INCOSE International Symposium
Las Vegas, NV
June 30 - July 3, 2014

Can Systems Engineering Support An Owner-Operator To Be A Design Authority?

By

Cleave Systems Limited
Doug Cowper

ALTRAN
Ian Gallagher &
Nick McGrogan

amec
Andrew
Krolikowski

Contents

1. Introduction
2. Design Authority (Models & Responsibilities)
3. Technical Governance
4. Lack of Guidance
5. Proposed Approach
6. A Graded Approach
7. Mutual Assurance
8. How SE Technical Processes Support The DA
   - Managing Different Assurance Life Cycles
   - Setting Requirements & Specifications
   - Architecture Design
   - Verification
9. Challenges And Lessons
10. Conclusions

Introduction

- Shift in design authority roles and tasks from customer to supplier
  - High risk strategy, especially with novel and complex programmes
  - Requires requirements to be defined and for them not to change

- The customer needs to take responsibility for the design as it matures due to:
  - Regulatory practice of holding the operating company responsible for the design as well as for its safe operation;
  - The legal position taken to hold the operator solely liable for damages in the event of an accident;
  - Or the risks of project failure is so large it needs to be shared across the extended enterprise

Terminology Minefield

Design Assessment

Intelligent Customer

Design Authority

Operator / Owner

Designer / Supplier

Approving Authority

Technical Assurance

Quality Assurance

Fitness For Purpose

Technical Authority

Independent Advice

Governance

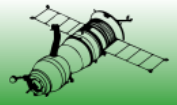
????

Responsible Designer

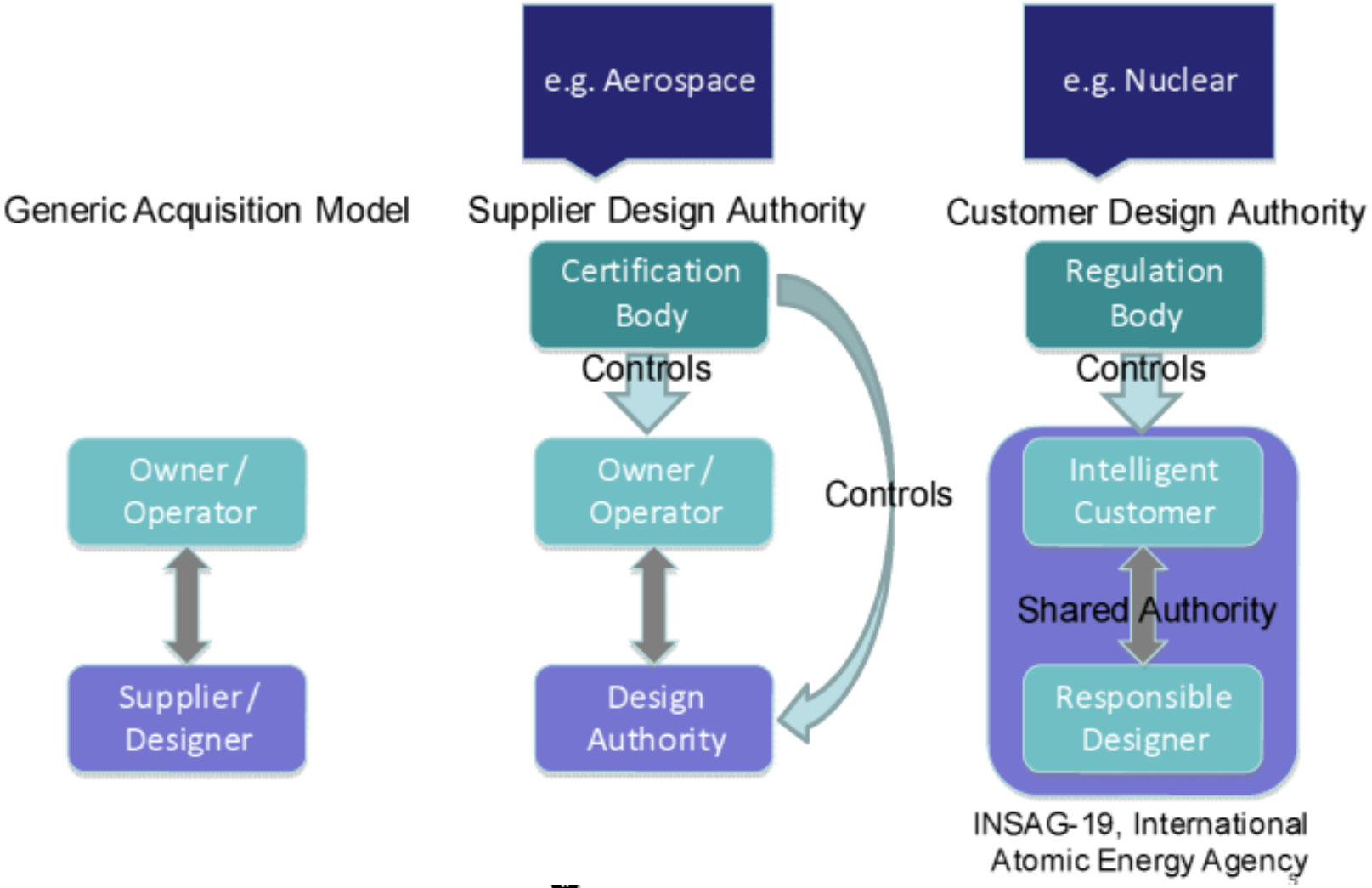
Regulation

Qualification

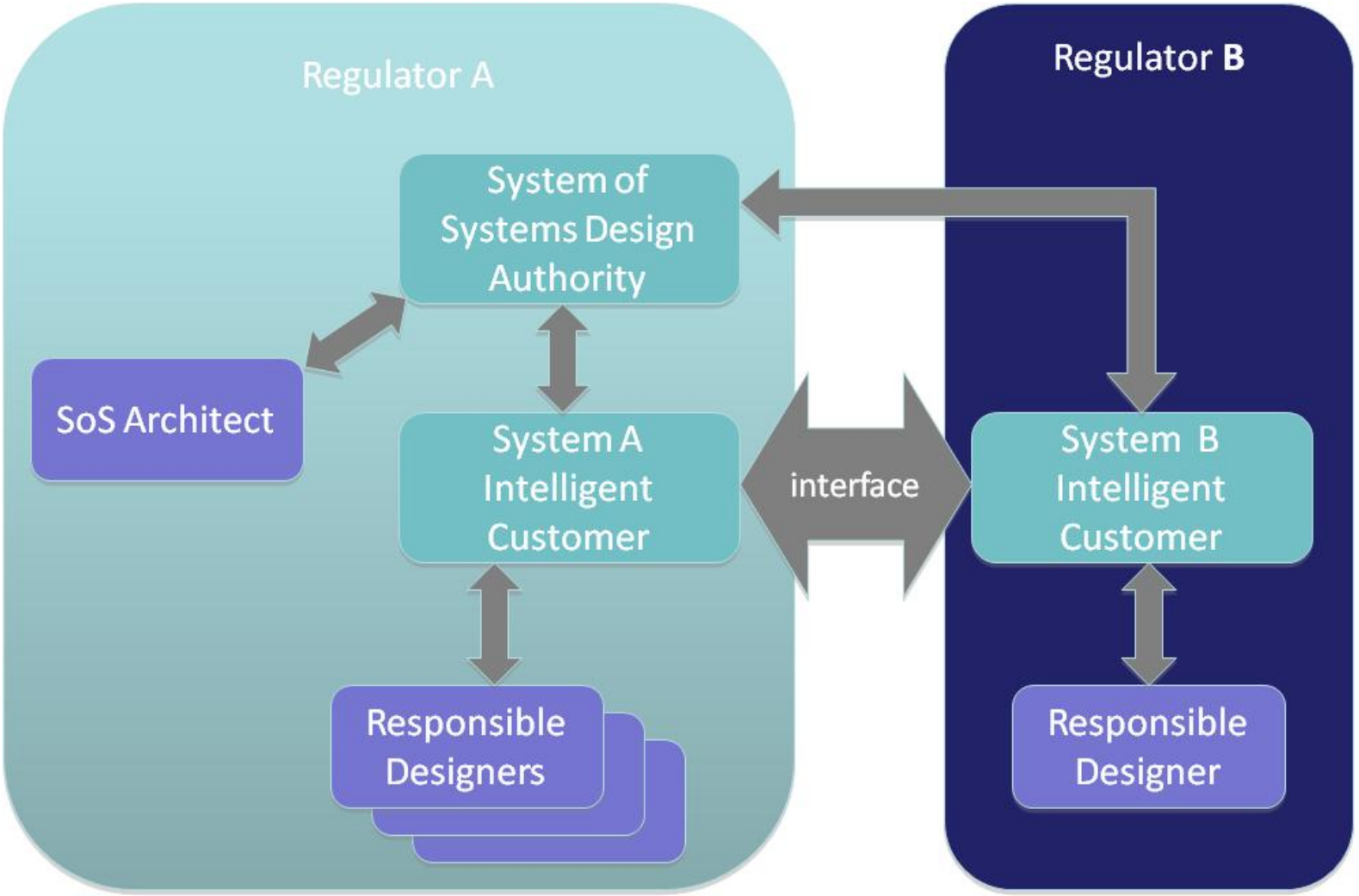
Certification


Design Authority Models

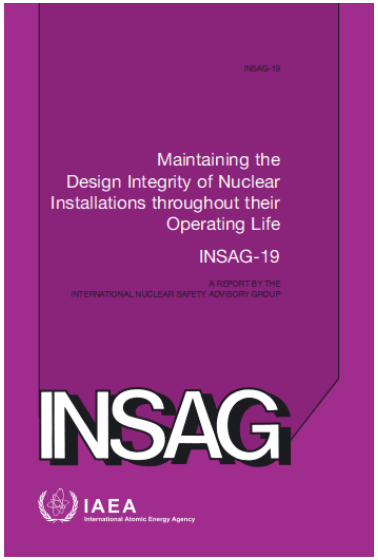


Complex Design Management Arrangements



Design Authority Responsibilities

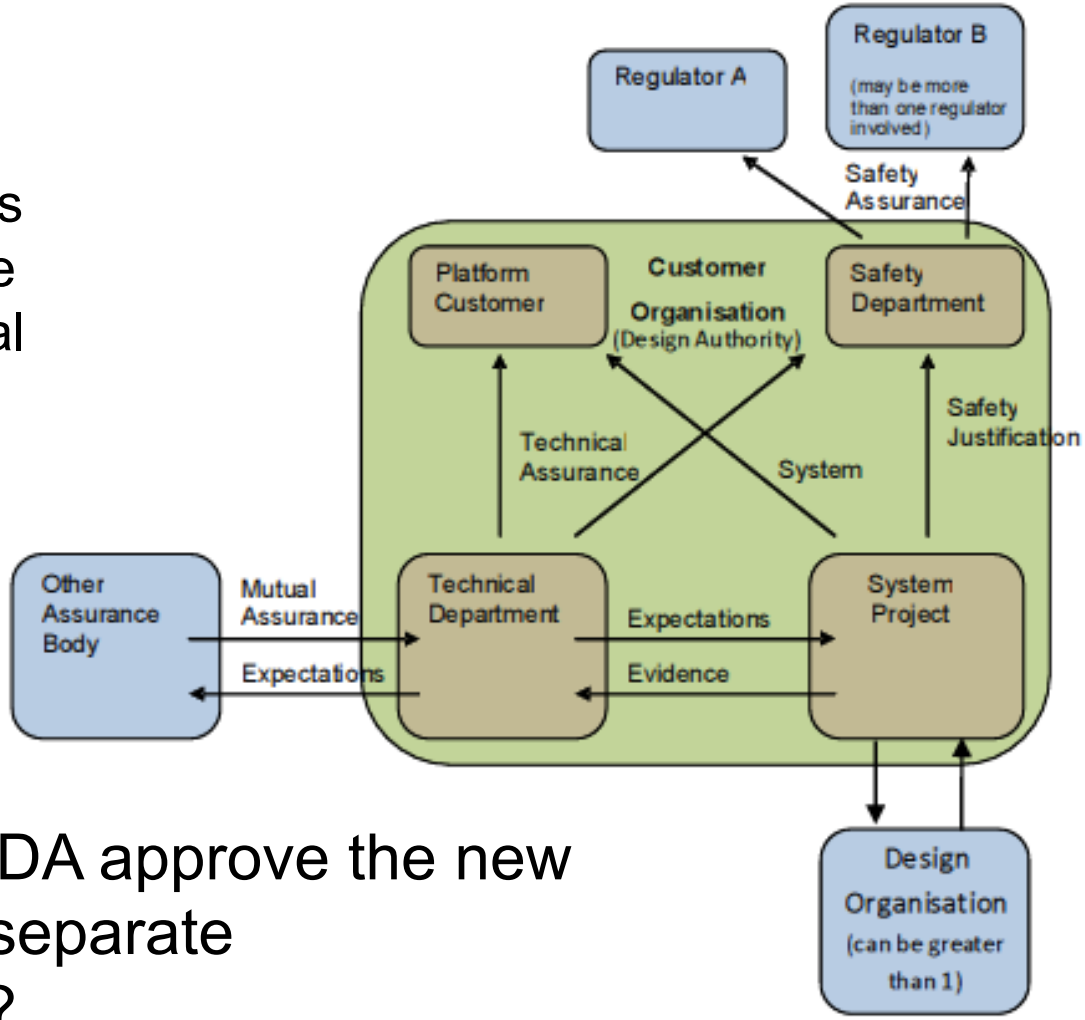
- A Design Authority is responsible for:
  - Establishing, preserving and expanding the design knowledge base and its recovery should it become lost
  - Quality Assurance
  - Requirements
  - Reviewing, verifying and approving (or rejecting) design changes
  - Maintaining design integrity
  - Design configuration control (e.g. Drawings, specifications, manuals, design standards, engineering calculations, supporting data)
  - Controlling interfaces with designers and suppliers of design work
  - Maintaining SQEP skills & knowledge (including research programmes)



INSAG-19, International Atomic Energy Agency

Technical Governance

- Activity which is undertaken to:
  - ensure a design remains Fit for Purpose and Safe throughout is operational life
  - maintain control of design.
- An owner-operator is unlikely to be “design capable”
- Therefore how does a DA approve the new design produced by a separate Responsible Designer?

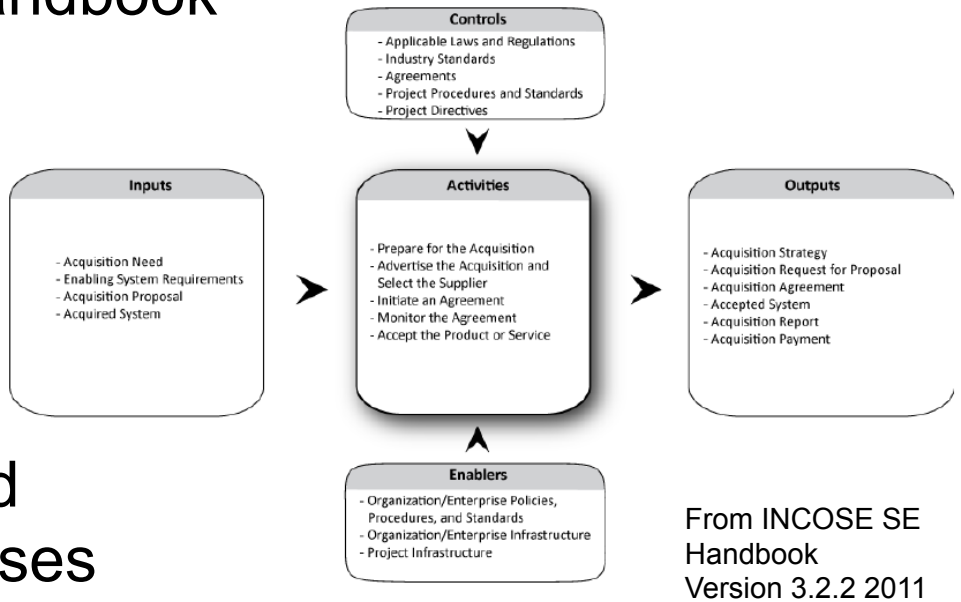


Lack of Guidance

So where can a DA turn to for help?

- Agreement processes of ISO 15288 and the INCOSE Systems Engineering Handbook

  only discuss:
  - Negotiating,
  - Monitoring
  - Confirming Delivery

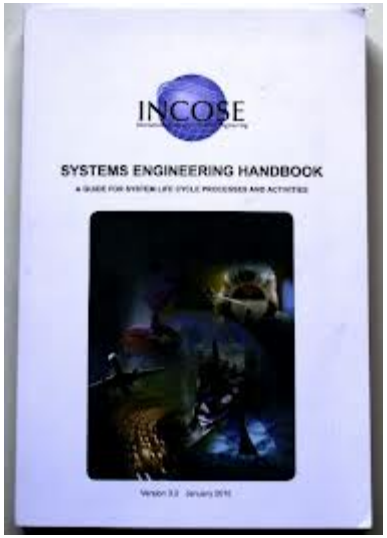


From INCOSE SE Handbook Version 3.2.2 2011

- Decision management and Risk management processes provide good guidance:
  - technical decision making,
  - technical risk management.

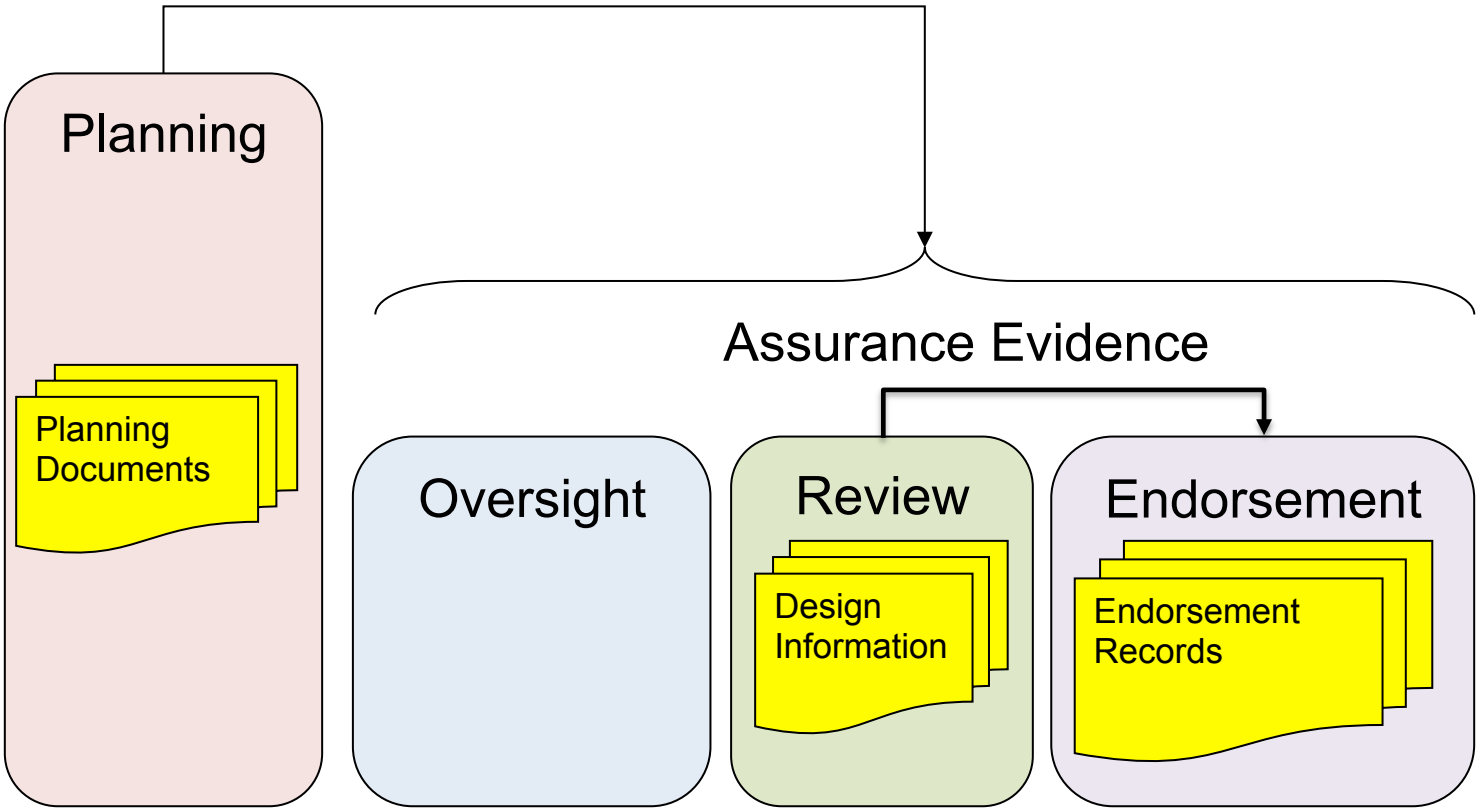
Lack of Guidance

- ISO 15288 and INCOSE Systems Engineering Handbook are focused towards the DO rather than the DA.

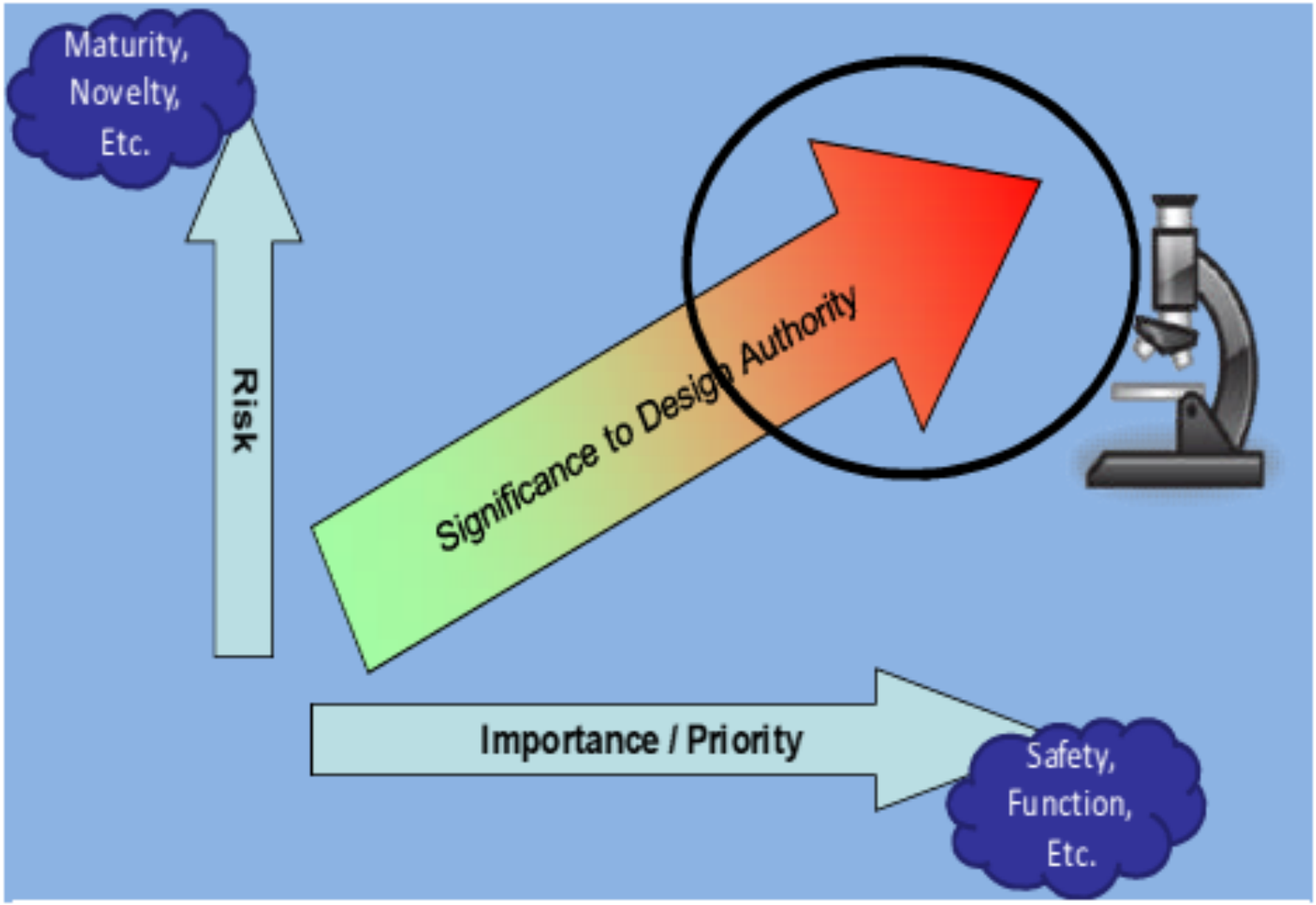


- The DA is responsible for much more than what is contained within ISO15288.
- One of the weaknesses of ISO15288, when used in regulated/non prescriptive industries, is that it does not have coverage of all the elements needed to support engineering judgment and the ability to justify the case for the end output.
- The authors believe that there is scope here for INCOSE to provide this guidance.

Proposed Approach



A Graded Approach



Mutual Assurance

- The means by which one organisation is able to take credit for another's assurance activities without having to repeat them.
- For an owner / operator who is the Design Authority, they need to
  - be satisfied that the Design Organisation's assurance process meet the DA's and any Regulator's requirements
  - and that they are following these processes.
- Mutual Assurance must not be confused with a passive, unquestioning approach.

How SE Technical Processes Support The DA

- Not exploring new approaches to SE but
- How You As A Systems Engineer Can Help
- SE addresses two key points:
  1. Assurance of engineering processes to ensure control of design;
  2. Provide evidence to allow technical governance to happen.


INTERNATIONAL STANDARD ISO/IEC 15288

First edition 2002-10-15

Systems engineering — System life cycle processes

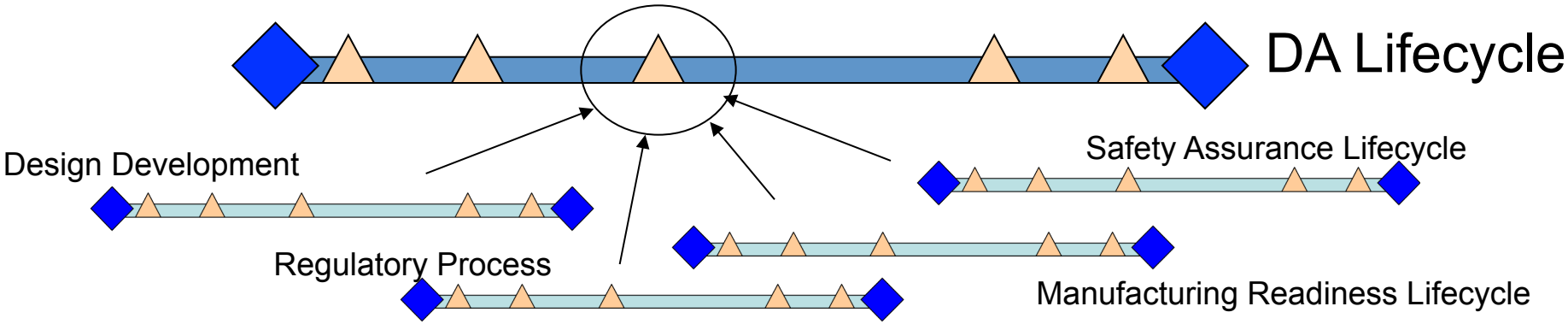
Ingénierie systèmes — Processus de cycle de vie des systèmes

Reference number ISO/IEC 15288:2002(E)

© ISO/IEC 2002

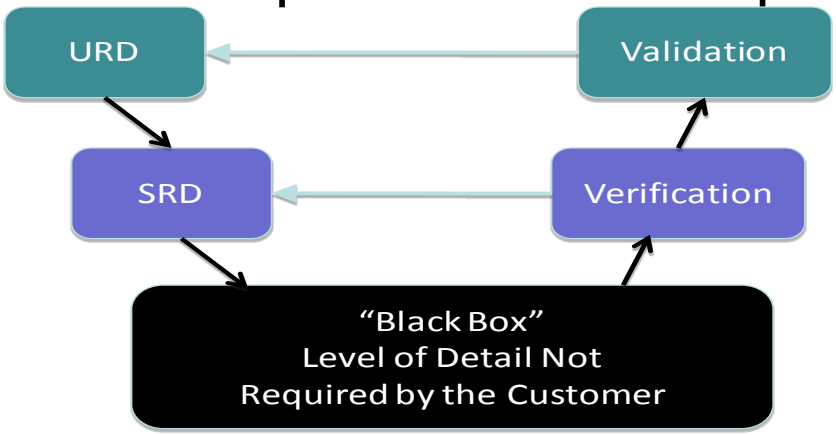
Managing Different Assurance Life Cycles

- Issues:
  - Aligning multiple life cycles from differing responsibilities across different organisations
  - Definition and purpose of reviews
  - Long lead items
  - Maintaining design integrity across the life cycle
  - Differing alignment of maturity points
- DA Customer needs to
  - Set their own purpose for decision gates and criteria
  - Take mutual assurance credit to DO reviews to avoid duplication

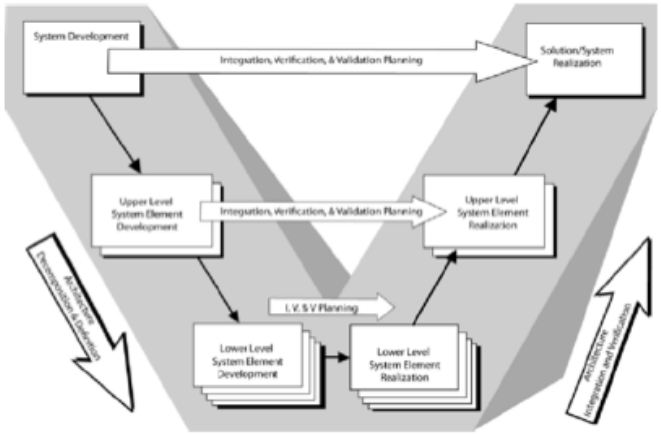


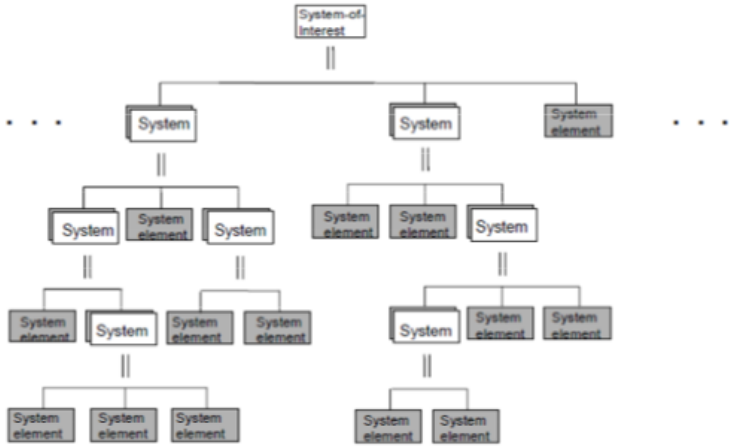
Setting Requirements & Specifications

Black Box View of Requirements and Specifications



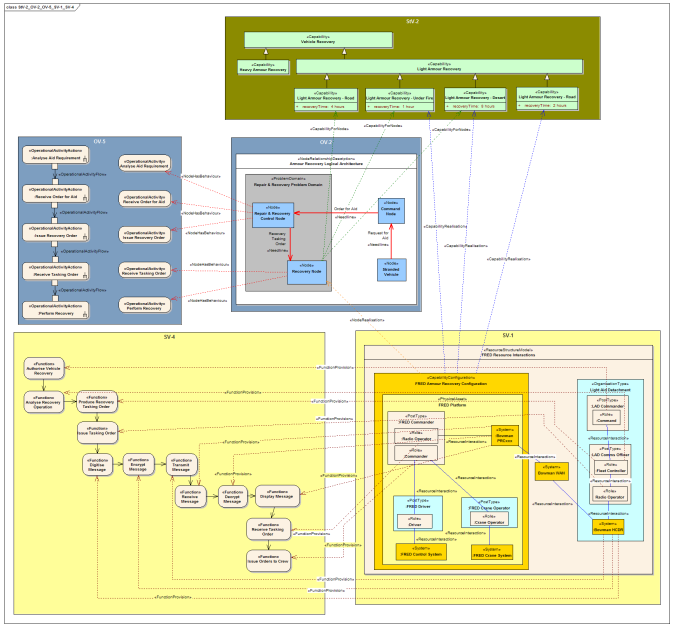
vs. Design Authority / Intelligent Customer View





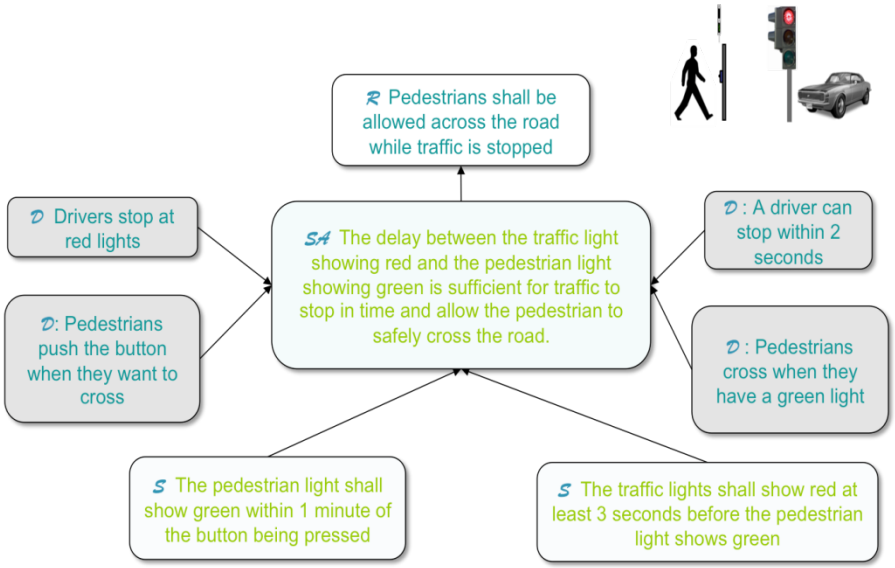
Architectural Design

- Architecture design underpins claims of compliance against top-level system requirements
- A *shared* Architectural Design supports clear definition of the boundaries of systems within the operating environment
- Design Authorities need coherent, shared & controlled Architecture Design information
- Owner / operator organisations not always knowledgeable about or comfortable with formal Architecture methods



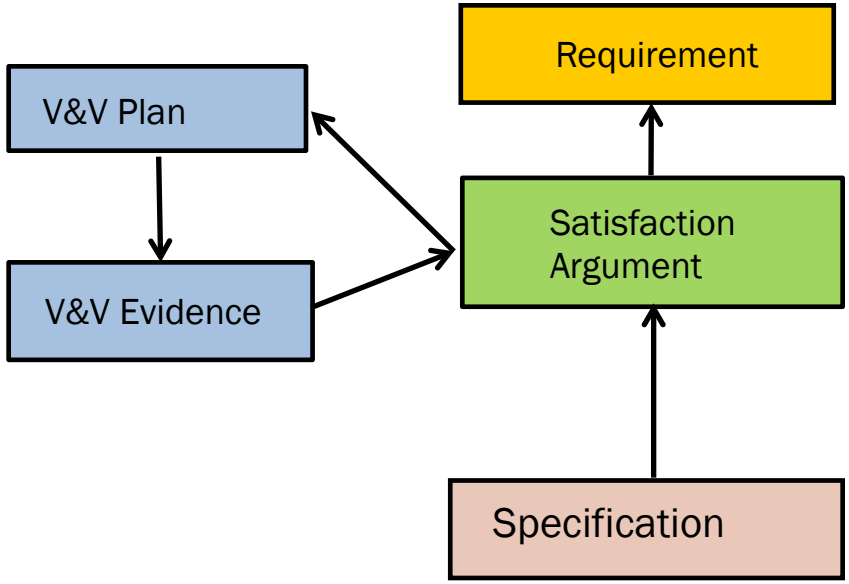
Verification

Satisfaction Arguments



Further info: Hammond, Rawlings & Hall, *Will It Work*, IEEE International Symposium on Requirement Engineering 2001

Progressive, Evidence Based-Assurance



Further Info: Dick & Russell, *Evidence Based Development*, INCOSE ASEC 2012

Challenges and Lessons

- Some of the challenges and lessons experienced on this piece of work:
  - Shared Common Vision
    - in terms of boundaries, role and responsibilities
  - Early Planning
  - Proportional Approach
    - Graded-Risk Based Approach
    - Sampling Strategy
  - Design Evidence
    - Information Sharing
    - Significant IT Investment
    - Contract for Technical Governance
  - Resource Capability, Competence and Experience
    - Aligned skills to responsibilities

Conclusions

- Supplier as DA = high risk strategy on novel and complex programmes.
- Not acceptable in regulated environments.
- Customer (DA) needs to take responsibility for the design as it matures.
- Customer as DA has implications on the capability required.
- Not a great deal of guidance available.
- Systems engineering can be used to support technical governance.
- Introducing SE in a DA environment can be challenging!

Any Questions?