SAFETY CRITICAL MECHANISMS

Brandan Robertson

NASA-Johnson Space Center

1.1 Introduction

Spaceflight mechanisms have a reputation for being difficult to develop and operate successfully. This reputation is well earned. Many circumstances conspire to make this so: the environments in which the mechanisms are used are extremely severe, there is usually limited or no maintenance opportunity available during operation due to this environment, the environments are difficult to replicate accurately on the ground, the expense of the mechanism development makes it impractical to build and test many units for long periods of time before use, mechanisms tend to be highly specialized and not prone to interchangeability or off-the-shelf use, they can generate and store a lot of energy, and the nature of mechanisms themselves, as a combination of structures, electronics, etc. designed to accomplish specific dynamic performance, makes them very complex and subject to many unpredictable interactions of many types. In addition to their complexities, mechanism are often counted upon to provide critical vehicle functions that can result in catastrophic events should the functions not be performed. It is for this reason that mechanisms are frequently subjected to special scrutiny in safety processes. However, a failure tolerant approach, along with good design and development practices and detailed design reviews, can be developed to allow such notoriously troublesome mechanisms to be utilized confidently in safety-critical applications.

1.2 Designing for Failure Tolerance

The essence of a failure-tolerant approach is to identify potential hazards and to ensure that proper controls or redundancies are in place to prevent undesirable incidents from occurring.

For the present we will neglect the time that it may take for a detrimental incident to actually manifest itself after the hazard is created (often called the “time to effect”) and assume that the incident happens the instant the hazard is created. From a safety perspective then, the basic goal in the design of any safety-critical mechanism is to prevent the creation of any hazard that could result in an undesirable incident. There are two approaches to this: designing for reliability, and designing for failure tolerance.

1.2.1 Reliability in Space Mechanisms

In an ideal world with unlimited schedules and budgets, designing mechanisms for reliability is the best approach. If your systems can operate reliably without failure, not only can you avoid hazards but you can avoid the operations problems associated with using backup systems. To create a mechanism with the kind of reliability typically required for use on human-rated spacecraft the design must go through many expensive and time-consuming iterations involving development design life testing. The initial design iteration must go through a life test after which any failures or unacceptable performance degradations observed must be addressed with design modifications followed by retesting. Once a satisfactory life test has been completed on one unit, more units of that design must be constructed and run through their life tests again in order to gain statistical confidence in the design and to work out any problems that may be a result of the assembly process. Only when enough units to generate meaningful statistical data have demonstrated sufficient life can the mechanism be assigned a credible reliability number for use in a probabilistic risk assessment.

Even when a reliability approach can be used, requirements are usually instituted that the mechanisms fails into a safe configuration, which in practice often (but not always) equates to failure tolerance. But most space hardware development programs do not have the luxuries of budgets or schedules large enough to build and test the dozens or hundreds of units needed to pursue a reliability approach. Reliability cannot be sufficiently demonstrated on a qualification unit that is the first of its kind. When only a small number of units can be built,

as is almost always the case with space hardware, a failure-tolerant approach must be followed. For that reason, the rest of this chapter deals mainly with the aspects of the failure tolerance approach.

1.2.2 Failure Tolerance Assessments and Recognizing Failure Modes

The first step in designing a failure tolerant mechanism is performing a proper failure tolerance assessment and identifying the operations or constituent mechanisms that require failure tolerance. The key to this step is making sure that all possible failure modes have actually been assessed. This can be more difficult than it sounds. The most obvious and easily identified failure modes are generally a failure to function when needed, and inadvertent operation at all other times. However there are often cases where the failure of a mechanism in mid-travel presents a unique failure mode that can have safety implications.

For example, imagine you are determining mechanism safety implications of the following scenario. The Space Shuttle Orbiter is to rendezvous with a very large orbiting satellite, grapple it with the robotic arm and berth the satellite to the Orbiter near a new piece of equipment to be attached to the satellite such that the long axis of the satellite is perpendicular to the axis of the orbiter's payload bay. To cut down on mass of the attachment mechanisms, the new equipment is retained on the Orbiter with an attachment system that latches the equipment onto the satellite at the same time that it is released from the orbiter payload bay. Once attached, the new equipment undergoes system checks. If the new equipment operates correctly, the satellite is unberthed and released back into orbit with its upgrade, but if the new equipment does not work properly then the new equipment is to be removed and returned to Earth to be fixed while the satellite is released into orbit without its upgrade.

If the attachment mechanism fails to operate in the first place the mission can be aborted and the satellite released back into orbit without its new equipment. This is a failed mission,

which has its own consequences, but the Shuttle and crew are safe. Now consider a case in which the mechanism works correctly when attaching to the satellite, but the new equipment fails its checkout and when the mechanism is commanded to release from the satellite and reattach to the Shuttle, the mechanism fails. In this case, the satellite can once again be released, albeit with useless equipment attached to it. This results in another mission failure, a worse one because a new mission with new operations and support hardware will have to be created in order to repair the failed mechanism, launch a second upgrade, and swap the failed equipment. But everyone is still safe and no catastrophic problems are encountered.

Assuming that inadvertent actuation is properly guarded against, at this point a cursory look says that there are no catastrophic failure modes associated with the release mechanism. Now let's say that you take a closer look at the operation of the latching mechanism. You learn that system uses a clever single mechanism to move the system through the following series of states during its operation:

1. Prior to operation, structural connection with the Orbiter.
2. Upon initial actuation, the structural connection is released but the mechanism remains soft-captured to the Orbiter. The mechanism achieves capture of the satellite prior to fully releasing the Orbiter, so that the mechanism can't accidentally float away.
3. The mechanism moves further, releasing the Orbiter and captures only the satellite.
4. The mechanism creates a structural attachment with the satellite.

Failures in states 1, 3, or 4 have the same consequences as those initially assessed before looking into the mechanism. But there is a new problem hidden in state 2. If the mechanism were to seize up in an unrecoverable way while the mechanism is capturing both the satellite and the space shuttle, the satellite can no longer be released and it is stuck on the orbiter in a position that is not structurally sound and that prevents the payload bay doors from closing, a prerequisite for returning to Earth. The mechanism may pass through this critical range of motion quickly, but that makes no difference under a fault tolerance approach. You have

uncovered a catastrophic failure mode that probably requires a design change in order to meet failure tolerance requirements.

Another error that can be made when determining failure modes is to miss mechanisms completely. This may seem unlikely, but the type of mechanisms most often missed are usually missed not because they were forgotten, but because they weren't considered mechanisms. This is where the previously stated definition of a mechanism becomes important.

One class of mechanisms peculiar to human spaceflight that is frequently disregarded is threaded fasteners. Bolts and other fasteners are commonly used both internal and external to habitable volumes for assembly and latching. When properly installed and left undisturbed during flight, a threaded fastener is considered structure. However, as soon as a fastener configuration is intentionally altered in any way during flight, it becomes a mechanism because new failure modes are introduced that are mechanical in nature, not structural. For example, the bolt threads can gall during installation or can jam due to thread damage or debris.

Maintenance and contingency actions are also frequently overlooked in failure tolerance assessments because they fall outside of the normal operations concepts. For example, one panel of a structure may be able to be removed during flight to allow for failure investigation or maintenance of the system it encloses. But if this panel is necessary to maintain structural integrity during subsequent loading events, then the inability to reinstall the panel is a safety-critical hazard, and the fasteners or latching devices required to attach the panel must be considered safety-critical mechanisms.

1.2.3 Failure Tolerance Assessments During the Design Phase

As can be easily imagined, figuring out that a mechanism design does not meet failure tolerance requirements can be very expensive if design changes are required once the hardware reaches the manufacturing stage and beyond. Like any other piece of hardware, the more rigor that is put into a mechanism during the design phase, the fewer problems that will be experienced later, and a failure tolerance analysis is an important part of that rigor that is too often overlooked. Recognizing all failure modes early can lead to elegant design solutions with little or no mass penalty.

1.3 Design and Verification of Safety-Critical Mechanisms

Once a mechanism is recognized as safety-critical and its failure modes are understood, the next step is to perform the detailed design and verification of the mechanism such that it can operate robustly, fail gracefully if failure does occur, accurately represent its status, and provide confidence that its performance in all these modes will be as intended. There are several important areas to which the development should pay particular attention: positive indication of status, torque/force margin, debris shielding, lubrication, thermal-tolerance analysis, and qualification and acceptance testing (including design life testing and run-in). Each of these will be discussed briefly.

1.3.1 Positive Indication of Status

Positive indication of status is perhaps the most important feature of any safety-critical mechanism. Put another way, positive indication of status means that you are *directly* (and reliably) able to measure the actual state that forms the potential hazard. Indication of status so important because in most cases in order for failure tolerance provisions to be put into

effect, someone or something must know there is a failure in the first place. And every effort must be made to measure this condition with direct, not indirect, means.

Consider the case of a door mechanism on the belly of an entry vehicle. This door must be fully closed to prevent hot gases from burning a hole in the vehicle structure during atmospheric entry. One way to provide an indication of the status of the mechanism would be to place a limit switch near the shaft of the actuator that powers the door hinge such that when the door is fully closed, a cam correspondingly positioned on the shaft strikes a set of redundant limit switches to indicate closure. The problem with this approach is that it's not the position of the shaft that causes the hazard; it's the position of the door. If a piece debris were to have lodged itself in the door cavity or damaged the mechanism or door itself on ascent, the door may not be able to fully seat but the inherent flexibility or kinematics of the door and mechanism may still allow the actuator shaft to reach the measured position. In this case, with no other indications available, the crew would assume all is well and initiate a potentially catastrophic de-orbit burn. A better solution is to place a limit switch where it is actuated by contact with the door itself.

1.3.2 Torque/Force Margin

Torque or force margin is a way of measuring how much force or torque a mechanism has in reserve, beyond that anticipated to be needed in its predicted function. In order to operate, the available torque (or force for linear devices such as springs or linear actuators—torque will be used in the remainder of the chapter for simplification) in the mechanism must exceed the sum of all of the resisting torques. The resisting torque can come from a number of sources (e.g. friction, the bending of cables, material deflections, inertial motion, etc.) but it is often difficult to predict all of the potential sources of resisting torque, and sometimes circumstances may result in an unforeseen drop in the available torque. As a result, having extra torque in reserve is crucial when designing dependable mechanisms.

In general, torque margin can be defined as

$$TM = \left(\frac{\text{Available Torque}}{\text{Resisting Torque}} - 1 \right).$$

The proper torque margin to use in a mechanism generally depends on the uncertainty in the design conditions, but most programs have specific requirements for the minimum required torque margin. Even with state-of-the-art analysis and testing techniques, it is very difficult to predict how a mechanism will function in a space environment after being exposed to a launch environment. Thus, with the exception of some special cases, there should always be a torque margin in the completed hardware. Based on experience with past programs, the torque margin should always be at least 1.0 under worst-case conditions, unless otherwise specified by the specific program. To account for increased uncertainty in early design phases, it is also recommended that the design torque margin should start higher than 1.0 and be decreased as the design matures, ending with a minimum measured margin of 1.0 imposed at hardware qualification and acceptance. Table X.1 illustrates a commonly utilized torque margin management approach, consistent with that recommended in AISS S-114-2005, Moving Mechanical Assemblies for Space and Launch Vehicles.

[Table X.1 Here]

The above recommendations are for static conditions, so the kinetic energy from the motion of the mechanism should not be considered in the calculation of the available torque. This ensures that even if the motion of the mechanism should stop for some reason, there is enough torque available to resume motion. These recommendations also represent minimum values; in general mechanisms should try to achieve the highest margin possible within the design constraints such as load or acceleration limits.

1.3.3 Debris Shielding

Debris is a constant concern for spacecraft and aircraft. Whereas the concern for aircraft is primarily that of engine damage, debris can cause a variety of problems for spacecraft due to

the microgravity environment encountered during spaceflight: it can damage structure or instruments during liftoff, ascent or landing, it can contaminate scientific instruments rendering them useless, or it can find its way into mechanisms and prevent them from operating. For this reason, it is important to shield mechanisms from debris to the largest extent practical.

It should be noted that debris can come in two types: debris from external sources not associated with the mechanism (commonly called foreign object debris, or FOD) and debris that is generated by the mechanism itself. FOD is easy to imagine is what most people think of when they consider debris shielding. FOD can be almost anything; a washer dropped during ground processing, a tool left behind, paint chips from a nearby surface, or orbital debris from previous spacecraft, or even insects are just a few examples of FOD that have been encountered. This type of debris is fairly easily guarded against. For example, closeout panels and flexible boots can be added to most mechanisms to protect the mechanism on their interior from intrusive debris.

Self-generated debris can be a little harder to catch or protect against. For example, misaligned mechanisms or improper gear meshing can create metal shavings that can cause galling or can build up and act as debris. Dry film or solid film lubricants that are not properly burnished can generate a similar buildup. Internal features such as wiper seals can be useful in controlling self-generated debris. In addition the usefulness of closeouts to prevent self-generated debris from becoming FOD for another system should not be overlooked.

1.3.4 Lubrication

Nearly all space mechanisms contain surfaces that move relative to each other and which can or are planned to come into contact. The use of a proper lubricant on these surfaces can extend the life of the mechanism and help it to meet its service life requirements.

Tribology is a very intricate and complicated subject prone to frequent advances in technology. For this reason and due to the wide array of possible applications to mechanisms, it is not practical to include a comprehensive discussion of lubrication within the confines of this book. Thus it is important to ensure that lubrication experts are consulted during the determination of lubrication strategies. However, a few often overlooked lubrication pitfalls can be addressed.

One class of subtle lubrication problems is one of migration. Due to the microgravity, thermal, and vacuum conditions, liquid or grease lubricants can, through various methods, travel from place to place within a mechanism. This can present three problems. First, on occasion there are components of mechanisms such as brakes where friction is crucial and lubricant contamination can cause severe mechanism malfunction. Second, lubricants can contaminate surfaces that are sensitive for other reasons, such as optical surfaces. And third, lubricants can travel to locations utilizing materials or even other lubricants that are incompatible with the migrating lubricant. This can alter the chemical properties of the material and result effects ranging from degraded lubricant performance to corrosion of the mechanism to the destruction of seals. It is therefore important to ensure that lubricants are properly contained within the mechanism. When possible, material choices should be made such that incompatible materials are not used in the same mechanism even if physically separated. It is also important not to overlook ground operations. A liquid lubricant that is perfect for an in-space application can pool, leak, or evaporate from a mechanism when operated or stored on the ground.

Another subtle issue is the proper specification of lubricant quantity. Drawing notes often specify to apply a lubricant to a surface without specifying a quantity or thickness. Whereas this can obviously cause problems if an insufficient quantity of lubricant is used, what is not so obvious is that different problems can be created if too much lubricant is used. Overfill of lubrication is a recognized concern in bearings, but several examples of past problems outside

of this category are available. One example involves dry film lubricant applied too thickly to thread surfaces causing a bolt to jam upon insertion. Another had excess grease being applied to a mechanism. This excess grease collected, froze in the cold thermal environment, broke off and subsequently jammed another sensitive portion of the mechanism.

1.3.5 Thermal Tolerance Analysis

A proper tolerance analysis is one of the most important design and verification steps that can be performed on a mechanism. Occasionally circumstances arise wherein a mechanism function cannot be adequately tested in the proper environment before flight, in which case a thermal tolerance analysis may provide the sole verification that a mechanism will function reliably in its design environment. A 2004 survey of the root causes of International Space Station mechanism failures and anomalies revealed that half of all tracked events had tolerancing problems as a sole or contributing cause (McCann, 2004).

When performing a tolerance analysis it is crucial that thermal effects be included. This is particularly true for mechanisms located external to the vehicle. Though such external influences are often the driving conditions for the thermal environment, heat generated by the mechanism itself can cause significant distortions that must be considered. For this reason, thermal effects should not be neglected, even in thermally controlled environments.

Thermal effects can manifest themselves in two ways. First, materials with different coefficients of thermal expansion will change size at different rates when exposed to the same uniform temperature. Thus, choosing an arbitrary example, an aluminum component that had sufficient clearance with a steel component at room temperature may have an interference at elevated or reduced temperatures. The second way is if two components brought together have different temperatures. For components of an integrated system, this is not often a problem because the two components will be in thermal equilibrium by virtue of their close

proximity and contact. However, situations can arise where this effect becomes important. For example, consider a component removed from the international space station for return to Earth in the payload bay of the Space Shuttle. Say that the removed component has been exposed to the sun for a long period of time and is transferred to flight support equipment that is shaded within the payload bay. Though the materials may be identical, they will be at a different temperature, and an interface that fit together when the two were at the same temperature may no longer fit. A related situation occurs when a large mechanism such as a docking mechanism is shaded on one side and exposed to the sun on another. The temperature gradient across the system can cause a thermal distortion that brings the mechanism out of its natural shape, which can cause interface problems with the mating half. Though this type of effect can be controlled operationally by allowing the two components to come into thermal equilibrium prior to installation, this is not always operationally convenient or even possible.

Thermal tolerance stack-ups can be extremely complicated, especially if the mechanism contains many parts with many different materials. The use of a geometric dimensioning and tolerancing standard such as ASME Y14.5-1994 can make the analysis much easier to perform and eliminate ambiguities in the interpretation of drawings by providing a well-defined vector analysis method, thereby reducing or eliminating common sources of error in the analyses.

A word of caution: do not superficially discount thermal effects in an analysis because the same material is used throughout the mechanism and the system does not experience temperature differences between parts. There is a difference between similar materials and identical materials when speaking of their coefficients of thermal expansion (CTE), and the difference can be significant. For example Custom 455, a common aerospace stainless steel, has a CTE between 78° F and 200° F of 5.9 in/in/° F, while the CTE of A-286, another common aerospace stainless steel, is considerably higher at 9.2 in/in/° F. Though the

magnitudes of the differences vary, the existence of these differences is common to all metal alloys.

1.3.6 Mechanism Testing

Of all considerations involved in the development of safety-critical mechanisms, the most important is undoubtedly the performance of adequate testing. In the end, the suitability of a design and its ability to meet its performance requirements can be demonstrated in the most straightforward manner by demonstration of this performance in the design environment.

In general, mechanism testing falls into one of three categories. First is development testing. Development tests are very useful and are often performed at the component level and use non-flight designs to accomplish a variety of objectives including characterizing specific performance parameters or sensitivities, trading or proving various design concepts, or meeting incremental success gates of a larger development. Though the purpose of individual tests vary, development tests only provide aid in the development of the final design; they are not used as the final verification of requirements. They help establish confidence in the design as the development progresses and can serve to demonstrate an understanding of the design constraints.

The next test category is qualification testing. Qualification tests prove that the *design* of the mechanism meets the requirements imposed upon it. Such tests are performed at levels and in environments above and beyond the design environments to demonstrate robustness and margin in the design. These are a wide variety of qualification tests for any given system, but for mechanisms the most important types of qualification tests are performance tests, vibration tests, thermal vacuum tests, and design life tests, all of which mimic the design environment. Because the qualification test levels exceed those expected during service, they are performed on flight or flight-like units that are dedicated specifically to the tests so that

potentially damaged units are not used in service. Sometimes if a system design has only very minor differences from a system that has already passed qualification testing, it can be considered “qualified by similarity.” This should be used with great caution as small design changes can have unintended and unexpected effects.

Certain inadequacies in the qualification test plans are often encountered. Vibration and thermal testing are usually planned appropriately but certain design life test inadequacies are frequently encountered. The factor to be applied to design life testing can vary depending on the program and consequence of failure, and it is important that the correct factor is used, and applied to the sum of all design cycles. However, the calculation of the required number of design cycles to be used in the test is often made incorrectly and must be done carefully. Proper design life testing includes not only duty cycles during flight, but also all cycles incurred during acceptance tests, functional tests, troubleshooting, maintenance, and other ground operations. Often scenarios arise where cycles that were never planned are accumulated by a mechanism. One scenario where this is prone to occur is during the planned testing of associated mechanisms. Take for example the Space Shuttle payload bay door actuators. These doors have cycle requirements imposed upon them to account for their ground testing. However, there are several mechanisms within the payload bay that cannot be operated with the payload bay doors closed. Unless the full range of flight operations and ground operations scenarios are understood, the fact that the doors have to open and incur cycles just so that other mechanisms may undergo their planned testing could be missed in the calculation of the required door cycles. This type of unforeseen cycle accumulation is often difficult to predict. For this reason, it is recommended that some reserve number of cycles be added to the cycle calculation prior to applying the required factor.

The last category of testing is acceptance testing. Whereas qualification testing serves as proof that the mechanism *design* can operate as intended during service, it does not prove that a subsequent individual unit manufactured per that design is up to the task. That is the

purpose of acceptance tests. Acceptance tests are performed on every manufactured unit to screen out workmanship flaws and prove that the unique unit is capable of performing as designed. Acceptance testing is usually performed on qualification units before qualification testing so that workmanship issues can be excluded as possible causes of any qualification test failures. Important acceptance tests for mechanisms include run-in tests (sometimes called wear-in tests), random vibration tests, thermal vacuum tests, and sometimes benchmarking tests that will aid in later diagnosis of problems.

Attempts are often made to waive various acceptance tests. Acceptance vibrations test waiver submissions often mistakenly use a low expected flight vibration as rationale. However, this is not the purpose of an acceptance vibration test, which simply uses a random vibration environment as a disturbance to test workmanship issues such as soldering and fastener installation. It is not associated with expected random vibration levels during flight. Developers often ask for relief from thermal tests citing a completed thermal tolerance analysis as sufficient. However, as has been discussed previously thermal tolerance analyses are notoriously prone to error so in all but the simplest of mechanisms this is not sufficient rationale. Run-in tests are one of the most frequently neglected tests. The purpose of the run-in test is two-fold. First, it serves as a workmanship test to identify improper component assembly issues that manifest themselves quickly when placed in service, and second, it serves as sort of a burnishing process, wearing down initial rough spots and smoothing out transient behavior of new components. This is important in order to ensure that the mechanism operates within its steady-state regime during acceptance testing and during service and avoids spurious test failures that are functions of transient behavior rather than a hardware or design defect. For this reason it is important that the run-in test be performed before all other mechanical acceptance testing. Developers often cite initial functional tests as serving as the run-in tests. However, there are minimum cycle requirements for run-in tests that are designed to accomplish the two objectives that are not met by a few functional tests in most circumstances. Finally, note that whereas a design can be qualified by similarity, by

definition a mechanism cannot be accepted by similarity, and an attempt to do so must never be permitted.

On occasion, when the cost of a hardware unit is very expensive or for some other reason the creation of a dedicated qualification article is impractical, another testing technique called protoflight testing is used. Protoflight testing combines qualification and acceptance testing on a flight unit. Environmental levels used are generally less than those used on a dedicated qualification unit due to the consequence of damaging the article, but are generally higher than those used for acceptance. Protoflight testing can introduce many unique pitfalls so the decision to use protoflight testing, the testing regimen, and the environments used in those tests need to be carefully examined.

Though deserving special scrutiny in protoflight situations, environments used in mechanism testing in general need careful attention. Testing is not worth much if it uses inadequate environments. If resources allow, testing beyond certification limits is very valuable. Often one will find that the environment encountered during flight is not quite what was predicted, or circumstances arise that make operation beyond certification limits desirable, or a life extension is needed. In all of these cases a decision must be made regarding the risk involved with operating a mechanism outside of its certification. This decision can be very difficult and must rely on engineering judgment based on available data. Having such data (and having it well documented) can pay for itself many times over during the course of a program. Without data, evaluation in these situations extends beyond engineering judgment into the realm of engineering intuition, greatly increasing risk.

1.3.7 Other Considerations

Though the areas mentioned above tend to play the most significant roles in good design and verification, there are numerous other factors that should be addressed that occasionally present significant problems.

1.3.7.1 Fasteners

Fasteners are so common an element in structural and mechanical design that they can often be overlooked when reviewing designs. However, they can be the root of a host of problems. Design practices that should be verified include the use of qualified verifiable secondary locking features, specification of preload torques as “above running torque” on drawings, and required measurement and documentation of all running torques. Additionally, liquid locking compounds (LLC’s) generally should not be used as secondary locking features. There are a few problems with LLC’s. First, their locking effect is not verifiable as it requires a broken bond to verify the locking and once the bond is broken the LLC no longer serves to lock the thread. Second, the quality of the application (and thus the locking effect) is very process-dependent and can be highly variable. LLC’s can have a tendency to migrate in a vacuum and can end up locking together unintended surfaces. This can obviously be catastrophic for mechanisms and has been identified as the root cause of testing failures in the past. And lastly, when the LLC’s do work, the strong bond can make removal difficult and can sometimes cause damage to the hardware if removal proves necessary.

As mentioned earlier, threads that are operated during flight have mechanical failure modes and should be treated as mechanisms. This includes fasteners that can be used during maintenance operations. Such fasteners applications should always be examined in the light of failure tolerance considerations.

1.3.7.2 Design for Assembly and Maintenance

Sometimes a mechanism is doomed to fail before it ever leaves the ground, due to improper installation during manufacture or maintenance. Although human error can never be entirely eliminated, it is possible in some instances to design a mechanism to preclude certain types of human error. Mechanisms should always be designed to either preclude installation in an incorrect orientation or be clearly labeled in a manner that indicates proper installation orientation and prevents improper installation. Space program failures in the past have been traced to parts that were designed to be operated in only one direction and were installed backwards, yet had an interface that allowed this improper installation without clear indication that something was wrong.

1.3.7.3 Strength

Designing a mechanism to have adequate strength seems obvious, but the difficulty can lie in the details, particularly in the assumptions used in performing the analysis and deriving loads. One critical aspect to make sure is understood is the mechanism boundary conditions. Mechanisms are usually mounted to structure, and this mounting is assumed to behave rigidly. However, due to the lightweight nature of most aerospace structures, this mounting often has an inherent flexibility that can cause a change in both the external loads transferred to the mechanism and the behavior of the mechanism due to its own induced loads. For example, a motor mounted to a flexible structure can produce a rotational motion about its mount, generating moments or angular displacements on shaft couplings that are not predicted by a rigid mount.

Another problem that can be difficult to detect is an improperly understood load path. This is often manifested in one of two ways. The first is poor or neglected free body diagrams, particularly in the effect that an offset force (a force that generates a moment on a component's support) has on a component. The moments created are often assumed to be of low enough magnitude that they do not contribute or are omitted altogether. Small moments can be surprising effective at binding surfaces designed to slide on one another. Precautions

should always be taken to fully accommodate such moments and deal with the misalignments and friction that they generate. The second manifestation of a poorly understood load path is the existence of unintentional load paths. Often mechanisms are designed such that two separate parts of the mechanisms are meant to share load equally, but natural tolerances and variations in assembly can produce an uneven load sharing if the proper degrees of freedom are not included or the parts are not adequately shimmed. This is a fairly consistently recognized design issue; however, the opposite situation can also arise—mechanisms designed to withstand load in only one way can find this load being shared by components not designed to handle such loads, due to manufacturing tolerances and assembly clearances as well as material flexibility. Often the assembly models and drawings will not represent the true configuration the hardware will take once subjected to the actual preloads and constraints that it will see once physically constructed. This can be a frustrating problem as these issues can be very difficult to detect without an extremely thorough review of the design, including drawings, models, tolerance stack-ups, and analysis.

Finally, strength problems can turn up in failure scenarios. Mechanisms and the structures they move should be designed such that they will meet all necessary structural requirements (such as strength and fracture control) under redistributed loads after mechanism failure, commensurate with the hazard level. Operational procedures can be used to restore the load path or limit the subsequent loads, but this approach should be developed and accepted prior to flight.

1.4 Reduced Failure Tolerance

Situations can arise where failure tolerance can actually lower overall system reliability or simply cannot be implemented in a feasible or practical way. In these situations, mechanisms must be subjected to a thorough review to eliminate as many potential problems as possible in order to minimize the risk incurred with such reduced failure tolerance. While increased

scrutiny can certainly be applied, realistically there should be little that can be done to the design process beyond normal design practice.

The first step in implementing reduced failure tolerance is determining whether this reduction is necessary. Care must be taken not to provide this reduced fault tolerance approach as simply an alternative to full failure tolerance. There must be a solid reason for needing to increase the risk. Occasionally the driving reason is that the nature of the particular mechanism is such that certain levels failure tolerance will actually reduce the overall system reliability, but more often the issue is just that it's highly impractical to implement a particular level of failure tolerance without significant impacts. Rationale for the reduction typically includes reliability analyses comparing the full and reduced failure tolerant systems, trade studies detailing the impacts of implementing the full failure tolerance (including cost, schedule, and vehicle packaging and performance impacts), the nature and severity of the hazards mitigated by the failure tolerance, detailed failure modes and effects analyses including the influence of the failed system on other systems, potential real-time workarounds, etc.

In most cases where reduced failure tolerance is warranted, the reduction is from two-failure tolerance to single-failure tolerance, where there is still a level of physical redundancy in place. At the cost of a more rigorous development and testing program, this reduction can often be achieved without an excessive increase in risk. Even so, reductions of this type should be limited to systems that utilize mechanisms having a demonstrated history of high reliability, such as pyrotechnic devices, and which result in hazards that have high potential for operational intervention prior to the occurrence of the catastrophic event. The design and testing should be subjected to periodic independent reviews at various life-cycle stages (conceptual design stage, preliminary design stage, critical design stage, and acceptance stage for example) and be very closely documented. These reviews should be conducted by a dedicated group of independent (not associated with the project) mechanisms specialists to a

greater depth of penetration than is usually associated with standard milestone design reviews. The review group should have access to the designers and all design and analysis information, and should check against a well-defined set of evaluation criteria, such as AIAA-S-114-2005, NASA-STD-5017, or a similar set of guidelines and lessons learned.

In a small number of cases, it is necessary or highly desirable to operate a mechanism with catastrophic failure mode with no failure tolerance. For obvious reasons, such reduction should be granted only under special circumstances. Granting zero-failure tolerance to a catastrophic mechanism is equivalent to saying that there's no possible way that a given mechanism is going to fail, so great care should be taken in making this decision. The types of mechanisms that can legitimately be considered for this reduction are of the simplest nature, so simple that there may be dispute whether they are even mechanisms—things like hinges, dovetails in slots, and the insertion of pins into holes. As with the single-level reduction, applications should be limited to systems that utilize mechanisms having a demonstrated history of very high reliability and which result in hazards that have high potential for operational intervention prior to the occurrence of the catastrophic event. A similar type of rigor as that used for the single-level reduction should be employed in the independent review for this case, with increased attention to thorough testing and positive indication of status. No exceptions or waivers to any mechanism development or verification requirements should be allowed.

1.5 Review of Safety Critical Mechanisms

Thorough review of design and verification is of great importance and value not only for mechanisms with reduced failure tolerance, but for all safety-critical mechanisms in general. It is highly recommended that a team of experienced, independent mechanisms specialists be formed with the responsibility for reviewing and approving the designs of all safety-critical mechanisms.

Independence is very important. For one, it provides a new set of eyes unfamiliar with the design and the history behind it that is able to see things with a fresh perspective and can challenge assumptions. Design practices and analysis assumptions are often subject to a sort of creep wherein the evolution of a design can drag assumptions and techniques that were once appropriate into inappropriate regimes without becoming obvious to those involved with the development. Independence also frees the reviewers to make unbiased assessments, being free from the schedule and budgetary pressures that may be at work among the design team.

Experience with mechanical systems is also crucial. Having a high degree of mechanisms experience resident in the review team provides a large pool of lessons learned that can be applied to new designs. Often the experiences of different people can supply different types of lessons producing a very complete review, particularly when the group consists of specialists in different sub-fields, such as tribology, bearings, testing, motors, etc. As more and more systems are reviewed, more and more experience can be obtained by the group by learning from others' mistakes, so having a consistent team that can conduct such reviews is very useful and can quickly build expertise that can benefit the overall organization.

The review should be made as detailed as possible within the constraints of the project. The first step should be to conduct a technical meeting with the hardware developers to understand the requirements, environments, function, and operational scenarios of the mechanisms. Next, with the aid of the hardware developers, all possible failure modes should be mapped out. In addition to being useful for safety personnel creating hazard reports later in the design process, this mapping will provide the group with a clear direction regarding which failure modes are the most critical and which mechanisms or components may be candidates for reduced failure tolerance. Once the operation and the failure effects are established, the detailed review can begin. This includes reviews of the drawings, tolerance stack-ups, materials, dynamic and strength analyses, verification and test plans, and any development

hardware. It is helpful if the review team has available to them a set of requirements or checklist that can be used to systematically assess the mechanisms. Standards such as AIAA-S-114-2005 or NASA-STD-5017 have been used successfully in the past. In concert with this detailed review, it is important that the team document the compliance with each of the items in the standard along with the supporting data and rationale. This is invaluable for reference later. It is useful to have such compliance, along with the failure tolerance mapping and a general discussion of the mechanism and its operation, documented in a single report that can called up when issues arise.

When properly implemented, such a review process can add significant value and aid in increasing the reliability of safety-critical mechanisms.

1.6 References

1. McCann, David. "Review of International Space Station Mechanical System Anomalies", *Proceedings of the 37th Aerospace Mechanisms Symposium* [NASA/CP-2004-212073], (Galveston, TX, 19-21 April 2004) p. 291.

2. *Moving Mechanical Assemblies for Space and Launch Vehicles*, American Institute of Aeronautics and Astronautics, AIAA-S-114-2005, 2005.

3. *Design and Development Requirements for Mechanisms*, National Aeronautics and Space Administration, NASA-STD-5017, 2006.