27th annual INCOSE international symposium
Adelaide, Australia
July 15 - 20, 2017

ENGINEERS AUSTRALIA
SESA

Use of the Goal Structuring Notation to Argue Technical Integrity

Scott Simmonds
University of South Australia

Professor Stephen Cook
University of Adelaide

Outline

- 1. Introduction
- 2. Technical Integrity
- 3. Design Acceptance
- 4. Goal Structured Notation for Design Acceptance
- 5. Conclusion

1. Introduction

- In this paper, we introduce the use of the **Goal Structuring Notation** (GSN) as a means of formulating a Design Acceptance argument to assure the Technical Integrity of a new or modified system

2. Technical Integrity

- The Australian Defence Force Service Chiefs, as capability output managers, are accountable for the ‘Technical Integrity’ of materiel introduced into and operated by the Services.

- Technical Integrity of a system comprises consideration of
  - safety
  - fitness for service
  - environmental compliance

Elements of Technical Integrity

- Examining further the three elements of Technical Integrity:
  - Safety
  - Fitness for Service
  - Environmental Compliance

Safety

- Of the three elements, safety is perhaps the most analysed,
- Considerable literature, tools, techniques and standards available to apply to development of systems
- e.g. processes described in:
  - Def-Stan 00-56 and
  - MIL-STD-882E

- The Safety Case provides an argument that the system is safe
- This is supported by evidence describing how safe and in what context

Fitness for Service

- Fitness for Service means:
  - The system is Fit for Purpose;
  - The system's configuration, use, and maintenance are documented, indexed and traceable
  - Personnel have been trained and authorised in the system use and maintenance
  - A supply support chain has been established for parts, consumables, licenses, updates, OEM and specialist advice etc.

- Thus Fitness for Service means that the system is ready to be used throughout its service life

- Note: there is a distinction between
  - Fitness for Service – all of the above
  - Fitness for Purpose – the system has been validated against its operational concept

Fitness for Purpose

- The system has been validated against its operational concept – the purpose for which it was designed and built.
  - see (Pyster & Olwell, 2013)

Fitness for Service

- In addition, to be Fit for Purpose
  - The system's configuration, use and maintenance is documented, indexed and traceable;
  - Personnel have been trained and authorised in the system use and maintenance; and
  - A supply support chain has been established for parts, consumables, licenses, updates, OEM and specialist advice, and anything else required to support the system through life

Environmental Compliance

- The Environment Protection and Biodiversity Act of 1999 (Commonwealth of Australia, 1999) requires consideration environment impacts of systems
  - across their whole lifecycle where there exists potential for adverse environmental impacts
- Act ensures
  - Ongoing environmental management while undertaking military and civilian activities
  - Use of ecologically sustainable development principles and objectives

- Defence is required to consider the impact to the environment throughout the lifecycle of a system

Assurance of Technical Integrity

- Compliance of a system with requirements for achieving Technical Integrity can be presented as an **assurance argument**
- i.e. a system can be argued as meeting Technical Integrity requirements based upon claims of satisfying
  - Safety
  - Fitness for Service
  - Environmental Compliance
- Satisfaction of these claims is based upon appropriate evidence

3. Design Acceptance

- Design Acceptance is a ***process*** that examines the system in terms of its:
  - functions
  - construction
  - ability to be safely used
  - and maintained through its service life.
- The DA process has the **goal** of ensuring a design, sourced from a design agency, has:
  - met its specification as determined by verification
  - been developed by competent personnel within the design agency
  - as part of that development, been subjected to independent review and certification.
- DA is the ***process*** whereby the Technical Regulator (on behalf of the Service Chiefs) accepts the evidence presented by a design agency that:
  - The "design" meets its specification
  - The systems has been
    - designed
    - constructed
    - tested
    - documented

  using approved standards, processes, procedures and source data
- DA is Undertaken by the Design Acceptance Authority Representative (DAAR)

How to Design Accept ?

- Question arises:
  - How to present this information in a structured and consistent way that presents the DAAR with the necessary information to facilitate a determination that the system can be Design Accepted?
- This can be achieved by presenting claims about the safety, fitness for service and environmental compliance

Safety Claim

- The system is safe to own and operate:
  - Based upon a strategy of conducting a system safety program that:
    - performs a hazard search
    - assesses the hazards
    - develops mitigations
    - analyses the residual risk
  - Various subclaims regarding safety of components and subsystems

- Evidence is produced supporting the subclaims
- This supports the top-level claim regarding the safety of the system

Fitness for Service Claim

- Based upon a strategy of assessing:
  - Fitness for purpose:
    - System meets its specification
    - Test and analysis evidence created during system development program supporting this claim (e.g. test reports, analysis reports, VCRM etc.)
    - System's configuration, use, and maintenance is documented, indexed and traceable
  - Maintenance support:
    - Maintenance, repair facilities and personnel are capable and authorised to provide support
  - Supply support chain has been established for parts, consumables, licenses, updates, OEM and specialist advice etc.
  - Training:
    - Training material and training courses are performed to "train the trainer";
    - Personnel have been trained and authorised for system use and maintenance.

Environmental Compliance Claim

- Supported by design of a strategy that:
  - Examines the subclaims of the system's impact on the environment
  - Examines through-life use, support, and disposal
  - Provides evidence supporting the claims

More on the Design Acceptance Argument

- Design Acceptance process is an assessment of the acceptability of the design over time.
- In assessing the acceptability of the design it considers:
  - does it meet its functional and performance requirements; and
  - has the design been produced in accordance with defined processes such that reliance can justifiably be placed in the design

- i.e. a systematic review of product and process evidence forming an argument the system being introduced or modified can be accepted into service

The Design Acceptance Challenge

- How to present the necessary information in a structured and consistent way to the Regulator to facilitate a determination that the system can be Design Accepted?

- Solution: Goal Structuring Notation (GSN) (Attwood et al., 2011; Kelly, 1998, 2004)
  - A graphical notation
  - A structured approach to presenting arguments

Graphical Representation

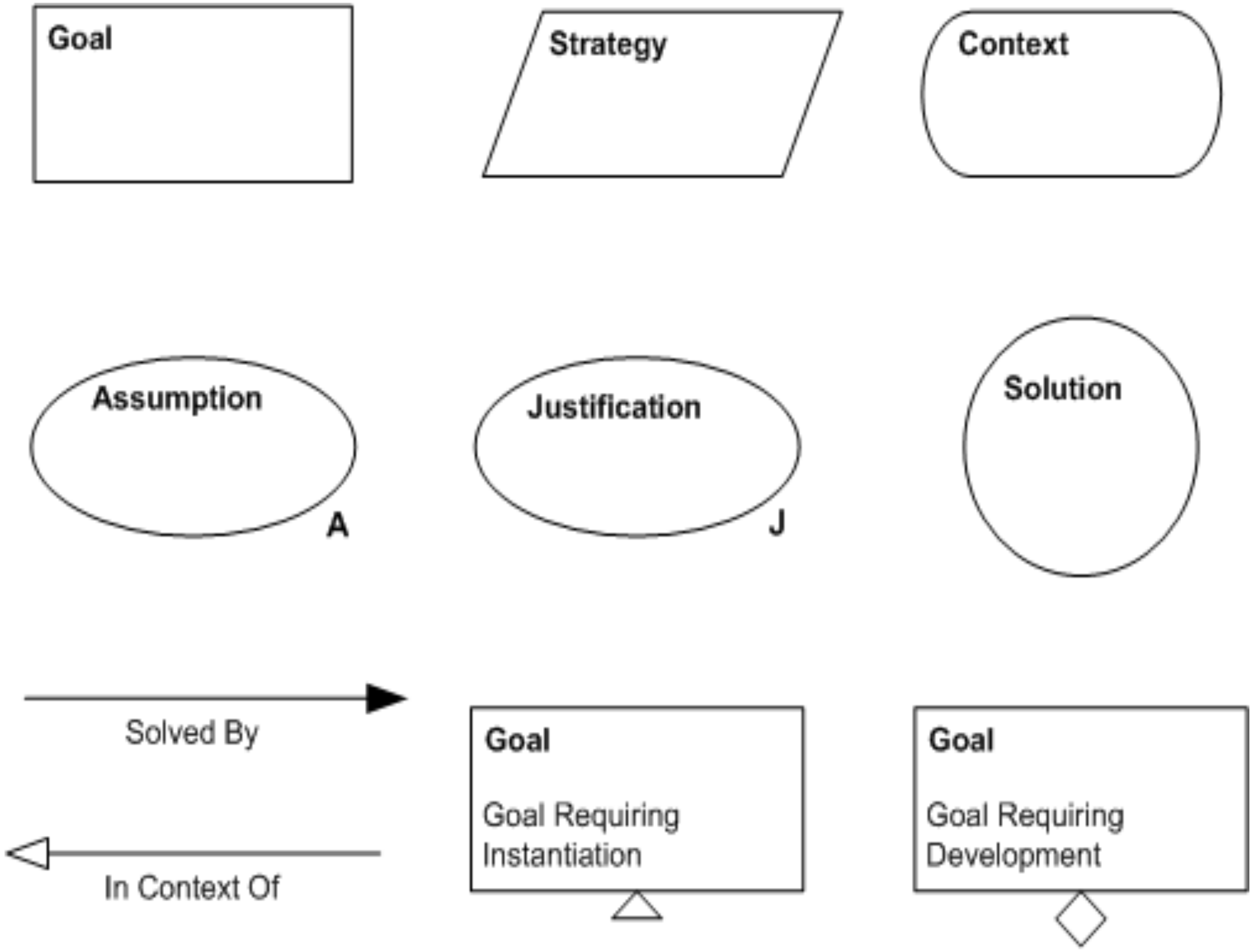
- These arguments can be expressed in Goal Structuring Notation (GSN)
- Presents a graphical "roadmap" to support describing the Technical Integrity of the system
- GSN is
  - "…a graphical argumentation notation that can be used to explicitly document the individual elements of any argument (requirements, claims, evidence and context) and … the relationships that exist between these elements. (Attwood et al., 2011)

Goal Structuring Notation

- GSN originated at the University of York in the early 1990s
- Developed as a means to document safety case arguments (Kelly, 1998, 2004; Kelly & Weaver, 2004)
- Has been extended to consider other argument based domains
  - in particular dependability and assurance cases (Alexander, Hall-May, Kelly, & McDermid, 2007; Despotou, 2007; Despotou & Kelly, 2004, 2008)

Elements of GSN

- Basic GSN elements –
  - Goal (Claim)
  - Strategy
  - Context
  - Assumption
  - Justification
  - Solution (Evidence)
- A goal not yet fully developed has an open diamond at the bottom edge of the symbol
  - Can also be applied to the Solution – where evidence is predicted but not yet available
- A goal requiring instantiation to complete the argument has an open triangle at the bottom edge



Design Acceptance Argument Using GSN

- Using Goal Structuring Notation, graphically develop the argument structure
- Need to make claims about the acceptability of a design, then show evidence that the claims are valid
- To support the claim, we need to argue the case by
  - providing context
  - describing assumptions
  - describing the strategy that supports the claim being made
- The context of the claim is where the type of system and the interfaces are defined
- Proceed to define types (and completeness) of evidence that supports the argument

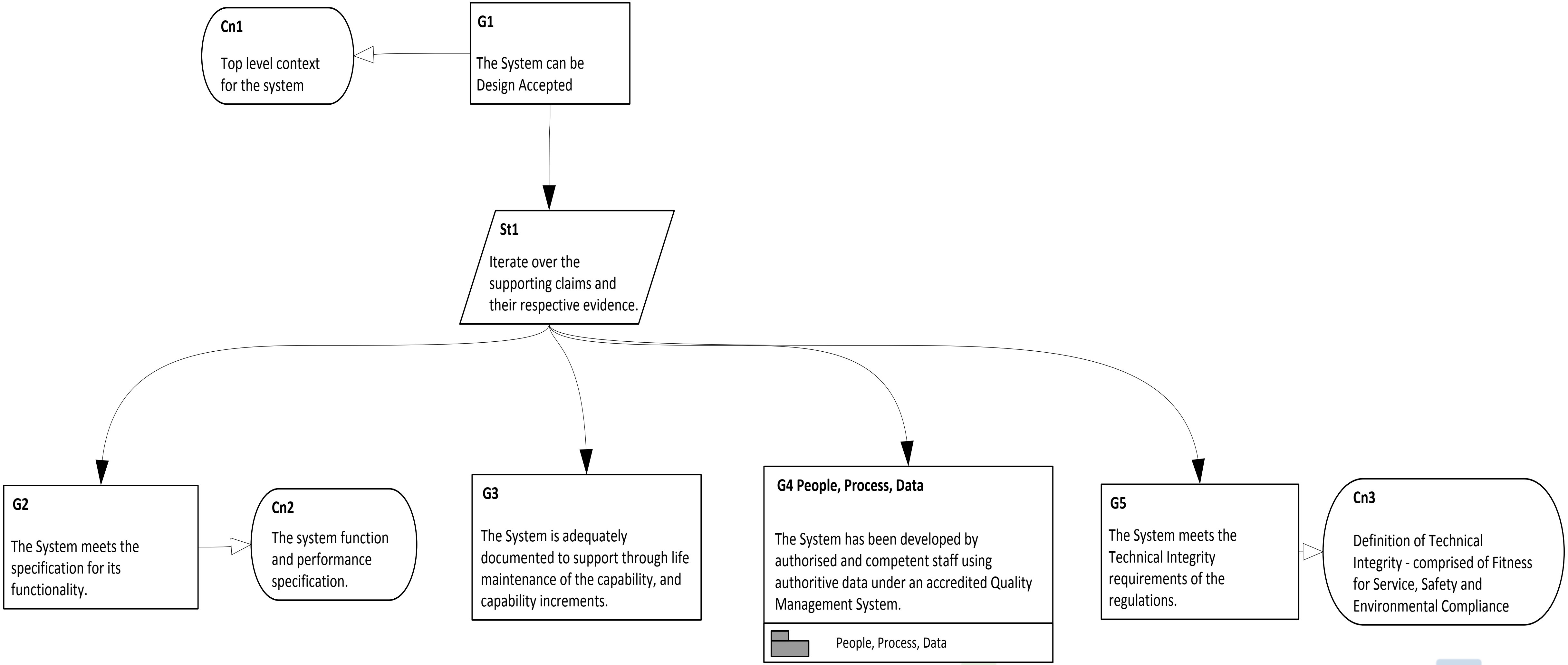
Example Design Acceptance Strategy based upon GSN

- Top-level claim:
  - *The System can be Design Accepted*

- Claim is supported by the strategy:
  - *Iterate over the supporting claims and their respective evidence*

- The strategy is supported by lower level claims that decompose the acceptance strategy into a number of principal arguments:
  - *The System meets the specification for its functionality*
  - *The System is adequately documented to support through life maintenance of the capability, and capability increments*
  - *The System meets the Technical Integrity requirements of the regulations*
  - *The System has been developed by authorised and competent staff using authoritative data under an accredited Quality Management System*

GSN Based Design Acceptance Strategy



Cn1

Top level context for the system

G1

The System can be Design Accepted

St1

Iterate over the supporting claims and their respective evidence.

G2

The System meets the specification for its functionality.

Cn2

The system function and performance specification.

G3

The System is adequately documented to support through life maintenance of the capability, and capability increments.

G4 People, Process, Data

The System has been developed by authorised and competent staff using authoritive data under an accredited Quality Management System.

People, Process, Data

G5

The System meets the Technical Integrity requirements of the regulations.

Cn3

Definition of Technical Integrity - comprised of Fitness for Service, Safety and Environmental Compliance

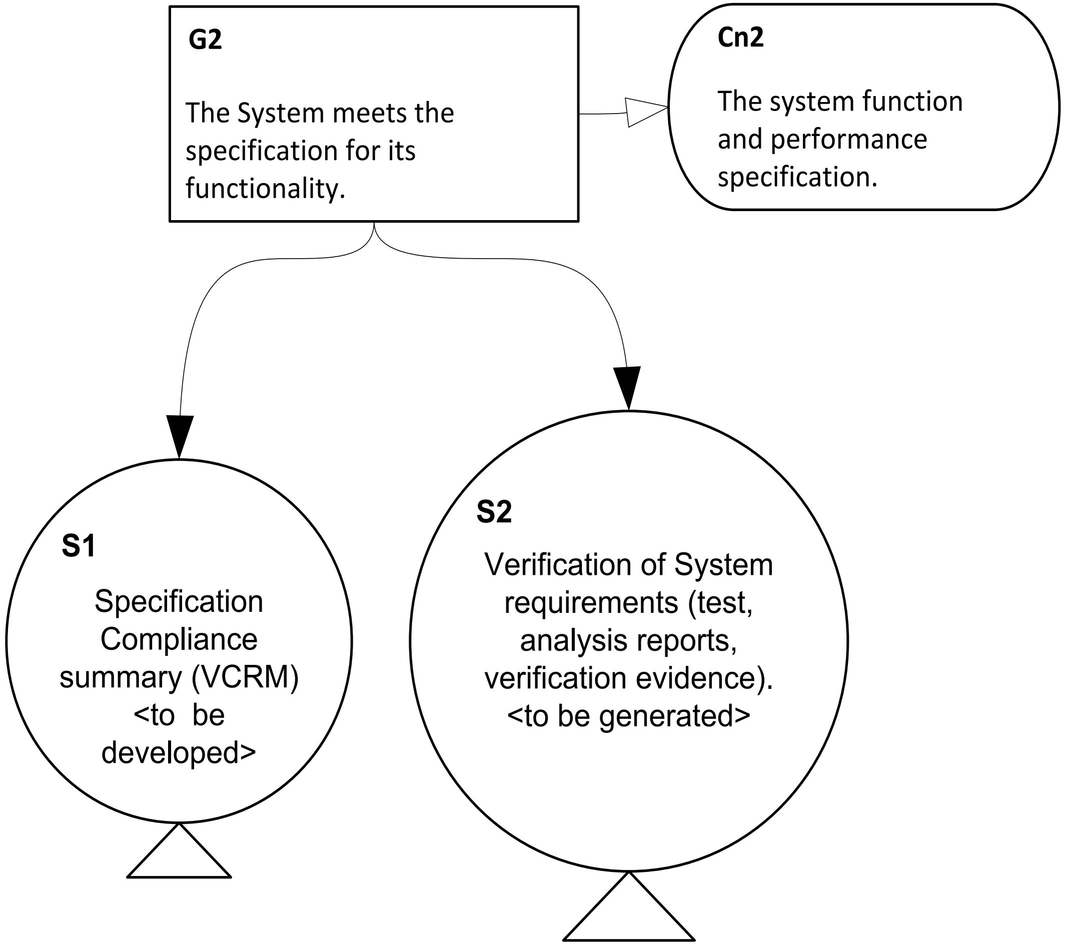
Product vs Process

- By splitting the argument into separate goals, the Product versus Process argument can be balanced appropriately
  - the design specification drives verification of achievement of product functionality and
  - process specifications support the assurance argument

- Results in a reliable, robust product of defined quality

Further Decomposition

- Lower level claims deal with detailed aspects of the system,
- e.g
  - *The System meets the specification for its functionality*
  - claim is readily supported by evidence in a Verification Cross Reference Matrix (VCRM) and
  - test and analysis results showing compliance with the specification requirements



G2

The System meets the specification for its functionality.

Cn2

The system function and performance specification.

S1

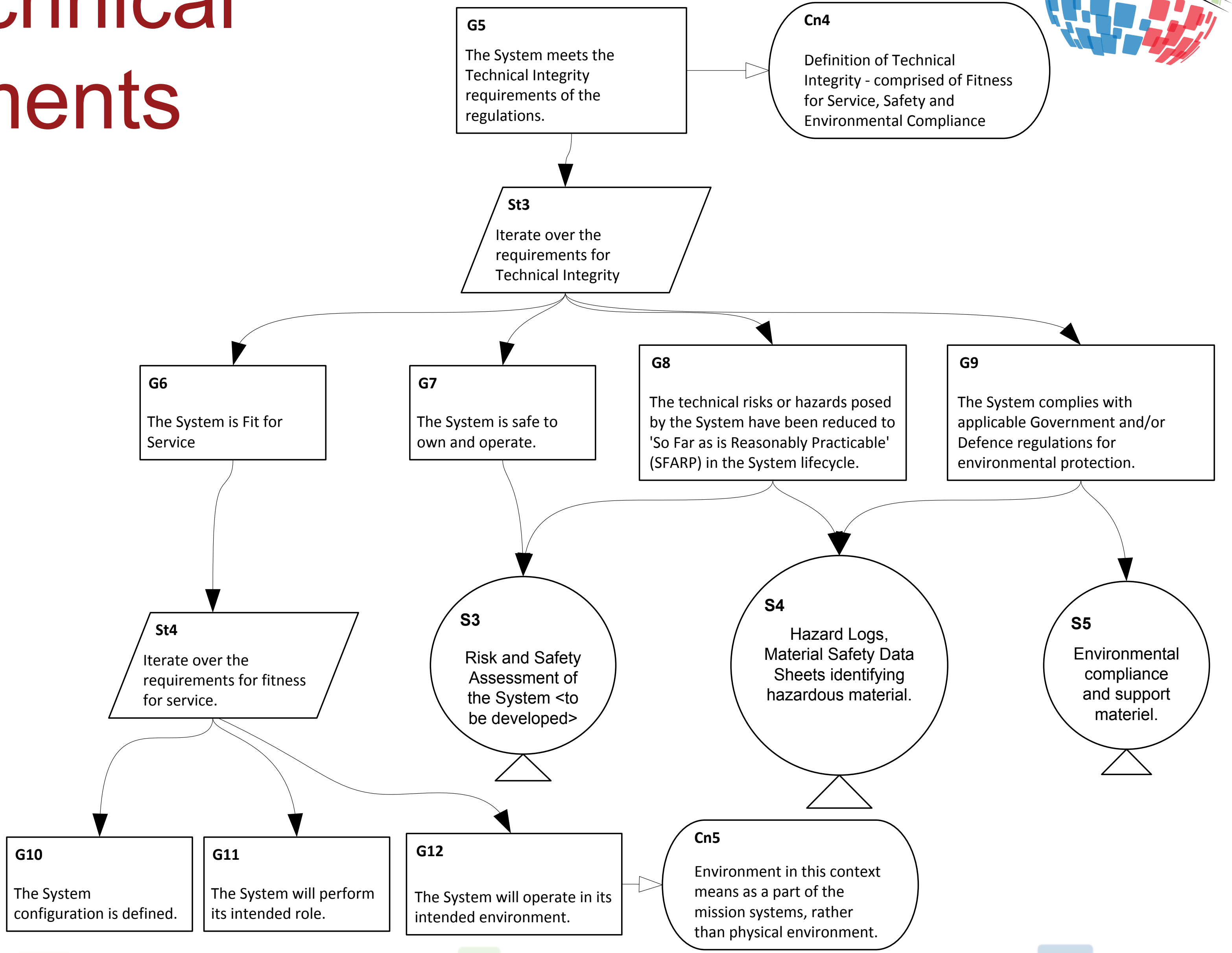
Specification Compliance summary (VCRM) <to be developed>

S2

Verification of System requirements (test, analysis reports, verification evidence). <to be generated>

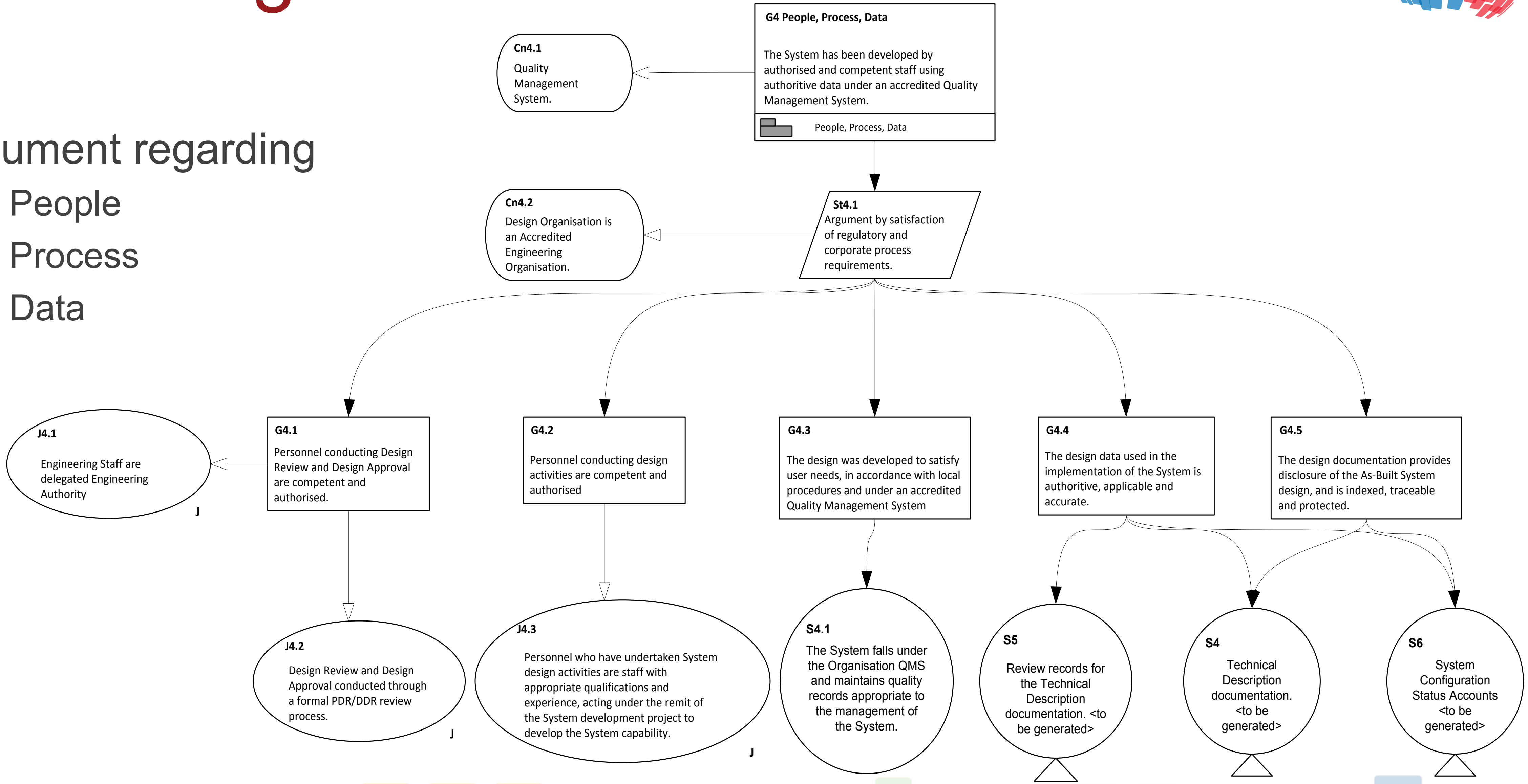
Satisfaction of Technical Integrity Requirements

- Can be argued based upon claims and evidence regarding individual aspects of Technical Integrity:
  - Safety
  - Fitness for Service
  - Environmental Compliance


G5
The System meets the Technical Integrity requirements of the regulations.
Cn4
Definition of Technical Integrity - comprised of Fitness for Service, Safety and Environmental Compliance
St3
Iterate over the requirements for Technical Integrity
G6
The System is Fit for Service
G7
The System is safe to own and operate.
G8
The technical risks or hazards posed by the System have been reduced to 'So Far as is Reasonably Practicable' (SFARP) in the System lifecycle.
G9
The System complies with applicable Government and/or Defence regulations for environmental protection.
St4
Iterate over the requirements for fitness for service.
S3
Risk and Safety Assessment of the System <to be developed>
S4
Hazard Logs, Material Safety Data Sheets identifying hazardous material.
S5
Environmental compliance and support materiel.
G10
The System configuration is defined.
G11
The System will perform its intended role.
G12
The System will operate in its intended environment.
Cn5
Environment in this context means as a part of the mission systems, rather than physical environment.

Process Argument

- Argument regarding
  - People
  - Process
  - Data



G4 People, Process, Data

The System has been developed by authorised and competent staff using authoritive data under an accredited Quality Management System.

People, Process, Data

Cn4.1

Quality Management System.

St4.1

Argument by satisfaction of regulatory and corporate process requirements.

Cn4.2

Design Organisation is an Accredited Engineering Organisation.

G4.1

Personnel conducting Design Review and Design Approval are competent and authorised.

J4.1

Engineering Staff are delegated Engineering Authority

J

G4.2

Personnel conducting design activities are competent and authorised

G4.3

The design was developed to satisfy user needs, in accordance with local procedures and under an accredited Quality Management System

G4.4

The design data used in the implementation of the System is authoritive, applicable and accurate.

G4.5

The design documentation provides disclosure of the As-Built System design, and is indexed, traceable and protected.

J4.2

Design Review and Design Approval conducted through a formal PDR/DDR review process.

J

J4.3

Personnel who have undertaken System design activities are staff with appropriate qualifications and experience, acting under the remit of the System development project to develop the System capability.

J

S4.1

The System falls under the Organisation QMS and maintains quality records appropriate to the management of the System.

S5

Review records for the Technical Description documentation. <to be generated>

S4

Technical Description documentation. <to be generated>

S6

System Configuration Status Accounts <to be generated>

Completeness

- Design Acceptance is intended to be a process
  - Takes place over time, not at the completion of design activity
  - Completeness requires a complete a set of evidence

- In complex projects, it is particularly difficult to bring all elements of a design together in a single assurance "event"
  - However this is typically how things are scheduled
  - Design Acceptance is treated as a milestone rather than an activity

- GSN provides mechanisms to identify incomplete arguments and incrementally populate these arguments over time

- Completeness of the argument can be identified at any time (using the notation) and satisfied over time as evidence is developed

Benefits of the GSN-based Design Acceptance Structure

- Allows the incremental build up of evidence over the design acceptance process:
  - Starting at None through to a body of evidence generated through the design activity
  - Requirements satisfaction records, Process records, Certification

- Partitions the system into appropriately sized pieces
  - can be aligned with the system breakdown structure

- Modular nature of GSN allows the development of "generic" goal structures
  - Supports partitioning the elements of the Design Acceptance argument into modular acceptance strategies
  - E.g.:
    - Module A can be Design Accepted,
    - Module B can be Design Accepted, etc.,
    - the system comprising Module A, B, ... can be design accepted

- A simple graphical notation, readily interpreted – therefore aids communication as to how Design Acceptance to be achieved for the system in question

Other Considerations

- Focus of this paper is on the Technical Integrity argument
- However, the principles described are applicable to other application domains where the concept of regulatory "acceptance" is used:
  - E. g. GSN support to Design Acceptance within a Technical Airworthiness regulatory framework in Simmonds (2014)

Summary

- A method for describing the overall strategy for Design Acceptance using GSN is discussed, with a particular focus on assurance of the Technical Integrity of the system
- GSN provides a structured graphical method to describe the Design Acceptance process
- GSN can support the Design Acceptance process throughout the system development process
- GSN's ability to instantiate elements of the strategy based on the systems development structure is key to the flexibility provided by this approach, while ensuring that all necessary evidence is identified and assessed
- Capturing the acceptance goals and rationale for the types of supporting evidence provides articulation of system acceptability, readily supporting regulatory acceptance of the design

Conclusion

- Using GSN to document the Design Acceptance strategy, provides a robust and well documented methodology for supporting acceptance arguments
- This approach can ease the process of conducting Design Acceptance Certification at the end of a project development phase
- It can also provide a basis for modular change management throughout the sustainment phase