Making Human Spaceflight Practical and Affordable: Spacecraft Designs and their Degree of Operability

Alan R. Crocker

As we push toward new and diverse space transportation capabilities, reduction in operations cost becomes increasingly important. Achieving affordable and safe human spaceflight capabilities will be the mark of success for new programs and new providers. The ability to perceive the operational implications of design decisions is crucial in developing safe yet cost competitive space transportation systems. Any human spaceflight program – government or commercial – must make countless decisions either to implement spacecraft system capabilities or adopt operational constraints or workarounds to account for the lack of such spacecraft capabilities. These decisions can benefit from the collective experience that NASA has accumulated in building and operating crewed spacecraft over the last five decades.

This paper reviews NASA's history in developing and operating human rated spacecraft, reviewing the key aspects of spacecraft design and their resultant impacts on operations phase complexity and cost. Specific examples from current and past programs – including the Space Shuttle and International Space Station– are provided to illustrate design traits that either increase or increase cost and complexity associated with spacecraft operations. These examples address factors such as overall design performance margins, levels of redundancy, degree of automated failure response, type and quantity of command and telemetry interfaces, and the definition of reference scenarios for analysis and test. Each example– from early program requirements, design implementation and resulting real-time operations experience – to tell the end-to-end "story"

Based on these experiences, specific techniques are recommended to enable earlier and more effective assessment of operations concerns during the design process. A formal method for the assessment of spacecraft operability is defined and results of such operability assessments for recent spacecraft designs are provided. Recent experience in applying these techniques to Orion spacecraft development is reviewed to highlight the direct benefits of early operational assessment and collaborative development efforts.

Making Human Spaceflight Practical and Affordable: Spacecraft Designs and Their Degree of Operability

A. Crocker[1]
NASA Lyndon B. Johnson Space Center, Houston, Texas 77058

As we push towards new and diverse space transportation capabilities, reduction in operations cost becomes increasingly important. Achieving affordable and safe human spaceflight capabilities will be the mark of success for new programs and new providers. The ability to perceive the operational implications of design decisions is crucial in developing safe yet cost competitive space transportation systems. Any human spaceflight program – government or commercial – must make countless decisions either to implement spacecraft system capabilities or adopt operational constraints or workarounds to account for the lack of such spacecraft capabilities. These decisions can benefit from the collective experience that NASA has accumulated in building and operating crewed spacecraft over the last five decades. This paper reviews NASA's history in developing and operating human rated spacecraft, reviewing the key aspects of spacecraft design and their resultant impacts on operations phase complexity and cost. Specific examples from current and past programs – including the Space Shuttle and International Space Station– are provided to illustrate design traits that either increase or decrease cost and complexity associated with spacecraft operations. These examples address factors such as overall design performance margins, levels of redundancy, degree of automation, type and quantity of command and telemetry interfaces, and the definition of reference scenarios for analysis and test. Based on these experiences, specific techniques are recommended to enable earlier and more effective assessments of operations concerns during the design process. Recent experience in applying these techniques to Orion spacecraft development is reviewed to highlight the direct benefits of early operational assessment and collaborative development efforts. This paper serves as a companion piece to the earlier published "Designing a Better Spacecraft: Assessing Flight Operability of Human Rated Spacecraft," presented at the AIAA SpaceOps 2010 conference. Where the previous paper described a method for formal flight operability assessment during spacecraft development, this paper provides expanded examples of design practices and their impacts on operability.

I. Introduction

THE design of a human rated spacecraft is a complex and costly process requiring the integrated assessment of many individual criteria. Historically, it has been difficult to include in that integrated assessment the design's full impact on the flight operations community. The unique "operability" requirements have not been well understood, nor has there been a well-defined set of criteria for assessing operability. Spacecraft today are far more complex than their predecessors, implementing far larger requirements sets using advanced technologies and sophisticated software while providing more onboard capabilities, more telemetry and more operator command capabilities. Just as important as these architectural differences are the differences in missions. Today, there is a much higher expectation with regards to safety, mission success, mission frequency, and affordability. These all present challenges to the program and flight operations communities.

Spacecraft requirements definition, design, manufacture and test is a complex and demanding series of processes that must take into account a vast array of considerations and constraints including safety standards, schedule and cost constraints, and even political factors. With all of these competing factors influencing the design process, it is at best challenging to develop a spacecraft that enables low operations phase cost. However, an awareness of the factors that impact flight operations costs, and a method to directly measure these impacts, can arm future spacecraft development program management and engineering organizations to better address these costs during the earlier

[1] Deputy Chief, Mission Operations Directorate Exploration Systems Integration Office, NASA Lyndon B. Johnson Space Center, Mail Stop DS15, Houston, Texas, 77058.

phases of a human spaceflight program. This same understanding can also benefit non-government organizations as they make their first attempts to build and fly human-rated spacecraft.

II. The Flight Operations Job

To understand the impacts of a spacecraft design on flight operations cost, it is necessary to first understand the basic function of flight operations. Apollo 11 flight director and former director of NASA JSC's Mission Operations Directorate Eugene Kranz defined the flight operations infrastructure as a system designed to "maximize mission success, to minimize risks to the [vehicle] and the crew, to decrease operating costs, and to achieve an effective balance in the application of all operational resources.[1]" The flight operations community picks up where the development community leaves off, turning generic design reference missions and system test cases into plans, procedures, and operating guidelines to meet the requirements and constraints of real missions. The successes and shortcomings experienced in the development, integration and test phases directly impact the form that flight operations takes. Where system operating characteristics, limits and reliability are known quantities, the operations community can plan and execute missions with a predictable cost. When this key information is unavailable, or mission requirements grow beyond the scope of that information, operations cost are difficult to characterize and can grow significantly to meet mission demands.

Fundamentally, flight operations definition is a set of systems engineering tasks. Crewmembers, flight controllers, analysts and instructors must all understand the integrated operation of the vehicle – the capabilities and constraints of each vehicle subsystem as well as the subsystems interactions, dependencies and impacts on the rest of the spacecraft. Development of generic procedures and operating constraints (referred to as "flight rules"), such as the examples provided in figures 1 and 2, involves thorough analysis of all of these factors. This effort often uncovers new integration issues – unexpected consequences of the design implementation, often associated with the impacts of one subsystem's operation on that of another. For example, operations assessments in the International Space Station (ISS) Preliminary Design Review timeframe unveiled that too many of the critical electrical power cables were routed through the same portion of the US Lab module, resulting in a complete loss of power to critical US systems when smoke detection triggered an automatic power down of equipment and wiring in that volume. Once discovered, the wire routing was altered to provide a more robust design and a more operable spacecraft. In this and similar ways, flight operations performs critical systems engineering and integration tasks throughout the program's lifecycle.

KU-BD ACTIVATION

```
R14:C     cb MNB KU ELEC          – cl
                  √ANT HTR        – cl
                  √CABLE HTR      – op
            MNC KU SIG PROC       – cl

A1U       SIG STR                 – KU
         √SLEW RATE               – SLOW
         √KU BD SCAN WARN tb      – bp
               √TRACK tb          – bp
               √SEARCH tb         – bp
               √sel               – MAN SLEW
               √RDR OUTPUT        – HI
            √SIG PROC HDR sel     – TV
                     √LDR sel     – MMU 1
         √KU BD MODE              – RDR PASSIVE
                PWR               – ON
         √CNTL                    – PNL

          [SM ANTENNA]
CRT       I/O RESET KU – ITEM 8 EXEC (*)

                      NOTE
            System warmup takes ~4 min

          [SM 76 COMMUNICATIONS]
          When KU-BAND PWR OUT > 15 (watts), proceed

A2        DIGI DIS SEL – EL/AZ
         √R/EL ind:  +000.0
         √RR/AZM ind:  +000.0
          DIGI DIS SEL – R/R̄

          [SM ANTENNA]
CRT       SELF TEST – ITEM 7 EXEC (*)
          When SELF TEST complete (~3 min):
A1U          √KU BD SCAN WARN tb – gray
                   √TRACK tb     – gray
                   √SEARCH tb    – gray
A2           √R/EL ind:  +888.8
          If R/EL ind:  +333.3, √MCC
```

Figure 1. Example Space Shuttle procedure.

A9-51 FC Power Level Constraints

A. The FC's can be operated at any power level between 2 and 12 KW consistent with satisfactory DC bus voltage and FC temperature maintenance. To satisfy mission objectives and FC lifetime constraints, FC power levels should be managed as follows:

1. **2-10 KW – continuously**
2. **10-12 KW - not more than 15 minutes every 3 hours**

B. In the event of an FC failure, FC loading imbalance because of uneven FC performance characteristics, or other system failure, the remaining FC's may be operated at:

1. **2-12 KW – continuously**
2. **12-13 KW- for less than 4 hours**
3. **Up to 16 KW for 10 minutes consistent with Satisfactory bus voltage and FC temperatures**

At <2 kW the FC voltage may exceed 32 volts. Most orbiter equipment is only certified to 32 volts. At >12 kW, the FC thermal control system capability may become unable to maintain the FC at safe operating temperatures. Due to lifetime considerations, FC power should be limited to less than 8 kW for normal operations. However, continuous operation between 8 and 10 kW is allowable as long as accelerated lifetime decay is accepted.

Figure 2. Example Space Shuttle flight rule.

This systems engineering and integration role continues – and even expands – as the program enters its operations phase and the details of specific missions must be defined. Mission specific planning entails the analysis not only of the generic operations constraints defined during spacecraft development, but also the unique constraints imposed by the mission requirements and payloads. Typical challenges include complex power configurations and reconfigurations to meet power budget limits, reconfiguration of attitude control system settings to conserve propellant, and flight attitude restrictions imposed not only due to communications line-of-sight constraints, but also concerns over overheating or freezing of individual spacecraft components. At the same time, flight plans must provide for efficient use of crew time and communications bandwidth to support mission goals such as science, engineering tests, and in-space assembly operations. The flight plan, and associated mission-specific flight rules, procedures, analyses, and operator training, comprise a thorough, integrated system of its own – a flight operations system that interacts with the spacecraft to accomplish the mission. A sample page from a Space Shuttle detailed mission timeline is given in Figure 3.

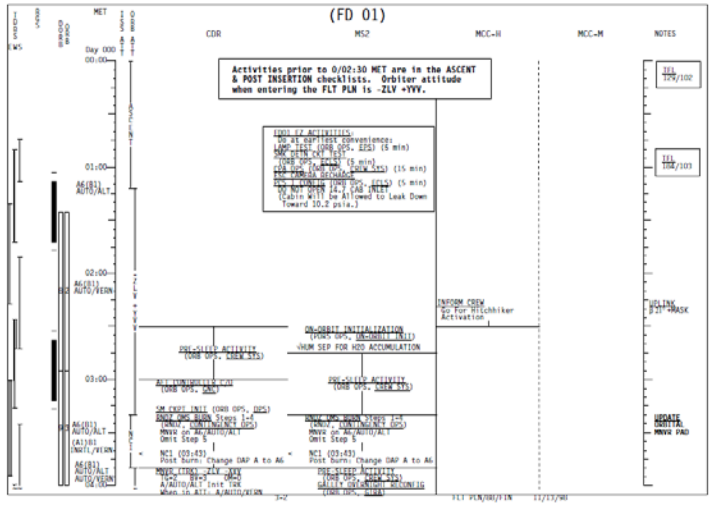


Figure 3. Example Space Shuttle detailed mission timeline.

A. The Role of the Flight Crew

From the beginning of the US human spaceflight program, the most critical part of the flight crew's job has been that of system management. Certainly, piloting skills are crucial for the astronaut, but the human's unique ability to assess and respond to unique circumstances make the entire spacecraft more robust. The primary role of the project Mercury astronaut was that of monitoring spacecraft system operation and intervening when necessary.[2] Onboard automation had successfully managed simple missions, but the onboard "sequencer" hardware proved to be a troublesome system to integrate and test.[3] The human flight crew was the ultimate backup and could take control of the vehicle in most phases of flight using a separate manual control system implemented alongside the automated systems.

The importance of this role was illustrated in numerous significant events during Mercury flight operations. On the United States' first human orbital mission, MA-6, John Glenn took manual control of spacecraft attitude when malfunctions in the automated attitude control system threatened to deplete the vehicle's propellant. On the later MA-8 mission, Wally Schirra overrode environmental control system functions to lower escalating suit temperatures, thereby avoiding an early mission termination.[4] Such flight experience demonstrated that this monitor and override role was a demanding, time consuming task for the crewmember.

As NASA gained experience and confidence in the abilities of humans to work effectively in space, it was recognized that further implementing human-in-the-loop solutions resulted in higher reliability. The Gemini spacecraft design capitalized on these findings, reducing the level of automation and providing better display and control capabilities to enhance the human's ability to operate the vehicle.

B. The Role of Mission Control

The Mission Control Center (MCC) provides a necessary capability both during normal operations and in the event of the unexpected. Real-time MCC support provides more insight, more experience, and more resource to augment the crew throughout mission execution. The MCC provides analysis results, generates plans and procedures to optimize the crew's productivity, performing spacecraft system monitoring and control, and coordinating with external engineering expertise as required to address problems encountered in flight. Overall, MCC provides a both a strategic planning capability and an additional systems management resource that make the crew more efficient and maximize the crew's opportunity for success.

During nominal operations, these services reduce the crew workload associated with managing onboard systems and preparing for upcoming events. International Space Station (ISS) flight controllers have the full capability to operate spacecraft systems just as can the onboard crew, with the exception of strictly manual tasks such as opening and closing hatches. By exercising these capabilities from the ground, MCC support enables the crew to concentrate on supporting the core mission of the ISS – execution of experiments and tests in the unique laboratory environment that ISS provides. Without MCC support, the onboard crew would be required to spend more time managing the spacecraft core systems and less time in meeting the scientific objectives of the ISS program.

During complex operations such as vehicle rendezvous and docking or response to onboard system failures, MCC provides more "eyes" and "hands." Again, MCC can execute procedures from the ground, offloading the crew during intense operations periods and allowing crewmembers to focus on physical tasks that only they can perform. The spacecraft's extensive telemetry and remote command capabilities, matched with extensive system specialist training give MCC flight controller the most detailed insight and skill in responding to system failures.

C. Evolution of Flight Operations Capabilities

Growth and change in mission scope accounts for much of the cost for the flight operations community. Initial plans for the Space Shuttle program included only a very limited set of Extravehicular Activity (EVA) operations requirements, focused on contingency operations such as manual payload bay door closure following a failure preventing nominal, automated door closure. However, the program expanded Space Shuttle EVA capabilities to become a part of normal operations for many flights. This change alone accounted for a significant increase in the cost and complexity of flight operations.[5]

Any new program experiences a steep learning curve as it first enters the operations phase. Despite the best test, integrations, and flight preparation efforts, early operations uncover previously unknown component operating characteristic, failure modes, and system interdependencies that can change the nature of spacecraft operations. Figure 4 illustrates the trend in in-flight anomalies experienced throughout the Space Shuttle program. The first 15 years of the program provided a wealth of experience in new conditions, and new challenges as NASA explored the limits of the Space Shuttle. It was only in the second half of the 30 year program that the rate of in-flight anomalies reached a relatively low and consistent level.

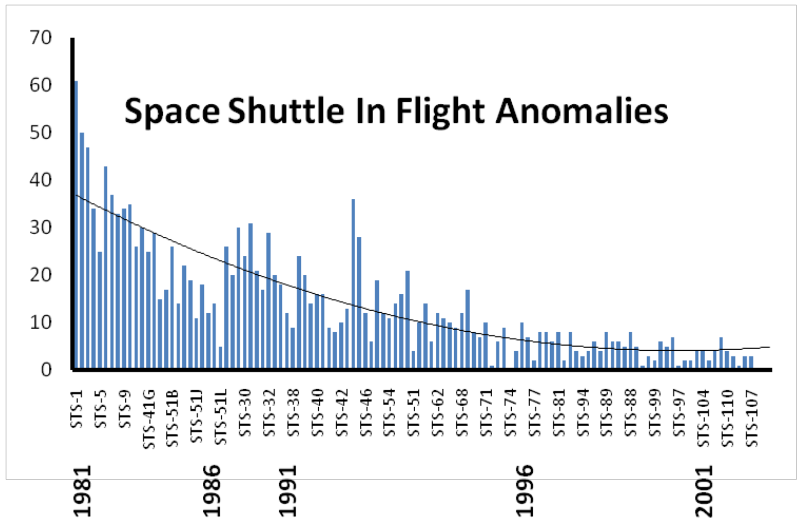


Figure 4. History of Space Shuttle anomalies per flight.

At the same time, the process of learning through operations enables greater efficiency. Over the latter two thirds of the Space Shuttle Program – from 1991 to 2011 – the size of the space shuttle flight operations staff shrank by over 50% while the number of mission objectives and the complexity of spacecraft systems grew. As the organization learned the true limits and capabilities of the spacecraft, pre-mission planning capabilities improved and became more efficient. The smaller staff proved capable of handling an amazing array of mission scenarios, in many ways far beyond the scope of those envisioned at the beginning of the program. Similar trends continue today as International Space Station flight control and instructor positions are combined to achieve a significantly smaller overall workforce.

Human Spaceflight operations will continue to evolve both as the commercial market for human spaceflight to Low Earth Orbit grows and our human exploration efforts reach deeper into the solar system where communications between the spacecraft and Earth are limited and delayed.

II. Flight Operability

The measure of a system's flight operability is the measure of the degree to which that system enables a balance of maximum mission success, minimal risk, and minimum operating cost. Traditionally, the human flight operations community has been held to the highest standards of safety and mission success, leaving operating cost as the most variable of these factors.

Any measure of flight operability must encompass the impact on cost, responsiveness and risk incurred in safely executing operations with a spacecraft as designed and manufactured. Cost is driven by both the developmental investments required to build the operations infrastructure (facilities, operations techniques and products, and trained personnel prepared to execute operations) and by the recurring cost of maintaining that infrastructure and by the expense of executing mission planning, training and operations over the entire operations phase. Responsiveness reflects the time required to plan and execute a given operation. Excessive time requirements reduce the availability and responsiveness of operations. Risk is the likelihood of success or failure of the operation. Additional consideration of risk must be given in the case that a failure endangers crew health, vehicle integrity or mission success. "Operations Integration" is the practice of weighing and balancing these factors.

Flight operability is not only a function of the vehicle design, but also the mission requirements that the system must support. Therefore, a given system design may have different operability "scores" for different types of mission scenarios and operations. Consider a vehicle designed solely to achieve and maintain Low Earth Orbit may exhibit significant propellant margin in performing that mission. That same vehicle design may provide little or no margin if the mission is changed to achieve and maintain a lunar orbit. Therefore, a complete measurement of flight operability begins with the definition of the system or vehicle under study and the operational scenario in which operability is to be assessed. For that specific set of design and mission conditions, operability assessments should identify and objectively assess the key items that impact flight operations ability to meet safety, mission success and operating cost constraints.

A formal method for the evaluation of flight operability is given in "Designing a Better Spacecraft: Assessing Flight Operability of Human-Rated Spacecraft.[6]" The basic decision process used in this technique is shown in Figure 5.

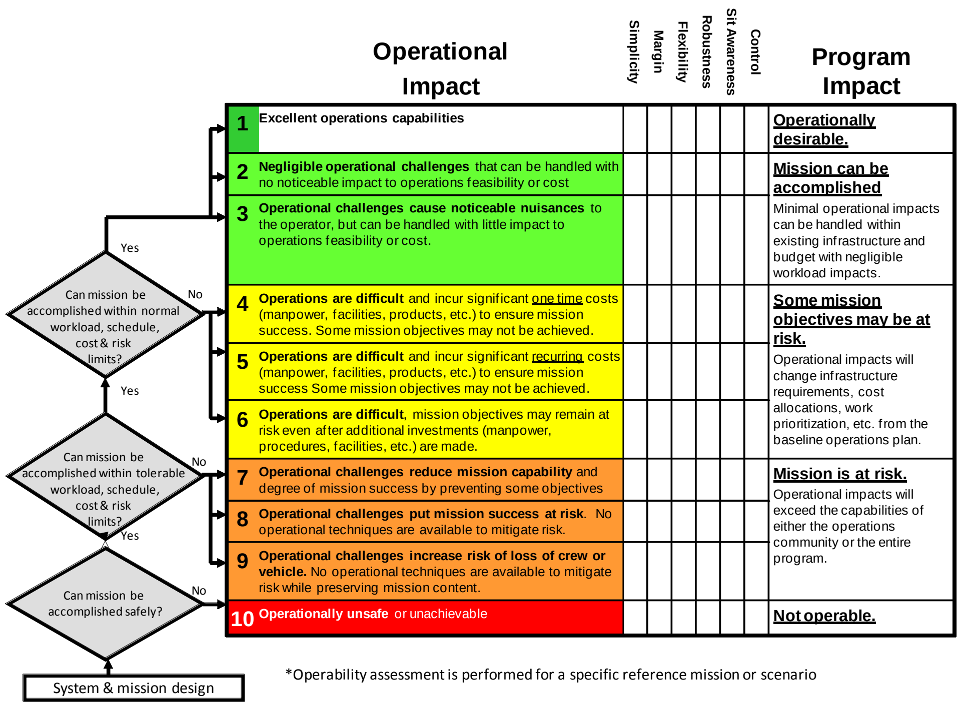


Figure 5. Spacecraft flight operability assessment scale format

III. The Elements of Flight Operability

A review of the many individual recommendations of the human spaceflight operations community indicates six major operability themes – simplicity, margin, robustness, flexibility, situation awareness and control. These themes are discussed below. Note that, if not properly balanced, these operability themes can pose conflict. Features that make a system more robust may also make the system more complex. The judgment of subject matter experts must be applied to strike balance in these cases.

Fundamentally, human flight operations support capability should be tasked primarily with dealing with the tough decisions and the less predictable scenarios. Expending significant human effort in executing the predictable, the mundane, and the formulaic can be a waste of resources and even a risk. While humans can conceive of and enact novel solutions to unexpected challenges – far more than any automated system – humans are less appropriate in performing repetitive tasks in a uniform manner. To support this decision making process, spacecraft systems should provide the flexibility, robustness, and margin necessary. This includes a well documented, analyzed and verified understanding of the real limits of the spacecraft both in the nominal configuration and through a reasonable range of off- nominal conditions such as unusual attitudes, contingency power downs, and post-failure operations. Armed with this knowledge and understanding, the human operator requires appropriate situation awareness and control capability to understand the context of his or her decisions and to efficiently take action on those decisions.

A. Simplicity

Simplicity – often referred to with its inverse, complexity – is the collective measure not only of the functions, interfaces and dependencies inherent in the system architecture, but also of the observations, decisions and actions required of the human operator. The number and ease of operation of functions and interfaces in the operational environment drive the number and cost of analyses, tools, procedures, plans, constraints and training required.

Simple systems that have few dependencies and few possible system configurations generally require fewer procedures, less training, and less effort to monitor and control.

Simplicity cannot be measured in the design of the spacecraft and its subsystems alone. One must also consider the challenges of the mission and the spacecraft's ability to meet those challenges. Consider the simplest version of a car – a pedal powered four wheeled vehicle with a minimum of moving parts and very simple operating and maintenance instructions. Though easy to operate in its intended environment – a driveway or a sidewalk, that same vehicle becomes extremely difficult and unsafe (as well as illegal) to operate on a city street or across long distances. Ultimately, a spacecraft design and operating characteristics must be matched to the mission.

1. Example – Apollo LiOH canister incompatibility

Perhaps the most well known example of complexity in the history of the US human spaceflight program is that of the Carbon Dioxide (CO2) scrubbing equipment on the Apollo Command Module and Lunar Module. The two spacecraft, though joined together for much of their mission and sharing both a common crew and a common atmosphere, used two separate and incompatible Lithium Hydroxide (LiOH) cartridges to remove CO2 from the cabin atmosphere. One of the more celebrated successes of the Apollo 13 contingency crew return was the real-time effort of the operations team to develop a means to use a Command Module LiOH cartridge in the Lunar Module system built for a cartridge of a completely different shape. The use of two entirely different components to perform the same function is a clear example of unnecessary complexity in the overall spacecraft architecture.

2. Example – ISS Antenna Management

The ISS boasts an impressive communications system, including redundant S-Band communication for voice, data and core commanding and a Ku-Band system for video, audio and payload data. Operation of this system requires the management of the antennae and their relationship to Tracking and Data Relay Satellites, ensuring that ISS stay in contact with satellites that are within line-of-sight. This function was intended to be managed by software onboard the spacecraft, but an effective onboard management function was not available in the flight software for the first decade of ISS operations. Instead, MCC actively managed the onboard system, uplinking commands every day to direct the communication system to change its selected target satellite as ISS traveled through its orbit. The calculation, generation, and management of the associated commands represented a significant workload for MCC, as well as an increased risk of temporary loss of communication in the event of a human error. Operationally, this ground-in-the-loop control process was overly complex. Today, the flight software capability to manage this system has been implemented, reducing the reliance on and workload of the MCC communications and tracking officer.

3. Example – Space Station Evolution from On-Orbit Component Assembly to Pre-Integrated Truss

Early designs for Space Station Freedom called for the main truss of the vehicle to be a built by hand – a lengthy and complicated process requiring astronauts to assemble a square truss from individual poles and connector nodes, adding wire harnesses and external avionics components as the truss grew out of the Space Shuttle payload bay. This difficult process involved as many as 7 separate robotic systems working in tandem with the astronauts and ultimately required the execution of final integrated test and verification of the spacecraft only after it was assembled on orbit. The complexity and risk of this approach became clear as assembly planning and analysis studies pointed to problems throughout the process. In the early 1990's, a fundamental design and philosophy change was enacted, implementing a "Pre-Integrated Truss" or PIT to decrease the risk and increase the efficiency of on-orbit assembly tasks.[7] This design matured as the Space Station Freedom Program evolved into the International Space Station Program, and was successfully implemented over the assembly phase of that program. Even with this fundamental simplification of the assembly sequence, ISS assembly proved to be a formidable engineering challenge.

4. Recommendations

To address operability concerns, hardware and software should be as simple as practical, minimizing the number of unique interfaces, algorithms, and functions that require separate operational techniques to monitor and control. Functions and interfaces should be common and consistent, requiring a reasonable number of tasks and methodologies on the part of the operator. Tasks themselves should be simple, allowing the operator to concentrate on decisions to be made rather than detailed operational sequences to be performed. There are reasonable limits on the operationally desirable level of simplicity. A system that is so simple that it does not provide the flexibility or robustness to perform in off-nominal scenarios is not operationally viable. Careful consideration of the other operability factors should be included in an assessment of the appropriate level of simplicity in a system.

B. Robustness

Robustness describes the system's ability to cope with changing conditions resulting from both nominal and off-nominal operations. Flight operations planning and analysis costs are often driven by the need to "protect" the system or vehicle from certain conditions and events. The nature and degree of these "protection" measures is determined by the system's or vehicle's robustness. Note that provisions such as performance margin and consumables margin is assessed in a separate "margin" category. The "robustness" category addresses redundancy, fault tolerance, cross-strapping and similar system architecture traits.

1. Example – Increased robustness in the Gemini Spacecraft Design

During Project Mercury, it was found that the pairing of electrically-sensitive computing equipment with mechanical components such as pumps left critical avionics prone to electrical transients that could interfered with or even interrupt their operation. Subsequent spacecraft designs addressed this concern through isolation of critical equipment on separate "essential" electrical buses. Similar approaches were used in other Gemini systems, as evidenced by the provision of a separate set of life support, electrical, and propulsion systems dedicated to provide a safe emergency return to the Earth's surface.[8] The Space Shuttle architecture reflects this same philosophy not only in its electrical power distribution system, but also in its data bus architecture. Similarly, ISS provides isolation of critical system command and control functions from non-critical payload and video systems. This method of compartmentalization and channelization can reduce operational risk, as well as analysis required to ensure that nominal and off-nominal subsystem configurations are safe.

2. Example – Thorough testing in the Apollo Program

Successful execution of the Apollo Program is attributed in part to its thorough approach to testing. The limits of the hardware and integrated systems were well understood, allowing the program and the operations community to make well informed decisions as contingencies, both before and during flight, arose.

3. Example – Space Shuttle Data Processing System (DPS) Redundancy

The Space Shuttle ushered in an era of greatly expanded software capability in human spaceflight. General Purpose Computers (GPCs) provided overall command and control capabilities for the spacecraft, including closed loop control of the systems and flight path during dynamic flight. To protect against both hardware and software malfunctions during these critical operations, the DPS provided both a set of four redundant, synchronized GPCs and a separate fifth Backup Flight System (BFS) that used identical computer hardware but dissimilar flight software. The BFS was never used in flight, but the redundant set of primary GPCs provided a robust capability to continue flight after failures in individual computers.

4. Recommendations for Achieving Appropriate Robustness

To achieve operational robustness, flight systems should be designed to maintain fail operational capability (no loss of functionality after first failure); the design should ensure no single failure puts the mission in to a contingency. Systems should remain partially capable in off-nominal scenarios, allowing the continued use of remaining functionality without requiring significant operator action to recover that functionality. In many cases, cross-strapping - interconnections between components of two or more separate strings - are effective means for improving robustness in off-nominal scenarios. Redundant strings should be supported by separate data and power utility feeds to allow continued system availability after a single failure.

No time-critical operator action should be required to prevent loss of mission, crew or vehicle. Time-critical operator actions are those that must be performed by a person within a limited time frame immediately following an event to ensure continued safe and effective mission execution. In general, the vehicle should automatically identify and reconfigure in response to failures that can impact mission success or crew/vehicle survival. Automated responses should result in predictable vehicle configurations that support crew and vehicle survival.

The need for robustness is somewhat bound by the overall goals and mission scenarios that define the system and its operation. For a given spacecraft, a set of reference missions and configurations defines cases in which the vehicle is expected to either complete or abort the mission. Robustness should be provided to support mission execution within the expected bounds (including off-nominal scenarios) and to support mission abort or early termination once the defined criteria have been met. Robustness beyond that needed for these cases may not be warranted.

C. Margin

Operational margin describes the amount of capability or consumable supplies available beyond that required to execute the mission. Operational margin provides assurance that the nominal mission may be safely executed and allows for continued operation in the event of unexpected conditions such as malfunction or mission scenario changes.

There are three categories of operational margin:

- Performance Margin - the ability of the system to provide greater capability than required for normal operation or in the event of any single failure. Measures of performance margin vary by vehicle subsystem. For example, performance margin for an electrical power system might be measured by power output capability while the measure for a communication system might be associated with the data bandwidth sizing.
- Resource Margin - the amount of consumable commodities (propellant, atmospheric gases, stored energy) available beyond that required to support nominal flight operations.
- Environmental Tolerance Margin - the system's ability to operate beyond the nominal operations environment for a given mission profile.

Often, operational constraints and controls are required to ensure that adequate capability is available throughout a nominal mission and after an anomaly. These constraints and controls typically impact the ability to successfully complete all mission goals, as they limit the use of capabilities and resources even before an anomaly occurs. They also require the addition of more techniques, tools, products and training to the operations infrastructure. All of these additions result in increased life cycle cost. Margin is considered available for operational consideration only when formal analysis documentation of that margin is made available to the operations community. Lack of margin can have profound impacts on mission planning as well as real-time operations. More detailed pre-flight analysis must be performed to ensure that mission objectives may be met within the available resources, that the vehicle can perform required operations within its normal performance envelope, withstand potential anomalies, and that the flight environment does not exceed the vehicle's limits. Lack of margin not only impacts the mission operations organization, but it also drives significant program sustaining engineering costs to provide additional case-specific analyses that support the flight operations community as well as program strategic planning.

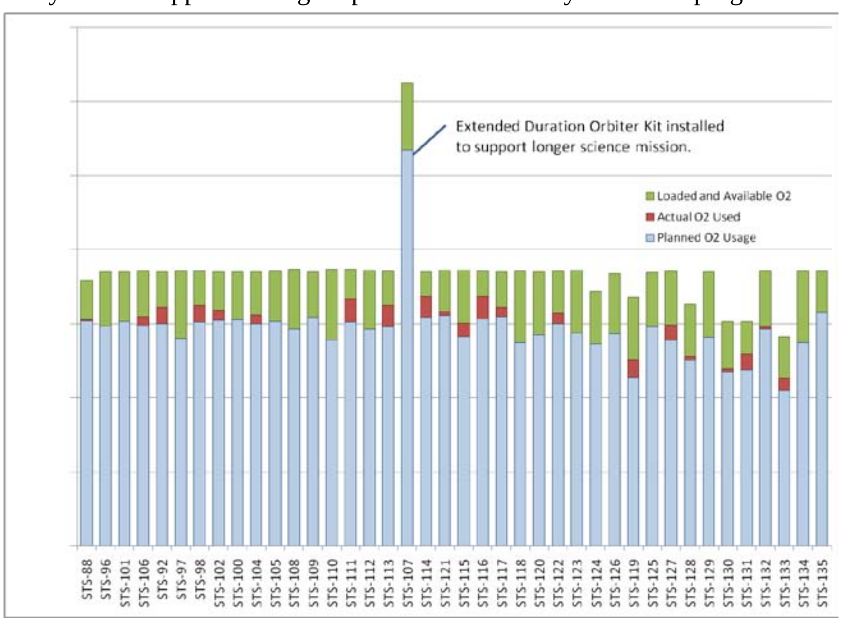


Figure 6. Space Shuttle cryogenic Oxygen loading and usage over the past decade.

Figure 6 provides a simple example of Space Shuttle cryogenic Oxygen resource margin over the last decade. The availability of a reasonable margin allows the operations community to deal with contingency situations and often add a day to the mission duration to allow for the completion of mission objectives. The red regions in each bar on this graph indicate occasions in which this margin was partially used in order to meet the needs of the mission. Also noteworthy is the ability to add an Extended Duration Orbiter (EDO) pallet kit, used on several mission including STS-107, to enable missions requiring additional time on-orbit. This and other forms of flexibility will be discussed further below.

1. Example – Creating Power Resource Margin During Early ISS Operations

During the early phases of ISS assembly, the US segment of the spacecraft had very limited redundancy in powering critical subsystems. With only 2 power channels available, the US power system was easily loaded to capacity in supporting not only the vehicle core systems, but also early science operations. Each power channel could support a load of approximately 18 kW, but the failure of any one of the three batteries would cause an immediate overload – and shutdown – of one of the two power channels. To make matters worse, loss of power to the critical command, control and communications systems would leave the crew and ground unable to take action for several minutes as the data system reconfigured in response to multiple computer loses. With the risk of a major setback early in the program, program and operations management determined that the power budget for each channel would be limited to ensure that each power channel could continue to operate after that first potential battery failure. In effect, a 1/3 margin was imposed on all operations. As vehicle assembly continued, the US power system grew from its early 2 channel configuration to a full 8 channel system.

2. Example – Environmental Tolerance Limits During ISS Assembly

Early in ISS assembly operations, the STS-92 mission gave a clear example of environmental tolerance limits and their impact on operations complexity. STS-92 delivered the Z1 element – a large square truss segment containing key power, communications, thermal and attitude control system components to the fledgling ISS. Until crewmembers could attach data and electrical umbilicals to power the Z1 components and heaters associated with those components, flight attitudes exposing those components to sunlight were necessary to maintain temperatures above individual component freeze points. Unfortunately, these same sun-pointing attitudes placed too much sunlight on the Space Shuttle's airlock water lines, risking overheating and damage to the airlock required to support the mission's EVAs. Further complicating the mission planning process, the lack of power and data connections to those components prevented the crew and ground from monitoring these temperatures directly. Instead, pre-flight thermal predictions alone would provide the basis for the operators' understanding of risk to ISS equipment. Thorough analyses of both Space Shuttle and ISS temperature profiles - analyses involving not just the flight operations community, but also the program office and spacecraft vendors to investigate secondary impacts to propellant usage, communications availability, and many other factors- were required to support the development of a flight attitude timeline that would meet all of the constraints placed on this mission. Ultimately, a carefully orchestrated series of attitude maneuvers were performed, flipping the mated Shuttle-ISS "stack" repeatedly throughout the EVA. The mission was successful, but at a cost of months of analysis employing a large community of engineers.

3. Example – Performance Limits Impacting ISS Operations

Changes in the Space Station assembly plan impacted the sequence in which vehicle elements would be delivered and the flight attitudes and environments that those elements to which those elements would be exposed. One of the many results was a significant increase in the rotation of solar arrays. Rotary joints intended to slowly pan back and forth over a period of weeks were now required to continuously rotate at 4 degrees per minute for years at a time. This far exceeded the performance requirements for the joints and, predictably, the joints began to exhibit the effects of wear in flight. Bearings developed increased resistance, occasionally exceeding their drive motor torque limit and "tripping" the joint control offline. The engineering and operations community worked together to develop a number of new operating techniques, procedures and modes both to reduce the frequency of rotation and to respond to the accumulation of torque resistance. These techniques were successful and allowed the continuation of ISS assembly to the point where such frequent and high rate rotation is not required. However, this serves as an example of performance and performance margin that was not properly matched to the mission requirements.

4. Recommendations for Achieving Appropriate Margin

Flight systems should provide margin in order to minimize operations constraints. Vehicle thermal, power, and communications capabilities should not be designed with operations constraints that result in the necessity for highly optimized mission timelines to accomplish normal operations such as rendezvous, proximity operations, and docking. Margin in all three of these categories is a significant driver in determining the amount and extent of mission- and activity-specific planning and analysis. Significant positive margins in key categories should be available in all mission phases.

At the same time, excessive margin is not operationally desirable and should be avoided. For example, a system that provides resource quantities beyond any credible need may use so large a fraction of the allowable mass that fewer redundant strings are provided in the design. Expectations on available margin should be bounded by the maximum needs for an operational scenario (including off-nominal scenarios). In addition, care should be taken in scenarios that involve failure "stacking" (inclusion of multiple separate failure cases in one scenario). Credible failure scenarios include those that would allow continued mission execution and those that would initiate the abort or early termination of a mission. Failures after those that drive a mission abort or early termination are generally out of scope.

D. Flexibility

Flexibility is the ability of the system to accommodate change. This change can be to the mission scenario or to the vehicle configuration. When a system is inflexible, even small changes to the mission or vehicle configuration may require operational workarounds – additional tasks and responsibilities placed on operations personnel and facilities. Flexibility is generally defined by the system's architecture.

1. Example – Space Shuttle Flexible Payload Capabilities

The space shuttle provided flexibility through a variety of standardized services. Standardized payload attachment systems allowed for a wide variety of payloads and missions. Add-on kits such as the Extended Duration Orbiter (EDO) Pallet kit further extended the space shuttle's capabilities, enabling greater science content and longer mission durations. Rather than engineering new solutions for each mission, the Space Shuttle program successfully managed an impressive array of separate payloads – from space telescopes and communications satellites to orbital laboratories and space station components – using such standardized interfaces.

2. Recommendations for Achieving Appropriate Flexibility

Flexible flight systems should be easily reconfigured or updated to account for new conditions and new capabilities during flight or between flights. Although this applies to both flight hardware and flight software, the impacts of inflexible software are the more acute. Operational experience often identifies necessary changes to limits, gains, and other parameters used by flight software. If recompilation of flight software is required to update such parameters, then these value updates will be costly and will require months or years to incorporate. Operational workarounds will be required for extended periods in order to account for discrepancies between the desired and provided values.

There are reasonable limits to the desired degree of flexibility for an operable system. While some amount of flexibility is desired to allow for slight variation in mission profile and vehicle configuration, excessive flexibility can result in additional operations challenges. Highly flexible systems may require more training, product development, and manual tending than is operationally desirable or affordable.

E. Situation awareness

Situation Awareness (SA) is the ability to perceive the state of the vehicle and its operational environment, to understand that state, and to project the future state based on that understanding. If systems do not inherently support SA, additional operator tools and techniques may be required to provide this insight and understanding. This may drive additional operations cost and infrastructure such as facility changes, procedures, training, or even additional flight control team staffing. The inability to identify specific anomalies in some scenarios may increase risks to mission, crew and vehicle. As a result, some activities or objectives may be disallowed when SA cannot be maintained.

1. Example – Mercury instrumentation

The very first US orbital flight provided valuable lessons in the importance of appropriate insight into system health and status. A single faulty sensor indicated that the landing bag had deployed, potentially compromising the heat shield and making atmospheric entry a deadly operation. The operations team scrambled to analyze the spacecraft's condition, and ultimately modified entry procedures to reduce the risk of heat shield loss. Ultimately, it was determined that the landing bag and heat shield had been intact and that the deploy sensor itself had failed. [9]Without a way to confirm this while in flight, the conservative approach taken by the crew and flight control team was the best course of action. Learning from this and similar experiences, NASA adopted a standard of providing "confirming cues" in the Gemini program and beyond, ensuring that secondary cues would be available to confirm indications of both nominal and off-nominal conditions.[10]

2. Example – International Space Station Caution and Warning

The International Space Station provides thousands of separate caution & warning messages to indicate specific problems. In the event of significant anomalies - such as loss of an electrical or data bus - dozens of messages may be issued to announce each of the multitude of system impacts. Without an automated management system or an overarching tool to "synthesize" caution and warning messages into clear indications of failure root cause and system impacts, the crew and ground must work through these messages to identify the root cause and critical impacts of that failure. This is enabled through the development and use of detailed procedures and significant training to ensure that the operations community is prepared to deal with such cases in real-time.

3. Recommendations for Achieving Appropriate Situation Awareness

A balanced approach should be taken in assessing situation awareness. Maintaining situation awareness requires the operator to have an overall understanding of the system's state, capabilities and environment. Too much data can make this understanding almost as difficult to maintain as can too little data. The best approach to achieving balanced situation awareness is the direct involvement of the flight operations community – both crewmembers and flight control personnel – in the process of defining system instrumentation and user interfaces.

Situation awareness should be assured through appropriate telemetry and caution and warning messages which allow unambiguous detection and verification of all nominal and off-nominal events. Critical instrumentation, such as temperature, mechanism position, and current sensors, should be carefully positioned to directly measure the most critical points in the system, reducing or eliminating the need to infer critical information from indirect measurements. The instrumentation strategy should provide a means to confirm the indications of one sensor using another measured value to mitigate the risk of a single sensor failure Appropriate sensor locations and quantities, as well as telemetry display/downlink capabilities should allow the operator to verify automatically generated cues. Simple indications should be provided to the operator to identify failures with widespread vehicle impacts. No false positive or false negative failure indications should be provided to the operator.

F. Control

Control measures the degree and difficulty with which the operator can direct the system's performance during operation. This includes not only the availability of all of the control capabilities to appropriately configure the system, but also the level of control that the operator must exercise. Use of low level commands – those that control individual items at a fine level – may be necessary at times to accomplish specific needs. However, reliance on only these low level commands can result in high operator workload because each component must be individually configured to accomplish a goal. Higher level commands – those that cause the system to perform multiple steps to achieve a predefined configuration – can greatly reduce the level of difficulty in operating the system. Accordingly, one effective measure of control is the average count of the number of commands required to implement desired courses of action.

Ineffective commanding capabilities may require the development of additional ground-based software tools to support the configuration management, processing, and issuance of commands in an effective manner. Additional procedures may be required to support the configuration and processing of commands. Additional training is required to enable operators to use these tools and procedures. All of these add to the infrastructure, cost and time associated with controlling the spacecraft.

1. Example – Mercury Manual Control Capabilities

Project Mercury mangers recognized the technical risks they had undertaken in launching a man into space. Not only were they rapidly developing new flight systems, but they also had no knowledge of the human’s ability to function in a weightless environment. In response, Mercury was designed to provide both fully automated and manual control for most flight phases including ascent . As mentioned above, this approach greatly benefited the program by enabling the astronaut to assume control when automated systems malfunctioned, but the cost and complexity associated with fully automating systems proved a daunting challenge.

2. Example – ISS Command Complexity

As compared to its predecessors, the ISS incorporated a staggering number of separate computers and firmware controllers, creating a diverse and distributed network of control loops across the vehicle. The tiered structure of hardware control, firmware control, and software control resulted in a complex command architecture. Although common Orbital Replaceable Units (ORUs) and firmware controllers were used wherever possible, flight software for the ISS’s US segment was developed separately by each of the four major development contractors. Remote Power Control Modules (RPCMs) – the basic building block of the electoral power distribution system – were integral parts of each contractor’s contribution to the vehicle. Each contractor therefore developed and delivered its own separate RPCM control software and implemented the operator command capabilities in a different form. Despite the use of common equipment, the user’s command interface appeared overly complex due to these variations. Ultimately, the operations community invested significant effort in creating embedded logic within the crew displays, forcing a consistent user interface from the crewmember’s viewpoint.

In other portions of the power system, commands were unnecessarily complex, including such items as “Hot Switch Open Override Inhibit Arm” – the first of two commands sent to allow the operator to subsequently command open a switch even when the firmware was set to reject such a command. Such double- and triple-negative commands are relatively commonplace and require careful re-naming on operator displays to make user interfaces intuitive for the operators.

3. Recommendations for Achieving Appropriate Control

Command capabilities should allow the operator to control vehicle functions by setting goals and making decisions when queried. Once these goals and decisions have been provided by the crew, the vehicle implements them with little or no additional work required on the part of the crew. Routine functions (those that always involve the same steps executed in the same order) should be automated. Where appropriate, low-level commands should still be provided to allow for effective operations in off-nominal situations. A tell-tale sign of inappropriate command strategy is the prevalence of operational procedures that include few decision points but many sequential command or switch throw steps. In such cases, automation\of those non-decisional steps should be considered as a means to reduce crew workload and system sensitivity to human error.

The system should operate and respond in a repeatable, predictable manner to each command. The operator should have control over the execution of automated capabilities, allowing him/her to proactively prevent or reactively terminate the execution of inappropriate actions. The operator should have the capability to correct the vehicle configuration when automation either fails to do so or places the vehicle in an undesirable configuration.

Automation may be applied to address some control needs, but automation may also create other operability challenges. In general, automation of well understood operations is achievable and operationally desirable. However, automation of actions or responses to scenarios that are not well understood can make operations more difficult. Where automation functions must be monitored by operators, halted as required, and replaced by operator actions, the automation function may be operationally undesirable. Even in well understood scenarios, the flexibility to modify automation through the use of reconfigurable scripts, settings, and other flexibility measures is highly recommended.

III. Challenges in Achieving Operability

If we understand the problems, why do we not fully address them? Although program managers and subsystem designers alike may understand the need for spacecraft flight operability, there remain programmatic challenges in implementing operationally desirable features. Recognizing and addressing these challenges early in a development program is an essential step in establishing reasonable design and operations solutions.

A. Development Cost – Now v. Later

Any spaceflight program faces significant challenges as design, development and test efforts encounter problems. Cost increases and schedule slips place increased pressure on program management to reduce program content where possible. Priorities shift from optimizing operations phase cost performance to preserving enough funding for the delivery and testing of hardware and software.

During the development phase of Space Station Freedom - the original design that evolved into today's ISS - then prime contractor predicted a 50% reduction in operations costs through the implementation of onboard monitoring and management functions.[11] The Onboard Management Application (OMA) would track resource availability and usage and collaborate with other onboard software to ensure that the vehicle automatically adjusted in response to resource issues. As the design matured, the top tier of the data processing system was deleted; with it the OMA also disappeared. The associated tasks of tracking, predicting, and managing onboard resources was relegated to the Mission Control Center, where unique tools and separate console positions were defined to perform these functions. The design changes judged necessary to reduce development cost and risk ultimately erased the potential for achieving the originally predicted operations costs savings.

Breaking this cycle – the deferral or deletion of future cost savings enablers in the interest of meeting near term goals – is a difficult program challenge and ultimately requires increased development phase funding.

B. Verification & Validation – Risk and Cost

Every feature and function of a spacecraft invokes both a risk and a cost associated with verification and validation. Program managers are faced with the option of deleting or reducing spacecraft capabilities in order to reduce cost and schedule risks. Where spacecraft capabilities cannot be reduced, reducing the number of unique tests and analyses to be completed remains a tantalizing option to address cost and schedule concerns.

Unfortunately, these risk reduction efforts can negatively impact the flight operations community. When a vehicle system is tested and analyzed only for the conditions nominal design reference mission conditions, the performance and limits of the vehicle in off-nominal conditions remains unknown. Concerns over possible damage to the spacecraft in such unknown conditions increases the need to "protect" the vehicle from such cases and ultimately drives the operations community to perform their own analyses, impose more operational constraints, develop more contingency procedures, and provide more training to their personnel. The cost of flight operations increases to compensate for the losses incurred in reducing development phase costs.

Early Space Shuttle operations proved difficult as the flight operations team worked to understand the complex interaction of the vehicle's subsystems even as they provided real-time flight control support. Incomplete analysis of these interactions during the development phase left the operations team with a significant workload to discover and fully understand the complex ways in which the vehicle behaved. The engineering and flight operations communities alike invested years of operations in understanding these interactions and formally documenting the interactions and responses in procedures and operational flight rules.[12]

The International Space Station "inherited" much of its design from its predecessor – the Space Station Freedom Program. The basic vehicle system architecture, as well as its components, were designed for environment in a relatively low inclination orbit – 28.5 degrees. As the reborn ISS, however, these systems and components are subjected to the extremes of a much higher inclination orbit – a 51.6 degree inclination – to enable inclusion of Russian elements and Russian launch vehicles in the overall vehicle assembly. This simple change in mission profile, coupled with other major vehicle architecture changes, had significant impacts on overall vehicle operability. New extremes in thermal environment included days-long periods of continuous daylight as well as shadow patterns cast by the vehicle's own structure. Time and budget allowed for analysis of some – but not all – possible combinations of vehicle attitude and sun exposure, leaving open many questions as to the true environmental tolerance of the vehicle. Lack of a thorough understanding of the ISS thermal environment and spacecraft component thermal tolerances prior to the operations phase drove the need for significant effort *during* the operations phase to analyze specific cases of unusual attitudes for specific events such as docking and undocking.

C. Lack of Flight Operations Inclusion in Early System Engineering Processes

The flight operations infrastructure - facilities, people, and processes - are an integral part of the overall system, "closing the loop" to control the spacecraft throughout it's mission. As such, that flight operations infrastructure is itself a critical control loop that should be carefully designed and measured just as any other spacecraft system or program process. However, funding for flight operations specialists in the early phases of a program is typically minimal and prioritized much lower than funding for other personnel. This often stems from a basic misunderstanding of the role and contribution of the operations community as systems engineers. As a result, true cost implications of design solutions are generally not understood or appreciated in time to make informed decisions.

Involvement in definition of operations concepts, requirements, functional allocation of capabilities, and implementation trade studies are all essential to addressing operations phase cost performance. Involving the operations community only once the requirements and design have been determined will result in higher operations complexity, risk and cost. Where integrated design solutions – those that address the balance of onboard capabilities, ground capabilities, and human interaction with both – could be developed, a process that does not include the operations community typically shifts (rather than reduces) cost from the development of onboard capabilities to the investment in additional ground-based resources and task loading.

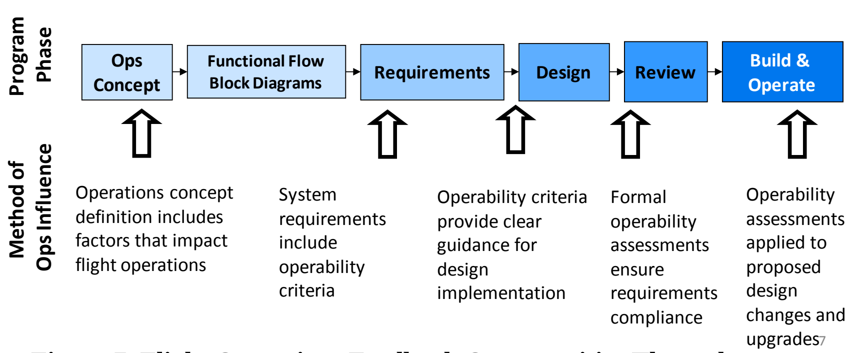


Figure 7. Flight Operations Feedback Opportunities Throughout the Program Lifecycle.

A comprehensive strategy of flight operations involvement throughout the program lifecycle, as illustrated in Figure 7, can benefit human spaceflight programs, both in terms of mission success and program affordability.

IV. Application to Future Programs

NASA has applied these lessons learned in supporting the development of the Orion Spacecraft – now the basis for the Multipurpose Crew Exploration Vehicle (MPCV). Flight operations team member involvement in defining design reference missions, fault management schemes, subsystem architectures, and flight software functionality have helped the program improve the operability of its vehicle and enable future cost savings. For example, early analysis of the Orion Active Thermal Control System hardware and software design by flight operations personnel identified opportunities to significantly improve system robustness through better control schemes and judicious addition of flexibility in the control software. These changes were adopted with no net cost to the program. Continued collaboration between the spacecraft development and flight operations will allow the MPCV Program to continue to identify and address opportunities to improve flight operability.

Flight operability concerns will become even more critical to the success of human spaceflight endeavors as we develop and operate spacecraft that venture farther into space. Deep space flight imposes new operational constraints including the inability to execute a timely emergency return as well as time delayed communications and reduced communications bandwidth that reduce the ability to apply ground-based real-time support in response to real-time events. The next generation of space exploration vehicles must address operability concerns to enable their crews to survive and succeed.

Similarly, the emerging commercial human spaceflight sector must address flight operability concerns in order to achieve cost effective operations and realize profitable overall corporate operations. NASA's lessons learned can be a valuable resource in developing cost effective solutions.

V. Conclusion

Future human spacecraft development programs can directly benefit from analysis of previous programs' successes and failures in addressing flight operability and its associated costs. Direct involvement of flight operations personnel in the development of operations concepts, requirements, and design solutions is a critical step in addressing operations phase cost. Formal methods such as use of the Flight Operability Assessment Scale, can identify issues and impacts earlier in the development processes. Application of the lessons learned in the first 50 years of NASA's human spaceflight campaign can directly benefit new programs by improving spacecraft designs and reducing flight operations costs and risk.

VI. Acknowledgments

The author wishes to acknowledge the accomplishments and dedication of the men and women of the Mission Operations Directorate – and, before it, the Flight Operations Directorate – at NASA Lyndon B. Johnson Space Center, whose collective flight operations experience is the motivation for this work.

VII. References

[1] Kranz, E. "STS Flight Operations – Concept versus Reality." *AIAA Shuttle Environment and Operations Conference I1*, 1985.

[2] Voas, R. "A Description of the Astronaut's Task in Project Mercury", NASA Report, 1961.

[3] "Project Gemini Design Philosophy," NASA News Release, February, 1963.

[4] Hammack, J. and Kapryan, W., "Gemini: Mercury Experience Applied"

[5] Kranz, E. "STS Flight Operations – Concept versus Reality." *AIAA Shuttle Environment and Operations Conference I1*, 1985.

[6] Crocker, A. "Designing a Better Spacecraft: Assessing Flight Operability of Human-Rated Spacecraft," AIAA 2010-2031, AIAA SpaceOps 2010 Conference, Huntsville, AL, April 2010.

[7] "Space Station Freedom Restructuring Plan Completed," NASA Release 91-45, 21 March 1991.

[8] Lindley, R. "The Gemini Program from an Engineering Viewpoint," Royal Aeronautical Society, Manchester, England, 15 March 1967.

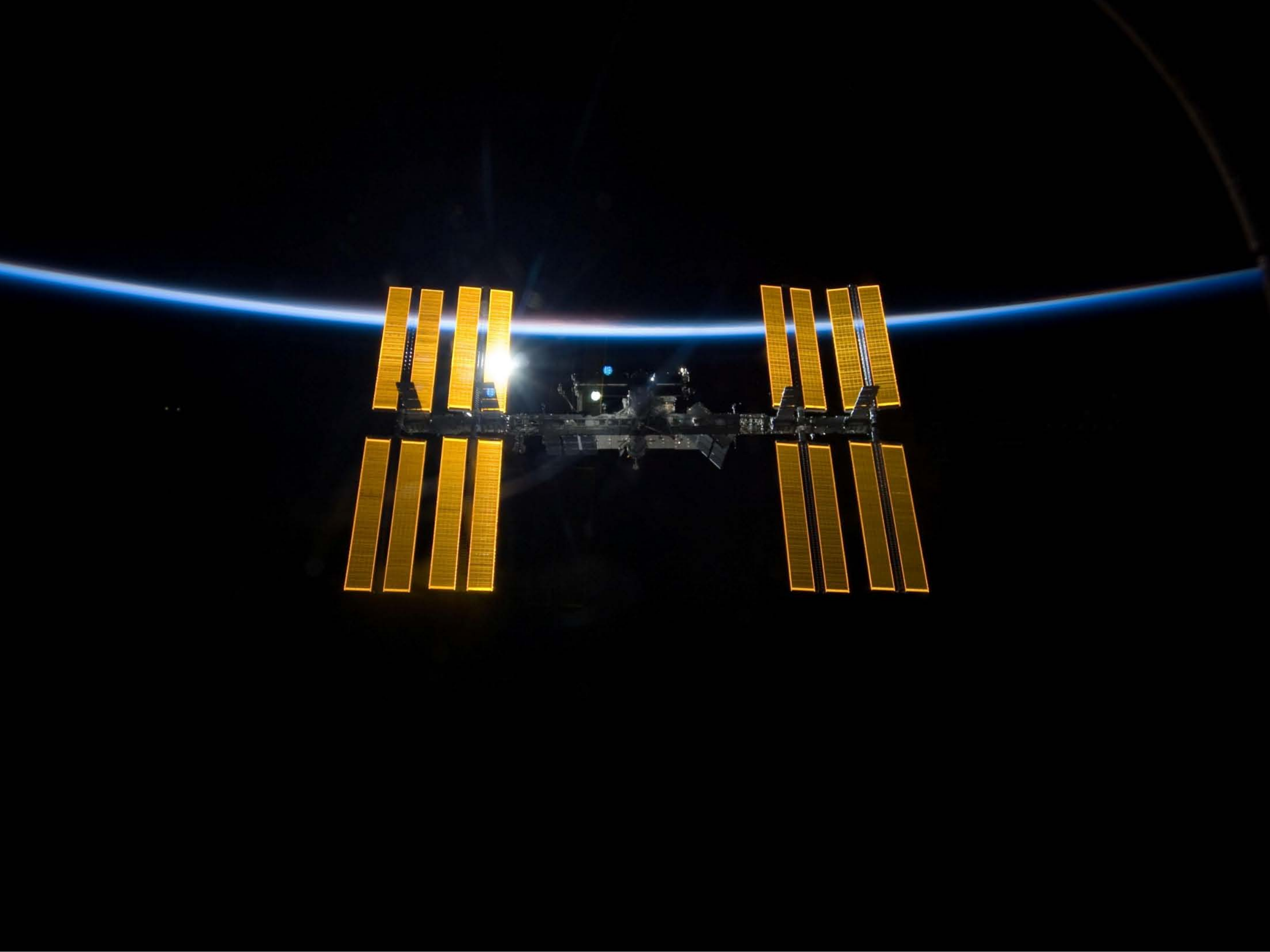
[9] Kraft, C. "Mercury Operational Experience", Institute of Aerospace Sciences National Meeting on Man's Progress in the Conquest of Space, St. Louis, MO, April, 1962.

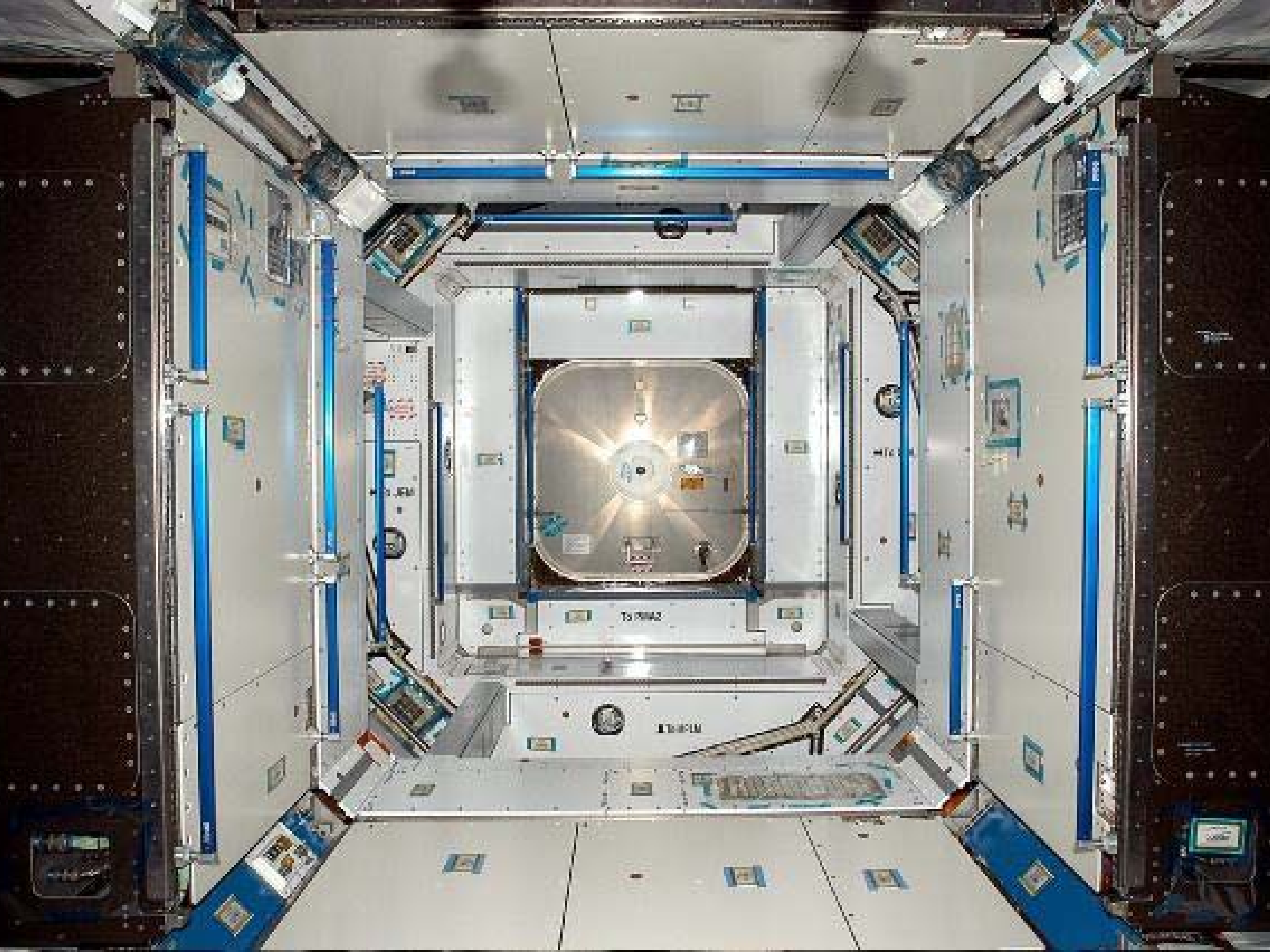
[10] “Project Gemini design philosophy,” NASA News Release, February, 1963.
[11] Bennett, G. and Paddock, S., “Design for Operations Productivity on the Space Station Program.” AIAA Space Program and Technologies Conference, June 23, 1988.
[12] Kranz, E. “STS Flight Operations – Concept versus Reality.” *AIAA Shuttle Environment and Operations Conference I1*, 1985.

Making Human Spaceflight Practical and Affordable: Spacecraft Designs and Their Degree of Operability

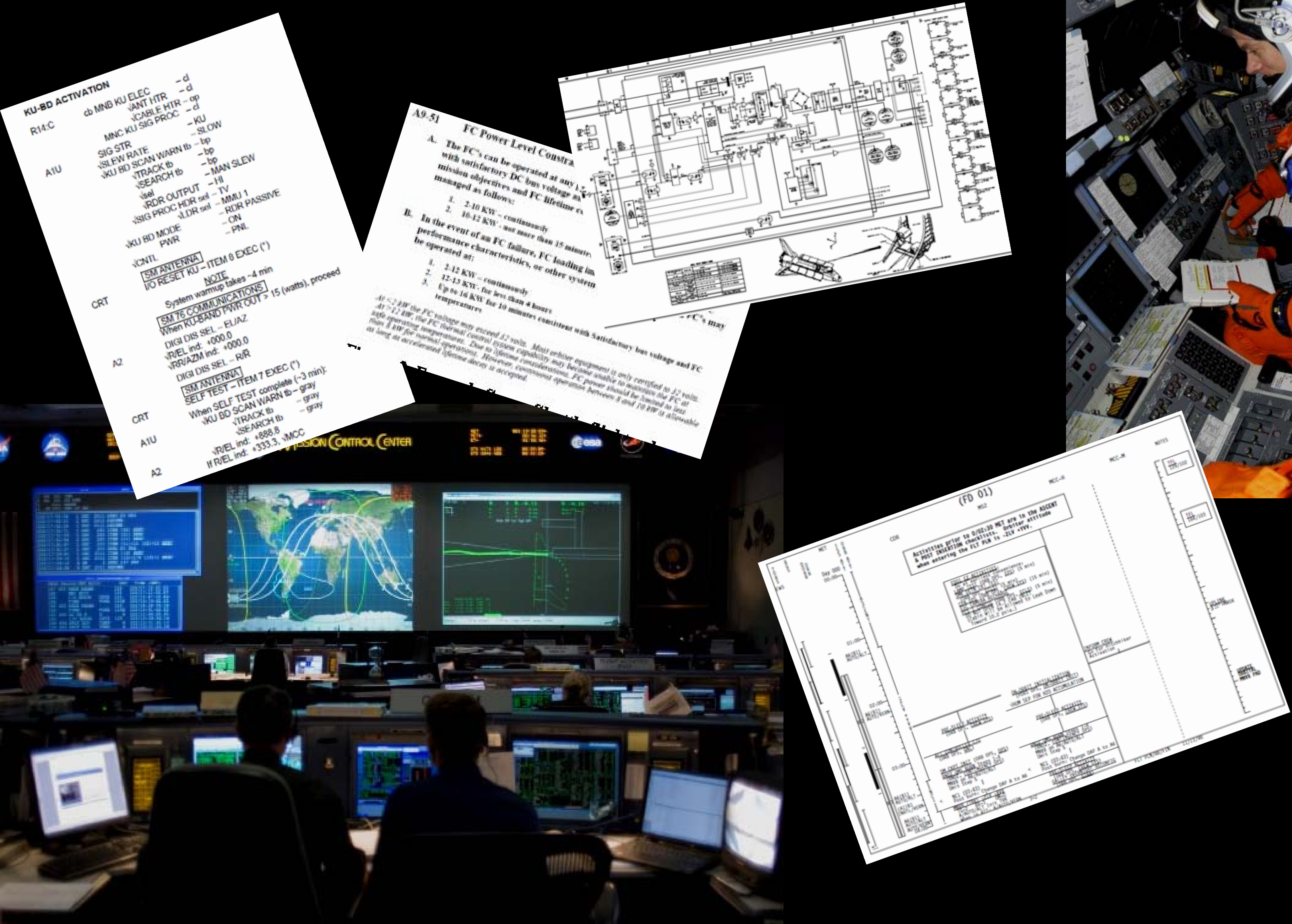
Alan Crocker

National Aeronautics and Space Administration
Lyndon B. Johnson Space Center
Mission Operations Directorate

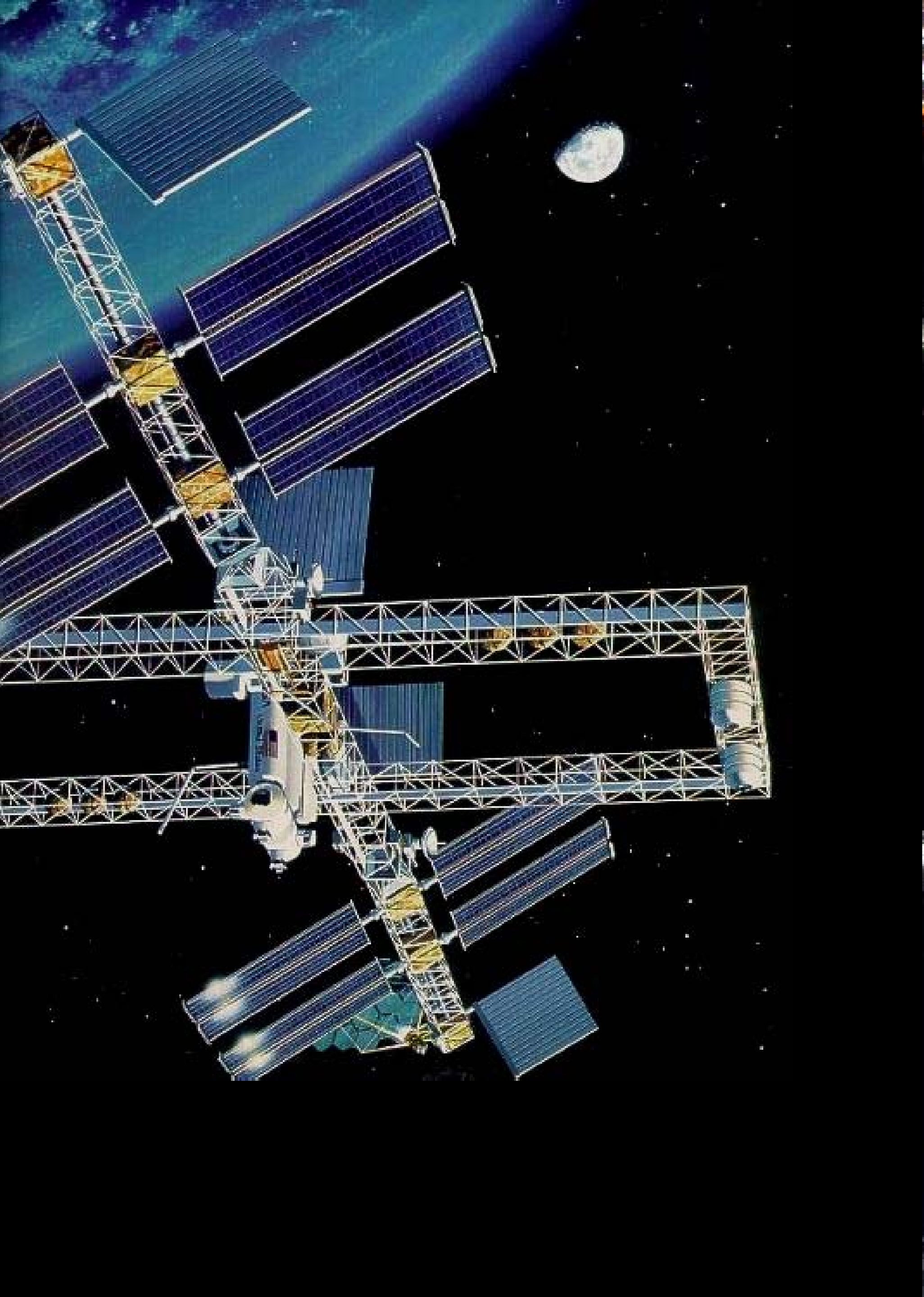
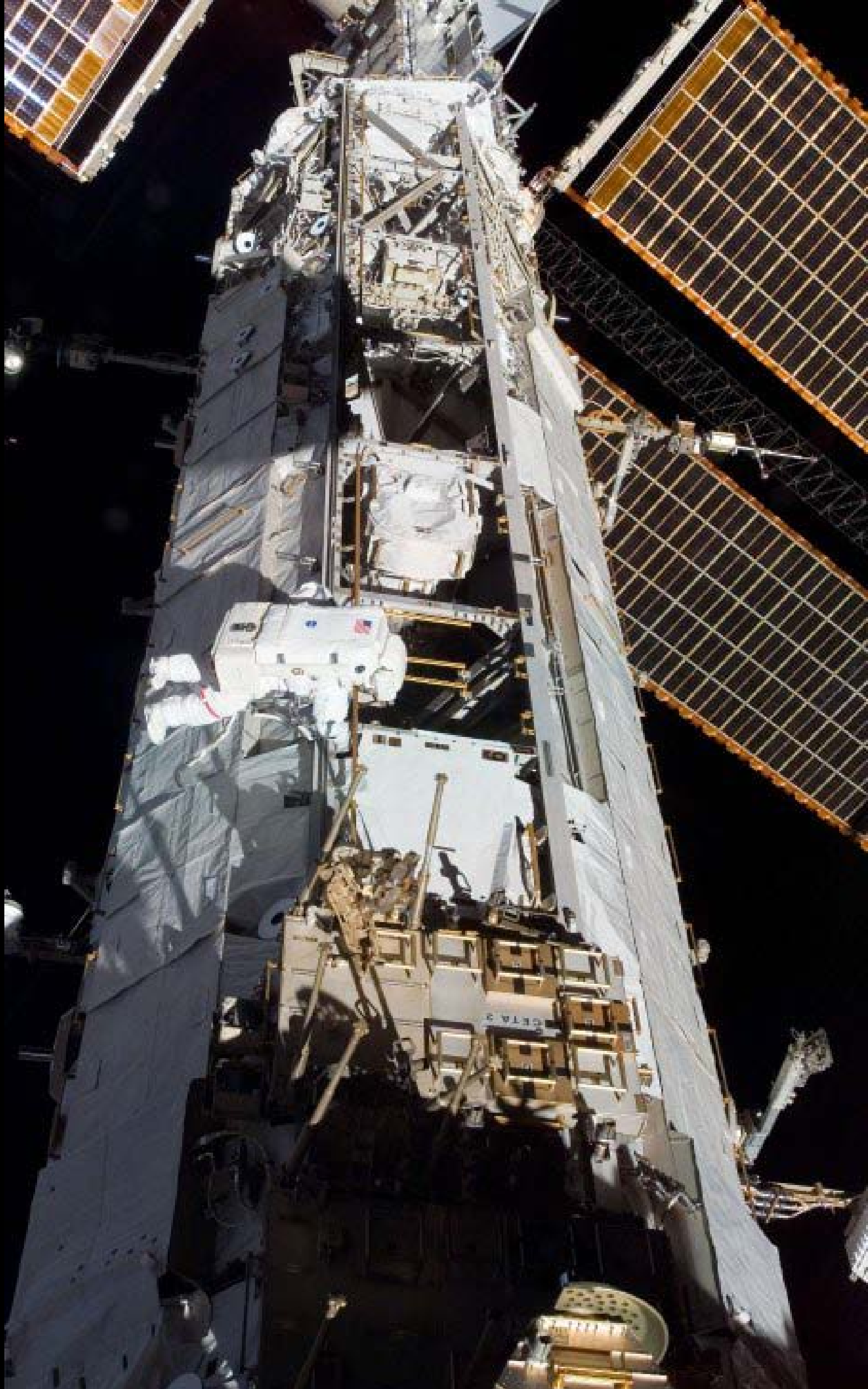


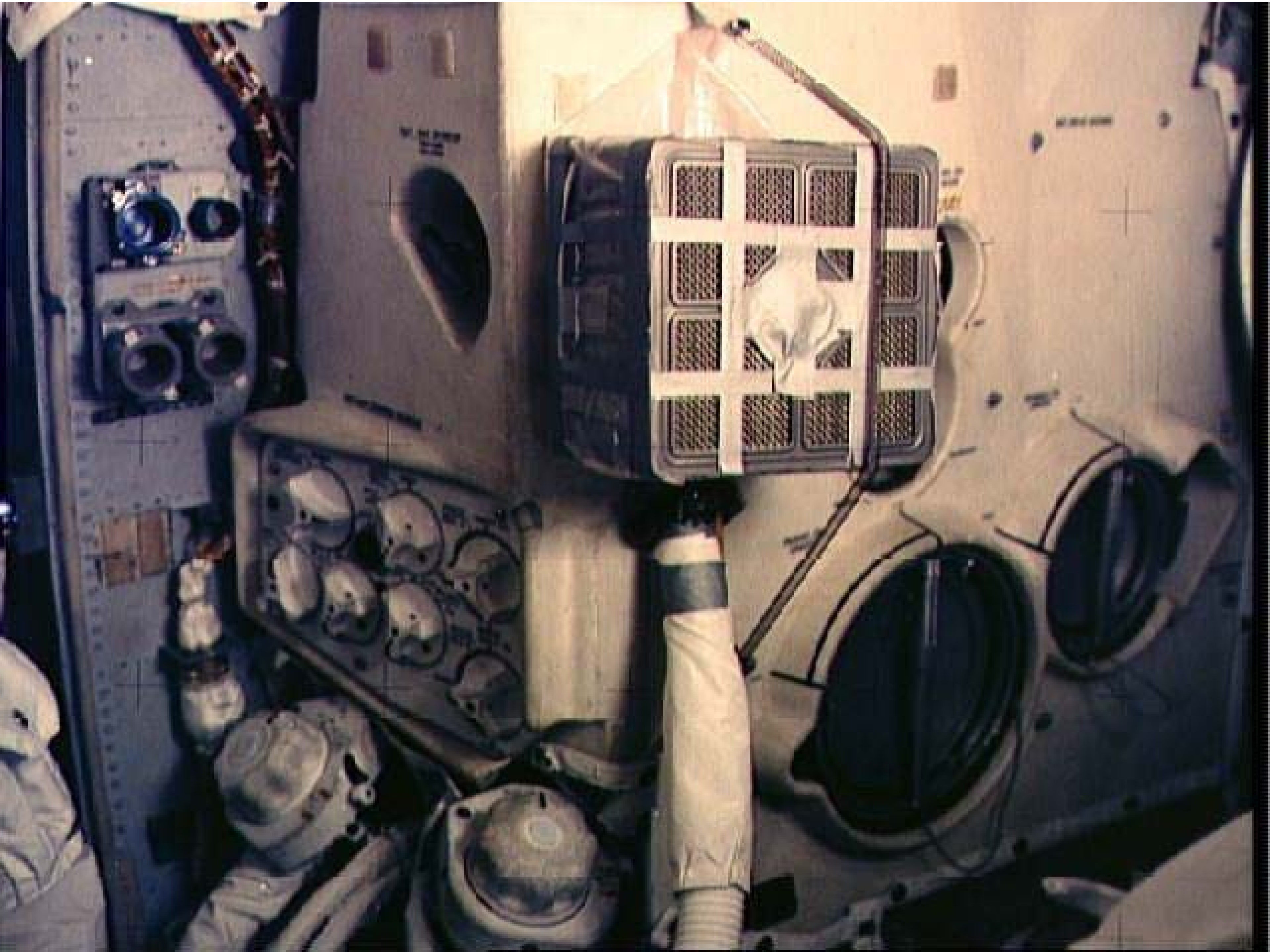


Flight Operations as a Systems Engineering Discipline.



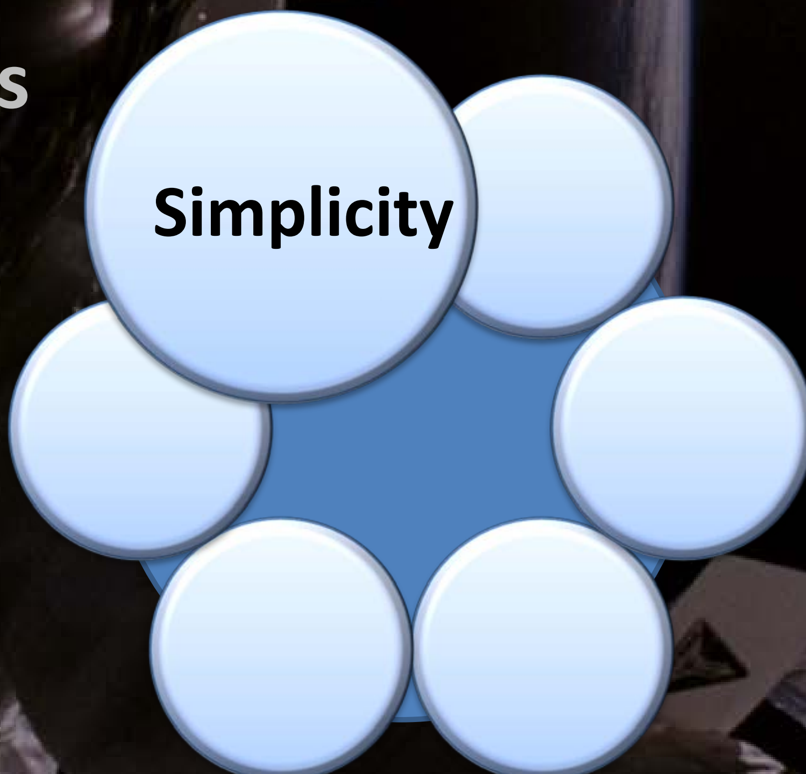
Six broad factors that characterize operability.



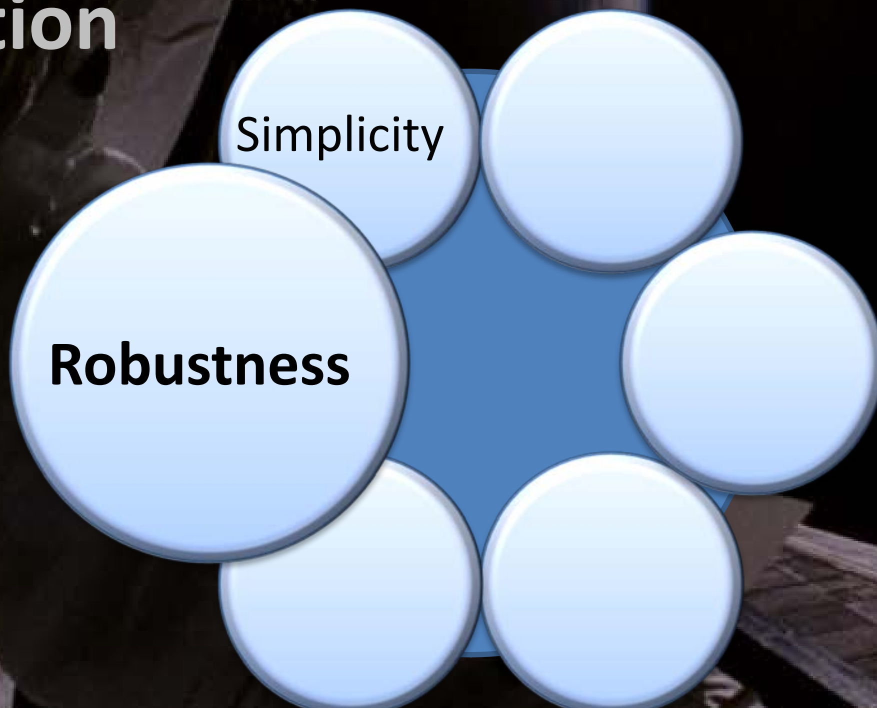
Simplicity

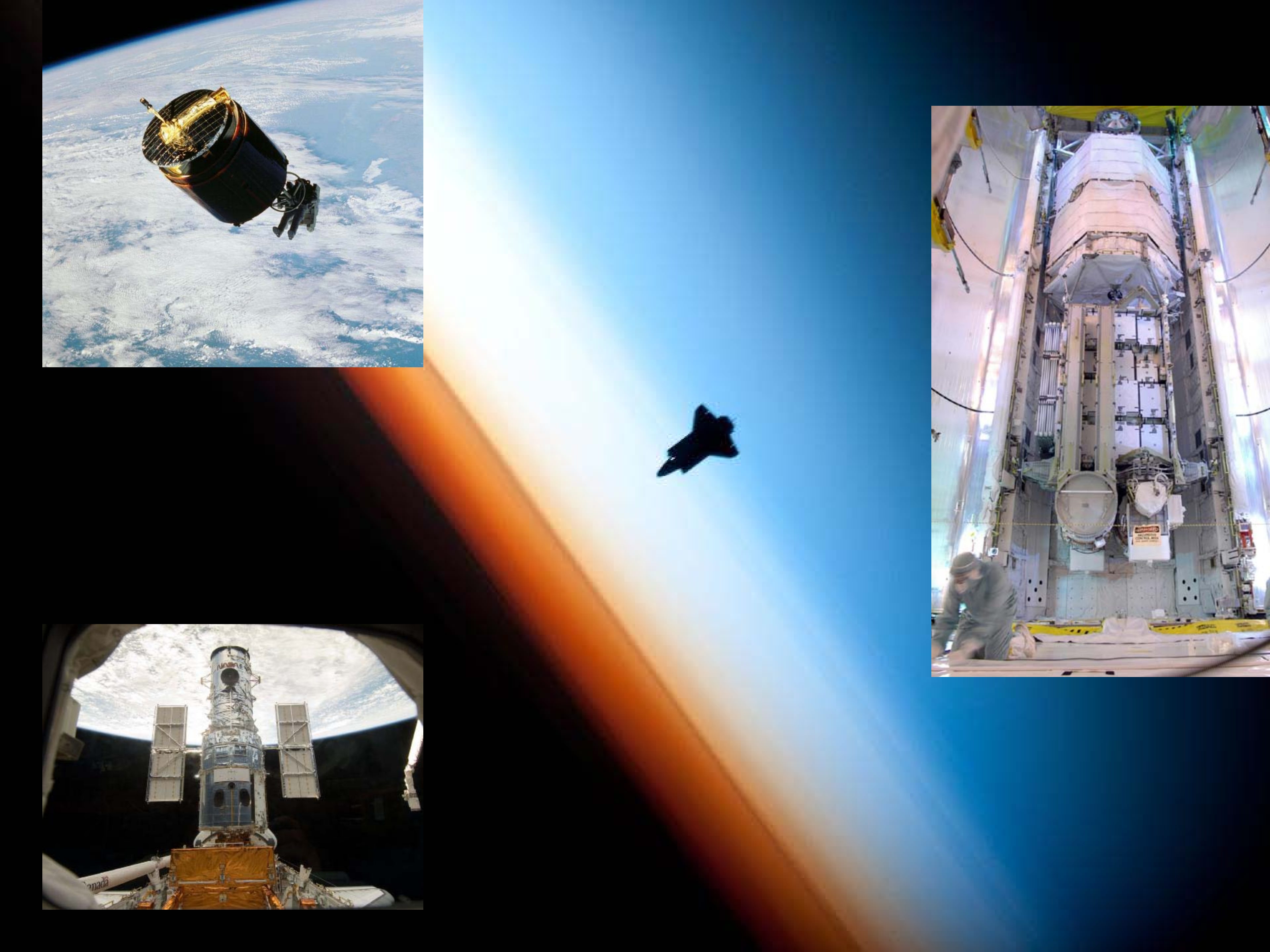
- Commonality and consistency
- Simple functions and interfaces
- Simple tasks



Robustness

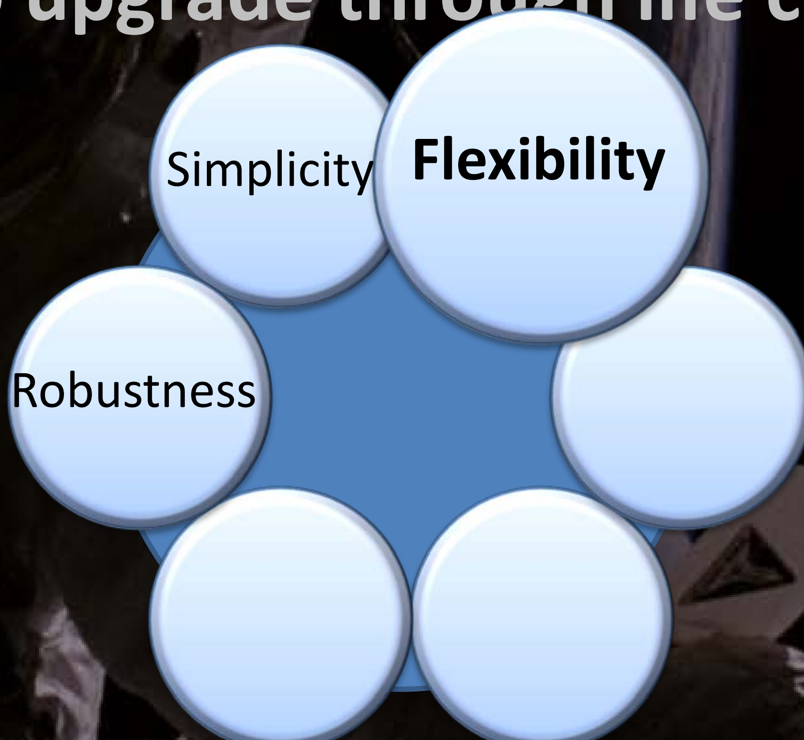
- Fail operational
- Graceful degradation
- Appropriate automation time-critical reconfiguration





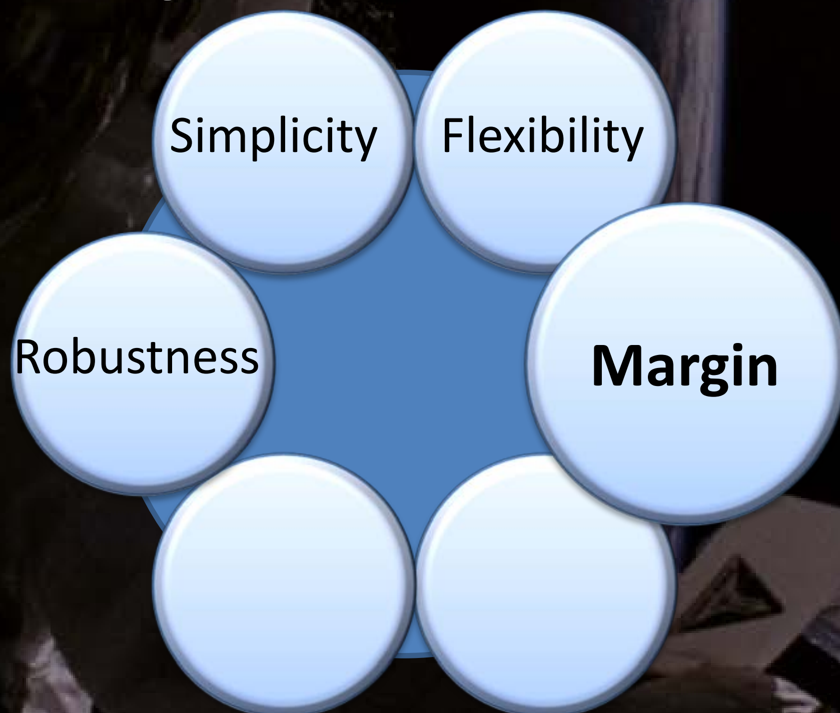
Flexibility

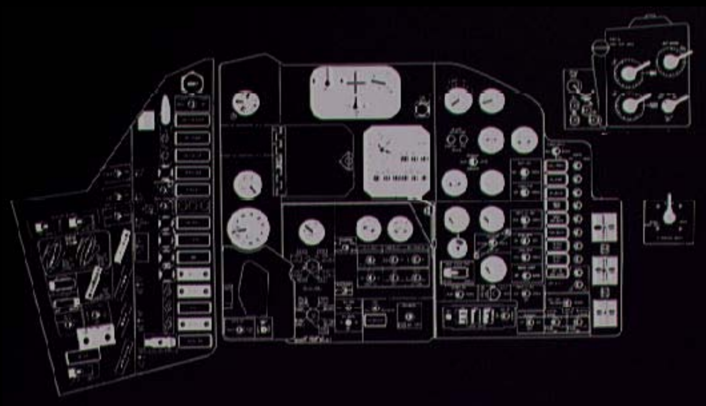
- Easy reconfiguration
- Ability to make minor updates (limits, control gains, etc.)
- Ability to upgrade through life cycle

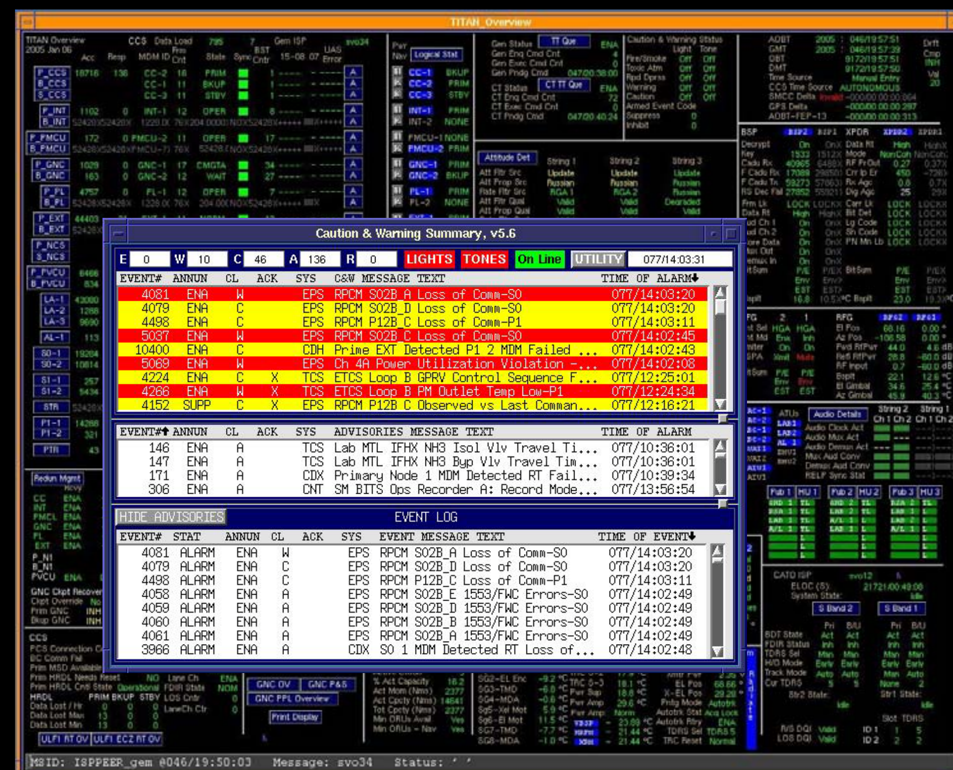


Margin

- Performance margin
- Resource margin
- Environmental tolerance (temperature, radiation, etc.)







TITAN_Overview
Caution & Warning Summary, v5.6
E 0 W 10 C 46 A 136 R 0
LIGHTS
TONES
On Line
UTILITY
077/14:03:31
EVENT# ANNUN CL ACK SYS C&W MESSAGE TEXT TIME OF ALARM
4081 ENA W EPS RPCM S02B_A Loss of Comm-S0 077/14:03:20
4079 ENA C EPS RPCM S02B_D Loss of Comm-S0 077/14:03:20
4498 ENA C EPS RPCM P12B_C Loss of Comm-P1 077/14:03:11
5037 ENA W EPS RPCM S02B_C Loss of Comm-S0 077/14:02:45
10400 ENA C CDH Prime EXT Detected P1 2 MDM Failed ... 077/14:02:43
5069 ENA W EPS Ch 4A Power Utilization Violation -... 077/14:02:08
4224 ENA C X TCS ETCS Loop B GPRV Control Sequence F... 077/12:25:01
4266 ENA W X TCS ETCS Loop B PM Outlet Temp Low-P1 077/12:24:34
4152 SUPP C X EPS RPCM P12B_C Observed vs Last Comman... 077/12:16:21
EVENT# ANNUN CL ACK SYS ADVISORIES MESSAGE TEXT TIME OF ALARM
146 ENA A TCS Lab MTL IFHX NH3 Isol Vlv Travel Ti... 077/10:36:01
147 ENA A TCS Lab MTL IFHX NH3 Byp Vlv Travel Tim... 077/10:36:01
171 ENA A CDX Primary Node 1 MDM Detected RT Fail... 077/10:39:34
306 ENA A CNT SM BITS Ops Recorder A: Record Mode... 077/13:56:54
HIDE ADVISORIES
EVENT LOG
EVENT# STAT ANNUN CL ACK SYS EVENT MESSAGE TEXT TIME OF EVENT
4081 ALARM ENA W EPS RPCM S02B_A Loss of Comm-S0 077/14:03:20
4079 ALARM ENA C EPS RPCM S02B_D Loss of Comm-S0 077/14:03:20
4498 ALARM ENA C EPS RPCM P12B_C Loss of Comm-P1 077/14:03:11
4058 ALARM ENA A EPS RPCM S02B_E 1553/FWC Errors-S0 077/14:02:49
4059 ALARM ENA A EPS RPCM S02B_D 1553/FWC Errors-S0 077/14:02:49
4060 ALARM ENA A EPS RPCM S02B_B 1553/FWC Errors-S0 077/14:02:49
4061 ALARM ENA A EPS RPCM S02B_A 1553/FWC Errors-S0 077/14:02:49
3966 ALARM ENA A CDX S0 1 MDM Detected RT Loss of... 077/14:02:48
MSID: ISPPEER_gem @046/19:50:03 Message: svo34 Status: ' '

Situation Awareness

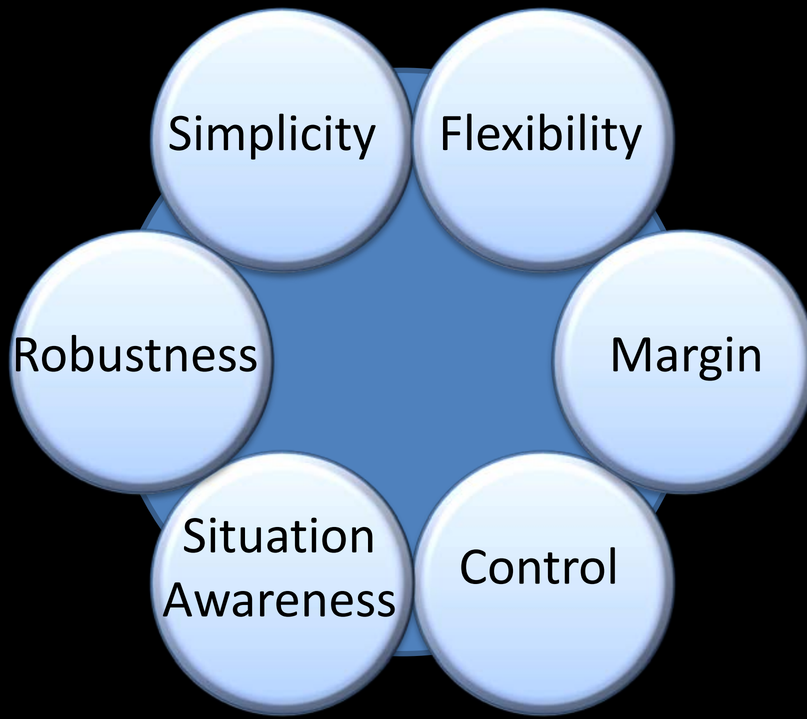
- Telemetry and caution & warning
- Sensor locations and quantities
- Simple indications for the operator


EVENT TIMER
RESET/ COUNT
RESET
UP
DOWN
TIMER CONT
START
STOP
SLEW CONT
MIN
TENS
UNITS
SEC
TENS
UNITS
RCS SYS A/B-2
QUAD 1
AUTO
OFF
MAN
QUAD 4
AUTO
OFF
MAN
QUAD 2
AUTO
OFF
MAN
QUAD 3
AUTO
OFF
MAN
RCS
QUAD 2
QUAD 3
QUAD 4
S-BAND
LIGHTING
SIDE PANELS
ON
OFF
FLOOD
OVHD/ FWD
OVHD/ FWD
OFF
ALL
DIM
BRIGHT
LUNAR CONTACT
X-POINTER SCALE
HI MULT
LO MULT
EXTERIOR LTG
OFF
TRACK
DOCK
LAMP/TONE TEST
ENG PB-C/W 2
C/W 3
C/W 1
C/W 4
ALARM TONE
OFF
OFF

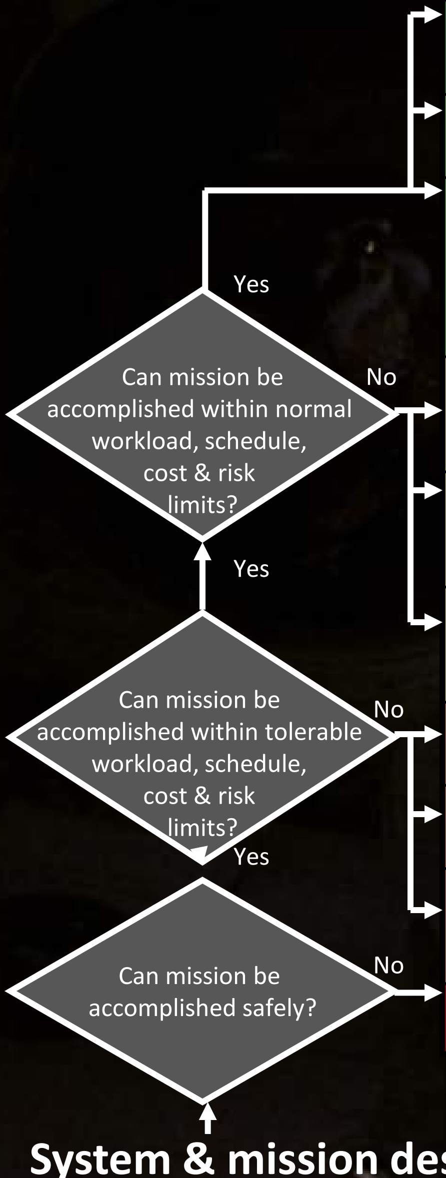
Control

- Command capabilities
- Control of automated capabilities
- Systems operate in a repeatable, predictable manner.

Six broad factors that characterize operability.



Spacecraft Flight Operability Assessment Scale



	Operational Impact	Simplicity	Margin	Flexibility	Robustness	Sit Awareness	Control	Program Impact
1	**Excellent operations capabilities**							**Operationally desirable.**
2	**Negligible operational challenges** that can be handled with no noticeable impact to operations feasibility or cost							**Mission can be accomplished** Minimal operational impacts can be handled within existing infrastructure and budget with negligible workload impacts.
3	**Operational challenges cause noticeable nuisances** to the operator, but can be handled with little impact to operations feasibility or cost.							
4	**Operations are difficult** and incur significant one time costs (manpower, facilities, products, etc.) to ensure mission success. Some mission objectives may not be achieved.							**Some mission objectives may be at risk.** Operational impacts will change infrastructure requirements, cost allocations, work prioritization, etc. from the baseline operations plan.
5	**Operations are difficult** and incur significant recurring costs (manpower, facilities, products, etc.) to ensure mission success Some mission objectives may not be achieved.							
6	**Operations are difficult**, mission objectives may remain at risk even after additional investments (manpower, procedures, facilities, etc.) are made.							
7	**Operational challenges reduce mission capability** and degree of mission success by preventing some objectives							**Mission is at risk.** Operational impacts will exceed the capabilities of either the operations community or the entire program.
8	**Operational challenges put mission success at risk**. No operational techniques are available to mitigate risk.							
9	**Operational challenges increase risk of loss of crew or vehicle.** No operational techniques are available to mitigate risk while preserving mission content.							
10	**Operationally unsafe** or unachievable							**Not operable.**

"Designing a Better Spacecraft: Assessing Flight Operability of Human Rated Spacecraft," AIAA SpaceOps 2010.

*C[illegible]ability assessment is performed for a specific reference [illegible] or scenario

Formal definitions and criteria for operability can benefit the Program throughout its life cycle.

Ops Concept → **Functional Flow Block Diagrams** → **Requirements** → **Design** → **Review** → **Build & Operate**

Method of Ops Influence

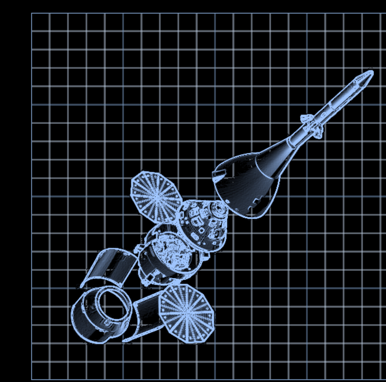
Ops Concept	Requirements	Design	Review	Build & Operate
Operations concept definition includes factors that impact flight operations	System requirements include operability criteria	Operability criteria provide clear guidance for design implementation	Formal operability assessments ensure requirements compliance	Operability assessments applied to proposed design changes and upgrades

Questions?

Alan Crocker

National Aeronautics and Space Administration
Lyndon B. Johnson Space Center
Mission Operations Directorate

How Operable is Your Spacecraft?

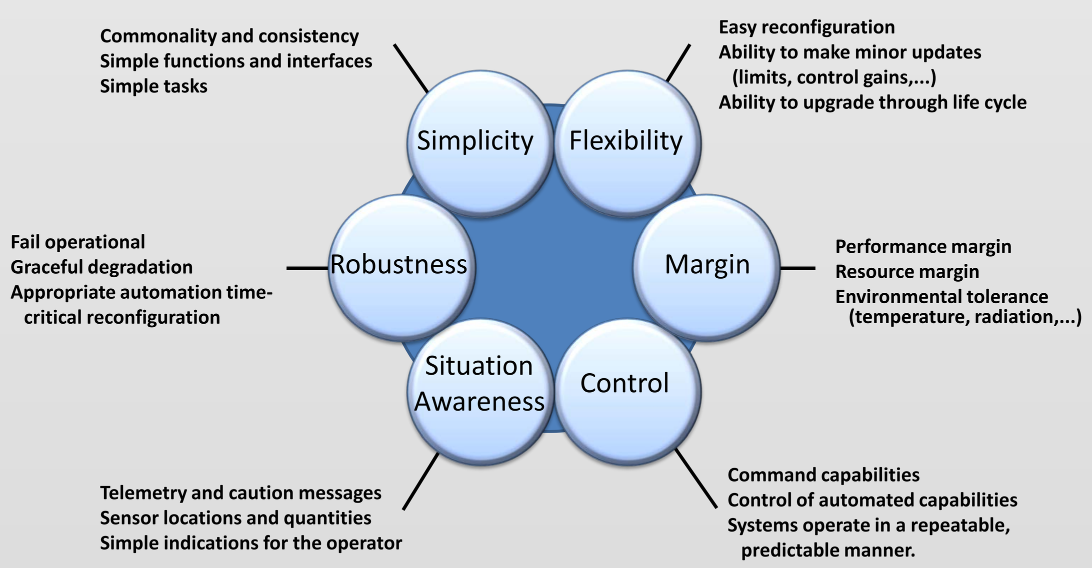
Find out here…  *…instead of waiting until you get there.* 

Making Human Spaceflight Practical and Affordable: Spacecraft Designs and their Degree of Operability

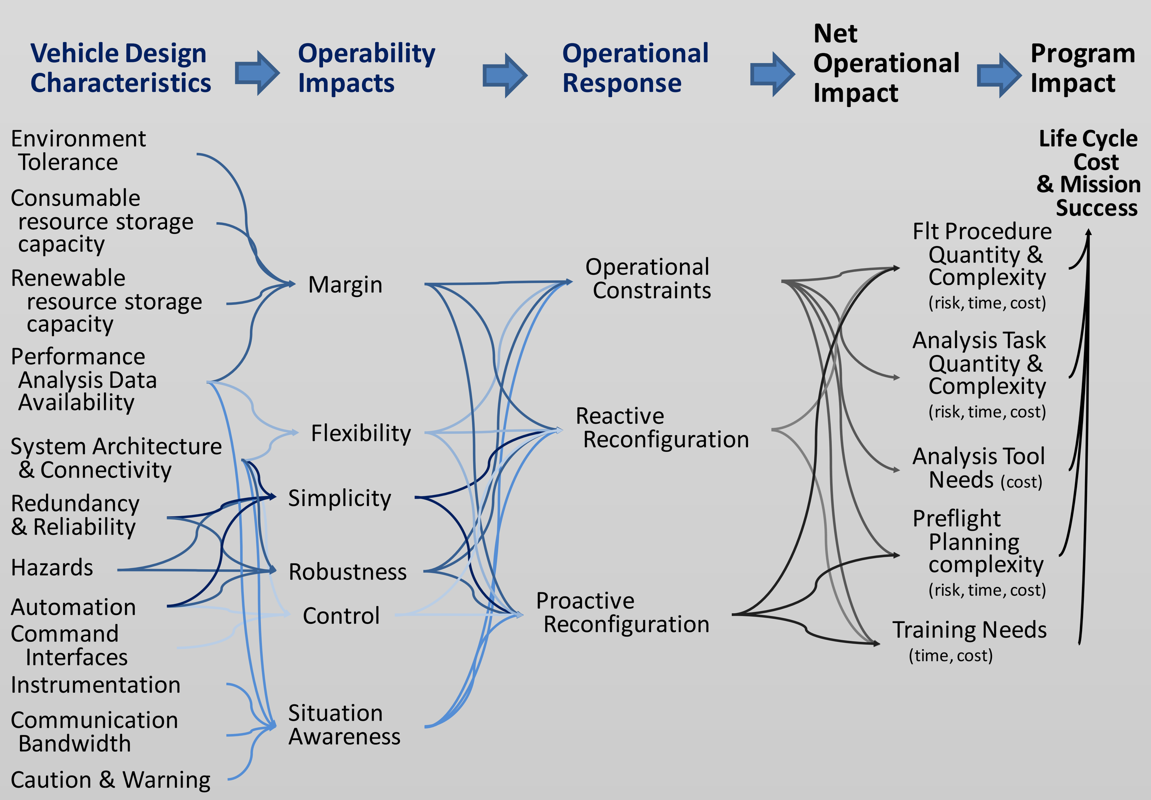
What is flight operability?

Flight Operability - flīt ä-p(ə-)rə-bi-lə-tē, *noun.*
1. The degree to which a flight system design enables a balance of maximum mission success, minimal risk, and minimum operating cost.

Six key factors influence operability.



There are complex relationships between system design, flight operability, and program impact.



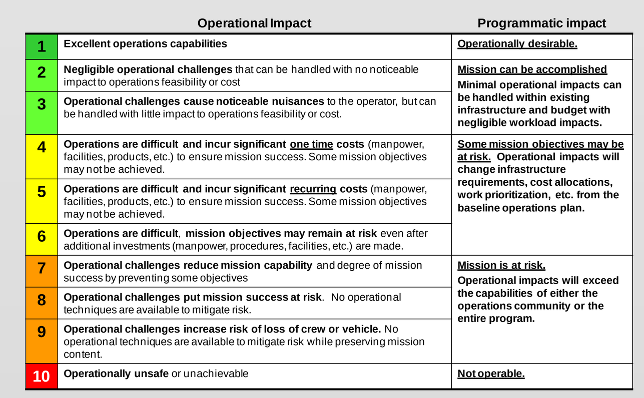
Flight operability factors can conflict.

Understanding – and evaluating – flight operability requires active participation from the flight operations community during the requirements definition and design processes.

How is flight operability measured?

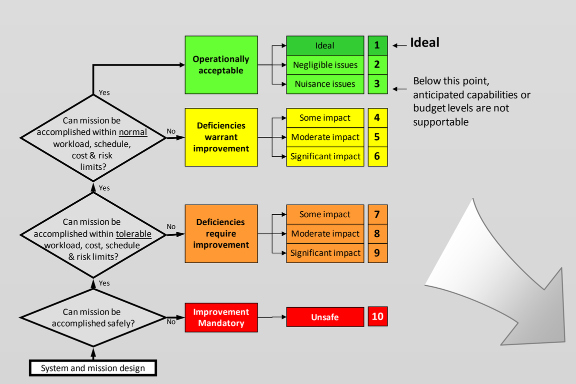
The Spacecraft Flight Operability Assessment Scale provides a formal, structured approach to measuring operability.

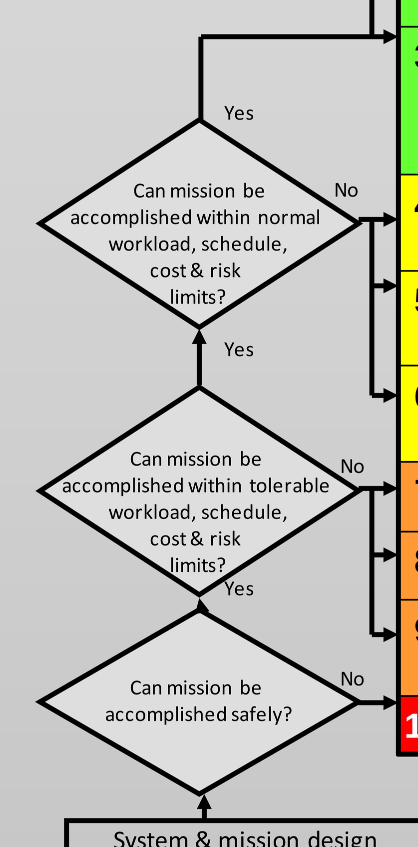
Grading scale
- Define the range of possible scores and their implications to ops and the program
- The resulting grades must have meaning for both the operations community and the program management community.



Operability Factors
- Capture the general factors that drive ops complexity
- Include description of desired characteristics in each theme

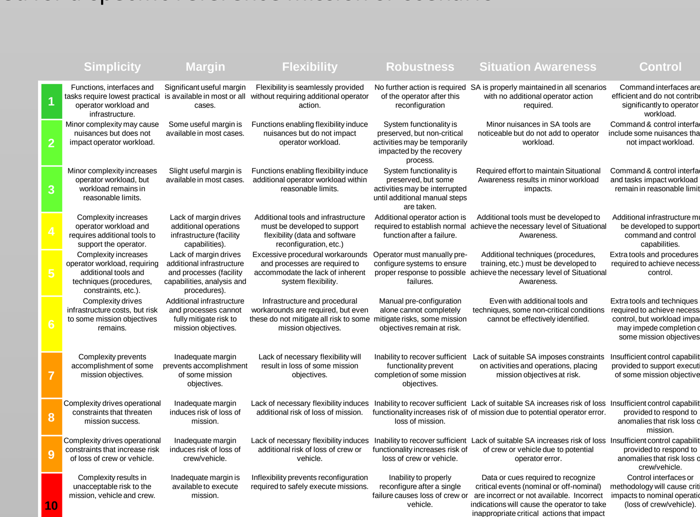
Criteria
- General questions that characterize operations impact
- Can be customized for each theme





	Operational Impact	Simplicity	Margin	Flexibility	Robustness	Sit Awareness	Control	Program Impact
1	**Excellent operations capabilities**							**Operationally desirable.**
2	**Negligible operational challenges** that can be handled with no noticeable impact to operations feasibility or cost							**Mission can be accomplished**
3	**Operational challenges cause noticeable nuisances** to the operator, but can be handled with little impact to operations feasibility or cost.							Minimal operational impacts can be handled within existing infrastructure and budget with negligible workload impacts.
4	**Operations are difficult** and incur significant one time costs (manpower, facilities, products, etc.) to ensure mission success. Some mission objectives may not be achieved.							**Some mission objectives may be at risk.**
5	**Operations are difficult** and incur significant recurring costs (manpower, facilities, products, etc.) to ensure mission success Some mission objectives may not be achieved.							Operational impacts will change infrastructure requirements, cost allocations, work prioritization, etc. from the baseline operations plan.
6	**Operations are difficult**, mission objectives may remain at risk even after additional investments (manpower, procedures, facilities, etc.) are made.							
7	**Operational challenges reduce mission capability** and degree of mission success by preventing some objectives							**Mission is at risk.**
8	**Operational challenges put mission success at risk**. No operational techniques are available to mitigate risk.							Operational impacts will exceed the capabilities of either the operations community or the entire program.
9	**Operational challenges increase risk of loss of crew or vehicle.** No operational techniques are available to mitigate risk while preserving mission content.							
10	**Operationally unsafe** or unachievable							**Not operable.**

*Operability assessment is performed for a specific reference mission or scenario



How can this benefit your program?

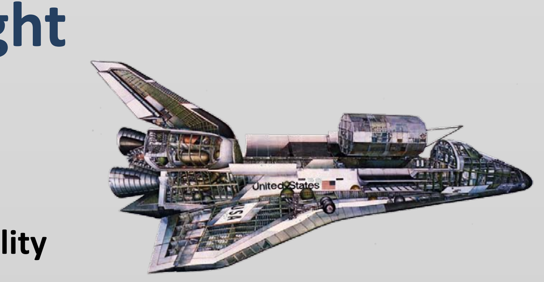
Flight operability assessment adds another capability to the program manager's toolset

Operability issues are linked to safety, reliability, performance, etc., but there are other tools available to assess these topics. The operability assessment tool adds to the program management toolset.

Affordability
Maintainability Sustainability
Operability
Reliability
Safety

By identifying ways in which operations techniques can address problem areas, flight operability assessment can also identify opportunities to make the system developer's job easier.

Sample Space Shuttle Flight Operability Assessment



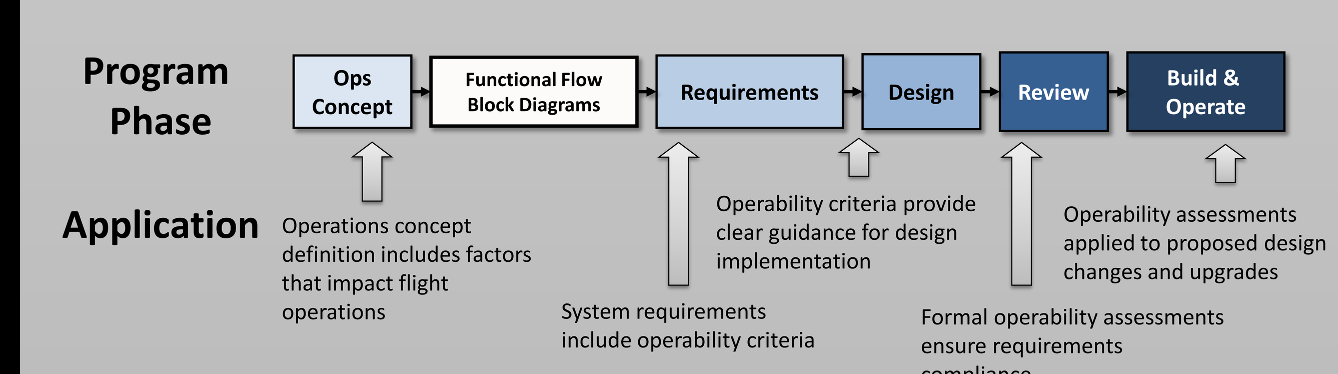
Docking attachment system operability assessment for docking operations

Operability Theme	Score	Description	Operational Impact	Program Impact
Simplicity	5	Multiple nominal and off nominal procedures as well as operational workarounds to disable and release dampers indicate inherent undesirable complexity in the system.	Complexity increases operator workload, requiring additional tools and techniques (procedures, constraints, etc.).	Some mission objectives may be at risk.
Margin	8	Little margin is available in the APDS hooks. Single hook out cases drive the need for significant system workarounds (PMA hooks, FR constraints etc). Single point jam on the ball screw mechanism could lead to loss of mission.	Inadequate margin induces risk of loss of mission.	Mission is at risk.
Flexibility	3	The semi-automatic docking sequence allows for much greater system flexibility but also poses issues with added training due to it's complexity.	Functions enabling flexibility induce additional operator workload within reasonable limits.	Mission can be accomplished.
Robustness	8	Capture latches require manual reconfiguring after the first failure to return to a nominal configuration. A single point jam on the ball screw mechanism can cause loss of mission.	Inability to recover sufficient functionality increases risk of loss of mission.	Mission is at risk.
Situation Awareness	3	In general, enough insight into the health and operation of the docking system is available to MCC. Some coordination with crew to attain crew only insight (A7 panel lights add to MCC workload.	Required effort to maintain Situational Awareness results in minor workload impacts.	Mission can be accomplished.
Control	3	Lack of ground control capability limits MCC ability to operate the docking system in off nominal situations.	Command & control interfaces and tasks impact workload but remain in reasonable limits.	Mission can be accomplished.

Scores in simplicity, margin and robustness scores reflect the significant operational impacts of even a single failure in the subsystem.

Scores relatively well in the categories of flexibility, situation awareness and control, though some limitations capabilities are noted.

Formal definitions and criteria for flight operability can benefit the Program throughout its life cycle.



The Spacecraft Flight Operability Assessment Scale is a product of the Mission Operations Directorate at NASA's Johnson Space Center.

Point of Contact: Alan Crocker, alan.r.crocker@nasa.gov