# Design for Minimum Risk

Jon Wetherholt, Co-author, NASA Marshall Space Flight Center, Huntsville, Alabama, USA
Timothy J. Heimann, Co-author, NASA Marshall Space Flight Center, Huntsville, Alabama, USA

Keywords: Redundancy, Failure Tolerance, Design for Minimum Risk, Safety Analysis Processes

## Abstract

Design for Minimum Risk (DFMR) is a term used by NASA programs as an expansion of the general hazard reduction process where if an identified hazard cannot be eliminated, the design is modified to reduce the associated mishap risk to an acceptable level. DFMR is a set of specific requirements to minimize risk. DFMR is not well understood and there are many misconceptions concerning the meaning and use. This paper will provide insight into the use of DFMR for space applications; it's comparison to other hazard mitigation strategies and examples of how the approach has been used in the past. It will also highlight documents used by NASA on various programs to determine DFMR.

## Background

Since most projects/programs use failure tolerance as the primary and preferred approach to control hazards, it will be discussed first. Failure tolerance is the concept of having redundant means to provide a function to protect against failure of one of the means. A simple example is having matches to back up failure of a lighter for starting a fire. A second lighter would work but may be prone to the same failure mode of the first lighter. A more complex example might be a spacecraft with multiple batteries, each able to perform the function of providing power without the other battery.

Failure tolerance increases the likelihood that a required function is available when needed by increasing reliability of the safety function through redundancy. This does not alleviate the need for quality of the chosen components. Three low quality or poorly designed redundant components do not assure function and may provide a sense of false security. Another aspect of redundancy is common cause failures. This leads to design with unlike redundancy. In the previous example of matches and lighter, the lighter may not be as prone to moisture issues while the matches may be less of a long term storage issue.

As the redundant item becomes more difficult to integrate, it may inject additional failure modes, complexity, or sometimes prevent the overall function of the system. In the case of the batteries, diodes or fuses must protect the additional batteries from each

other so that failure of one does not propagate a failure to another. This means diodes, fuses, and switches, all of which could fail, preventing the system from providing the required power. The structure of a pressure vessel is a more obvious example. Is it practical to provide two pressure vessels, one inside the other, to mitigate leakage or rupture? If there is a rupture of the inner vessel, the effectiveness of an outer vessel is very much in question. The rupture of the inner vessel may very well contribute to a rupture of the outer vessel. It may be more effective to reduce the stress in one vessel by thickening the wall. How much thickening is sufficient and does thickening cause additional failure modes? The mass of the system may also be prohibitive. For example if a redundant battery system and its associated protection hardware becomes too heavy, it may prohibit the overall function of the space craft. This is the beginning of the DFMR investigation.

The NASA Procedural Requirements (NPR) for Human-Rating Space Systems (Reference 1) states this clearly “First and foremost, the failure tolerance is applied at the overall system level – to include all capabilities of the system. While failure tolerance is a term frequently used to describe minimum acceptable redundancy, it may also be used to describe two similar systems, dissimilar systems, cross-strapping, or functional interrelationships that ensure minimally acceptable system performance despite failures, or additional features that completely mitigate the effects of failures. Even when assessing failure tolerance at the integrated system level, the increased complexity and the additional utilization of system resources (e.g. mass, power) required by a failure tolerant design may negatively impact overall system safety as the level of failure tolerance is increased.

Ultimately, the level and type of redundancy (similar or dissimilar) is an important and often controversial aspect of system design. Since redundancy does not, by itself, make a system safe, it is the responsibility of the engineering and safety teams to determine the safest practical system design given the mission requirements and constraints. Additionally, the overall system reliability is a significant element of the integrated safety and design analysis used in the determination of the level of redundancy. Redundancy alone without sufficient reliability does not meet the intent of this requirement.

When a critical system fails because of improper or unexpected performance due to unanticipated conditions, similar redundancy can be ineffective at preventing the complete loss of the system. Dissimilar redundancy is very effective provided there is sufficient separation among the redundant legs. (For example, dissimilar redundancy where the power for all redundant capability was routed through a common conduit would not survive a failure where the conduit was severed). It is also highly desirable that the spaceflight system performance degrades in a predictable fashion to allow sufficient time for failure detection and, when possible, system recovery even when experiencing multiple failures.

There are examples of dissimilar redundancy in current systems. For Earth reentry, the Soyuz spacecraft has a dissimilar backup ballistic entry mode to protect for loss of the

primary attitude control system and a backup parachute for landing. Other examples include backup batteries for critical systems that protect for loss of the primary electrical system and the use of pressure suits during reentry to protect for loss of cabin pressure. Ultimately, the program and Technical Authorities evaluate and agree on the failure scenarios/modes and determine the appropriate level of failure tolerance and the practicality of using dissimilar redundancy or backup systems to protect for common cause failures."

## Understanding DFMR

Design for Minimum Risk (DFMR) is more than increased margin; it is an approach that relies on years of proven capability. DFMR relies on robust design, standard approach, and high quality to provide the increased likelihood the required function is available. These aspects require a well-understood desired function together with a fully developed quality system to be effective. Safety Design for Space Systems (Reference 2) states, " The selection of this approach is not simply an alternative to failure tolerance because of cost, schedule, or noncompliance with failure tolerance but rather a deliberate decision to select a proven design concept that has been demonstrated through experience the characteristic of eliminating or reducing credible failures."

The NPR for Human-Rating Space Systems (Reference 1) states, "Failure of primary structure, structural failure of pressure vessel walls, and failure of pressurized lines are excepted from the failure tolerance requirement provided the potentially catastrophic failures are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance. Other potentially catastrophic hazards that cannot be controlled using failure tolerance are excepted from the failure tolerance requirements with concurrence from the Technical Authorities provided the hazards are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance. Rationale: The overall objective is to provide the safest design that can accomplish the mission given the constraints imposed on the program. Since space system development will always have mass, volume, schedule, and cost constraints, choosing where and how to apply failure tolerance requires integrated analyses at the system level to assess safety and mission risks…

Where failure tolerance is not the appropriate approach to control hazards, specific measures need to be employed to: (1) Recognize the importance of the hazards being controlled; (2) Ensure robustness of the design; and (3) Ensure adequate attention/focus is being applied to the design, manufacture, test, analysis, and inspection of the items. In the area of design, in addition to the application of specifically approved standards and specifications, these measures can include identification of specific design features which minimize the probability of occurrence of failure modes, such as application of stringent factors of safety or other design margins. For manufacture, these measures can include establishing special process controls and documentation, special handling, and highlighting the importance of the item for those involved in the manufacturing process. For test, this can include accelerated life testing,

fleet leader testing program, testing to understand failure modes or other testing to establish additional confidence and margin in the design. For analysis (in lieu of tests), these measures can include correlation with testing representative of the actual configuration and the collection, management, and analysis of data used in trending failures, verifying loss of crew requirements, and evaluating flight anomalies. For inspection, these measures can include identification of specific inspection criteria to be applied to the item or the application of Government Mandatory Inspection Points for important characteristics of the item. This approach to hazard control takes advantage of existing standards or standards approved by the Technical Authorities to control hazards associated with the physical properties of the hardware and are typically controlled via application of margin to the environments experienced by the design or system properties effected by the environment. Acceptance of these approaches by the Technical Authorities avoids processing waivers for numerous hazard causes where failure tolerance is not the appropriate approach. This includes, but is not limited to, Electro-Magnetic Interference, Ionizing Radiation, Micrometeoroid Orbital Debris, structural failure, pressure vessel failure, and aerothermal shell shape for flight."

In addition to the NPR for Human-Rating, NASA has a number standards which have been developed over many years considering failures and successes which define specific DFMR requirements. These standards must be either met or exceeded. NASA-STD-6016, Standard Materials and Processes Requirements for Spacecraft, provide the requirements to assure that the materials used are sufficient to perform and are handled correctly to prevent degradation. NASA-STD-5019, Fracture Control Requirements for Spaceflight Hardware, establishes the fracture control requirements for all Human-Rated spaceflight systems including payloads, propulsion systems, orbital support equipment, and planetary habitats. NASA-STD-6008, NASA Fastener Procurement, Receiving Inspection, and Storage Practices for Spaceflight Hardware, establishes fastener procurement, receiving inspection, and storage practices for all fasteners used for spaceflight hardware that are procured, received, tested, inventoried, or installed for space flight. NASA-STD-5001A, Structural Design and Test Factors of Safety for Spaceflight Hardware, establishes NASA structural strength design and test factors, as well as service life factors to be used for spaceflight hardware development and verification. NASA-STD-5012, Strength and Life Assessment Requirements for Liquid Fueled Space Propulsion System Engines, provides strength and life assessment requirements for liquid fueled space propulsion system engines. NASA-STD-5009, Nondestructive Evaluation Requirements for Fracture-Critical Metallic Components, establishes the nondestructive evaluation (NDE) requirements for any NASA system or component, flight or ground, where fracture control is a requirement.

The Constellation Program provides a list of candidate DFMR items in CxP 70038, Constellation Program Hazard Analyses Methodology (Reference 3). The candidate list must be applied with caution due to the fact they are candidates only, the rationale for acceptance must be provided and approved by the Constellation Safety and Engineering Review Panel (CSERP) as well as the Engineering Technical Authority. The specific implementation of DFMR must be understood. One cautionary aspect is that the system may have components considered DFMR while other functions are

failure tolerant. An example of this is a pressure vessel. Structurally, the ability to contain the fluid at the vessel's rated pressure is typically DFMR (when not connected to a pressurized system). The control of its internal pressure is controlled by redundancy (when connected to a pressurized system). There is usually a combination of multiple relief valves and/or burst disks on a pressurized system to prevent over-pressurization (See figure 1). Pressure vessels maintain a Safety Factor when considering ultimate strength. But, additional cycle life should be considered. The technique for determining cycle life and performing initial crack size inspections is also standard throughout NASA. Typically, there is also a Safety Factor of 4 applied to cycle life. There are standard material property values that are allowed and ways to protect against standard causes for failure such as specifications for the ability to withstand corrosive environments and for handling of composite pressure vessels to prevent damage. The previously mentioned top level NASA documents were used to create a Constellation specific structures document, CxP 70135, Constellation Program Structural Design and Verification Requirements; which covers these pressure vessel containment aspects.

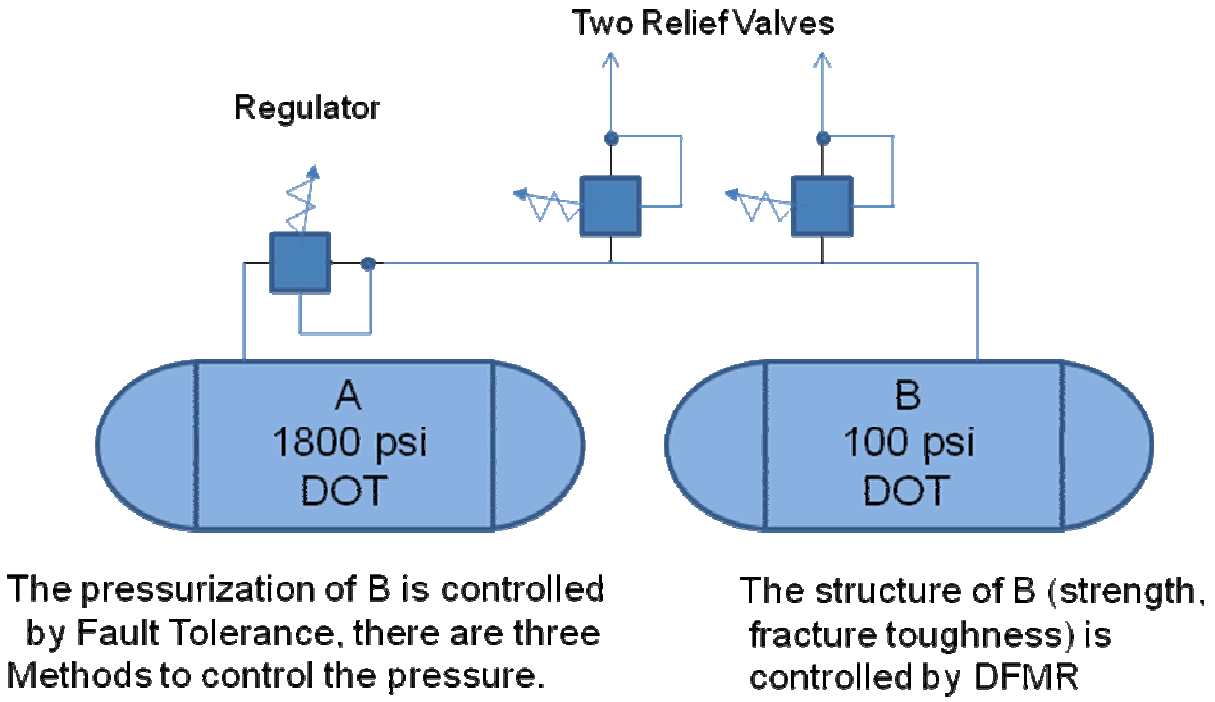



Figure 1

Another example of a DFMR candidate for Constellation is the use of wire for providing power. Typically redundant wires are not run to power a safety critical function. Rather, the wire is sized or derated to handle a larger load than would be necessary for

the worst case draw from the load. For example, a wire having a nominal current requirement of 4 amps would be sized to carry 16 amps and would also maintain a fuse rated well above the worst-case anticipated load which would be well below 16 amps. This allows for the hardware to continue functioning in the event of a surge or other unexpected anomaly without losing the function or heating up the wire. Along with this approach, there are materials, testing, and qualification requirements.

The Space Shuttle Payload Safety Requirements Document (Reference 4) states, "Payload hazards which are controlled by compliance with specific requirements of this document other than failure tolerance are called Design for Minimum Risk areas of design. Examples are structures, pressure vessels, pressurized line and fittings, functional pyrotechnic devices, mechanisms in critical applications, material compatibility, flammability, etc. Hazard controls related to these areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the payload organization and the NSTS." NSTS 1700.7B also points to a NSTS/ISS 13830, Payload Safety Review and Data Submittal Requirements (Reference 5), which provides specifics for many DFMR items and provides a list of items required for acceptance of structures and pressurized systems such as a fracture control plan and verification details. Many of the documents that are required for structures in this list are derived from the same top-level NASA documents stated above. The payload list of acceptable DFMR items is shorter than the Constellation list and the number of requirements is greater due to the nature of payloads. Payloads are typically produced by a wide variety of entities, ranging from universities to NASA Centers, therefore the requirements must be proscriptive. The Constellation Program is being designed and built by long standing NASA space flight contractors which have well developed requirements, plans and procedures.

## Summary

A safety panel does not usually accept DFMR easily: redundancy is preferred. There must be sufficient rational for why redundancy cannot be used and specific, well-understood certification techniques for the item.

DFMR is not an option or choice it is a state of being, being not able to accomplish redundancy. DFMR is not to be confused with zero Failure Tolerant, which is an option. If an item is not redundant and it is not considered DFMR by the safety panel it may be considered zero failure tolerant. If an item falls into the zero failure tolerant category it may not have a previously well documented and understood approach to insuring its adequacy. There must be waiver/deviation rationale provided to justify reasons why redundancy cannot be used and what means are going to be provided that the item will be reasonably assumed not to fail.

## References

**Reference 1.** NASA NPR 8705.2b, Human-Rating Requirements for Space Systems, Paragraph 3.2.2.

**Reference 2.** Safety Design for Space Systems IAASS Butterworth-Heinemann 2009, page 659

**Reference 3.** CxP 70038, Constellation Program Hazard Analyses Methodology, Paragraph 3.2.2.

**Reference 4.** NSTS 1700.7B, Safety Policy and Requirements For Payloads Using the Space Transportation System, Paragraph 200.

**Reference 5.** NSTS/ISS 13830, Payload Safety Review and Data Submittal Requirements, Paragraph 7.1

# Design For Minimum Risk

Jon Wetherholt
Tim Heimann

# Design Approaches to Safety

- The overall objective is to provide the safest design that can accomplish the mission given the constraints imposed on the program.
  - Fault Tolerance
  - Design For Minimum Risk

# HAZARD (RISK) REDUCTION ORDER OF PRECEDENCE

1) Eliminate the Hazard
2) **Design to Minimize Hazards (Failure Tolerance or DFMR)**
3) Incorporate Safety Devices
4) Provide Caution and Warning Devices
5) Develop and Implement Special Procedures

NOTE: Some hazards may require the combination of several of these approaches to adequately mitigate a potential hazard.

# Failure Tolerance

- Failure tolerance is the primary and preferred approach to control hazards.
  - Failure tolerance is an approach to controlling hazards which may include addition of redundant systems (similar or dissimilar), error checking, inhibits, protections against human error or inadvertent actions, or other methods incorporated into the design which preclude the occurrence of the hazard.
  - The level of failure tolerance should be commensurate with the severity of the hazard and the likelihood of occurrence.
  - Does not infer that low quality is acceptable or unlike redundancy is not desired.

# Failure Tolerance

- Dissimilar Redundancy
  - Matches
  - Lighter
- Susceptibility
  - Matches to Moister
  - Lighter to no Fuel
- Common cause
  - High Winds
  - Water

# Design for Minimum Risk

- DFMR is an approach to controlling hazards by providing design margin in the system to reduce the likelihood of occurrence of a hazardous effect. The hazards are controlled through a defined process in which approved standards and margins are implemented. Application of margin may be implemented through increased dispersion of the environment or system properties that respond to the environment.
  - DFMR is not an option or choice it is a state of being, which results from not being able to accomplish redundancy. Not simply an alternative to failure tolerance because of cost, schedule, or noncompliance with failure tolerance
  - More than increased margin, it is an approach that relies on years of proven capability. Relies on robust design, standard approach, and high quality to provide the increased likelihood the required function is available.

# Zero-Failure-Tolerance

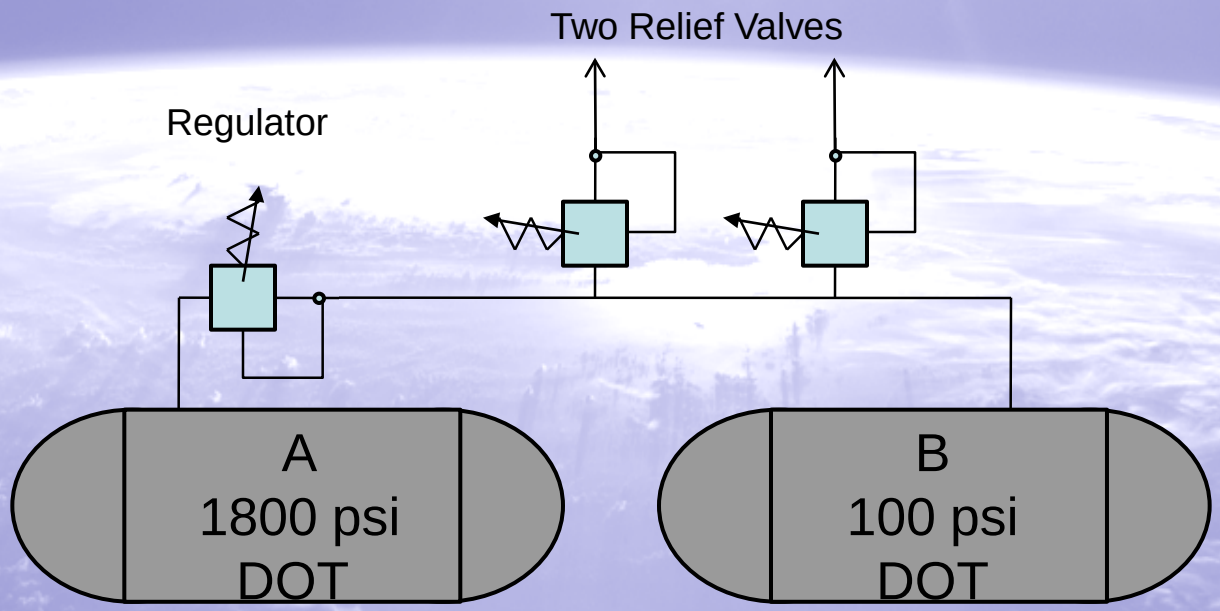
- If an item is not redundant and it is not considered DFMR, it is most likely zero-failure-tolerant.
  - The item may not have a previously well documented and understood approach to insuring its adequacy.
  - There must be waiver/deviation rationale provided to justify reasons why redundancy cannot be used and what means are going to be provided that the item will be reasonably assumed not to fail.

# DFMR or Redundancy?

Thermal Redundancy

- TPS ?
- Nozzles?

# DFMR and Redundancy



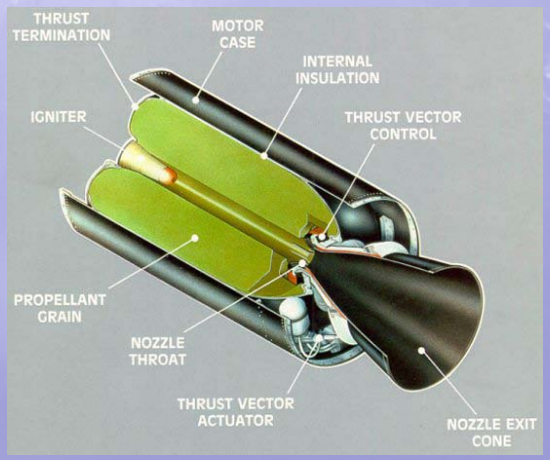

The pressurization of B is controlled by Fault Tolerance, there are three Methods to control the pressure.

The structure of B (strength, fracture toughness) is controlled by DFMR

# DFMR vs. Redundancy

Eight Motors, any seven capable of performing function (one motor out)- redundancy.

Two igniters possible- redundancy




Single Grain- DFMR
Single Case-DFMR

Two processors commanding firing - redundancy

Single Nozzle - DFMR

# Rationale for use of DFMR

- Where failure tolerance is not the appropriate approach to control hazards, specific measures need to be employed to:
  1) Recognize the importance of the hazards being controlled.
  2) Ensure robustness of the design.
  3) Ensure **adequate attention/focus** is being applied to the design, manufacture, test, analysis, and inspection of the items.
- This takes advantage of existing standards or standards approved by the Technical Authorities, to control hazards associated with the physical properties of the hardware and are typically controlled via application of margin to the environments experienced by the design or system properties affected by the environment.
- Acceptance of these approaches by the Technical Authorities avoids processing waivers for numerous hazard causes where failure tolerance is not the appropriate approach.

# What is adequate attention/focus?

- **Design (***in addition to the application of specifically approved standards and specifications )***:**
  - includes identification of specific design features which minimize the probability of occurrence of failure modes (e.g., application of stringent factors of safety or other design margins).
- **Build**
  - Includes establishing special process controls and documentation, special handling, and highlighting the importance of the item for those involved in the manufacturing process.
- **Verify**
  - Test:
    - includes accelerated life testing, fleet leader testing program, testing to understand failure modes, or other testing to establish additional confidence and margin in the design.
  - Analysis (in lieu of tests)
    - includes **correlation with testing representative of the actual configuration** and the collection, management, and analysis of data used in trending failures, verifying loss of crew requirements, and evaluating flight anomalies.
  - Inspection
    - includes identification of specific inspection criteria to be applied to the item or the application of Government Mandatory Inspection Points for important characteristics of the item.

# Summary

- DFMR requires understanding the hazard, known controls, and a good system of implementation.