Fault Management Techniques in Human Spaceflight Operations

Brian O'Hagan
NASA Johnson Space Center
brian.ohagan-1@nasa.gov

Alan Crocker
NASA Johnson Space Center
alan.r.crocker@nasa.gov

Abstract

This paper discusses human spaceflight fault management operations. Fault detection and response capabilities available in current US human spaceflight programs - Space Shuttle and International Space Station - are described while emphasizing system design impacts on operational techniques and constraints. Pre-flight and in-flight processes along with products used to anticipate, mitigate and respond to failures are introduced. Examples of operational products used to support failure responses are presented. Possible improvements in the state of the art, as well as prioritization and success criteria for their implementation are proposed.

This paper describes how the architecture of a command and control system impacts operations in areas such as the required fault response times, automated vs. manual fault responses, use of work-arounds, etc. The architecture includes the use of redundancy at the system and software function level, software capabilities, use of intelligent or autonomous systems, number and severity of software defects, etc. This in turn drives which Caution and Warning (C&W) events should be annunciated, C&W event classification, operator display designs, crew training, flight control team training, and procedure development. Other factors impacting operations are the complexity of a system, skills needed to understand and operate a system, and the use of commonality vs. optimized solutions for software and responses.

Fault detection, annunciation, safing responses, and recovery capabilities are explored using real examples to uncover underlying philosophies and constraints. These factors directly impact operations in that the crew and flight control team need to understand what happened, why it happened, what the system is doing, and what, if any, corrective actions they need to perform. If a fault results in multiple C&W events, or if several faults occur simultaneously, the root cause(s) of the fault(s), as well as their vehicle-wide impacts, must be determined in order to maintain situational awareness. This allows both automated and manual recovery operations to focus on the real cause of the fault(s). An appropriate balance must be struck between correcting the root cause failure and addressing the impacts of that fault on other vehicle components.

Lastly, this paper presents a strategy for using lessons learned to improve the software, displays, and procedures in addition to determining what is a candidate for automation. Enabling technologies and techniques are identified to promote system evolution from one that requires manual fault responses to one that uses automation and autonomy where they are most effective. These considerations include the value in correcting software defects in a timely manner, automation of repetitive tasks, making time critical responses autonomous, etc. The paper recommends the appropriate use of intelligent systems to determine the root causes of faults and correctly identify separate unrelated faults.

Introduction

Vehicle complexity, flexibility, and operational margin largely drive the operational resources required to develop and sustain a human-rated spacecraft flight capability. Although the tools and formats have changed over the years, the basic practices and processes supporting mission operations remain much the same as they were decades ago. These system engineering and integration processes apply equally to the wide array of vehicles and missions NASA has flown since the early years of Mercury, Gemini and Apollo[Error! Reference source not found.].

The Flight Operations Team

Human spaceflight involves the crewmembers on the Space Shuttle and International Space Station (ISS), flight controllers in the Mission Control Center (MCC), the training team, and the Engineering Support team. The Flight Director leads the flight control team and maintains overall responsibility for the mission, with the crew's commander responsible for immediate response actions necessary to preserve crew safety. The flight controllers have the needed expertise to address faults that are beyond the ability of the crew to handle and are used to perform the more routine tasks so the crew can be used for the tasks that require their presence on the spacecraft.

The flight control team includes specialists in several system disciplines, as well as dedicated planners. In addition to the widely recognized "front" room or Flight Control Room (FCR) flight controllers, there are additional flight controllers in nearby "back" rooms or Multi-Purpose Support Rooms (MPSRs). This team includes the Flight Director, the "Capsule Communicator" (CAPCOM) who provides a focal point for communicating with the crew, system specialists responsible for the operation of individual spacecraft systems, and planners who maintain the timeline and assist the team in executing that plan. Additional specialists support intensive tasks such as launch, landing, Extravehicular Activity (EVA), robotic manipulator operations and docking. Each of these many team members is exhaustively trained and certified in the execution of flight operations.

During nominal orbit operations, three shifts of flight controllers provide around-the-clock support. Two of these shifts support activities while the crew is awake, and the third "planning" team continues to support while the crew sleeps. Although all three shifts actively participate in the plan review and replanning process, it is this third team that produces the final set of replanned products, including revised procedures, plans, and reference material, as an "execute package" for the next day's activities

Representatives of the design community and spacecraft vendors support flight operations as well in the Mission Evaluation Room (MER) in Houston and Engineering Support Centers (ESCs) at vendor facilities. These engineering support personnel stand ready to perform detailed analysis of telemetry, quick turnaround laboratory-based testing of flight-like hardware and development of recovery plans. All of these team members play a role in failure response, and many of them share a common way of assessing and communicating failure-related information.

While complex vehicle operations such as launch, rendezvous and Extravehicular Activity (EVA) require the support of a full flight control team, there are quiescent periods during which a smaller flight control team may suffice. Team staffing decisions are made on the basis of multiple factors including complexity of flight activities, the workload induced by these activities on each flight controller, and the potential risks and failure modes associated with these activities. International Space Station (ISS) operations have adopted a reduced manning model such that a minimal number of flight controllers are required to support overnight and weekend shifts. In these cases, a full flight control team remains "on call" and able to staff the MCC within 2 hours. During high activity daytime periods, as well as complex operations, the team expands to handle additional workload.

Recent trends allow the crew to take on more responsibility in spacecraft systems monitoring and for fault response. However, unlike the flight control team, the crew does not watch the status of the systems on a continuous basis. They rely on an annunciation system to let them know when action is required. In order to reduce the reliance on the flight control team, ISHEM systems will need to fill in the gap of systems monitoring and assist in fault responses.

System Architecture Implications

The architecture of a spacecraft plays a large role in determining how operations will be performed, how many flight control team members are needed, the number of crew members needed for failure responses, the level of training needed for operators, the needed operator response time, and the cost of long term operations. This section examines some of the possible architectural choices and their impacts on operations.

Faults

A fault is defined as an abnormal condition or defect at the component, equipment, or sub-system level which may lead to a failure[2]. A failure is the result of a fault, or in other words, what was lost. Typically the Failure Detection, Isolation, and Recovery (FDIR) process is used to detect faults, accurately isolate the failure, and respond in a timely manner. FDIR is an important aspect in determining the needed training and staffing for the operations team. If there is too little FDIR or if it doesn't work properly, then the training and staffing must be increased to handle the possible failures. With too much FDIR, the complexity of the system increases along with the need for testing and training.

Fault Prevention

Reliability is the ability of a system or component to perform a required function under the stated conditions for a stated period of time[3]. Fault prevention is the process of increasing reliability through the elimination of as many possible faults, such that the probability of system failure is an acceptably low value[6]. Its goal is to eliminate single points of failure or their effects and to ensure spacecraft system integrity under anomalous conditions. Other factors include the use of Commercial Off the Shelf (COTS) versus customized hardware, whether to use radiation hardened systems, and the Mean Time Between Failures (MTBF) of each component.

Each architecture must balance the need for reliability versus the cost of fault prevention. Without enough reliability, the crew will spend too much time addressing failures, performing in-flight maintenance, etc. This requires more training, procedures, spares, etc. Also the flight control team staffing will need to be increased during periods of time their expertise will be needed to address possible failures. In contrast, too much fault prevention will drive the cost of the vehicle up to the point where other needs may be under-funded or eliminated. This could lead to excessive requirements for manual operations or work-arounds which again increases the needed training, procedures, staffing, etc.

Reliability is not limited to hardware. Unreliable software will increase operations costs by requiring more testing to understand how the system actually operates, procedure changes to address each software defect, more training, and more operators to handle frequent failures. Since operations staffing is based on the potential risks of what could or will happen, the more reliable the system, the more that on-call support can be used.

Fault Mitigation

Mitigation is the process of reducing the impact of a failure through the use of fault tolerance. Fault tolerance is the ability to handle either expected or unexpected failures. The goal of fault tolerance is to provide a robust recovery mechanism by preventing a significant loss in the performance or function of a system. Typically this is performed by using redundancy or another method of compensation. Redundancy is a method of implementing fault tolerance by providing a backup system or component for a particular function. For example, a single fault tolerant system could handle a fault by switching to a backup system, but may not be able to handle another fault in the same system. Ideally, a fault tolerant design should be able to support degraded modes of operation when acceptable. The fault tolerance capability applied to a system should be directly proportional to the criticality of the system. The trade off is between a system that can not adequately respond to failures versus the cost of too much redundancy or redundancy where it is not needed.

Redundancy can be implemented via a primary/backup system or multiple parallel units with a voting architecture. These units may be grouped into separate strings of units such as a primary unit controlling string 1 and a backup unit controlling string 2. By implementing redundancy, the need for immediate response to a fault by the crew or flight control team is reduced. This reduces the staffing needs, training, procedures, etc.

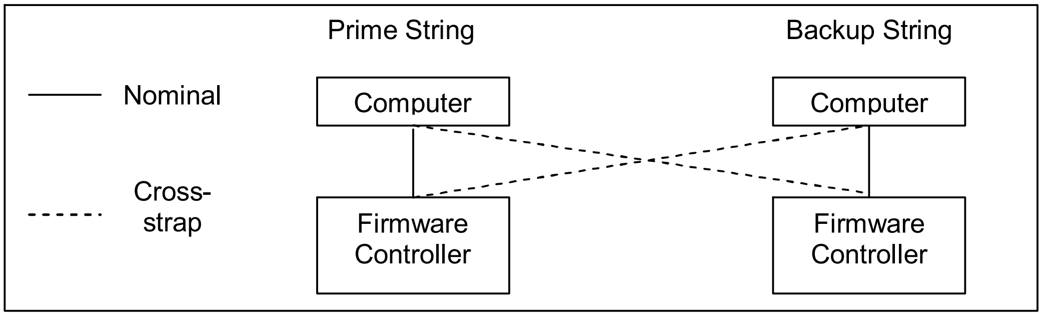


Figure 1: Cross Strapping Redundant Strings

Fault tolerance is enhanced by allowing the cross strapping of units in one avionics string with the other string such that a single failure does not result in the loss of an entire string. Another enhancement is the use of dual attachments. This means a single unit could communicate on multiple networks, receive power from multiple sources, etc. These enhancements increase the ability of the crew or flight control team to work around a failure while minimizing the exposure to multiple failures. This leads to an increased ability to achieve the mission objectives. The downside to cross strapping and dual attachment is the possibility of certain failures affecting both strings due to their common connectivity.

The use of a primary/backup system requires some way for the backup system to remain synchronized with the primary system. This can be achieved through “checkpointing” of data from the primary to the backup system or by mirroring the functionality of the primary in the backup system. The former methodology requires additional measures to prevent the propagation of faults through the backup systems for a single failure or a common defect in the handling of that fault. If this is not accounted for, the procedures and training will need to not only account for the failures but also methods to restart the system when all redundant units are lost.

In a voting architecture, the units vote on whether a failure occurred, with the minority being voted out of set. This has advantages over a primary/backup system in that each unit is kept up to date and such that there is a minimal gap during the failure over from a primary to the backup unit. This requires the operators to replace and/or restart the unit that was voted out and to integrate it back in the set.

The use of a degraded mode of operation for certain faults allows continued operator insight and system control during troubleshooting. This may require powering off non-critical systems and only performing mandatory operations for vehicle and crew survival. By providing some level of insight and control, the crew and flight control team can maintain situational awareness and speed up the recovery process.

Software can also mitigate the possibility of a failure through the use of modes, validating command input, etc. Modes are used to specify when commands are appropriate and therefore allowed and when they are not. Commands should also be validated to prevent out of range values, invalid operations, etc. It goes without saying that the system should be able to protect itself from operator error whenever possible.

Fault Detection

Fault detection is the process by which a fault is detected. There are several methods of detecting faults such as Built-In Testing (BIT), using sensors, a loss of communications, etc. [7] Fault detection must account for failures in the BIT or sensors, the sampling rate of the sensors or data from other computers, data validity flags, and network throughput. This detection process and the by which faults are annunciated directly impacts the ability of the crew and flight control team to maintain mission cognizance and determine which faults require a response.

BIT can be continuously operated, interleaved with other operations, or initiated on command. BIT can be implemented through the use additional hardware and provide a fail-safe which does not affect system performance. Additional measures should be taken to avoid the utilization of erroneous BIT output in recovery measures. Erroneous annunciation of faults or the non-annunciation of a fault make it more difficult for the operators to understand why a fault occurred or may result in the incorrect response to a fault.

When using a centralized architecture, a centralized unit acts as a "watch dog" in detecting and reporting system faults. This could use a tiered architecture or a single bus. The central unit then determines if a failure has really occurred based on the data from a lower level then annunciates the fault. An example from the US segment of ISS, where one Primary Multiplexer/ Demultiplexer (MDM) per system or module decides if a failure has occurred. The downside to this approach is that the hardware and software in each unit must have additional checks to detect failures in within that unit. In contrast, a voting architecture is it easily allows for voting a differing unit out of the redundant set.

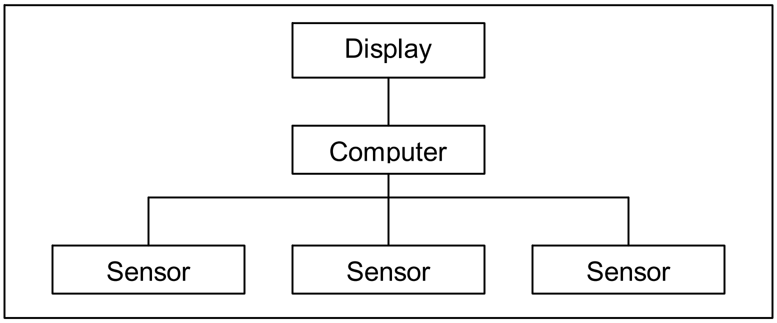


Figure 2: Centralized Architecture

When using a decentralized architecture, several computers (usually 3 or more) are used to detect faults. Fault Detection can be reported to a higher level or one of the units could take the lead for fault annunciation. Alternatively, a voting scheme could be used by three or more redundant computers. A fault is only declared when the majority of the units agree. This method can be used to vote out the differing unit to insure units experiencing a fault are not used. The system must also account for situations where there is no majority vote. An example of this is the General Purpose Computers (GPC) on the Space Shuttles and the Service Module Central Computers (SMCC) in the Russian segment of ISS. The downside to this approach is the need for extra software to addresses ties (even number of units in set). Otherwise, the unit voted out of the set must be replaced and/or restarted in a timely manner.

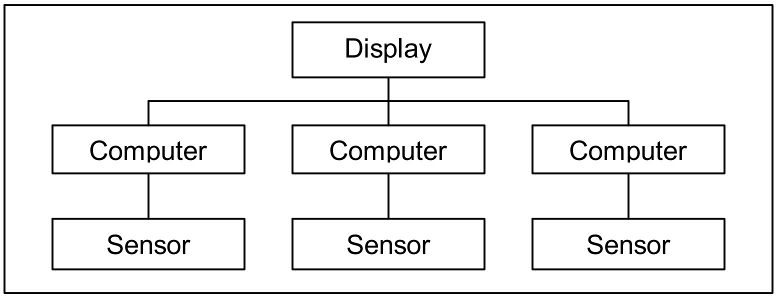


Figure 3: Decentralized Architecture

The reporting of faults is usually prioritized to allow the system and operators to address the most important failures first. Examples are the Onboard Fault Summary (OFS) used by the Shuttle and Caution & Warning (C&W) system on ISS. This is an area where an intelligent system would be of great value in quickly determining the root cause of a fault and initiating the correct response. An intelligent system could also serve as a knowledge repository which in turn would decrease the time and cost of training the operators.

Fault Isolation

Fault isolation is the process of determining the exact cause and location of a failure[7]. Through the use of BIT or another type of automated testing, it may be possible to determine which component in a system has failed. However, there may be times when the exact cause can only be isolated to the system or unit level such as in a voting system with only two computers or for components in series.

Fault Protection

Fault protection is the process by which the system protects itself and responds to a fault. Systems should be capable of recovering from multiple successive or coincidental faults: ideally, they should be able to handle multiple independent faults. For example, fault protection responses to a loss of power could be to load shed low priority equipment. Typically this process is automated in order to rapidly respond to and put the spacecraft in a safe state from which recovery operations can be performed. However, during critical periods the primary purpose of fault protection is to ensure the completion of the critical event prior to safing the system. Fault protection should also account for known faults and should only be used if FDIR is unable to restore the lost functionality. It is desirable, but usually not technically feasible, to provide autonomous fault protection for spacecraft design limitations.

The fault protection process can be either automatic or autonomous. Autonomy is the capability of a system to respond to a fault on its own. Automation is the process by which a task can be performed by a computer without the need for crew or ground intervention. This means an automated process can be started by manual control or an autonomous process[1]. From an operations perspective, autonomy does not require the crew or flight control team to take action, while an automated process may require the operator to initiate the process. The former should be used for time critical responses when possible along with a capability to inhibit the response, while the latter is preferred for non-critical responses that may not be the desired response in all situations. Fault protection should not be an entirely manual process. It is desirable to automate a process (using a script or other predefined response sequence) that will be repeated multiple times. This reduces the chances of operator error.

As part of the fault response, the failed system may be power cycled to determine if the fault is a transient error. Depending on the criticality of the fault, if recovery is not successful the spacecraft may stay in a degraded mode or go to a "safe" or "survival" mode. This provides a safe state for the spacecraft hardware with minimal uplink, downlink, environmental, and life support control. To achieve these goals, critical operations are completed, non-critical operations are terminated, and non-essential spacecraft loads are powered off. This minimizes the usage of consumables while maintaining the critical set of spacecraft functionality.

Recovery

In the case of any failure, the system must to be able to safe itself and recover any critical functionality without operator intervention. For instance, on ISS the S-Band system requires manual configuration after being powered up, such that any failure other than a swap to the other string results in a loss of communications. This loss of communications occurs when the crew would most likely want help.

From an operations perspective, it is preferred that the crew be the prime responder to emergencies such as fires, loss of pressure, atmospheric contamination, and other events that require a physical presence or time critical response. Other failures can be addressed by the flight control team depending on the amount of scheduled communications, the communications delays, and the required immediacy of the response. Based on experience with ISS, the crewmembers must train on a regular basis in order to maintain current knowledge of the necessary responses and procedures. It is not acceptable to place the crew in a time critical fault situation if they are unfamiliar with the associated response procedure.

The recovery stage also involves troubleshooting by the flight control team. This requires adequate telemetry and the ability to dump areas of computer memory for software analysis. It is generally not advisable to require crew involvement in this process, since this can be very time consuming. This process may also involve coordination with outside expertise such as from the engineering community, software developers, and other experts.

To complete the recovery process, the crew may need to replace failed equipment or the flight control team may need to load software patches. This usually requires the creation of new procedures, work-arounds, and other unique plans. The crew should be used only when necessary.

Other Factors

The complexity of a system has a large influence over the amount of needed procedure development and training time. Whereas simple systems are easier to understand, it usually takes more testing to understand how a complex system works. The same is true for training time. It is also easier for the crew or flight control team to maintain situational awareness during failures with simpler systems since it is easier to remember the details of how the system works. Finally, a complex system provides more opportunities for failures and more lengthy troubleshooting.

The interdependencies of systems are also an impact to operations. For instance on ISS, the operation of the US segment Guidance, Navigation, and Control (GNC) system is tightly interwoven with the Russian segment GNC system. A failure in one system can lead to a failure in the other system. Therefore to operate the system, integrated testing is needed to understand how the complete system works, what the impact of a particular failure will have on both systems, and for procedure development. This limits the ability to use less costly stand-alone simulators and greatly increases the training time and cost.

Commonality in components, systems, and software allows for reduced development, testing, sparing, procedure development, training, and operations. It also make it easier for the operators to understand the system. By reducing these factors, the vehicle is easier to operate so fewer people are needed for nominal operations, the need for spare parts is reduced, and maintainability is increased by the need for fewer spares and the ability to “cannibalize” parts from elsewhere when needed. However, the downside to commonality is the vulnerability to the propagation of failures. If common systems and software are used with a common limitation or error, a single fault could propagate through all redundant systems or to another subsystem. It is also possible that it could prevent a switch-over to a redundant unit. Different hardware or software could be used in the primary and backup systems to prevent this from occurring, but this means additional costs for development, testing, spares, procedure development, training, and operations. As such, a balance must be achieved between commonality and the prevention of fault propagation.

Another factor in the ability of the crew or flight control team to respond to a failure is the use of hardware switches or software control. If a hardware switch is used, then the crew is needed to perform any operations using that switch. This is the case with older spacecraft like the Space Shuttle where for even routine operations, a procedure must be “called up” to the crew. However if the same function is software controlled (though it may also have a hardware switch) such that it can be remotely commanded, then the crew can focus on the most important responses while the flight control team handles the rest.

Software defects also impact training, procedures, and operations. If the software is not thoroughly tested and debugged prior to use on-orbit, the defect must be worked around during operations. This requires changes to the procedures, additional training, and may require more operators. The impact to operations is directly proportional to the amount of defects and how long they are open.

Operations Processes and Techniques

Proper spacecraft Fault Detection, Isolation and Recovery (FDIR) requires the integration of several types of information to formulate an appropriate anomaly response. A complete determination of real-time response to an anomaly contains 3 categories of information - Failure, Impact and Workaround (commonly labeled “FIW”). The FIW answers the questions “What happened?,” “What does that mean to the crew, vehicle, and mission?” and “What will we do about this?” Root cause data at an appropriate granularity is necessary, but in and of itself, is not sufficient to make this complete determination.

Operational responses to failures are further complicated by the changing role of vehicle systems in different operational scenarios. Systems that are critical in the execution of one operation may be non-critical (or even sacrificial) in another operation or scenario. In every case, the operator must prioritize failure response actions with respect to ongoing activities.

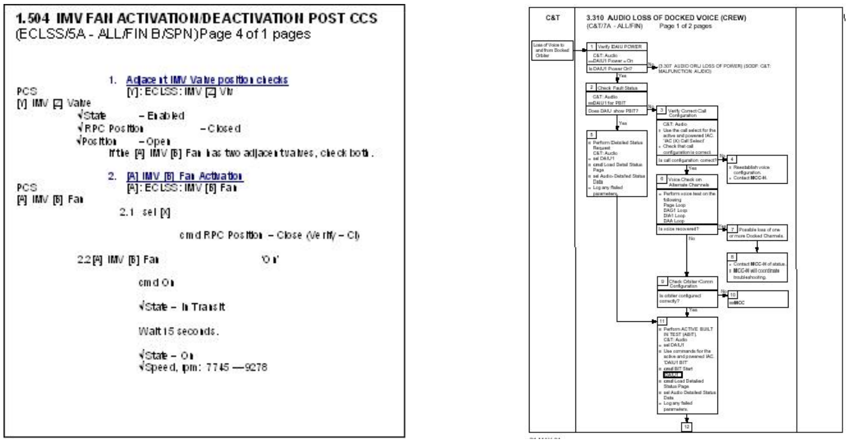
Operations Products

Flight controllers generate a wide array of documents tailored to support real-time mission execution. Key products such as plans procedures, flight rules, and systems documentation, form the basis for both nominal operations and response to failures. Preparation and update of these documents is a significant portion of the off-console responsibilities for flight control personnel.

Procedures

Procedures document the steps to be taken to accomplish a given operational goal. This goal may be activation of an avionics string, nominal reconfiguration of on-line equipment, or response to an anomaly. Procedures may be written in a variety of formats, including “checklist” text-only procedures, “logic flow” flowcharted procedures, and other formats customized to meet the specific requirements of the procedure. See Figure 4.

There are multiple procedure documents intended to serve different purposes. Procedures intended to support specific flight phases such as ascent, orbit operations, or atmospheric entry may be organized in corresponding phase-specific books. This is the predominant structure used for Space Shuttle procedures. In comparison, International Space Station procedures are typically organized in separate documents for each flight system. Critical emergency response procedures are stored in a separate volume for easy retrieval. For ISS, procedures are stored electronically in PDF or XML format and are accessed using the Integrated Procedure Viewer (IPV). Procedures can also be accessed by selecting the associated activity in the Onboard Short Term Plan Viewer (OSTPV).



1.504 IMV FAN ACTIVATION/DEACTIVATION POST CCS
(ECLSS/5A - ALL/FIN B/SPN)Page 4 of 1 pages

1. Adjacent IMV Valve position checks

PCS
[Y] IMV [Z] Valve

[Y]: ECLSS: IMV [Z] Vlv

√State – Enabled
√RPC Position – Closed
√Position – Open

If the [A] IMV [B] Fan has two adjacent valves, check both.

2. [A] IMV [B] Fan Activation

PCS
[A] IMV [B] Fan

[A]: ECLSS: IMV [B] Fan

2.1 sel [X]

cmd RPC Position – Close (Verify – Cl)

2.2 [A] IMV [B] Fan 'On'

cmd On

√State – In Transit

Wait 15 seconds.

√State – On
√Speed, rpm: 7745 —9278

C&T
3.310 AUDIO LOSS OF DOCKED VOICE (CREW)
(C&T/7A - ALL/FIN) Page 1 of 2 pages
Loss of Voice to and from Docked Orbiter
1 Verify DAIU POWER
C&T: Audio
DAIU1 Power = On
Is DAIU1 Power On?
No
(3.307 AUDIO ORU LOSS OF POWER) (SODF: C&T: MALFUNCTION: AUDIO)
Yes
2 Check Fault Status
C&T: Audio
DAIU1 for PBIT
Does DAIU show PBIT?
No
3 Verify Correct Call Configuration
C&T: Audio
Use the call select for the active and powered IAC. 'IAC (X) Call Select'
Check that call configuration is correct.
Is call configuration correct?
No
4
Reestablish voice configuration.
Contact MCC-H.
Yes
5
Perform Detailed Status Request
C&T: Audio
sel DAIU1
cmd Load Detail Status Page
sel Audio-Detailed Status Data
Log any failed parameters.
Yes
6 Voice Check on Alternate Channels
Perform voice test on the following
Page Loop
DAG1 Loop
DIA1 Loop
DAA Loop
Is voice recovered?
Yes
7 Possible loss of one or more Docked Channels.
8
Contact MCC-H of status.
MCC-H will coordinate troubleshooting.
No
9 Check Orbiter Comm Configuration
Is orbiter configured correctly?
No
10
MCC
Yes
11
Perform ACTIVE BUILT IN TEST (ABIT).
C&T: Audio
sel DAIU1
Use commands for the active and powered IAC. 'DAIU1 BIT'
cmd BIT Start
DAIU1
cmd Load Detailed Status Page
sel Audio Detailed Status Data
Log any failed parameters.
12

Figure 4: Typical Procedure formats

An Emergency procedures book (commonly referred to as the “Red Book”) provides the crew with immediate steps to respond to emergency conditions. The Red Book is maintained in paper form as well as electronic form to ensure that the crew can quickly access any needed emergency procedures. As its name implies, the Warning book provides response steps for warning messages. Procedures in both of these books are simple and brief in order to allow for quick execution. More detailed response procedures for failure isolation and full system recovery are included in separate procedure books for each flight system.

In addition to the procedures available to both the crew and the ground, additional procedures may be provided for ground-only use. Typically, these procedures involve the use of functions, data, and analysis tools available only to flight controllers.

Each flight control discipline also maintains a “console handbook” to document procedures related to configuration and operation of the console, technical specifications and constraints of flight system hardware and software, historical performance and failure data and other technical reference information. The content of each console handbook is written by the flight controllers themselves

Plans

Flight plans and timelines enable the crew and flight controllers to coordinate their activities and make effective use of every minute of a flight. The flight plan is developed by the flight control team months before the flight in order to support training simulations for all personnel involved in mission execution. Through the repeated execution of the timeline, any challenges, interdependencies and problems with the flight plan can be identified before on-orbit execution. See Figure 5.

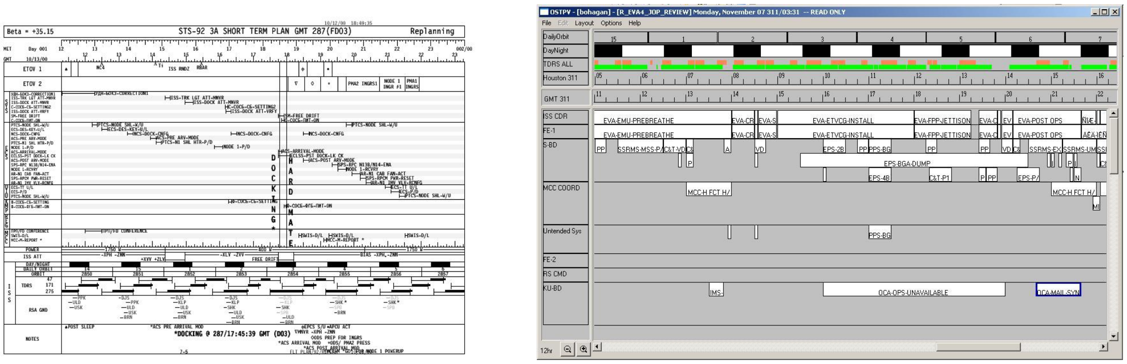


Figure 5: Typical timeline format for Shuttle and ISS (OSTPV tool)

In general, the timeline is created with the assumption that the vehicle and payloads will operate as expected. In some critical cases, extra time may be allotted to accommodate potential difficulties and associated workarounds. In many cases, however, a failure causes cascading impacts to activities on the flight timeline, and the real-time replanning is required.

Flight Rules

Flight rules constitute a predetermined set of decisions approved by program management and the operations community. These rules serve to minimize the effort required to reach reasonable decisions in the real-time environment. Flight rules can define mission priorities, abort criteria, required system configurations, and other anticipated requirements and constraints.

Flight rules can provide guidelines and constraints in support of failure response. In some cases, flight rules may provide very clear direction regarding specific post-failure actions or goals. This information can be crucial to the flight control team as they work to define new procedures and plans in response to a problem. In contrast, some flight rules may be either impractical or impossible to meet after certain failures. With appropriate coordination, the Flight Director may waive or modify a flight rule in real-time if the rule does not properly address the scenario at hand.

B2.2.1-11 RETURN VEHICLE ACCESS

```
Crewmembers must always have a clear path to their planned Earth
return vehicle.  If a crewmember does not have the required equipment
to return on a vehicle, he/she must not be isolated in that vehicle
(from the vehicle from which he/she is able to return to Earth) by a
depressurized element (except for EVA crewmember).
```

Station crewmembers should always have a clear path to their planned earth return vehicle so that a rapid contingency return can be performed.

Reference: JSC 36252, October 1995, Para 2.11.2.

FLIGHT/INCREMENT APPLICABILITY: 2A AND SUBS

Figure 6: Example Flight Rule

The design and performance data supplied by the spacecraft vendor serves as the basis for these operations products. Software requirements specifications, hardware drawings, test results, and interface definitions play key roles in capturing detailed knowledge of operational requirements, constraints and techniques.

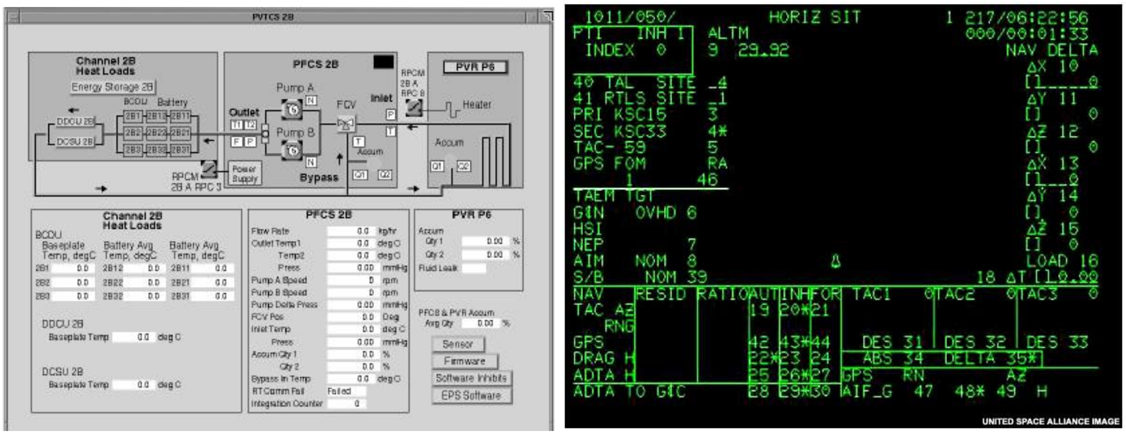
Situational Awareness

The information available to vehicle operators, both onboard crewmembers and ground-based flight controller, plays a large part in determining their ability and role in failure responses. The operator's understanding of the present configuration and capability of the vehicle, along with knowledge of the environment in which that vehicle operates, is the operator's "Situational Awareness." Onboard display interfaces provide the information required by the crew to maintain good situational awareness and perform nominal and critical failure response tasks. More detailed data and analysis tools are in the MCC to enable performance monitoring and prediction as well as detailed failure analysis.

Displays

Telemetry displays provide operators with quick access to comparatively large amounts of data. Often, these same displays provide at least some of the capabilities necessary to send commands and reconfigure onboard systems.

Onboard displays are designed to organize and present critical data to crewmembers in support of onboard procedure execution. To that end, data in these displays may be grouped based on the applicability to specific procedures or by system architecture. Space Shuttle displays are generally text-only displays, while International Space Station more often combine text and graphics. Flight controllers can see telemetered data using the same display formats used by the crew. The graphical displays use a GUI standards guide to insure a consistent look and feel. The Shuttle displays allow the ground to watch the crew as they execute procedures. While the ISS displays show the same telemetry to the crew and ground, we can not see the commands sent by the crew. See Figure 7.



Channel 2B Heat Loads

BCDU Baseplate Temp, degC		Battery Avg Temp, degC		Battery Avg Temp, degC	
2B1	0.0	2B12	0.0	2B11	0.0
2B2	0.0	2B22	0.0	2B21	0.0
2B3	0.0	2B32	0.0	2B31	0.0

DDCU 2B
Baseplate Temp 0.0 deg C

DCSU 2B
Baseplate Temp 0.0 deg C

PFCS 2B

Flow Rate	0.0	kg/hr
Outlet Temp1	0.0	degC
Temp2	0.0	degC
Press	0.00	mmHg
Pump A Speed	0	rpm
Pump B Speed	0	rpm
Pump Delta Press	0.00	mmHg
FCV Pos	0.0	Deg
Inlet Temp	0.0	deg C
Press	0.00	mmHg
Accum Qty 1	0.0	%
Qty 2	0.0	%
Bypass In Temp	0.0	degC
RT Comm Fail	Failed	
Integration Counter	0	

PVR P6

Accum Qty 1	0.00	%
Qty 2	0.00	%
Fluid Leak		

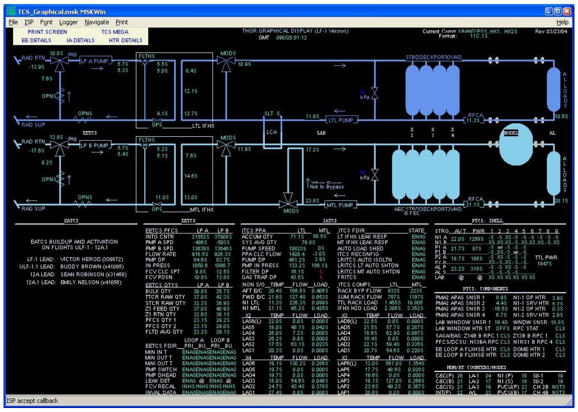
PFCS & PVR Accum
Avg Qty 0.00 %

```
 1011/050/           HORIZ SIT          1 217/06:22:56
PTI     INH 1   ALTM                     000/00:01:33
 INDEX   0      9  29.92                    NAV DELTA
                                              ΔX 10
40 TAL   SITE  _4                             []_____0
41 RTLS SITE  _1                              ΔY 11
PRI KSC15      3                              []     0
SEC KSC33      4*                             ΔZ 12
TAC- 59        5                              []     0
GPS FOM        RA                             ΔẊ 13
     1        46                              []___0
TAEM TGT                                      ΔẎ 14
G&N    OVHD 6                                 []  0
HSI                                           ΔŻ 15
NEP          7                                []  0
AIM    NOM   8                                LOAD 16
S/B     NOM 39                           18 ΔT []0.00
NAV    RESID RATIOAUT INH FOR TAC1     0TAC2     0TAC3     0
TAC AZ             19  20*21
    RNG
GPS                42  43*44   DES 31   DES 32   DES 33
DRAG H             22*23  24   ABS 34   DELTA 35*
ADTA H             25  26*27  GPS    RN          AZ
ADTA TO G&C        28  29*30  AIF_G   47   48*  49   H
```

UNITED SPACE ALLIANCE IMAGE

Figure 7: Crew displays for ISS (left) and Space Shuttle (right)

Computer displays designed specifically for ground-based operator use tend to show even larger amounts of data in high density text form. These displays provide visual indication not only of parameter values, but also limit violations and availability status (stale data, missing data, beyond calibration limits, etc.) through the use of color changes and letter codes. See Figure 8.



```
THOR GRAPHICAL DISPLAY (LF-1 Version)        Current Comm SBAND:ESS, HK1, HK2S    Rev 03/23/04
GMT    090/20:01:12                          Format:   11C.1S
```

```
EATCS BUILDUP AND ACTIVATION
ON FLIGHTS ULF-1 - 12A.1

    LF-1 LEAD:   VICTOR HEROD (X39872)
 ULF-1.1 LEAD:   BUDDY BROWN (x41095)
     12A LEAD:   SEAN ROBINSON (x31459)
   12A.1 LEAD:   EMILY NELSON (x41056)
```

```
EETCS PFCS        LP A     LP B
INTG CNTR       21552S   37908S
PMP A SPD        -496S    -503S
PMP B SPD       13639S   13645S
FLOW RATE       916.5S   926.3S
PMP DP           84.6S    83.7S
IN PRESS        1050.6   1098.7
FCV CLC SPT       9.8S    12.5S
FCV POSN         10.8S    13.8S
EETCS QTYS        LP A     LP B
BULK QTY         30.8S    35.7S
TTCR RAW QTY     37.0S    42.3S
STCR RAW QTY     32.3S    36.9S
Z1 FEED QTY      37.0S    40.9S
Z1 RTN QTY       32.6S    36.1S
PFCS QTY 1       23.1S    29.2S
PFCS QTY 2       23.1S    29.0S
FLTD AVG QTY     23.2S    29.1S
                LOOP A   LOOP B
EETCS FDIR__PRI__BU__PRI__BU
MIN IN T      ENASENASENASENAS
MIN OUT T     ENASENASENASENAS
MAX OUT T     ENASENASENASENAS
PMP SWTCH     ENASENASENASENAS
PMP DHEAD     ENASENASENASENAS
LEAK DET      ENAS  @  ENAS  @
FCV RECAL     INHSINHSINHSINHS
INVAL DATA    ENASENASENASENAS
```

```
ITCS PPA            LTL     MTL     ITCS FDIR                    STATE
ACCUM QTY         71.1S   88.5S     LT IFHX LEAK RESP            ENAS
SYS AVG QTY          79.8S          MT IFHX LEAK RESP            ENAS
PUMP SPEED       18823S      0S     AUTO LOAD SHED               ENAS
PPA CLC FLOW     1420.4   -3.0S     ITCS RECONFIG                ENAS
PUMP DP          451.2S    3.9S     LRITCS AUTO ISOLTN           ENAS
PMP IN PRESS     133.2S  186.1S     LRITCS LT AUTO SHTDN         ENAS
FILTER DP         16.1S       L     LRITCS MT AUTO SHTDN         ENAS
GAS TRAP DP       43.5S       L     FRITCS                       ENAS
NON S/O  TEMP    FLOW    LOAD       ITCS COMPS            LTL     MTL
AFT E/C  20.4S  108.5S  0.405S      RACK BYP FLOW        633S    223S
FWD E/C  21.6S  127.4S  0.653S      SUM RACK FLOW        787S   1197S
N1 LTL   11.3S  226.3S  0.099S      TTL RACK LOAD      1.455S  10.805
N1 MTL   21.1S   95.2S  0.425S      IFHX H2O LOAD      2.306S  3.352S
X2       TEMP    FLOW    LOAD       X3         TEMP    FLOW    LOAD
LAS6(L)  22.0S    0.0S  0.000S      LAD6(L)   22.5S    0.0S  0.000S
LAS5     18.0S   48.1S  0.042S      LAD5      21.5S   57.7S  0.287S
LAS4     26.0S    7.2S  0.000S      LAD4      18.6S   62.9S  0.097S
LAS3     26.2S    0.0S  0.000S      LAD3      18.4S    0.0S  0.000S
LAS2     17.5S   63.1S  0.023S      LAD2      22.1S   59.4S  0.335S
LAS1     20.3S    0.0S  0.000S      LAD1      20.7S   54.6S  0.220S
X4       TEMP    FLOW    LOAD       X3         TEMP    FLOW    LOAD
LA06     19.1S  130.2S  0.286S      LAP6(L)   13.0S  561.0S  1.354S
LA05     19.7S    0.0S  0.000S      LAP5      17.7S   48.6S  0.028S
LA04     19.7S    0.0S  0.000S      LAP4      19.6S    0.0S  0.000S
LA03     18.0S   54.6S  0.048S      LAP3      19.1S  127.0S  0.269S
LA02     24.7S   43.4S  0.378S      LAP2      23.6S   49.2S  0.367S
LA01     27.4S    0.0S  0.000S      LAP1      20.6S    0.0S  0.000S
```

```
STRG   AVT    PWR    1  2  3  4  5  6  7  8  9
N1 A  22.0S  1258S  -S -S XS -S -S -S -S -S -S
N1 B                XS XS XS -S XS XS XS -S XS
P1 A  21.7S    87S  -S @  -S -S -S
P1 B                -S XS -S @  -S
P2 A  18.7S   185S  -S XS -S -S -S         TTL PWR
P2 B                XS -S XS -S -S          1847S
AL P  23.2S   318S  -S -S XS -S -S
AL S                -S -S -S -S
LAB     @      @    XS XS XS XS XS XS
```

```
PMA2 APAS SNSR 1        8.9S    N1-1 OP HTR     3.9S
PMA2 APAS SNSR 2        4.4S    N1-1 SRV HTR    5.7S
PMA2 APAS SNSR 3      -16.5S    N1-2 OP HTR     0.3S
PMA2 APAS SNSR 4        6.7S    N1-2 SRV HTR    2.6S
LAB WINDOW SNSR 1      19.4S    WNDW SNSR      18.8S
LAB WINDOW HTR ST      OFFS     RPC STAT         CLS
SASA/EAS: Z14B B RPC 1  CLS     Z13B B RPC 1     CLS
PFCS/DCSU: N13BA RPC    CLS     N1RS1 B RPC 4    CLS
EE LOOP A FLXHSE HTR    CLS     DOME HTR 1       CLS
EE LOOP B FLXHSE HTR    CLS     DOME HTR 2       CLS
```

```
C&C(P)  26   LA-1  24   N1 (P)    18   SD-1     19
C&C(B)  21   LA-2  17   N1 (S)    18   SD-2     19
C&C(S)  21   LA-3  19   PVCU(P)   23   CH 2B  NSTS
INT(P)  22   A/L   23   PVCU(B)   17   CH 4B  NSTS
```

```
ISP accept callback
```

Figure 8: Typical ground display

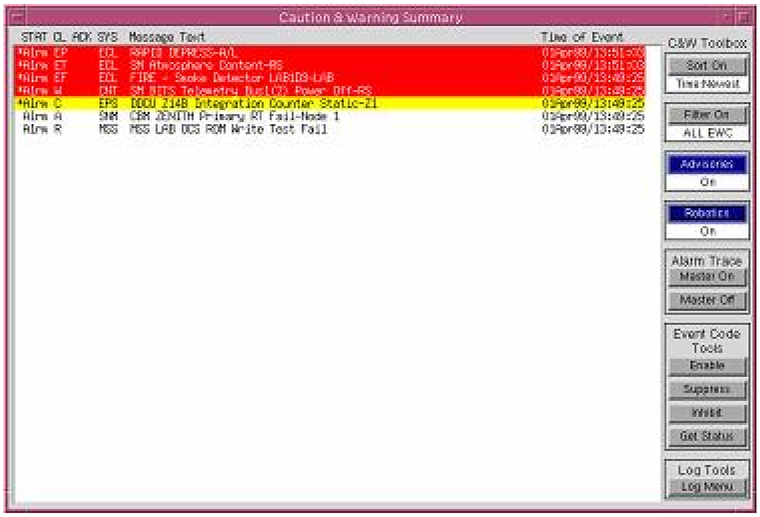
Caution & Warning

Caution and Warning (C&W) functions provide text messages to alert crew and ground operators to anomalous conditions. In general, the same C&W messages and interfaces are available to both the crew and flight controllers.

ISS Caution and Warning messages are grouped into several classifications – Emergency, Warning, Caution and Advisory. Space Shuttle C&W classifications are similar.

- Class 1 (Emergency) events - fire, rapid depressurization and toxic spill - require all onboard crewmembers to respond immediately. These Emergency messages are accompanied by audible alarms, silenced upon crew or ground acknowledgment. Associated immediate response procedures only attempt to identify and isolate the failure to the degree necessary to safe the crew and vehicle.
- Class 2 (Warning) events require that an operator take action immediately to safe the system. Response to a warning event typically requires that either an operator or flight software perform a major system reconfiguration.
- Class 3 (Caution) events are typically issued for a loss of redundancy in a critical system. Immediate crew action is not required in most cases, but flight controllers will respond and reconfigure systems as necessary.
- Class 4 (Advisory) events are issued primarily for ground monitoring purposes. In some cases, advisories are used to indicate nominal system state changes. An advisory may provide more detailed indications

Both the Space Shuttle and International Space Station provide audible tones, illuminated pushbuttons, and computer displays to indicate issuance of these alarms. Downlinked telemetry and ground-based C&W software mirroring functions provide flight controllers with C&W status insight similar in content and format to that shown onboard. See Figure 9.



```
STAT CL ACK SYS  Message Text                                   Time of Event
*Alrm EP    ECL  RAPID DEPRESS-A/L                              01Apr99/13:51:03
*Alrm ET    ECL  SM Atmosphere Content-RS                       01Apr99/13:51:03
*Alrm EF    ECL  FIRE - Smoke Detector LAB1D3-LAB               01Apr99/13:49:25
*Alrm W     CNT  SM BITS Telemetry Bus1(2) Power Off-RS         01Apr99/13:49:25
*Alrm C     EPS  DDCU Z14B Integration Counter Static-Z1        01Apr99/13:49:25
 Alrm A     SNM  CBM ZENITH Primary RT Fail-Node 1              01Apr99/13:49:25
 Alrm R     MSS  MSS LAB DCS ROM Write Test Fail                01Apr99/13:49:25
```

Figure 9 : ISS Caution and Warning Display

The crew and ground have limited capabilities to reconfigure C&W functionality. Space Shuttle crewmembers can modify sensing thresholds used to trigger some C&W messages; flight controllers have similar capabilities. In addition, crew and ground can modify annunciation functions to prevent the issuance of audible alarms ("alarm suppression") or even illumination of C&W lights ("alarm inhibition"). Such modifications to annunciation mechanisms can be used to prevent anticipated irrelevant "nuisance" alarms from disturbing crewmembers during sleep or critical activities.

Current C&W systems do not determine nor indicate the root failure. Failures that have widespread impacts across vehicle systems also result in large sets of annunciated C&W messages indicating the many impacts of a single failure to all vehicle systems.

Limit Monitoring

Limit monitoring systems, used extensively in the MCC, automate testing of telemetered values using predefined limit values. Limit values are set and managed by individual flight controllers. For each limit specified, the console may be configured to indicate limit violations by changing the color of the displayed value and, if desired, sounding an alert tone. Limit values may be modified by the operator during real-time operations, and large sets of limit may be reconfigured at once by operator selection.

In general, limit sets in MCC are set to alert flight controllers to comparatively small changes in telemetered values so that the flight control team can take action before the corresponding onboard limits (specified in onboard software and C&W functions) are violated.

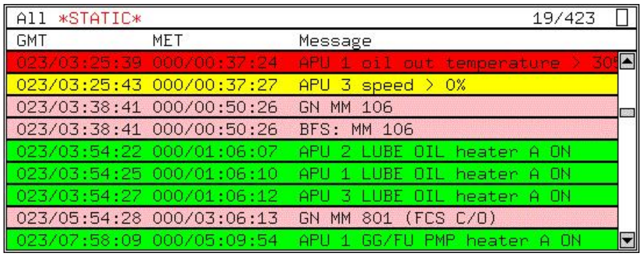
Limit value criteria may be set to match constraints defined by the system developer (e.g. maximum operating temperature), limits set by operators based on analysis (maximum allowable power usage rate based on resource availability analysis), or as standard "deadbands" around nominal observed values. In many cases, multiple limit sets are defined for a single parameter to implement several of these limit definitions.

Plots

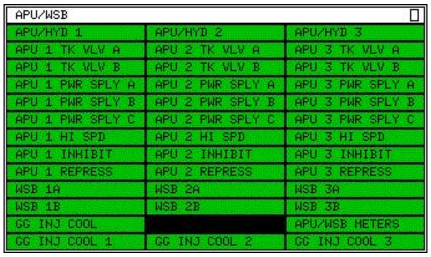
Plotting functions allow flight controllers to identify trends and specific signatures. Observation and comparison of plotted data can confirm nominal operation of a system or identify off-nominal behavior. For example, the curved shape of electrical current data plotted as a function of time may indicate degradation of a pump before the pump completely fails. Comparing historical data with plots observed in real time can confirm the recurrence of a known anomaly or confirm that the observed behavior is unique. On ISS, there are literally hundreds of heaters and temperature sensors. Using plots, sensors for similar systems or areas on the module shells can be plotted together, to watch the overall trend and to identify a failed sensor or heater.

Event Logging and Rule-Based Monitoring

Two tools automate the processes of logging events and analyzing multiple parameters against predefined limit sets. Event Logger (ELOG) generates text messages when telemetry values pass simple predefined logic checks. More complex logic tests are performed by the Configurable Real-time Analysis System (CRANS). CRANS presents the operator with color coded virtual status lights rather than text messages, allowing the operator to identify complex through visual pattern recognition. See Figure 10.



```
All *STATIC*                                   19/423
GMT          MET          Message
023/03:25:39 000/00:37:24 APU 1 oil out temperature > 30
023/03:25:43 000/00:37:27 APU 3 speed > 0%
023/03:38:41 000/00:50:26 GN MM 106
023/03:38:41 000/00:50:26 BFS: MM 106
023/03:54:22 000/01:06:07 APU 2 LUBE OIL heater A ON
023/03:54:25 000/01:06:10 APU 1 LUBE OIL heater A ON
023/03:54:27 000/01:06:12 APU 3 LUBE OIL heater A ON
023/05:54:28 000/03:06:13 GN MM 801 (FCS C/O)
023/07:58:09 000/05:09:54 APU 1 GG/FU PMP heater A ON
```



APU/WSB

APU/HYD 1	APU/HYD 2	APU/HYD 3
APU 1 TK VLV A	APU 2 TK VLV A	APU 3 TK VLV A
APU 1 TK VLV B	APU 2 TK VLV B	APU 3 TK VLV B
APU 1 PWR SPLY A	APU 2 PWR SPLY A	APU 3 PWR SPLY A
APU 1 PWR SPLY B	APU 2 PWR SPLY B	APU 3 PWR SPLY B
APU 1 PWR SPLY C	APU 2 PWR SPLY C	APU 3 PWR SPLY C
APU 1 HI SPD	APU 2 HI SPD	APU 3 HI SPD
APU 1 INHIBIT	APU 2 INHIBIT	APU 3 INHIBIT
APU 1 REPRESS	APU 2 REPRESS	APU 3 REPRESS
WSB 1A	WSB 2A	WSB 3A
WSB 1B	WSB 2B	WSB 3B
GG INJ COOL		APU/WSB METERS
GG INJ COOL 1	GG INJ COOL 2	GG INJ COOL 3

Figure 10: Example ELOG (left) and CRANS (right) Applications

Command Capabilities

The Space Shuttle and the International Space Station provide significantly different command interfaces and capabilities. These differences have a significant impact on the ability of flight controllers to perform failure response actions themselves.

Space Shuttle flight controllers can send commands similar to those the onboard crew executes through a keyboard interface, but this is only a subset of the capabilities available to the crew. Thousands of switches and circuit breakers give the crew additional and unique capabilities to reconfigure onboard systems. In many cases, the flight controller’s role is to determine the correct course of action and relay instructions for execution by the crew. The flight control team still provides a crucial role in uplinking data directly to onboard computers, and sending commands where that capability is available.

In comparison, ISS flight controllers have much more capability to command from the ground. Most of the command and systems reconfiguration capability is accessed through the common computer displays that both the crew and ground share. In general, this provides both the ground and the crew with the same capabilities, though both have additional unique capabilities as well. The ground can build, test and uplink new commands in response to onboard failures that change system performance unexpectedly. The crew, in turn, has the added capability to manually reconfigure switches, valves, cables and other physical interfaces onboard. Some ISS system reconfiguration procedures require the careful orchestration of both ground-based commanding steps and the physical “rewiring and replumbing” actions performed by crewmembers.

ISS operations has adopted additional capabilities to partially automate the command process. Command sequences may be assembled on the ground and executed either from the MCC or onboard. Simple ground-based command scripts contain the command sequences defined in published procedures. Use of these scripts in conjunction with the associated procedure allows the flight controller to more quickly and reliably execute response actions. Onboard, the use of Draper Laboratory’s ”Timeliner” application allows not only the automated sequencing of commands, but also logic checks to assess system response to commands.

Fault Detection

Initial identification of a failure may be accomplished through a variety of means, typically dependent on the nature of the failure. While C&W messages are available for the set of predetermined and well understood failure modes, there are many other potential conditions that may not have been anticipated. For such cases, successful failure identification depends largely on the ability of the human operator to observe, interpret and understand the available data.

Slow degradation in flight system components may be identified first by observation of telemetry plot trends or even comparison of recorded values over the span of weeks or months. For example, cabin atmosphere temperature and pressure values are recorded and analyzed over very long time spans to identify slow leaks. While onboard software can quickly identify rapid depressurization conditions, slow leaks can be more challenging to accurately detect.

Often, the first indication of an anomaly is the ground-based annunciation of a telemetry limits violation. By maintaining sensitive parameter limits in MCC, flight controllers can identify, diagnose and sometimes even respond to a problem before onboard alarms are triggered. For example, life support system flight controllers can be alerted to increasing indications of smoke before a fire alarm is triggered onboard, allowing the ground to advise crewmembers

Other failure conditions may not be evident until specific commands are attempted. Failure of a remotely commanded electrical power switch may not be detected until an attempt to close the switch is made. For this reason, nominal procedures include steps to verify that the system correctly responds to any command. This practice is referred to as the use of “confirming cues.”

Confirming cues play a dual role in failure detection. While the confirming cues identified in nominal procedures serve to identify problems, some confirming cue checks in failure response procedures serve to verify that telemetry indications are correct. A second confirming cue eliminates the possibility that an observed out-of-limits telemetry value is not due to failure or degradation of the associated sensor. It is the flight controller’s challenge to identify indications of anomalies before they result in a problem that impacts the crew’s ability to perform the mission. Obviously, this is not always possible.

It is also important to be able to tell if a telemetry parameter is valid. This is needed so the controlling computers, crew, or ground don't act on a static or invalid parameter. This is especially true for analog data when there is a sensor anomaly. It is recommended that all telemetry have a validity indicator. Telemetry can be grouped such that one validity indicator is used for multiple telemetry parameters.

Failure Analysis

Once a failure is detected, further analysis is performed to identify the nature of the problem, its effect on the vehicle and mission, and priority of failure response.

Proper failure response requires a reasonable level of root cause determination. In the real-time environment, such root cause analysis should determine which component has failed and the potential to recover the functionality of that component. For example, real-time analysis of an electrical bus failure would determine the particular switch that has failed and whether or not that switch may be reclosed. In some cases, root cause determination requires the collection of additional data including detailed firmware status messages, non-standard telemetry values, or even responses to subsequent test and reconfiguration commands.

Failure impact analysis is paramount in the formulation of appropriate failure response. A single failure may have cascading impacts across many or even all vehicle systems. The electrical bus failure cited above may cause loss of power to critical functions such as life support, attitude control and data processing. In many cases, the appropriate response to a failure will not address the root cause at all, but rather compensate for the vehicle-wide impacts of that failure. Regaining attitude control after a critical power loss may be the only timely way to maintain a viable spacecraft.

Additional off-line analysis may be performed by both the flight control team and engineering support functions. Cooperative Failure Investigation Teams (FITs) perform exhaustive post-failure analysis to determine ultimate root cause, potential design or manufacturing changes and long-term strategies to avoid repeated failures. Products used by these teams include failure event timelines, fault trees, ground test data, prior flight performance data and component manufacturing history. This analysis, although important for complete failure response, typically happens hours or even days after a failure. Therefore, crew members and flight controllers must be prepared to respond to failures without benefit of this additional analysis.

Failure Response

Failure response may be executed by the flight software, crew or the flight control team as dictated by circumstances. The availability of communication between the spacecraft and the ground obviously can limit the flight control team's ability to execute timely response to failures. Time critical responses may therefore be required of the crew.

Regardless of the failure, response actions are structured to accomplish the following in priority order:

1. Assure the safety and health of the crew
2. Preserve the viability and performance of the vehicle
3. Preserve the ability to accomplish the mission

Successful initial failure response merely "safes" the system and vehicle, preventing further damage to the crew or the vehicle. Subsequent reconfiguration procedures may perform additional troubleshooting to identify root cause failure (if not already known) and even recover system functionality where lost.

There are cases in which the first and second of these priorities far outweigh the third. To protect the crew and vehicle, flight rules dictate that the Space Shuttle land at the next available opportunity after the loss of certain critical redundant systems. Such a Primary Landing Site (PLS) aborts can result in the loss of some or all mission objectives while preserving crewmembers, flight hardware, and the ability to fly and succeed another day.

To the maximum extent practical, failure response procedures are written, tested, verified and published long before real-time operations begin. When a procedure is available to address an in-flight anomaly, the crew and flight controllers are trained to execute that procedure. Published failure response procedures not only reflect the best knowledge of the engineering and operations communities, they also represent validated and well-proven methods to safe or even recover vehicle functions.

However, failure response procedures have their own limits. The majority of flight procedures are written to an assumed nominal vehicle and system configuration. Exceptions are made for specific critical failure cases in which timely response to a second failure is essential to maintain vehicle integrity and/or crew safety. In addition, some procedures contain additional steps to address additional anticipated problems.

When an appropriate response procedure is not available, flight controllers must create new procedures in a timely fashion. Using an internal "Flight Notes" document, an operator may create and distribute updates to procedures, plan inputs, and other relevant data. These flight notes are reviewed and, if necessary, modified, by other members of the flight control team to ensure that all ramifications of the proposed actions have been considered. An approved flight note may result in a real-time voice call to the crew or an update to a plan or procedure, or additional actions performed by one or more flight controllers.

This interchange of humans modifying or even creating new plans and procedures underscores the role of the flight controller in today's human spaceflight programs.

Post-Failure

After immediate failure response actions have been taken, the flight control team performs additional tasks to better prepare for future actions or even future potential failures.

Degradation or failure of an onboard system component may also warrant changes in real-time monitoring criteria. C&W functions may no longer provide valid indications. In some cases, malfunction procedures may direct the operator to use alternate monitoring limits or inhibit inappropriate C&W messages, In other cases, the operator must determine the need for such changes.

A key component of proper post-failure response is the reconfiguration of remaining vehicle capabilities. Not only must active systems be properly configured to continue operation, these systems should also be properly prepared to withstand the next possible failure. In all cases, the flight controller's role is to ask "What could the next failure be, and how can we protect for it?" The answer to this question is dependent on the nature and architecture of the system in question.

Formal documentation of a failure is achieved through submittal of an anomaly report. An Anomaly Report captures the facts and actions associated with the failure in the FIW format already discussed. This report adds to the database of in-flight anomaly experience, providing further background for those who may experience similar problems in the future.

Following a major systems failure, each flight control discipline manually reviews system plans, procedures and flight rules to identify those products that will require modifications due to an in-flight anomaly. As required, flight controllers modify these products and submit them the rest of the flight control team for review and concurrence before publishing the results and uplinking them to the crew.

Lessons Learned

Based on Space Shuttle and ISS experience, there are several main lessons learned and areas in which improvements can be made. In addition to weighing the impacts of architectural decisions on long term operations, the following are a few of the recommendations:

Fault Detection

We recommend that an automated system be used to detect faults via direct measurement of sensors, etc. and way for the manual annunciation of a fault (fire, smoke, loss of power, etc.). Built-In Testing (BIT) or a more advanced system should be used to detect faults. Additional hardware should also be provided as a fail-safe.

It is also important to be able to determine the validity of a telemetry parameter. This is needed so the controlling computers, crew, or ground don't act on a static or an invalid value. This is especially true for analog data if there is a sensor anomaly. It is recommended that all telemetry have a validity indicator. Telemetry can be grouped such that one validity indicator is used for multiple telemetry parameters.

Fault Response

It is recommended that FDIR be automatic, since the crew and especially the flight control team should not be in the critical path to safe the system. This means that fault responses should be autonomous so as to not require real-time crew or ground response. For example, the switch from the primary system to a backup or redundant system should be an autonomous process. Systems should be cross strapped to allow for the recovery of functionality without the need for a full backup string.

Flight critical systems should be capable of operating in a degraded mode. If the recovery is not successful the spacecraft should go to a "safe" or "survival" mode. In the case of any failure, the system will need to be able to safe itself and recover any critical functionality without operator intervention.

In order to work around defective software or during times a FDIR function is undesirable, the crew and flight control team need the ability to enable/disable fault responses and to see whether a fault response is enabled or disabled. The avionics system should allow for enabling and disabling fault responses and for variable responses based on mission mode.

It is also important to have a load shed capability in the case of a shortage of power generation or battery power. Carefully consideration must be given to the order in which that equipment is powered down such that the core system for vehicle control, crew interfaces, ground interface, etc. are maintained for as long as possible. In extreme cases for a total loss of power, the system should be able to restart itself automatically when power is restored. It is essential that operator intervention be minimized in these situations. For example on ISS extreme load sheds can power off equipment needed for acquiring pointing data and communications with the ground. It is recommended that the load shed list be changeable based on the mission phase and any failures.

Troubleshooting

The ability to be able to downlink diagnostic data not normally downlinked can be critical when troubleshooting failures. All software systems must provide an error logging capability. This logging capability should be preserved during a power cycle such that the cause of a failure can be determined after a loss of all volatile data. This data must be downlinked for ground analysis so the capability to compress the data would speed up the process. Avionics systems require a safe mode with adequate telemetry and data dump capabilities.

Software Development

The software development process must be more agile. The testing process must be integrated into the software development and the user community must be involved in each step. Software releases must be done on a regular basis to allow for defect resolution and for software improvements. The software must not be “locked down” to far in advance of its use on-orbit. This “lock-down” must not occur until after the user community has a chance to adequately check-out the software.

Since with all software, change is an ongoing process, there also needs to be a way for the flight control team to update procedures quickly, validate the changes, and uplink them to the vehicle for use by the crew. Examples from industry are the use XML for storing the procedure, telemetry, and command metadata with a web browser like interface. These technologies could easily be adapted for use on spacecraft and in Mission Control.

Tools

It is recommended that an integrated planning system be used which allows for the time-lining of activities, linking to procedures, and for detecting conflicts between activities. The tool should be easy to use, allow for updates in real-time, track completed activities, and require few personnel to operate. Ideally this tool would be interoperable with the spacecraft planning system in order to schedule activities and to obtain the results. It is also recommended that tools be used to track anomalies, procedure updates, and communications between the flight control team, the crew, engineering community, and outside organizations.

Rather than forcing the crew or ground operators to manually execute each step in a procedure, it would be far more productive to automate all procedures and have the crew follow along. The crew would be able to start a procedure, pause it when necessary, make a decision if something unexpected happens, and to abort the procedure. The system should also provide a capability to undo steps if necessary. Ideally this process would be a procedure with telemetry and commands embedded in it.

The displays and system software should have protections for operator error such as wrong command parameters, invalid command for current mode, etc. The displays should be easy to use, follow common standards for usability and human factors, allow for the easy navigation between displays, etc.

System Control

There must to be a system provided to inform the crew and ground of the most important failures. This system should do more than just annunciate events. It should also provide status regarding the systems automatic responses to these events. For instance, the status of the fault and the automatic responses should be displayed. This system should also prioritize events such that the crew and ground can work the most important failure first. Combined with an intelligent system, the root cause of failures can be displayed. This display should also interface with the procedure execution system such that an operator can just tell the system to perform a procedure when an automatic response is not available.

It would also be useful to combine the procedures and displays with an intelligent system that could provide insight into any anomalies that occur. This system would also be able to take over for the crew if necessary and also provide the ability for a crew to perform an override. Likewise a tool for viewing the timeline of procedures which interfaces with the procedure viewing and execution tools would give the crew and ground controllers a seamless interface for procedure execution. This tool could also interface with an intelligent system for automated execution of procedures at the specified times. This timeline tool should also provide the capability to be updated easily, link to procedures, automatically adjust based on delays, etc.

Conclusion

In conclusion, in order to determine how the flight control team will be setup, the system architecture and tools must be analyzed in order to determine the needed expertise, when that expertise is needed, and the cost vs. benefits of additional crew training vs. using ground experts. Nominally support is only needed by the system experts when activities involving their systems as scheduled. However, if the analysis determinates that the system or crew cannot cover all possible emergency situations, then flight control team support will be needed during the periods of time those emergencies could occur. Typically this means around the clock support. It is all too often that cuts in capability and autonomy during the development of a spacecraft are not weighted against the cost of long term operations, which leads to the need for a larger operations team than expected.

Although present day human spaceflight operations are highly dependent on ground-based support of real-time operations, future deep space missions may demand a higher reliance on onboard autonomy. Increased vehicle autonomy will increase the crew training requirements. Crewmembers must be able to maintain situational awareness even when automated functions perform the failure responses.

The flight control team's role may evolve as human spaceflight reaches greater distances from earth. New tools and processes may be required to address the limitations imposed by communications delays and telemetry bandwidth. As a result, the development of the next generation ISHEM must take into account the human element to ensure that both the crew and flight controllers have the needed insight into and control over automated failure response functions.

References

1. Systems Engineering and Integration Processes of the National Aeronautics and Space Administration (NASA) Lyndon B. Johnson Space Center (JSC) Mission Operations Directorate (MOD), E. Kranz and C. Kraft, 19 December, 1990.
2. ISO/CD 10303-226
3. Federal Standard 1037C in support of MIL-STD-188
4. NASA Lesson Learned #837 - False Alarm Mitigation Techniques, Dec 1, 1994
5. NASA Lesson Learned #772 - Fault Protection, Feb 1, 1999
6. NASA Lesson Learned #707 - Fault Tolerant Design, Feb 1, 1999
7. NASA Lesson Learned #839 - Fault-Detection, Fault-Isolation and Recovery (FDIR) Techniques, Dec 1, 1994
8. Operational Considerations in the Development of Autonomy for Human Spaceflight
9. Reducing Risks and Costs in Automated Operations