



**Rolls-Royce**

## **RESG Goals Day 24<sup>th</sup> March 2010**

**Philip Wilkinson  
Rolls-Royce plc**

© 2007 Rolls-Royce plc

The information in this document is the property of Rolls-Royce plc and may not be copied or communicated to a third party, or used for any purpose other than that for which it is supplied without the express written consent of Rolls-Royce plc.  
This information is given in good faith based upon the latest information available to Rolls-Royce plc, no warranty or representation is given concerning such information, which must not be taken as establishing any contractual or other commitment binding upon Rolls-Royce plc or any of its subsidiary or associated companies.

## **Who am I?**

2

### **● Phil Wilkinson**

- Worked for Rolls-Royce for 20+ years.**
- Safety Engineer within the 'Controls Division' of Rolls-Royce.**
- Interested in how safety and systems engineers more effectively work together, particularly:**
  - How requirements interact with the safety process.**
  - The verification of safety requirements**



## Motivation

3

- Interested in the relationship between different types of requirements and the resulting structure.
- Particularly, general requirements and safety requirements as used in safety and satisfaction arguments.
- So, how similar are these 2 types of argument?
- Can safety arguments and satisfaction arguments be merged, to create a common approach?
- If they can be merged, is there a benefit?

## Background

4

- Safety Arguments
- Safety arguments have been used in numerous sectors for many years.
- The argument attempts to explain why a system is safe for use in a given context.
- 2 well-known approaches are:
  - Goal Structure Notation<sup>(1)</sup> (GSN), and
  - Claim Structures<sup>(2)</sup>
- Satisfaction Arguments
- For a long time, engineers have sought to demonstrate the relationship between parent and child requirements.
- A number of years ago, Praxis proposed the use of a method called REVEAL<sup>(3)</sup> to address this issue:
  - Rich Traceability
  - Satisfaction Argument
- This approach helps to demonstrate that the child requirements satisfy the parent requirement.

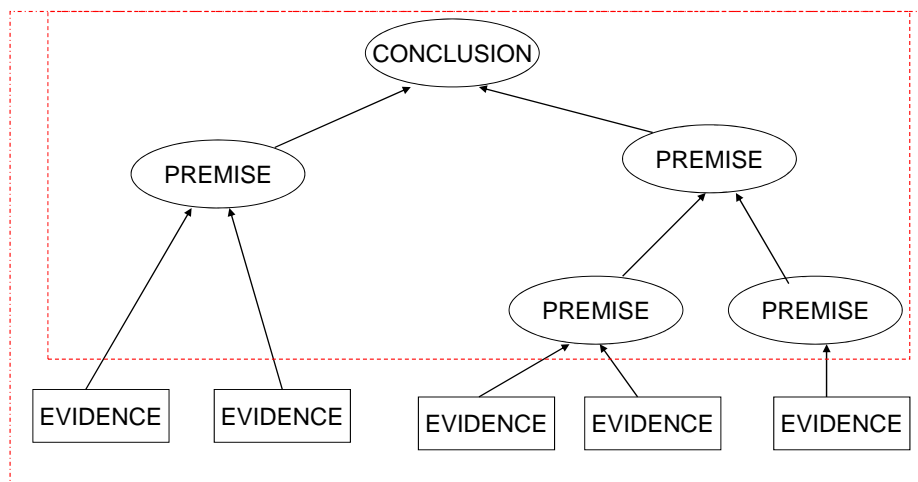
## The Safety Case or Argument

5

- What is a Safety Case or Safety Argument?
- “...a structured argument, supported by a body of evidence, that provides a compelling, comprehensive and valid case that a system is safe for a given application in a given environment ...”  
*Def Stan 00-56 Issue 4, section 1, part 9*
- So it's just an argument – The marshalling of reasons and evidence, in an organised and clear way, to convince someone of something.

## Argument Structure

6



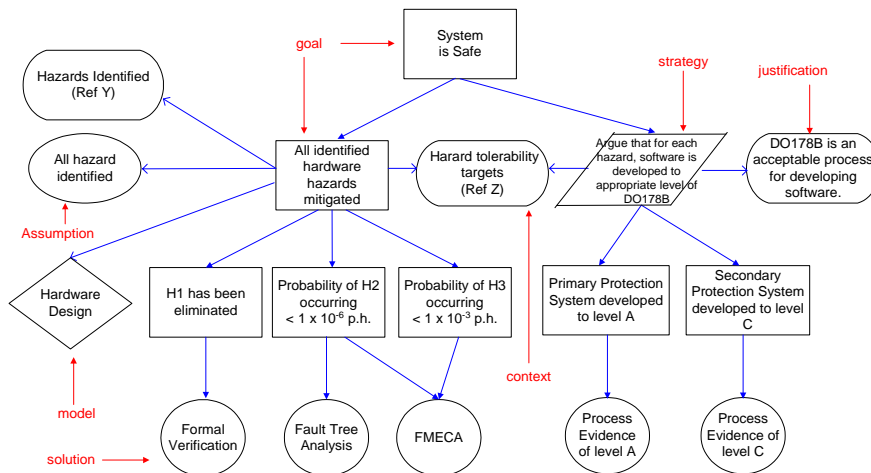
# Goal Structuring Notation (GSN)

7

- Graphical notation for the representation and development of safety arguments
  - Developed at University of York in 1990s
- Explicit representation of goal-based arguments
  - Gradual refinement of goals (noun-phrase & verb phrase)
  - Argument strategies – records argument structure (brief description)
    - Brief summary of the approach, expressed in form ‘Argument by ...’, ‘Appeal to ...’, ‘Argument across...’ etc.
  - Supporting evidence (solutions) and Models – usually a reference to some artefact (noun-phrase)
  - Justifications and Assumptions provide additional explanatory material (brief description)
  - Context reference to an artefact (noun-phrase) or explanatory text (brief description)
  - Logical relationships – AND default for goals; OR can be selected.

# Simple GSN Diagram

8



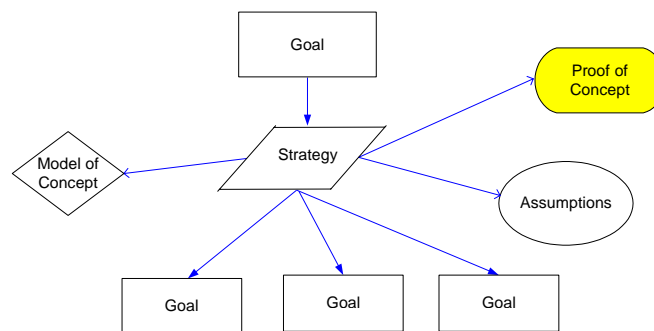
## Some Refinements

9

- **Closer integration of safety into early-stage design activities**
  - Help further drive safety into the design.
  - Reduce unnecessary rework, and more effective focus of the required effort.
- **Define Company best-practice for argumentation.**
  - **Which type of argument?**
    - Deductive, Inductive, Abductive
  - **What about argument by:**
    - Example, Analogy, Causes, Authority
  - **Fallacies**
  - **Argument vs. explanation**
- **Handle complex inferences**
  - Do goals & assumptions & strategies & model knowledge convince us that the conclusion is true?
  - Such instances, may need a Proof of Concept<sup>(4)</sup> to verify the claim.

## Some Refinements

10

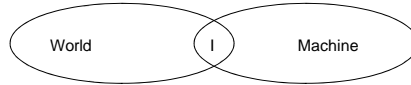


Note: Strictly speaking, Proof of Concept isn't part of the argument.

## REVEAL & Satisfaction Arguments

11

- REVEAL uses elements of Jackson's "World and Machine" model.



- Aspects of the real world that are relevant to achieving our goals are called the Application Domain.

- REVEAL uses the following definitions:

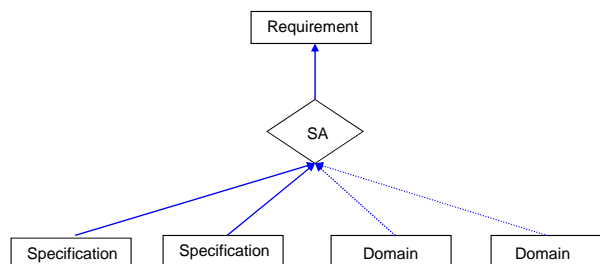
- Requirements (R) are statements about the World that we want to Machine help achieve.
- Specifications (S) are statements that defined the Machine's external behaviour to achieve the Requirements.
- Domain Knowledge (D) facts about the Application Domain, that are independent of the Machine, that we assume are true.

- Which leads to the statement:  $D, S \vdash R$

## REVEAL & Satisfaction Arguments

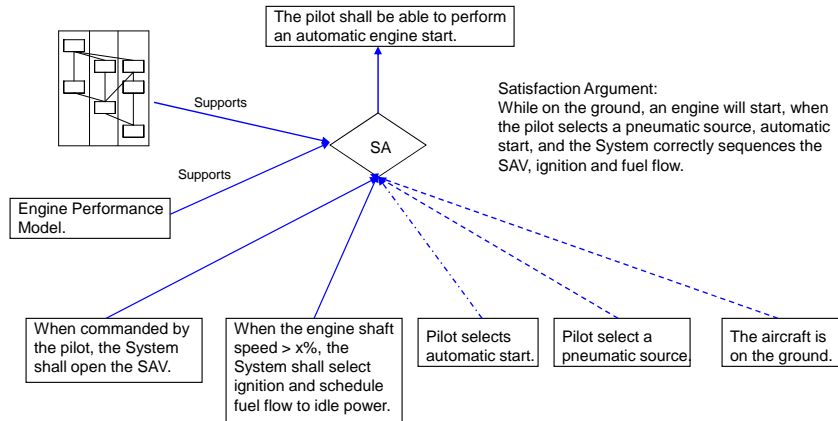
12

- This relationship  $D, S \vdash R$ , called a Satisfaction Argument (SA) should be read as:
  - When the relevant properties of the application domain (D) are combined with the specifications (S), it is possible to show that the requirements (R) will hold.
- Graphically, this is represented as:



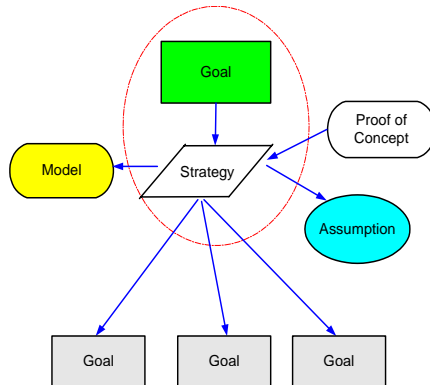
# REVEAL & Satisfaction Arguments

## Example Satisfaction Argument

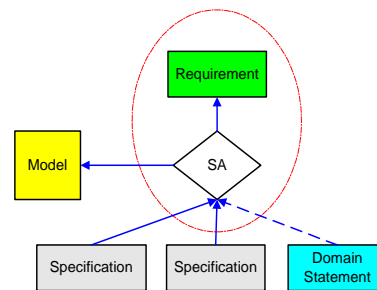


# Common Elements?

## Suitability Argument



## Satisfaction Argument



Most items in both models appear equate well, but not all.

Converting from a SA to a safety argument relatively easy, but the reverse is more problematic.

## The Bits That Don't Fit

15

- **Proof of Concept**
  - Complex relationships require verification.
  - Complex satisfaction arguments should be verified.
- **Strategy & Goal vs. Requirement & SA**
  - Don't need a strategy if the relationship is clear; similarly, where the relationship is clear no SA necessary.
- **Justifications and Context**
  - Useful supporting information.

## Do the Arguments Help?

16

- **Must be useful to understand why we think something is true.**
- **A understanding of arguments will assist cooperation between safety and requirements engineers.**
- **Safety engineers need confidence that:**
  - The higher-level requirements are satisfied by the lower-level requirements (necessary and sufficient).
  - Derived requirements are correctly identified.
  - The criticality relationship between requirements is well understood.
- **SA appears to assist the thought process used to construct a safety argument.**
  - Anecdotal evidence only.
  - Require a study to confirm initial impression.

## Concluding Remarks & Questions

17

- We should make more use of arguments.
- Both argument structures are very similar, and, with a little effort, could be merged.
- Difficult to quantify the benefits of a merged notation:
  - Requires further investigation, but anyway
  - improved use of arguments beneficial.
- What experience do you have of applying arguments to large, complex systems?

## References

18

- (1) Kelly, T., A Systematic Approach to Safety Case Management, Proceedings of SAE 2004 World Congress, Detroit, March 2004.
- (2) ASCAD, Adelard Safety Case Development Manual, 1998.
- (3) Hammond, J., Rawlings, R. & Hall, A., Will it Work?, 5<sup>th</sup> IEEE International Symposium on Requirements Engineering, 2001.
- (4) Attwood, K. & Wilkinson, P., An Argument-Based Approach to the Integration of Safety and Design, The Journal of the Safety and Reliability Society, Vol. 29, No 4, 2009.