
  - What interfaces does the system have and use ?

- Here we can capture the allocation of goals to systems (noting this allocation may be implicit)
- This design activity drives system procurement and implementation

# Assurance Requirements

- Generally with off the shelf equipment, product is described by what may be termed a product specification, “Quick Spec” or similar high level system description
  - often this is closer to marketing material !
- Usually contains claims of compliance to a variety of industry standards
- Often are international standards which  may or may not have an Australian version or equivalent
  - If they only have an International or even foreign national standard against which to assess, then additional work may be required to assure acceptability in the Australian environment

# Technical Integrity

- A useful assurance concept for acceptance of systems and equipment into service is the concept of Technical Integrity
  - Originally defined in Defence Instruction DI(G) Log-4-5-12 – now cancelled but conceptually useful
- Comprised of three elements – Safety, Performance (Fitness for Service), and Environmental Compliance (Department of Defence 2013; Simmonds & Cook 2017)
- These elements are expanded more fully below

# Fitness for Service

- The system is Fit for Purpose;
- The system's configuration, use and maintenance is documented, indexed and traceable;
- Personnel have been trained and authorised in its use and maintenance; and
- A supply support chain has been established for parts, consumables, licenses, updates, OEM and specialist advice etc.
- In short, the system is ready to be used throughout its service life

# Environmental Compliance

- The Environment Protection and Biodiversity Act of 1999 (Commonwealth of Australia 1999) requires consideration of the impact on the environment
- This extends to the effect of systems on the environment across their whole lifecycle
  - For off the shelf ICT systems, generally provided by OEMs as a statement of environmental consideration, and may also include a recycling or material recovery program

# Safe to Own, Operate and Maintain

- Of the three elements of Technical Integrity, safety is perhaps the most analysed
  - Considerable literature, tools, techniques and standards which can be applied to systems that need to consider safety in their development
  - E.g. Def-Stan 00-56 and Mil-Std-882E are two principal Defence Standards (Ministry of Defence 2007; US Department of Defense 2012)

- An argument that a system is safe, supported by evidence describing how safety objectives have been achieved and in what context
  - For off the shelf ICT systems, evidence is generally provided as some form of statement of compliance of their product range against international safety standards

# Accomplishment Summary

- The Accomplishment Summary is used to provide reference to evidence supporting the satisfaction of a Technical Integrity argument
  - describes satisfaction of goals rather than requirements
- E.g. artefacts created during the development process:
  - System Design Description – used to capture high level or detailed architecture and rationale for design decisions
  - Build standards, hardware and software installation instructions
  - Objective Quality Evidence may exist capturing results of informal or formal testing E.g. screen captures seem to be popular in ICT

- Intent is to provide sufficient evidence that will ***satisfice*** a reviewer (customer, design acceptance authority) that
  - The system has been designed, built and verified to the extent necessary to argue goal satisfaction

*Satisfice - permit satisfaction at some specified level, generally considered not optimal, but some lesser but acceptable path (Simon 1956)*

# Design Goal, and Goal Satisfaction Argument

| Design Goal | Goal Satisfaction Argument |
|---|---|
| 1. The system is a Virtual Windows Server Environment. | The system implements a virtualisation environment comprised of hardware and software that provides a virtualisation capable system, with adequate processing, memory, storage and network capacity. |
| 2. The system is composed of off the shelf hardware and software. | The Virtualisation Environment is comprised of COTS Information and Communication Technology (ICT) equipment, procured through direct commercial sale from Original Equipment Manufacturers (OEMs) (or their authorised agents) and supported under commercial maintenance support agreements.<br>The components chosen are currently commonly used within industry, with a view to leveraging commonality of hardware and software with existing systems, and utilisation of existing procurement and support agreements. |
| 3. The system requires ***sufficient*** processing, memory, storage and network interfaces to support a virtualisation environment. | The accomplishment of this goal is described in the System Design Description. |
| 4. … | |

# Conclusion and Summary

- We have claimed it is possible to provide an assurance argument for a system that does not have a defined requirements specification
- Have demonstrated a method to achieve that objective

- In reality, many acquisition programs, particularly where the intent is to use off the shelf systems, will deliberately skip the detailed development of testable engineering requirements captured in a formally endorsed specification

- Have found it is no use bemoaning this process –
- In many circumstances, this will simply not be considered as a risk mitigator to project success no matter how many detailed research studies are undertaken to provide evidence to the contrary

# Conclusion and Summary

- We've outlined a pragmatic approach to capture the intent of the system as a set of goals
- This is achieved through
  - A stakeholder analysis process,
  - Goal determination, and
  - Supported by providing evidence of goal satisfaction
- This is not a zero risk approach to systems engineering –
  - there are many many details that are omitted by only articulating the goals
- Risk tolerance assumption underpinning this approach to provide assurance is:
  - Nature of the COTS systems being acquired and assembled in to a functioning system
  - This relies heavily on the context of the target environment

# Confession

- The statement that assurance can be achieved without using the Systems Engineering V process is not really accurate –
  - By defining the goals and
  - Providing evidence of goal satisfaction
- We have created an informal proxy for user needs and requirements specification, and requirements verification and validation evidence
- The elements of design, construction and verification still sit where they always have on the left and right sides of the V respectively

SETE

ENGINEERS AUSTRALIA

SESA

INCOSE

SOUTHERN CROSS ITEA CHAPTER

QT CANBERRA | AUSTRALIA

29 APRIL – 1 MAY 2019

# References


- Alexander, IF 2005, 'A Taxonomy of Stakeholders: Human Roles in System Development', *International Journal of Technology and Human Interaction*, vol. 1, no. 1, pp. 23–59.
- Amyot, D, Horkoff, J, Gross, D & Mussbacher, G 2009, 'A lightweight GRL profile for i* modeling', in *Advances in Conceptual Modeling-Challenging Perspectives*, Springer, pp. 254–264.
- Civil Aviation Safety Authority 2018, *Electronic Flight Bag*, Text, November, viewed 7 March 2019, <https://www.casa.gov.au/aircraft/standard-page/electronic-flight-bag-efb>.
- Cockburn, A 2001, *Writing Effective Use Cases*, Addison-Wesley.
- Commonwealth of Australia 1999, *Environment Protection and Biodiversity Conservation Act 1999 (EPBC Act)*.
- Department of Defence 2013, *Regulation of Technical Integrity of Australian Defence Force Materiel*, Defence Instruction, 17 September, no. DI(G) LOG 4–5–012, Department of Defence.
- Department of Defence 2015, *Introduction to DASR for Technical Regulations : Future Regulations : Department of Defence*.
- DGTA 2015, *AAP 7001.053 electronic Technical Airworthiness Management Manual (eTAMM)*, Royal Australian Air Force (ed.), Australian Air Publication, Commonwealth of Australia.
- Gardiner, B 2015, 'Government ICT spend to reach $6.2 billion by 2018', *CIO*, viewed 15 February 2019, <https://www.cio.com.au/article/575210/government-ict-spend-growth-exceed-6-2-billion-by-2018/>.
- Hilliard, R 2011, *ISO/IEC/IEEE 42010: Conceptual Model*, Systems and Software Engineering — Architecture Description.
- Honour, EC 2013, 'Systems Engineering Return on Investment', Thesis thesis, UniSA.
- Hull, E, Jackson, K & Dick, J 2005, *Requirements engineering*, Springer-Verlag, London.
- IEEE 2000, *IEEE - 1471-2000 - IEEE Recommended Practice for Architectural Description for Software-Intensive Systems*, IEEE Computer Society.
- IEEE 2011, *ISO/IEC/IEEE 42010:2011, Systems and Software Engineering — Architecture Description*, S2ESC: Software & Systems Engineering Standards Committee (ed.), ISO/IEC/IEEE.
- INCOSE 2014, 'Why do Systems Engineering?', Poster.
- Jenkin, M 2018, 'Budget flags $2.4 billion in tech spending, ICT projects', CRN Australia, viewed 17 February 2019, <http://www.crn.com.au/news/budget-flags-24-billion-in-tech-spending-ict-projects-490549>.
- van Lamsweerde, A 2007, 'Kaos Tutorial', no. 1.0.
- McClinton, DF 1994, 'The Unwritten Laws of Systems Engineering', INCOSE International Symposium, vol. 4, no. 1, pp. 978–980.
- Ministry of Defence 2007, Defence Standard 00-56 Issue 4 Part 1, Safety Management Requirements for Defence Systems -
- Requirements, Ministry of Defence.
- NASA Safety Center 2008, System Failure Case Studies: Petrobas Platform 36 (P36), Case Study, October, NASA.
- Pyster, A & Olwell, DH 2013, Guide to the Systems Engineering Body of Knowledge (SEBoK), Version 1.2, The Trustees of the Stevens Institute of Technology, Hoboken, NJ, viewed 29 May 2014, <www.sebokwiki.org>.
- Redmill, F 2004, 'Analysis of the COTS debate', Safety Science, vol. 42, no. 5, pp. 355–367.
- Simmonds, S & Cook, S 2017, 'Use of the Goal Structuring Notation to Argue Technical Integrity', in INCOSE Symposium 2017, International Council on Systems Engineering, Adelaide, South Australia.
- Simon, HA 1956, 'Rational Choice and the Structure of the Environment.', Psychological review, vol. 63, no. 2, p. 129.
- The Standish Group 1994, The CHAOS Report 1994, The Standish Group.
- US Department of Defense 2012, Mil-Std-882E, Department of Defense Standard Practise - System Safety, Standard, 11 May, no. MIL-STD-882E, US Department of Defense, p. 104.
- Yu, ES 2009, 'Social Modeling and i*', in AT Borgida, VK Chaudhri, P Giorgini & ES Yu (eds), Conceptual Modeling: Foundations and Applications, Lecture Notes in Computer Science, Springer Berlin Heidelberg, pp. 99–121

SETE

ENGINEERS AUSTRALIA

SESA

INCOSE

SOUTHERN CROSS ITEA CHAPTER

QT CANBERRA | AUSTRALIA

29 APRIL – 1 MAY 2019

# Questions ?