University of Southampton

# SESA6085 – Advanced Aerospace Engineering Management

Lecture 12

2024-2025

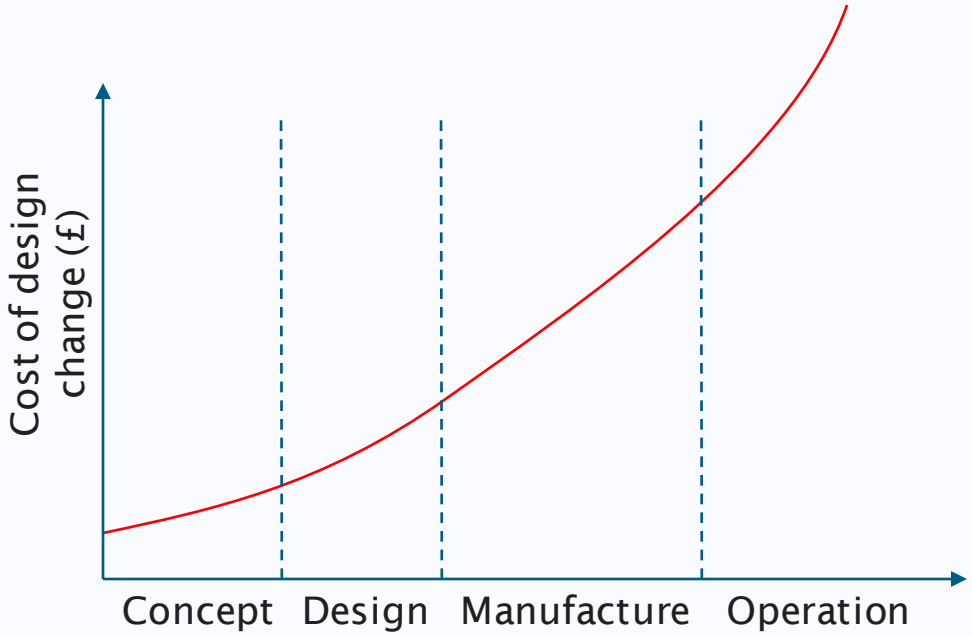
Dr David Toal

University of Southampton

# Design for Reliability

# Reliability Within Design

- Reliability is strongly linked to decision making as part of the design process
- Any design issues which impact reliability become progressively more expensive to correct as product development moves forward



# Reliability Within Design

- Design processes should therefore be employed which both minimise failure and detect design issues as early in the development process as possible
- The concept of “test analyse & fix” has no place in todays modern design processes due to constraints on cost, shorter development cycles etc.

# Design for Reliability

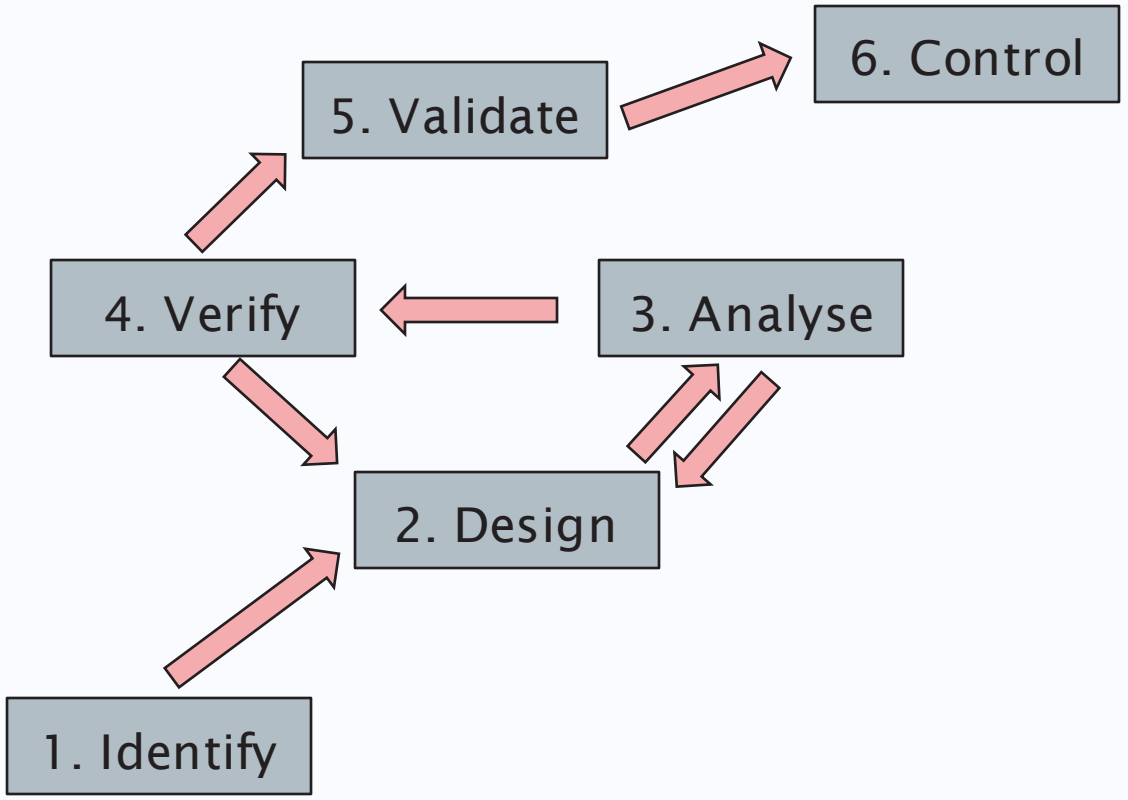
- Reliability must therefore be explicitly designed into the product
  - A process called Design for Reliability (DfR)
- To improve performance and reduce costs this process should be integrated throughout the whole life cycle of a product

# Design for Six Sigma

- The process of DfR is similar in some respects to Design for Six Sigma but there are a number of differences
  - Six Sigma aims to reduce variation in the final design and therefore mainly focuses on manufacturing
  - DfR, however, focuses on reliability
  - The two processes can be linked as manufacturing variations can impact reliability

# Design for Reliability Process

- A generalised sequence of engineering activities in order to design for reliability is illustrated below:



# Identify

- This defines the process whereby the system requirements are understood and translated into reliability requirements
  - If a car should run for 200,000 hrs without incident how does this translate to requirements for the reliability of the engine, brakes, transmission etc.
- Once defined these top level requirements can then be allocated to appropriate subsystem designers
  - Engine reliability requirements go to the engine design team etc.

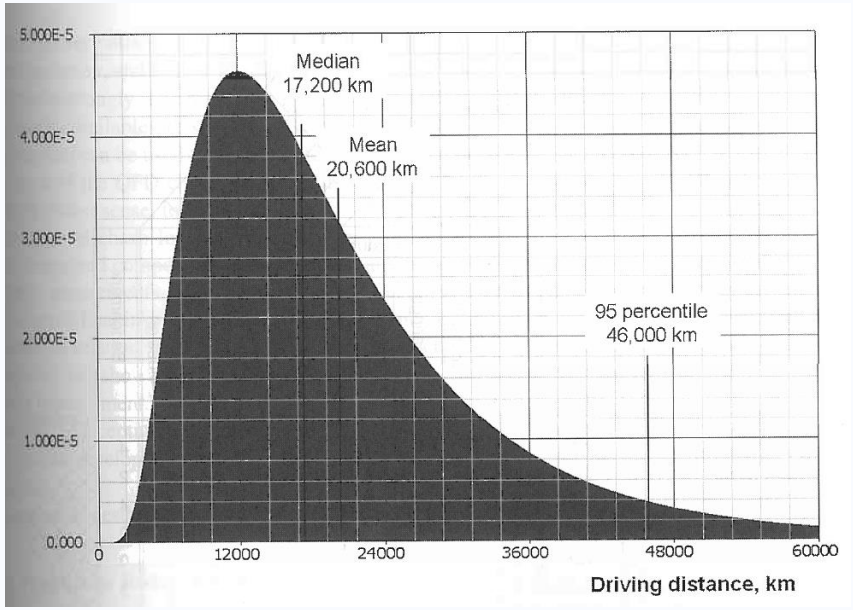
University of Southampton

# Identify

- The reliability team also begins to collect data which can be used to determine reliability
  - System usage profiles
  - Benchmarking data
- Differences relative to legacy products can be defined and used to help judge program risk
- New technologies within the system can be identified and work can begin on their reliability analysis
- Future testing and validation costs can also begin to be predicted at this stage

# System Usage Profiles

- System usage profiles are very important for designers as they help to give an indication of the loads that their design will be subjected to and the reliability performance that is expected
  - E.g. data on the distances driven by cars in Europe



# Benchmarking

- Benchmarking during the "identify" stage can include benchmarking against competing products or indeed processes
  - Helps to define the level of reliability expected by the customer
  - Helps to build a marketing case
  - Comparing and adopting rivals processes for reliability assessment and control

University of Southampton

# Design

- The "Design" stage defines the specific activities associated with design
- At this stage we start to gain a picture of the system's layout and its component parts
- This information means that more formal reliability analysis techniques can begin to be used
  1. Reliability block diagrams
  2. FMECA
  3. Fault tree analysis
  4. HAZOPS etc.
- Regular design peer reviews are held to highlight any issues as early as possible

# Failure Modes, Effects & Criticality Analysis (FMECA)

- Also known as Failure Modes & Effects Analysis (FMEA)
- In this process every failure mode is considered for every component and the effects on the system operation are considered
  - Can also be subsystem level failures
- Failure modes are then classified in relation to their severity
- This process is normally performed by a team of engineers with thorough knowledge of the design

# FMECA

- FMECA is performed using a table such as the following:

| Process Step/ Function / Requirements | Potential Failure Mode | Potential Effect(s) of Failure | Severity | Classification | Potential Cause(s) of Failure | Occurrence | Current Process Controls Prevention | Current Process Controls Detection | Detection | RPN | Recommended Action | Responsibility & Target Completion Date | Action Results | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | Actions Taken & Effective Date | Severity | Occurrence | Detection | RPN |
| | | | | | | | | | | | | | | | | | |

- Also included in the FMECA are the actions and the risk priority number (RPN) resulting from those actions
- It should be noted that there are multiple different standards defining the layout of such FMECA tables but they generally have a similar structure

# FMECA

- Each item in the table is assigned a risk priority number (RPN) or a similar metric to assess risk
  - The severity, likelihood of occurrence & likelihood of prior detection are rated on a scale from 0-10
  - 10 defines a high risk, 1 defines a low risk

$$RPN = severity \times occurance \times detection$$

- This metric helps to prioritise potential reliability issues

# FMECA Car Door Example

| Item / Function | Potential Failure Mode | Potential Effect(s) of Failure | Sev | Class | Potential Cause(s)/Mechanism(s) of Failure | Occur | Current Design Controls | Detec | RPN |
|---|---|---|---|---|---|---|---|---|---|
| 3 - Front Door L.H. | | | | | | | | | |
| - Ingress to and egress from vehicle.<br>- Occupant protection from weather, noise, and side impact.<br>- Support anchorage for door hardware including mirror, hinges, latch and window regulator.<br>- Provide proper surface for appearance items - paint and soft trim. | Corroded interior lower door panels | Deteriorated life of door leading to:<br>- Unsatisfactory appearance due to rust through paint over time.<br>- Impaired function of interior door hardware. | 7 | | Upper edge of protective wax application specified for inner door panels is too low. | 6 | Vehicle general durability test veh.<br>T-118<br>T-109<br>T-301 | 7 | 294 |
| | | | | | Insufficient wax thickness specified. | 4 | Vehicle general durability testing - as above.<br>- Detection | 7 | 196 |
| | | | | | Inappropriate wax formulation specified. | 2 | Physical and Chem Lab test - Report No. 1265.<br>- Detection | 2 | 28 |

# FMECA Car Door Example

| Potential Cause(s)/Mechanism(s) of Failure | Recommended Action(s) | Responsibility & Target Completion Date | Action Results | | | | |
|---|---|---|---|---|---|---|---|
| | | | Actions Taken | Sev | Occ | Det | RPN |
| Upper edge of protective wax application specified for inner door panels is too low. | Add laboratory accelerated corrosion testing. | A. Tate Body Engrg - 2/25/2003 | Based on test results (Test No. 1481) upper edge spec raised 125 mm. | 7 | 2 | 2 | 28 |
| Insufficient wax thickness specified. | Add laboratory accelerated corrosion testing. | A. Tate Body Engrg - 3/28/2003 | Test results (Test No. 1481) show specified thickness is adequate. | 7 | 2 | 2 | 28 |
| | Conduct Design of Experiments (DOE) on wax thickness. | A. Tate Body Engrg - 3/28/2003 | DOE shows 25% variation in specified thickness is acceptable. | | | | |

Recommended actions and the results of those actions can be recorded in the FMECA

# FMECA

- Reliability block diagrams and fault tree analyses can be used to help prepare the FMECA
- Generally the FMECA process should commence as soon as a design has been defined and it should be repeated throughout the design process
- The evolution of the FMECA therefore:
  - Helps document design decisions
  - As well as driving design decisions itself

# FMECA

- The FMECA can also help to identify important features of any eventual system test program e.g.
  - Helps to define diagnostic routines
  - Helps to identify where redundancy should be included

- Note: In practice FMECA is not a trivial process and can be quite involved and time consuming but is nevertheless an important part of a design for reliability process

# Hazard Operability Study (HAZOPS)

- HAZOPS is a process used to systematically determine potential hazards and hence the methods to remove or minimise them
- This is different from a risk assessment
  - HAZOPS identifies hazards which may be present
  - Risk assessment considers the likelihood and consequences of those hazards
  - A HAZOPS may form part of a risk assessment

# HAZOPS

- A HAZOPS study typically involves a multi-disciplinary team with expert knowledge about the system
- This team systematically consider each part of the system applying a set of guide words to determine the consequence of operating conditions outside the design intentions

# HAZOPS

- There are a number of terms used in a HAZOPS
  - *Intentions*: defines how the part is expected to perform
  - *Deviations*: departures from the design intent discovered through application of the guide words
  - *Causes*: the reasons for the deviations
  - *Consequences*: the results of the deviations
  - *Hazards*: consequences which cause damage, injury or loss
  - *Guide words*: simple words used to qualify intention and hence deviations

# HAZOPS

- Guide words are used to inspire the participants to stimulate thoughts to identify hazards
- Example guide words include

| | | |
|---|---|---|
| - No/not | -More | -Less |
| -As well as | -Part of | -Reverse |

- Other guide words can be more application specific

# HAZOPS

- As part of a HAZOPS the following questions might therefore be asked:
  - What actions are required to start/shutdown the machine safely?
  - If the machine is accidently switched on what damage might occur?
  - What happens if the machine is overloaded?

# HAZOPS

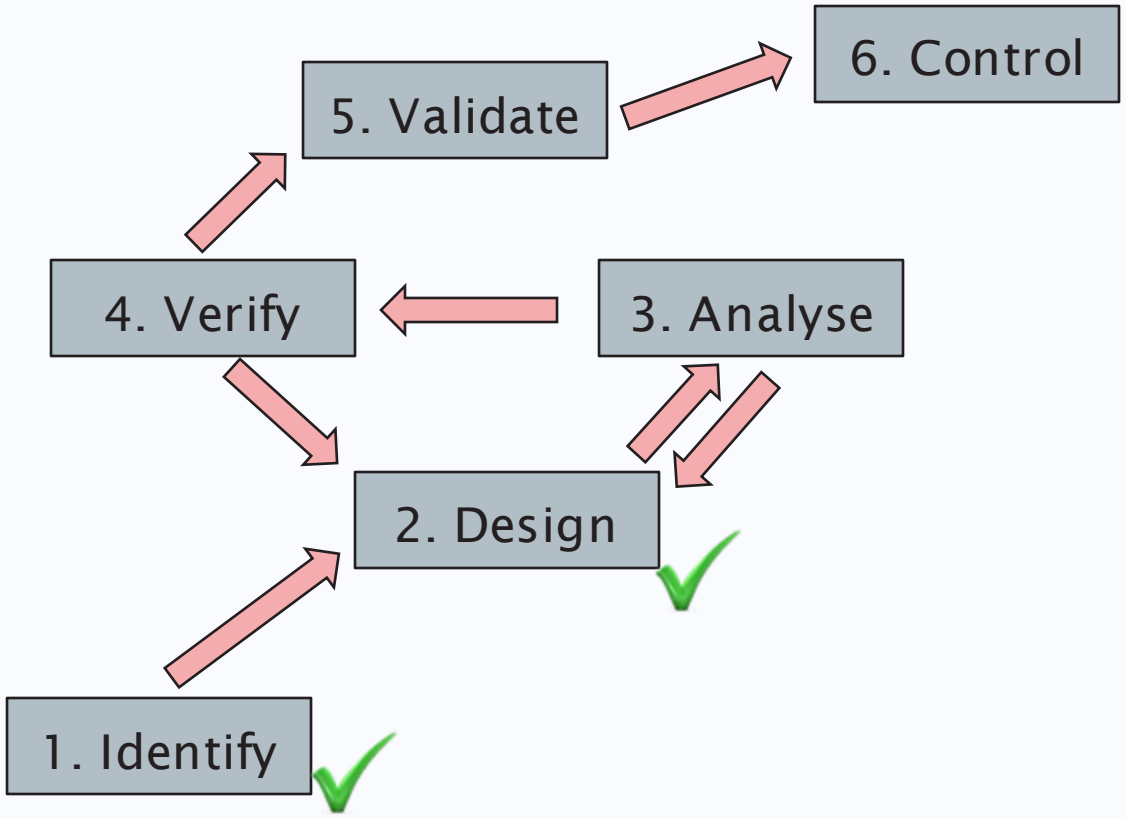
- Each HAZOPS proceeds in a structured manner
- As hazards are detected the study leader ensures that the team members fully understand them
- Solutions may be agreed and design changes implemented
  - Although if the team has no authority to make changes these are highlighted to the appropriate designer(s)
- During the session any identified hazards are recorded in a HAZOPS record sheet

# HAZOPS Record Sheet Example

| Guide word | Deviation | Possible cause | Consequences | Safeguards/ interlocks | Action required |
|---|---|---|---|---|---|
| System 23 process vent | | | | | |
| MORE OF | High flow | Failure to close off the UMV and WV with subsequent opening of EVV<br><br>Erosion of restriction orifice | Possible overpressure of vent systems. Orifice RO 022 sized to hold back wellhead pressure upstream and maintain pressure downstream at or below design pressure of vent system | Detection of flow is via TSL 503 set at –10 °C | Procedures should allow for inspection of orifice plate after the use of the blowdown system |
| LESS OF | Low flow<br>(i) Manual venting of test separator and liquid measurement drum | Blockage, especially of flame arrestor, especially by hydrates during venting | Vent pipework will see full system pressure. This will overpressure the vent system | | The removal of the flame arrestor should be considered because of the hazard potential of the blocked arrestor |
| | (ii) Emergency venting via EVV | As above but also the possibility that the valve does not open fully | Takes longer to depressurize, and thus may increase inventory | | HAZ1 – The whole of the ventilation system needs to be reviewed with respect to safe dispersion of released gases |
| | (iii) Relief valves | Failure of heat tracing downstream of PSV and a leaking PSV will lead to hydrate blockage. Subsequent relief requirement may not be met. Relief valve failure to lift | Possible overpressure of vessel in first case. Note that relief valves will not protect the vessel in the case of a jet fire | | Procedures to include periodic check of all heat tracing |
| NO/NONE | No flow | EVV fails to lift. As for low flow | No hazard because personnel available to correct the situation | | |

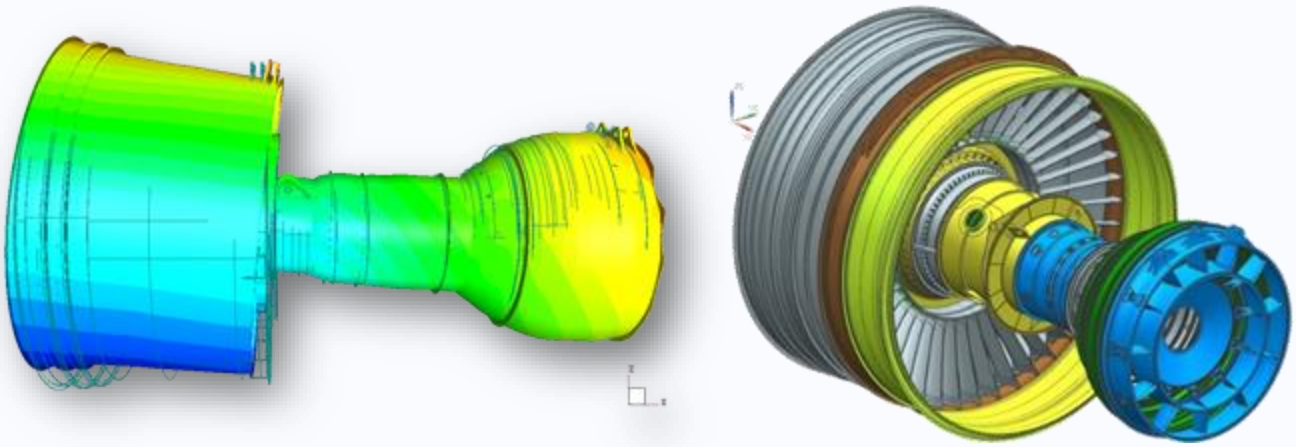
# DfR Process Recap

- Where have we got to?



# Analyse

- Potential causes of failure are further analysed once the design has been more physically defined
- Physics based analysis/simulation comes into play
  - FEA, CFD etc.
- Results of these analyses can be related to, or used in other models, to assess component, sub-system or system reliability



# Analyse

- Results of any analysis may be fed back to the design stage to update the design in an iterative manner
- Automated optimisation loops may even be employed with reliability as a design objective or constraint
- The modern design process puts heavy emphasis on such simulations within the process due to their relative speed and cost effectiveness

# Verify

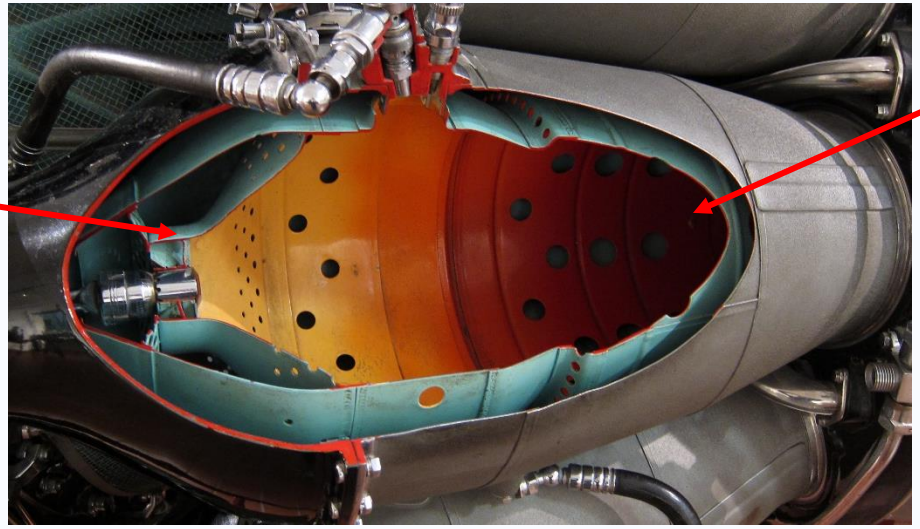
- At this stage a prototype is available and physical tests can be performed
  - Accelerated life testing can be carried out
  - Failure tests and degradation tests
  - Performance tests under environmental uncertainty
  - Typically this is at a sub-system or component level rather than at the full system level

# Verify

- Combustor component verification may include…

Isothermal swirler performance tests

Isothermal combustor flow tests



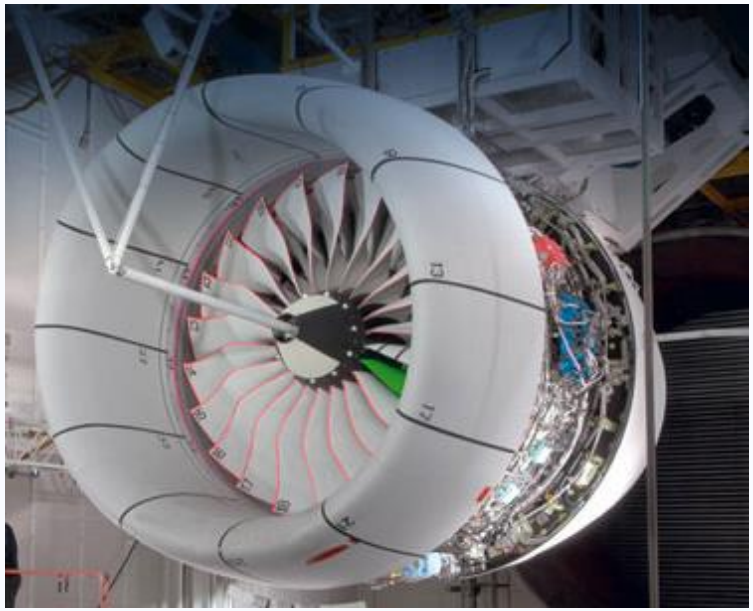
A gas turbine combustor

# Verify

- Results from the verification stage can be used to make design changes
- However, ideally we want these changes to be a few as possible (remember the cost of changes graph)
- But as we're at a component level changes cost less than when at the system level
- Results of this process can also be used to help future designs and increase confidence in their reliability predictions

# Validation

- The validation stage aims to ensure that all reliability requirements have been met
- Aims to resolve any remaining reliability issues
- At this stage system level tests are carried out



# Control

- The final stage of DfR aims to control the manufacturing process and reduce variability
  - As previously noted, variability can be a key driver when considering reliability
- The control stage has a lot in common with design for six sigma and techniques used in six sigma can be used here
- In reality some of these control aspects are employed through the entire design process e.g. design for uncertainty etc.


University of
Southampton