‘That wasn't meant to happen!' Managing the hidden risks of system novelty

Jonathan E. Holt, System Design Specialist

Richard Beasley, Engineering Associate Fellow & Global Chief of Systems Engineering

Rolls-Royce plc

Diversity, Complexity, Novelty

ROLLS ROYCE Rolls-Royce

Route Map

- Technology acquisition and risk mitigation
- Sources of novelty and risk
- Recommended terminology
- Proposed process for system technology maturation
- 2 case studies

Technology Acquisition *is* Risk Mitigation

- But what is meant by 'new technology'?
- The scope of the term is (like so much in Systems Engineering) underestimated.
  - Component level novelty
  - System level novelty
  - Environment level novelty

Component Level Novelty

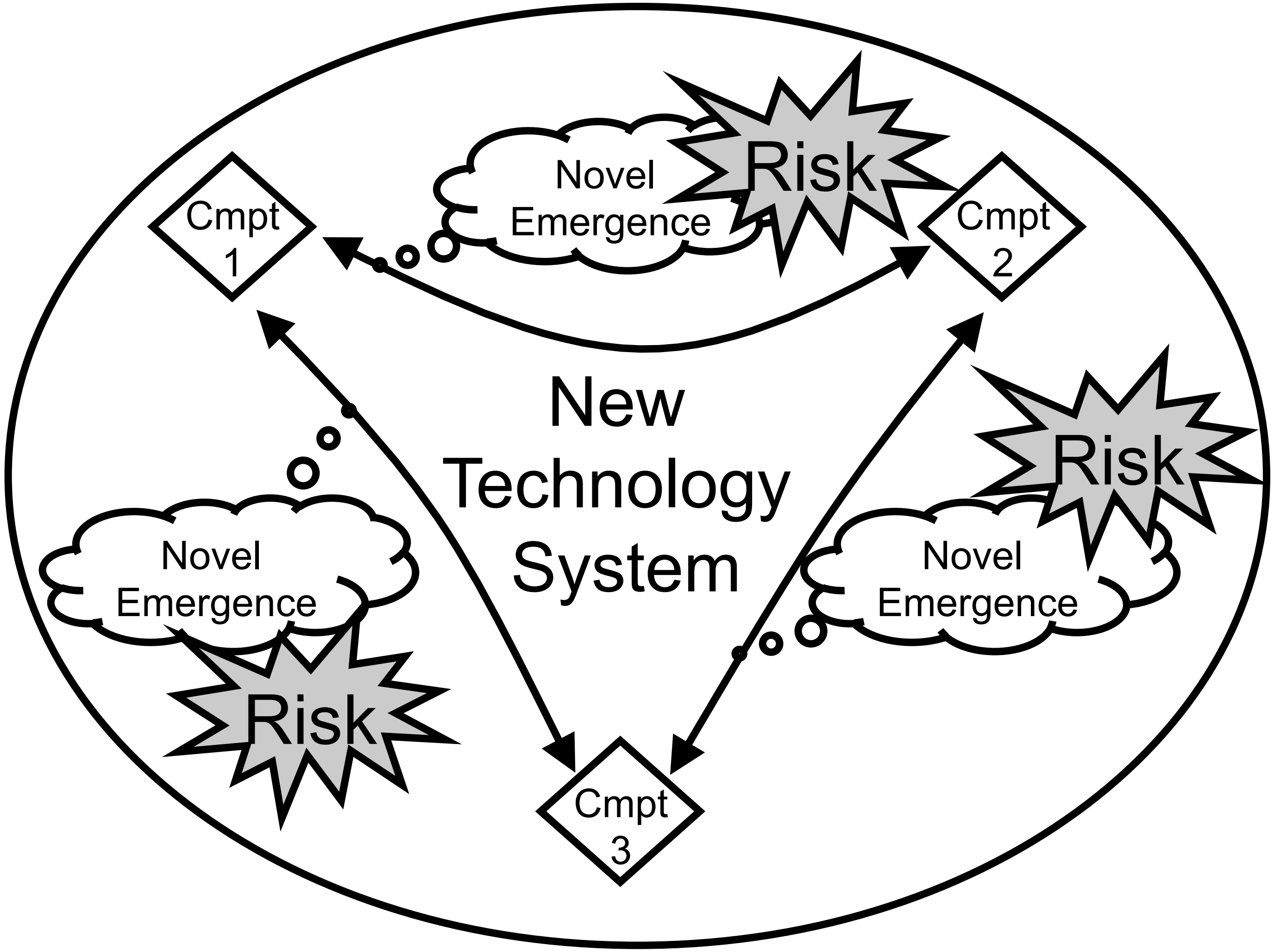
- …Readily recognised by most people

TRL	Definition
System validation:	
9	Actual system proven through successful mission operation
8	Actual system completed and service qualified through test and demonstration
7	System prototype demonstration in an operational environment
Technology validation:	
6	System/subsystem model or prototype demonstration in a relevant environment
5	Component and/or partial system validation in a relevant environment
Applied and strategic research:	
4	Component and/or partial system validation in a laboratory environment
3	Analytical and experimental critical function and/or characteristic proof-of-concept
2	Technology concept and/or application formulated
1	Basic principles observed and reported

Rolls-Royce Technology Readiness Level Definitions

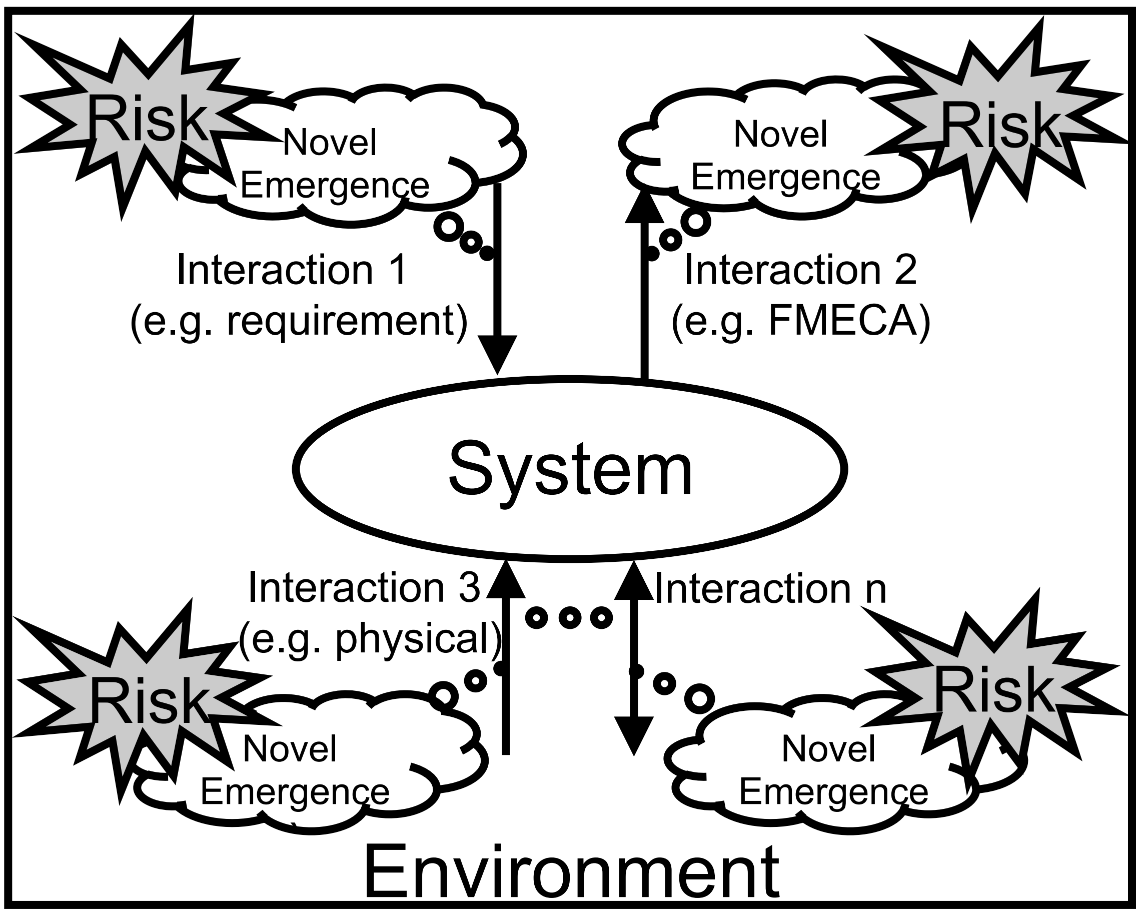
System Level Novelty

Consider a novel system of 3 non-novel components:



Environment Level Novelty

Consider a non-novel system inserted into a novel environment:



All Sources of Novelty and Risk

- Novelty and risk can be
  - contained within a component
  - contained within the way non-novel components are combined within a system
  - due to a novel environment (in the fullest systems sense) for an otherwise non-novel system.
- .... or any combination

$$Risk_{(system)} = f\left(\sum_{x=1}^{n} Risk_{(Component x)}, Risk_{(System)}, Risk_{(Environment)}\right)$$

Recommended Terminology

- ‘System Readiness’...?
  - Suggests Systems is somehow separate from other technology readiness.
  - Our view is there is no place for a separate TRL scale for systems

In fact: what is needed is *a Systems approach to* technology readiness.

Hence:

- ‘Technology Readiness of a System’

OR:

- ‘System TRL’

System Technology Development Dilemma

- Demonstrator engine run to confirm TRL6

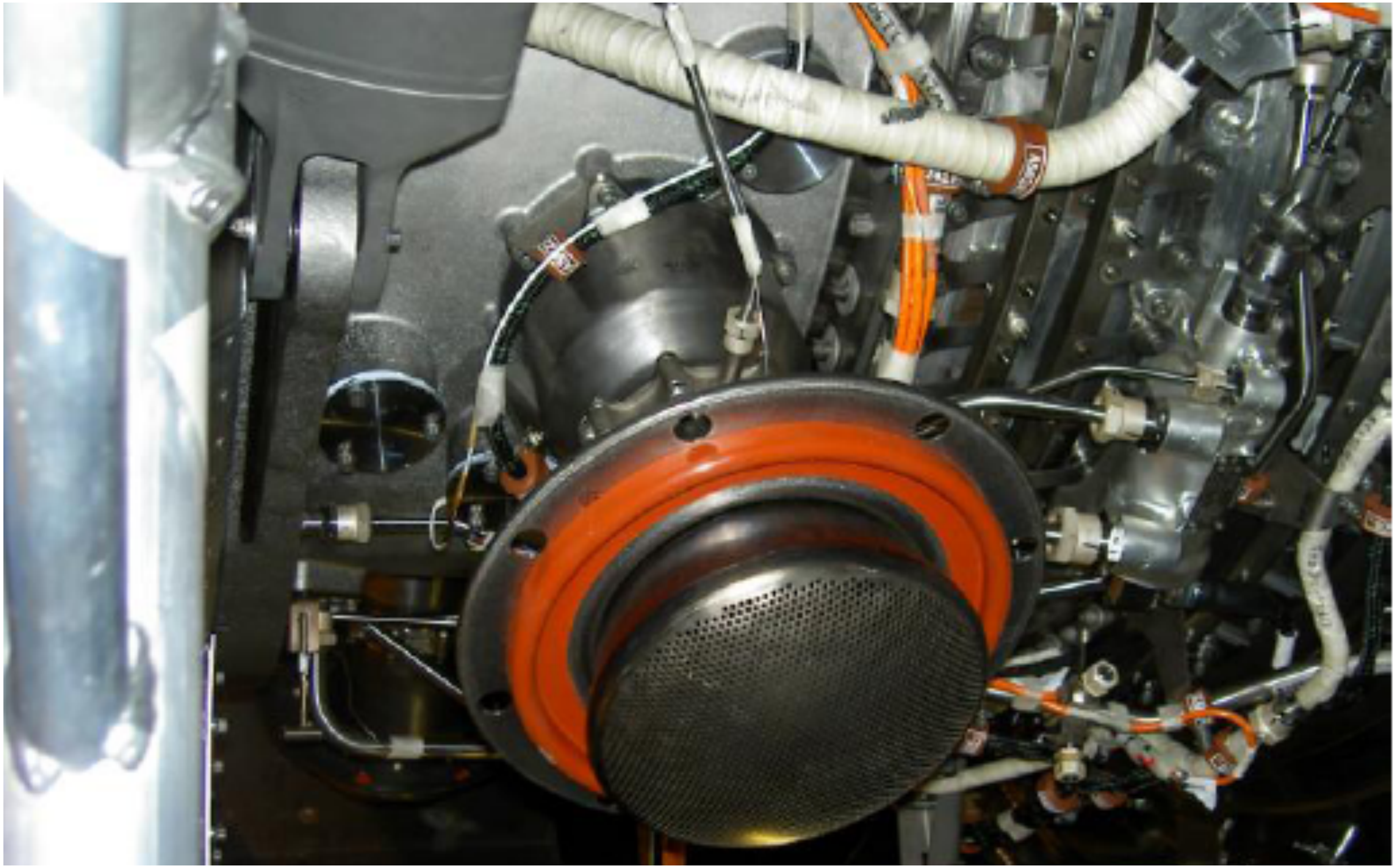
The key:

- Identify and de-risk every interaction
    - Identify and de-risk every interaction
    - Analysis
    - Simulation
- Full-scope prototype

System Technology Maturation Process

	System Maturity Process Step
1	Identify the system under consideration, including its components, role and environment.
2	Identify the specific types of risk and concern associated with both the system and the process of its development. In which category or categories are the focus of risk? This could be done via risk review.
3	Conduct a system failure assessment - This is similar to a Functional Hazard Assessment, but covers all failures, both those with a safety and a non-safety customer impact.
4	Employ Robust Design techniques to establish that the proposed system is capable of functioning across a practicably wide range of contexts. - This is needed not just to cover environment variation (for example. the use on more than one product) but also to cover the uncertainty as to the precise attributes of the environment.
5	Identify validation means to derisk the areas identified in step 2. - These might include running in a simulated context around the full range of conditions and scenarios to be considered in service.
6	Perform validation as identified
7	Validate any simulated context - Validation of any simulation is an integral part of the system technology validation. - If a simulation cannot be validated then the simulation route is not available for system technology validation. On the other hand, if the design is sufficiently robust (4), the fidelity required of the simulation may be lower.
8	Submit system technology validation evidence to review. The choice or reviewers is important; experts are needed who possess both the right domain knowledge and the capability to deploy appropriate systems thinking.

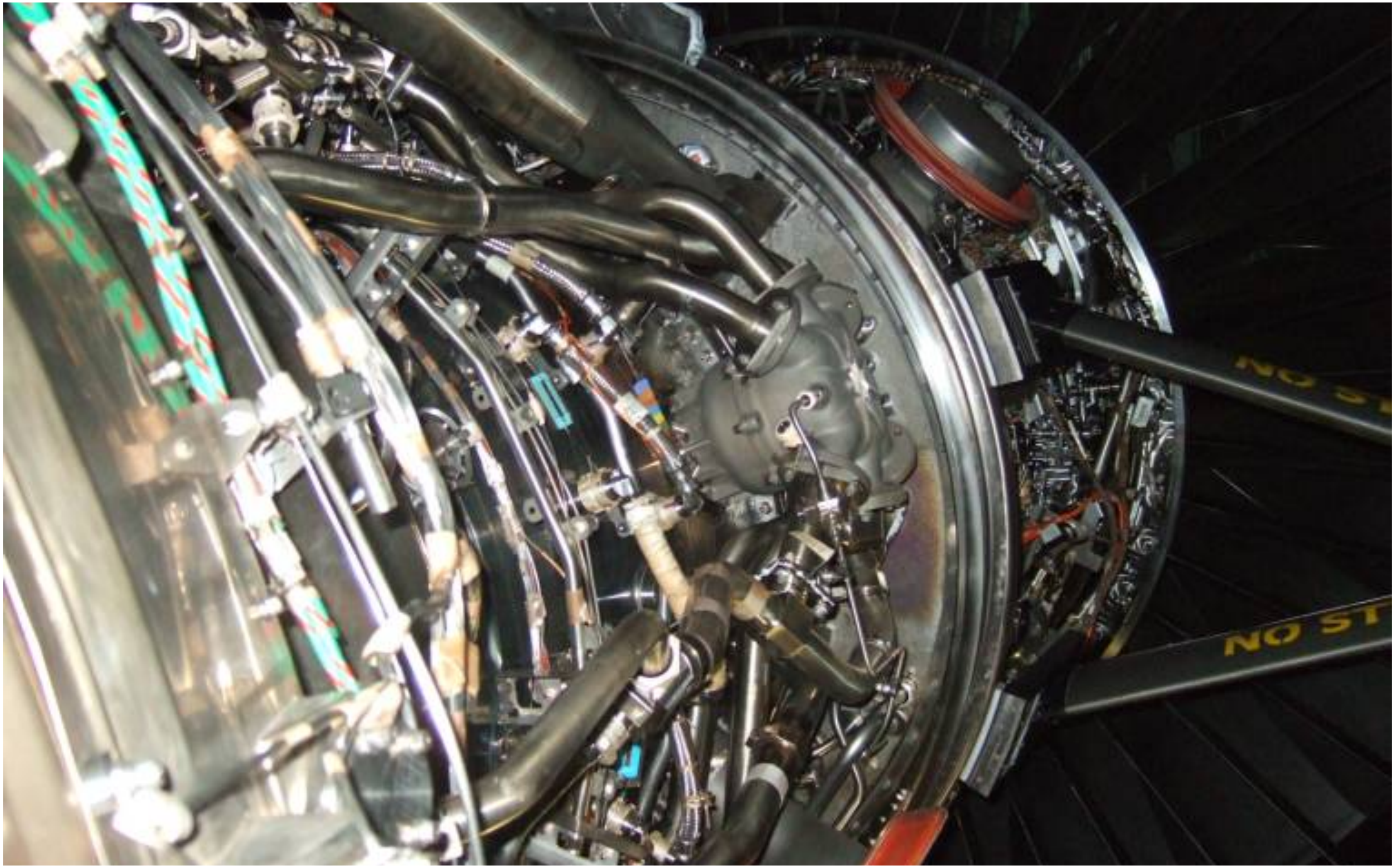
Case Study 1: Handling Bleed Valve



Process applied to Handling Bleed Valve

	System Maturity Process Step	Applied to Handling Bleed Valve
1	Identify the system under consideration, including its components, role and environment.	Electrical signal, solenoid valve, solenoid air line and bleed valve, mounted in ventilated zone around engine core.
2	Identify the specific types of risk and concern associated with both the system and the process of its development. In which category or categories are the focus of risk? This could be done via risk review.	Novelty in physical environment for valve (temperature and vibration); other compoents in system unchanged. Scheduling unchanged.
3	Conduct a system failure assessment - This is similar to a Functional Hazard Assessment, but covers all failures, both those with a safety and a non-safety customer impact.	Failure effects unchanged
4	Employ Robust Design techniques to establish that the proposed system is capable of functioning across a practicably wide range of contexts. - This is needed not just to cover environment variation (for example. the use on more than one product) but also to cover the uncertainty as to the precise attributes of the environment.	New design technicals and/or materials to cope with increase in temperature and environment *whilst still leaving margin.*
5	Identify validation means to derisk the areas identified in step 2. - These might include running in a simulated context around the full range of conditions and scenarios to be considered in service.	Qualification testing of bleed valve
6	Perform validation as identified	Performa qual testing
7	Validate any simulated context - Validation of any simulation is an integral part of the system technology validation. - If a simulation cannot be validated then the simulation route is not available for system technology validation. On the other hand, if the design is sufficiently robust (4), the fidelity required of the simulation may be lower.	Not appicable
8	Submit system technology validation evidence to review. The choice or reviewers is important; experts are needed who possess both the right domain knowledge and the capability to deploy appropriate systems thinking.	Simple review of qual test evidence; this will most likely be combined with an existing project gate review.

Case Study 2: Modulating Air System



Process applied to Modulating Air System

	System Maturity Process Step	Applied to Switched Air System
1	Identify the system under consideration, including its components, role and environment.	Electrical signals, solenoid valves, solenoid air lines, valve, pipework and sensors, all mounted in ventilated zone around engine core.
2	Identify the specific types of risk and concern associated with both the system and the process of its development. In which category or categories are the focus of risk? This could be done via risk review.	Novelty in physical environment for valve (temperature and vibration); novel and hard to understand system functional interaction with the engine; serious, novel and poorly understood failure effects; novel, complex and difficult to understand interaction
3	Conduct a system failure assessment - This is similar to a Functional Hazard Assessment, but covers all failures, both those with a safety and a non-safety customer impact.	Serious, novel and difficult to understand failure effects.
4	Employ Robust Design techniques to establish that the proposed system is capable of functioning across a practicably wide range of contexts. - This is needed not just to cover environment variation (for example. the use on more than one product) but also to cover the uncertainty as to the precise attributes of the environment.	Because of the difficulty of understanding of the interactions between the system and its environment, and because of constraints on the design, the design cannot be made robust.
5	Identify validation means to derisk the areas identified in step 2. - These might include running in a simulated context around the full range of conditions and scenarios to be considered in service.	Detailed dynamic simulation of the air system (perhaps stretching existing modelling capability); detailed thermal modelling and analysis of certain engine components to validate system failure assessment; full system integration test to assess robustness
6	Perform validation as identified	Perform system simulation, analysis and testing.
7	Validate any simulated context - Validation of any simulation is an integral part of the system technology validation. - If a simulation cannot be validated then the simulation route is not available for system technology validation. On the other hand, if the design is sufficiently robust (4), the fidelity required of the simulation may be lower.	Additional engine level testing to validate correctness of simulation and analysis. (Note that because robust design was difficult, accuracy of simulation needs to be good.)
8	Submit system technology validation evidence to review. The choice or reviewers is important; experts are needed who possess both the right domain knowledge and the capability to deploy appropriate systems thinking.	Separate systems expert review, covering simulation, analysis and test evidence and ensuring complete coverage of the system risks and concerns.