FAILURE DETECTION AND RECOVERY IN THE ASSEMBLY/CONTINGENCY SUBSYSTEM

Final Report

NASA/ASEE Summer Faculty Fellowship Program -- 1993

Johnson Space Center

Prepared by:	Rex E. Gantenbein, Ph.D.
Academic Rank:	Associate Professor
University & Department:	University of Wyoming Department of Computer Science Laramie, Wyoming 82071-3682
NASA/JSC	
Directorate:	Engineering
Division:	Tracking and Communications
Branch:	Systems Engineering
JSC Colleagues:	Sally D. Stokes David A. Overland
Date Submitted:	6 August 1993
Contract Number:	NGT-44-001-800

ABSTRACT

The Assembly/Contingency Subsystem (ACS) is the primary communications link on board the Space Station. Any failure in a component of this system or in the external devices through which it communicates with ground-based systems will isolate the Station. The ACS software design includes a Failure Management capability (ACFM) that provides protocols for failure detection, isolation, and recovery (FDIR).

The author reviews the ACFM design requirements as outlined in the current ACS software requirements specification document. The activities carried out in this review include:

(1) An informal, but thorough, end-to-end failure mode and effects analysis of the proposed software architecture for the ACFM; and

(2) A prototype of the ACFM software, implemented as a C program under the UNIX operating system.

The purpose of this review is to evaluate the FDIR protocols specified in the ACS design and the specifications themselves in light of their use in implementing the ACFM.

The basis of failure detection in the ACFM is the loss of signal between the ground and the Station, which (under the appropriate circumstances) will initiate recovery to restore communications. This recovery involves the reconfiguration of the ACS to either a backup set of components or to a degraded communications mode. The initiation of recovery depends largely on the criticality of the failure mode, which is defined by tables in the ACFM and can be modified to provide a measure of flexibility in recovery procedures.

The failure modes defined for the ACFM are grouped into three major categories:

- pointing vector failures, which indicate a problem in the positioning of the steerable antennae used for high data rate communications;
- hardware failures, which result from internal problems with ACS components; and
- extended losses of command link, which occurs when the ACFM detects a loss of signal but either is unable to isolate the source of the problem or cannot successfully recover communications due to multiple failures.

Other events are also detected by the ACFM, but do not immediately initiate recovery unless coupled with a detected loss of signal or a critical failure mode.

A prototype of the ACFM FDIR protocols, implemented as a set of modules corresponding to the subcapabilities of the ACFM specified by the requirements document, has been constructed and tested to branch coverage using fault injection techniques to demonstrate the behavior specified by the existing requirements document. This document, which is still in draft stage, is missing a number of descriptions relating to events identified in the fault mode and effects analysis. Furthermore, the existing descriptions are often inconsistent or incomplete in their specification of the expected behavior of the ACFM in response to events that can occur in the ACS. These problems need to be resolved before the document can be relied upon for construction of the actual system.

INTRODUCTION

The Assembly/Contingency Subsystem (ACS) is the primary communications link for the Space Station. It provides two-way audio and core data communications and supports ground-based tracking of the Station. The ACS is composed of two encapsulated *strings* of components. The primary components, or Orbital Replacement Units (ORUs), of each string, as shown in Figure 1, are:

- the ACS baseband signal processor (ACBSP), which provides the interface between the ACS and other onboard computer and audio subsystems,
- the ACS transponder (XPDR), which converts ACS information between analog radio frequency (RF) and digital form, and
- the ACS radio frequency group (ACRFG), which provides for transmission and reception of S-band signals between the Station and the ground via the Tracking and Data Relay Satellite System (TDRSS). This group consists of a high-gain and a low-gain antenna and the amplifiers for these antennae.

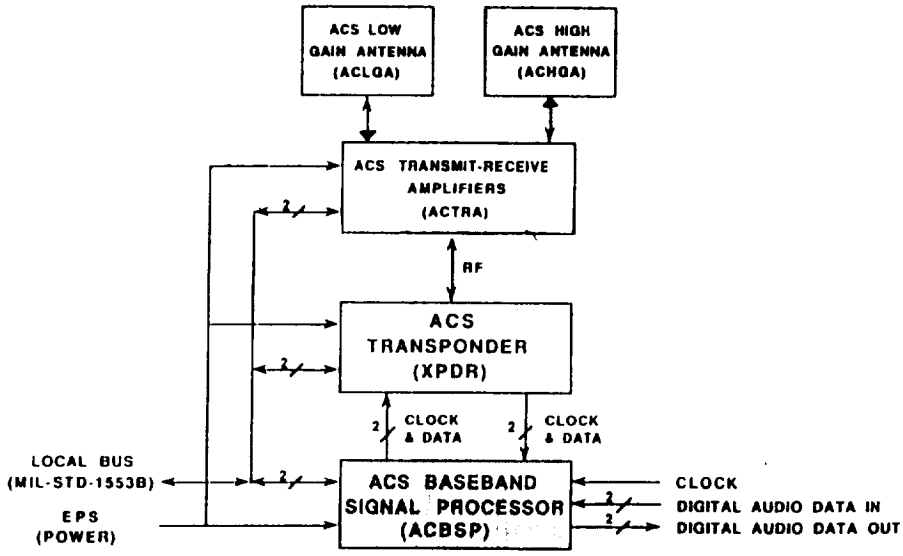

Figure 1.- Block Diagram of the Assembly/Contingency Subsystem (ACS).

Failure in any of the ORUs, or in the external units that provide the connections to both the ground and to other subsystems onboard the Station, have the potential to interrupt the link between the Station and the ground, effectively isolating the Station until such time as the linkage can be restored.

The absence of communications, even for extended periods, is under some conditions an inconvenience, while in other cases, such as extra-vehicular activity, it may be life-threatening. In any event, it is clear that some facility must exist to accomplish failure detection, isolation, and recovery (FDIR) in this subsystem, so that permanent communications loss can be avoided. Furthermore, during the early unmanned stages of the Station's deployment, all control will be initiated from the ground, making it difficult to repair any problems on board without

communications. Even in the manned operational phase, facilities for manual diagnosis and repair of the ACS will be limited, placing continued importance on the system's ability to detect and recover from failures autonomously.

For these reasons, among others, the ACS design includes a Failure Management subsystem (ACFM) for detecting the loss of communications capabilities in the ACS and providing mechanisms by which communications can be restored in the event of failure. The software requirements of this component are described in section 3.2.3.3.2.2 of the ACS Flight System Software Requirements (FSSR) [1]; those requirements state that the ACFM collects equipment status and performance data, and performs failure management functions including equipment and string isolation and redundancy management.

The ACFM itself is composed of three constituent capabilities (also called subcapabilities). Each of these subcapabilities provides a distinct set of services supporting FDIR in the ACS.

- ACFM External Control (ACFXC) is responsible for accepting failure indications from sources external to ACFM and establishes the monitoring mode for failure detection and isolation, determining the behavior of the ACFM in response to detected failures.
- ACFM Failure Detection and Isolation (ACFFDI) collects the raw equipment sensor data and status, and analyzes it to detect and isolate equipment faults within the ACS.
- ACFM Failure Recovery (ACFFR) is responsible for managing the redundant ACS resources at the string level for recovery from a detected failure.

Information used by the ACFM may be generated internally or input from external sources. There are two external sources of information, which may also be updated by the ACFM:

- the Run-Time Object Database (RODB), which maintains system management information from the Station subsystems in a common area and is the primary interface with the Tier 1 system, which provides Station capabilities such as the onboard system executive, the crew interface, and the Station control center, and establishes the operating environment for the ACS; and
- the ACS data base, which maintains ACS information that is not needed outside the ACS.

Additionally, the ACFM may exchange information with the ACS Services Management (ACSS) subsystem, the second subsystem in the ACS, both directly and through the RODB and ACS data base. The relationship among the three subcapabilities of the ACFM and the inputs and outputs for each are shown in Figure 2.

During his 1993 NASA/ASEE Summer Faculty Fellowship at the Johnson Space Center, the author carried out a review of the current design of the ACFM as specified in the FSSR. The purpose of the review was twofold: to evaluate the FDIR protocols proposed for the ACS and to evaluate the FSSR's specification of the ACFM subsystem design.

FAILURE MODE AND EFFECTS ANALYSIS

For review of the FDIR capability of the ACS, an informal Failure Modes and Effects Analysis (FMEA) was initiated on the ACFM design as specified in the FSSR and augmented by conversations with Kent Gaylor of LinCom Corporation. The goal of this work was to analyze the ACFM design on a functional basis, describing and documenting the FDIR system and identifying the expected *failure modes* (the ways in which failures can occur).

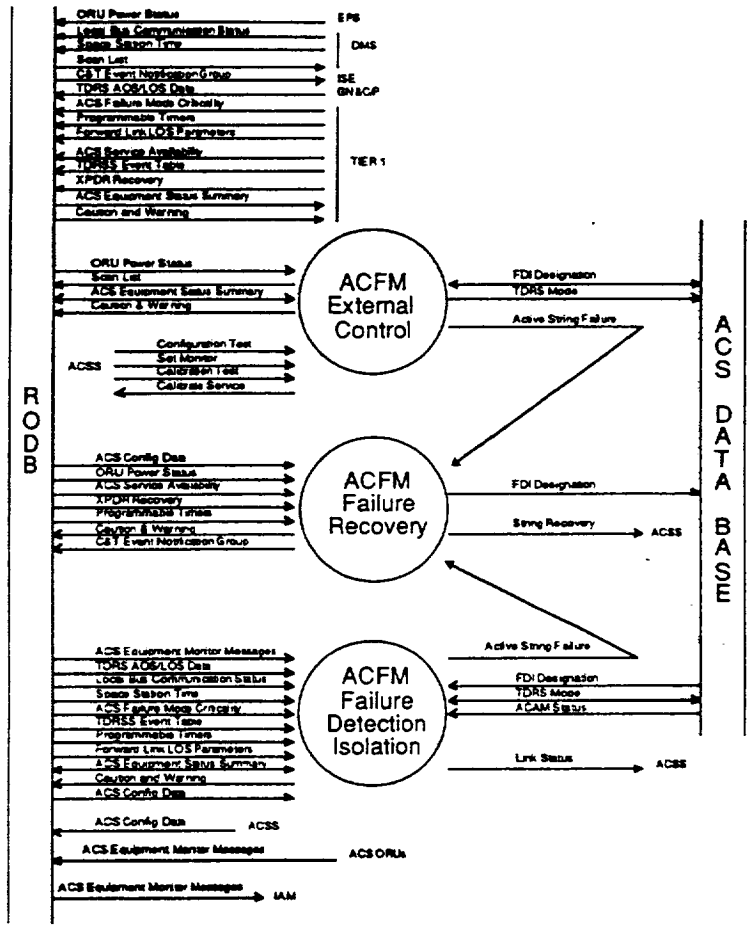

Figure 2.- Subcapabilities of the ACS Failure Management (ACFM) Component.

Failure and Recovery in the ACFM

A number of events have been identified as failure modes for the ACS. These events fall into three major categories, which correspond to the recovery strategies incorporated in the ACFM:

- pointing vectors failures,
- hardware failures, and
- extended loss of command link.

The overall *modus operandi* of the ACFM can be characterized as "if it ain't broke, don't fix it." Even if external or component faults have occurred and are detected in the system, no failure is declared as long as commands are successfully being transmitted and processed on the Station. The reasoning behind this approach is that it is preferable to have communications (even if failures exist within the system) than to attempt recovery that might not succeed. This approach also handles the problem of incorrect sensors triggering an unnecessary recovery.

Loss of signal

An interruption in the information flow between the Station and ground support is termed loss of signal (LOS). Both the forward (ground to Station) and reverse (Station to ground) communications links pass through the Tracking and Data Relay Satellite System (TDRSS). This system consists of two geostationary satellites, TDRS-E(ast) and TDRS-W(est). As shown in Figure 3, the Station passes from the range of one TDRS to the other as it orbits the Earth. Once in each orbit, the interposition of the Earth between the Station and the TDRS satellites, which causes the Station to experience LOS, defines a zone of exclusion (ZOE). Upon emergence from the ZOE, the Station attempts acquisition of the signal (AOS) to reestablish communications.

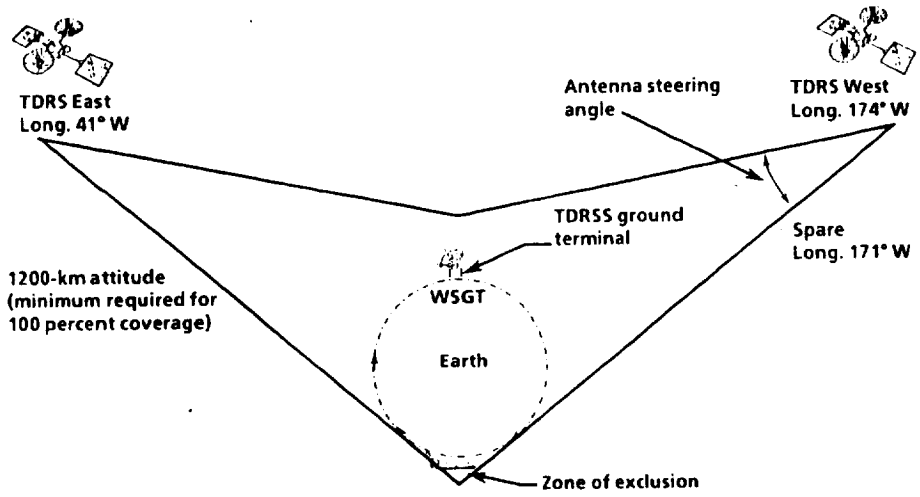

Figure 3.- The Tracking and Data Relay Satellite System (TDRSS).

LOS is detected in the ACFFDI through examination of the TDRS mode and the demultiplexer state, which determines the quality of the forward link. If the TDRS mode is "SEARCH" and the demux state shows "Degraded Frames" continuously for a specified TDRS Search Time, or if the TDRS mode is "ACQUIRED" and the demux state shows "Degraded Frames" continuously for the LOS Declaration Time, then LOS is declared by the ACFFDI. LOS caused by the Station's passing through the ZOE or by other, scheduled competition for use of the TDRSS is not considered a failure in the ACFM. However, LOS in the forward link that is *unscheduled* may result in ACFM declaring a communications failure. A failure may also be declared if the Station is unable to achieve AOS when emerging from the ZOE or passing from the range of one TDRS to the other.

To determine if a detected LOS is scheduled, the ACFM checks the internal TDRS event table, which lists the times when the Station is expected to be in (or near) the LOS period. An uncertainty time is applied to the event times for entering and leaving the period. If no event is found that indicates that the LOS is scheduled, then ACFM declares the LOS to be unscheduled.

The ACFM must also consider the situation in which no event schedule is available. Since the Station will be in long-term orbit, the TDRS event table must be regularly updated.

If such an update fails due to error or inability to communicate with the Station, the events in the table could become outdated in time. Should this occur, the ACFM will use AOS/LOS data in the RODB to see if one of the TDRS satellites is actually in view. This data can be manually confirmed if necessary. If LOS occurs when the event table is exhausted, the ACFM will attempt to determine whether a TDRS is in view. If the AOS/LOS data shows that a TDRS is in view, then such LOS is declared to be unscheduled.

Initiating recovery

The detection of an unscheduled LOS initiates additional effort in the ACFM to isolate the cause of the LOS and to recover communications. The conditions that lead to declaration of failure are described in the following sections. Recovery in the ACS is achieved by switching from one string of ORUs to another. These strings are functionally identical, but receive and transmit on slightly different frequencies to avoid interference. For this reason, the ACFM must keep track of which of the two strings is the *current* or operating string and which is the backup or *alternate* string.

Recovery from communications loss can take place at two levels. At the string level, operations are switched from the current string to the alternate; if successful, the current and alternate indicators are switched so that the current string becomes the backup and vice versa. Recovery may also take place at the data rate level. If external or internal failures make it impossible to use the High Data Rate (HDR) communications facility (which depends on the steerable high-gain antenna) on either the current or alternate string, another configuration, which uses the omnidirectional low-gain antenna, can provide a Low Data Rate (LDR) link.

In order to avoid spurious recovery and unneeded reconfiguration, as well as to provide some flexibility in the recovery actions, all ORU component events in the system have an associated *criticality*. Only an event identified as "CRITICAL" will initiate recovery. The default criticality values for the events in each ORU are defined in the FSSR. This status is maintained through a criticality table in the RODB. This table (which can be modified from the ground) determines whether a failure in a given component will initiate recovery or simply be noted. In the following descriptions of the failure modes, criticality will be mentioned where it affects the behavior of the ACFM.

Pointing Vectors Failure Mode

Once an unscheduled LOS has been declared, the ACFM will attempt to isolate the source of the problem that has caused the failure. One possible problem is that the Guidance, Navigation, and Control / Propulsion (GNC/P) subsystem is unable to correctly position the steerable antenna with respect to the TDRSS. This condition is detected in the ACFM by an unscheduled LOS and the ACS High-Gain Antenna Management (ACAM) subcapability of the ACSS indicating that the ACAM mode is "POINTING" (i.e., using the steerable, high-gain antenna) but ACAM pointing data is not available (this condition is derived by ACAM from AOS/LOS data in the RODB). Under these circumstances, the ACFM will declare an active string failure in the pointing vectors mode. Recovery from this error will be attempted, as described above.

Hardware Failure Modes

Failures due to faults within components of the ACS are broadly categorized as *hardware* failures. Several combinations of faults can result in a failure of this kind. All active string

failures in this mode will initiate an attempt by the ACFM to isolate the failure and recover communication.

Antenna faults

One form of hardware failure occurs when an unscheduled LOS is declared, the ACAM status shows the ACAM position as "NOGO" but the ACAM pointing data as available, and the ACS configuration data in the RODB (which defines the current configuration of the ACS) shows the high-gain antenna in use. This indicates a failure in the high-gain antenna's physical positioning by the ACSS. If the criticality table for the ACRFG component of the active string shows the antenna positioning as a critical event, then an active string failure in hardware mode is declared.

ORU faults

An ORU in the active string may also fail, interrupting the flow of information through the string. The status of the individual units is maintained by the RODB in the ACS Equipment Status Summary. If an unscheduled LOS has occurred, the ACAM pointing data is available, and the ACAM position indicator in the ACAM status is "GO" (meaning that the high-gain antenna is not experiencing problems), then a "NOGO" indicator for any event in the ACBSP, XPDR, or ACRFG on the active string, when matched with a "CRITICAL" entry in the criticality table for that event, will result in an active string failure in hardware mode.

Other hardware faults

Several other circumstances result in the ACFM declaring an active string failure in hardware mode. These are:

- a "NOGO" in a ACRFG BIT summary monitor message from the RODB for either the forward or reverse power indicator, when the indicated ACRFG is in the active string, the SSPA mute is disabled, and the corresponding entry in the ACRFG criticality table is "CRITICAL;"
- a notification from the Electrical Power Subsystem (EPS) through the RODB that an ORU in the active string has been powered off; or
- the ACBSP function status monitor message indicates the multiplexer output is inactive for the ACBSP in the active string, and the corresponding entry in the criticality table is "CRITICAL."

Under each of these three conditions, an active string failure in hardware mode is issued, regardless of whether an unscheduled LOS has been detected.

Extended Loss of Command Link

Under some circumstances, such as malfunction in the transmission system or corruption of transmitted data, it is possible for information to be received by the Station that does not correspond to any known command. Occasional occurrences of this type are not a major problem, since the command can be retransmitted once it is known on the ground that the Station did not respond. However, it is essentially impossible for the ACS to differentiate between corrupt and uncorrupt data, so the ACS may not detect LOS when, in fact, no usable information is being received. This can cause a long-term interruption of information or commands transmitted through the forward link.

To avoid this problem, the Integrated Station Executive (ISE), the software that performs the centralized coordination of the various command and control subsystems on the Station,

includes an "egg timer" that is periodically reset by telecommand. If this timer expires (that is, it is not reset within its expected period), it indicates that the system has experienced extended loss of command link (ELOC). In response, a preset sequence of recovery actions, designed to discover if any path exists through the ACS that will support communications, is initiated. If such a path exists, then communications can be restored.

Obviously, this mechanism would also be invoked if a failure occurs that cannot be diagnosed or recovered by the ACFM, resulting in total loss of communications. Conditions in which ELOC is known to occur due to the inability of the ACFM to respond to a detected failure are:

- an active string failure in pointing vector mode has occurred, but the LDR service on the current (active) string is not available, and an attempt to cycle power to the alternate string fails;
- an active string failure in pointing vector mode has occurred, but neither the current nor the alternate string LDR services are available;
- an active string failure in hardware mode has occurred, but the alternate string is not available and an attempt to cycle power to the current string also fails;
- an active string failure in hardware mode has occurred and the alternate string is indicated to be available, but an attempt to cycle power to the alternate string fails;
- an unscheduled LOS has occurred either while ACAM pointing data is available and either the ACAM status indicates that the ACAM capability of the ACSS is available, or LDR is in use, but no indicator of a critical failure in a component of any ORU exists; and
- an unscheduled LOS has occurred while ACAM pointing data is available, HDR is in use, and the ACAM status indicates that the ACAM position is "NOGO" but the ACAM pointing field is not defined as a critical failure mode by the criticality table.

Under these conditions, the Station will be unable to receive information through ACS until such time as the ELOC recovery procedure is carried out and communications restored.

Other Detected (Non-failure) Events

A number of other events are detected in the ACFM, but these are not immediately declared as failures. In general, they issue warning messages and set flags that, should an unscheduled LOS occur, may be used to isolate the cause and initiate an appropriate recovery action.

Asynchronous ORU events

Asynchronous events in the ACS ORUs involve changes in the ORU. These events, and the ORUs in which they can occur, are:

- BIT Go (ACBSP, XPDR, ACRFG),
- BIT NoGo (ACBSP, XPDR, ACRFG),
- Invalid Command (ACBSP, XPDR, ACRFG),
- Multiplexer Data Lost (ACBSP),
- Demultiplexer Data Lost (ACBSP),
- Pointing Function Status Change (ACRFG), and

- Low-Gain Antenna Switch Request (ACRFG).

As indicated, three of these events can occur in any ORU type. A BIT Go event (which is actually defined for a number of events in each capability) is signaled when a component of the ORU completes either its Power On Self Test (POST) or an Equipment Self Test (EST) or when the Go/NoGo flag in the BIT summary toggles from NoGo to Go. The ACS must report this as a BIT Go asynchronous event and update the appropriate Go/NoGo flags in the BIT summary, update the transmit vector word in the ACS Equipment Monitor, and set a service request bit in the 1553B (bus) status word. Similarly, a BIT NoGo event is reported if the POST or EST complete with failure or if the Go/NoGo flag in the BIT summary toggles from Go to NoGo. Again, the flags in the BIT summary and the 1553B status word are set. An Invalid Command event occurs when the ORU receives a message on the local bus that it doesn't recognize. This event is reported by updating the transmit vector word in the ACS Equipment Monitor and setting the service request bit in the 1553B Status Word (the message itself is discarded).

Two asynchronous ORU events affect only the ACBSP. A Multiplexer Data Lost event occurs when the length of a return link packet received does not match the length contained in the packet header. In this situation, the packet is discarded and the transmit vector word and service request bit are both set as above. A Demultiplexer Data Lost event occurs when data is not being removed from the forward link buffer fast enough to prevent the buffer from overflowing. In response to this event, ACFM again sets the transmit vector word and the service request bit.

Two other asynchronous events are unique to the ACRFG ORUs. A Pointing Function Status Change event occurs when the state of either the beta or alpha gimbals' stop sensors change (indicating that the antenna has passed a software-preset limit). In addition to updating the transmit vector word and setting the service request bit, this event also updates the ACRFG function status monitor message. A Low-Gain Antenna Switch Request event occurs after the ACRFG stops receiving pointing data for the high-gain antenna. Sixteen seconds after such loss, the ACRFG will start a linear extrapolation algorithm based on the last pointing commands. At some later time, if no pointing data has been received, the switch request event occurs; the ACFM reports this by updating the ACRFG function status monitor and the transmit vector word and setting the service request bit.

Internal ORU reset

Occasionally, the ORUs may internally detect a problem and reset themselves. This is done through an internal watchdog timer in the ORU firmware that is periodically reset, approximately every 100 milliseconds. The ACRFG signals this event by toggling the Go/NoGo bit in the ACRFG BIT summary monitor. The XPDR indicates it by the Processor Reset parameter located in the XPDR function status monitor. The ACBSP reports the event through the ACBSP throughput data monitor's ECM Reset since Last Report parameter. In the current ACS design, these events cannot be detected directly; however, if an unscheduled LOS occurred in a critical ORU because of such an event, then a string failure would be declared and recovery initiated. However, this means that some ORU resets may not be detected.

EVALUATION OF THE FDIR DESIGN THROUGH PROTOTYPING

To review the FDIR protocols and their description in the FSSR, the author implemented a prototype of the ACFM design for detecting and recovering from forward link communications failures. This program was written in C and implemented on a SUN workstation running

UNIX in the Control and Monitoring Systems Development Laboratory in Building 44. This section of the report briefly describes the components of the prototype and its implementation and testing.

Components of the Prototype

The prototype was constructed with modularity and testing in mind, using an object-based approach in which the functionality of each of the subcapabilities was encapsulated as a set of source modules corresponding to that subcapability. The interfaces between the modules modeled the ACS data base and the RODB, and all interaction among the subcapabilities used data in those two interfaces. Since the interfaces were designed first, the subcapability designs could be carried out independently.

Each module in the prototype contains code to handle the various FDIR activities specified for the associated subcapability in the FSSR (with extensions for omitted features, as identified by conversations with NASA colleagues and K. Gaylor of LinCom). For example, the ACFXC subcapability handles FDIR associated with events from external sources, such as calibration and configuration tests that are generated by ACSS, the ORU power status changes signaled by the EPS, and so on. The ACFFDI subcapability, which is the most complex of the three, detects failure and, where appropriate, initiates recovery based on a variety of sensor data, such as the ACS equipment status summary, the ORU BIT summary monitors, the pointing data from ACAM, etc. When either of these two subcapabilities detect an error, a number of messages and other indicators are sent through the RODB to other subsystems.

Recovery is initiated when the ACFXC or ACFFDI module declares active string failure. The failure, which will be in either hardware or pointing vectors mode as described above, is then acted upon by the ACFFR module. Given the nature of the failure, reconfiguration at either the current string or data rate level is attempted. If this recovery does not succeed, or if the detection process is unable to isolate the cause of the failure, then the prototype indicates that ACS communication is not available, a condition that would be handled through the ELOC recovery mechanism. The prototype does not simulate ELOC recovery, however, only its detection.

Implementation and Testing

The prototype consists of 23 modules of C code. In addition to the modules for the ACFXC, ACFFDI, and ACFFR subcapabilities, there are support modules for various subtasks not directly related to FDIR, an initialization module, and a number of modules used as test drivers to inject faults into the prototype. The prototype, as it currently is implemented, runs sequentially through a series of test cases. The conditions that activate a particular behavior in the subcapabilities are set in the driver code, then the appropriate detection module is called as a function. In this way, the driver simulates interrupts that would invoke the ACFM when an event or change in state occurs. The detection module looks for the injected fault, issues appropriate messages and updates, then initiates recovery when conditions warrant. The design of this prototype is illustrated in Figure 4.

For each execution of the prototype, the responses of the prototype (implemented as character strings sent to standard output) were collected for validation of the code against the specification. The prototype was tested to branch coverage using this method to ensure that all expected inputs produced the appropriate responses. A combination of black box and white box testing was used to design the test cases. A test plan consisting of 37 tests (some of which

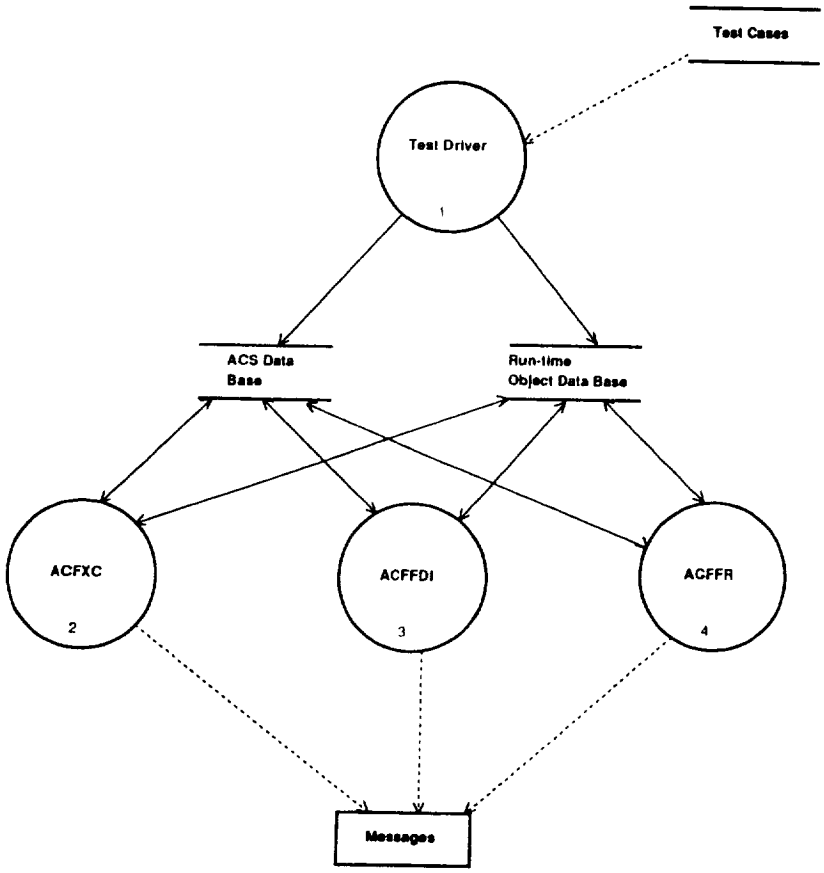

Figure 4.- Design of the ACFM Prototype.

tested multiple cases of the same response: failure and restoration of an ORU, for example) was developed and used to carry out the testing. Where revisions were made due to tests in later stages of the validation, regression testing was used to assure that the changes did not affect any previously validated code.

REVIEW OF CURRENT ACFM DESIGN

The final step in the review of the ACS FDIR capability was to look at the results of the previous analysis and determine what issues were still unresolved or unclear. The FSSR, which is still in a draft stage, is intended to provide both the high-level principal functional requirements as well as the detailed software requirements for the ACS. As such, it is an essential part of the FMEA process and the development of software for the ACS. The previous steps in the review represent preliminary versions of these two activities that exercise and evaluate the FSSR as it is currently defined.

This section of the report addresses two issues. The first part lists the events identified in the FMEA that are either omitted or incompletely addressed in the FSSR. The second part lists ambiguities or inconsistencies found in the document while building the prototype. Caveat: time did not permit a complete review of the FSSR, so the comments that follow are likely

incomplete. Furthermore, some of the items listed as omissions may be handled by subsystems external to the ACFM.

Undefined Events

A number of the events described in the previous sections are not included in the existing ACFM requirements. To address these problems, both the interfaces that provide the detection of these events and the response of the ACFM to them must be determined and added to the FSSR.

TDRS event table exhausted

If the TDRS event table does not contain any events beyond the current time, then the table cannot be used to determine scheduled vs. unscheduled LOS. There is a specification in the ACS FSSR for the activity of the ACS Service Maintenance (ACSM) subcapability of the ACSS when this table is exhausted, but the ACSM specification does not describe the expected behavior of the ACFM. The intent under these conditions is for the ACFM to use data from GNC/P to determine whether a TDRS is actually in view and determine whether a detected LOS is scheduled or unscheduled on that basis. The June 1993 version of the FSSR contains a description of this activity, but this version was not reviewed by the author.

Internal ORU reset

The effect of an ORU reset is not specified in the FSSR. It is assumed that a reset can either succeed or fail, where failure indicates that the ORU does not come back up and is therefore unavailable. There is no specification, however, of what flags should be set by ACFM to indicate detection of either of these events.

Also, the reset event indicators are different for each type of ORU, which makes detection difficult. As currently understood, an ACRFG reset is indicated by a flag in the ACBSP function data throughput monitor, but no such field exists in that data structure as specified. It was also reported by Gaylor that these resets could be handled in the ACS Control and Monitor Software (CMS) if its "Common Failures" parameters were changed, allowing an unsuccessful ORU reset to directly trigger recovery. At this time, however, it is not clear what the ACS's response should be to these events.

Asynchronous ORU events

Some of the asynchronous ORU events (Invalid Command and the ACBSP Multiplexer/Demultiplexer Data Lost events) are described in the ACFM portion of the FSSR. Only the Invalid Command event is completely defined in terms of the interface and response. The responses to the ACBSP Data Lost events are described, but the FSSR shows only that Caution and Warning Messages are issued. Gaylor describes other activities, as discussed in previous sections.

The ACRFG Low-Gain Antenna Switch Request event is shown as one of the possible values in the ACBSP vector word in the interface specifications, but no response to the event is specified. The ACRFG Pointing Function Status Change event is neither shown in the interface nor described in the response specifications. The BIT Go and BIT NoGo events are also omitted in both places for all three ORU types.

If these events are incorporated into the FSSR, the interfaces must also reflect their presence. For example, it appears that a response to an asynchronous ACRFG event would include updating the ACRFG function status monitor, based on comparison with the ACBSP description. However, this structure is not defined, either in the ACFM interface or in the data

structure tables. Similarly, the XPDR function status monitor, which is apparently the source of the XPDR internal reset flag, is not defined in either place.

Extended loss of command link

Recovery from ELOC is not addressed in the ACFM FSSR that was reviewed. It is not clear what capability of the ACS is responsible for either of these activities. The ISE contains the timer that is used to detect ELOC, but the interface between ISE and ACFM is not defined. The algorithm for responding to ELOC and the interfaces are defined in the June 1993 FSSR, but again this version was not reviewed by the author.

It should be noted here that the detection of ELOC when no local response to an unscheduled LOS is defined or possible in the ACFM is shown in the FSSR by the phrase "No additional processing is required." This phrase is also used to indicate the end of a successful mode restoration as well as the detection of recoverable failures. Even if detection of ELOC is the responsibility of some other capability, it would seem appropriate to distinguish the event from "normal" (i.e., non-failure) events in the ACFM description.

Other Comments

In addition to these events that are either omitted or incompletely described, there are several ambiguities and inconsistencies in the ACFM document.

A number of data structures are inconsistently specified among the ACFM context diagram (shown in Figure 2), the summary interface tables in the description of the ACFM, the tables for the individual subcapabilities, and the specifications of the subcapabilities' behavior. These include:

- the ORU FDI designation and the TDRS mode, which are both shown in the ACFM context diagram and in the subcapability tables, but do not appear in the summary tables;
- the ACS equipment summary, which is shown as external input and output in the context diagram, but (a) does not appear as input in the summary tables; (b) appears as external output in the summary and ACFFDI tables; (c) appears as internal input in the ACFFDI table; and (d) appears as internal input and output in the ACFXC tables; and
- the ACS configuration data shown as input to the ACFFDI subcapability includes only the TDRS identifier, while at least two other fields are needed (the SSPA mute field in paragraphs *l* and *m* of the ACFFDI description, and the audio channel status in paragraphs *e* and *f* of the same section).

Other problems arise in the descriptions of the ACFM subcapability. Among those discovered in this review:

- in paragraph *r* of the ACFFDI description, under the case in which the high-gain antenna is in use, the ACAM Position is "NO GO," and the ACS Failure Mode Criticality for Antenna Position is "CRITICAL," the criticality check is redundantly specified;
- in paragraph *p* of the ACFFDI description, the Demultiplexer State is defined to be "DEGRADED FRAMES" if the ACBSP function status monitor is not periodically updated, but no definition of "periodically" is provided; and
- in paragraph *a* of the ACFFR description, it appears that a failure that occurs while the ACS is configured for LDR transmission cannot be recovered by switching to HDR, even if that mode of transmission is available on the current or alternate string. There may be practical reasons that this option is not allowed, but no one with whom the author

consulted could confirm or deny this.

These ambiguities should be reviewed and resolved.

One pervasive problem in the FSSR is the lack of precise terminology to refer to data structures and other information. While the numerous redesigns of the Space Station are no doubt the underlying cause of many of these problems, this review exercise illustrated the difficulty of understanding the relationship between the description of the ACFM capabilities and the interface that provides the information with which they can be implemented. For example, in paragraph *r* of the ACFFDI description, once an unscheduled LOS has been detected, an active string failure in either pointing vectors or hardware mode can be declared. However, the pointing vectors case includes the condition where the ACAM mode is equal to "POINTING" while the first hardware case refers to the high gain antenna being in use. These two conditions are, in fact, exactly equivalent in the existing design. Such inconsistency can only be confusing to the implementor and is a source of potential error.

FUTURE WORK

While all software aboard a spacecraft like the Space Station is critical, the FDIR software must be more trustworthy than any other, since it is responsible for detecting and recovering failures generated elsewhere in the system. Our understanding of the processes and mechanisms that can support this level of reliability in software is still inadequate. For these reasons, the validation and evaluation of the ACFM and similar FDIR software for space-based communications systems are important tasks that require further study.

One immediate project being pursued is to extend this summer's work to a more realistic testbed that can generate events in real time and consider the effects of multiple (concurrent or cascading) failures on the reliability and performance of the system. We plan to port the prototype to a workstation environment at the author's university and create this testbed. We will also develop a test profile for the prototype based on communications outage data from recent Space Shuttle missions that the author has collected this summer. By implementing these real-time test drivers and applying the Shuttle outage data to the prototype, we should be able to measure with reasonable accuracy the error coverage and reliability of the proposed ACFM relative to the Shuttle data. We also hope to look at proposed outage schedules for the Station as well.

Longer range goals involve the exploration of methods by which the reliability, performance, and error coverage in space-based communications systems can be enhanced. In a harsh and still not completely understood environment like space, it is almost impossible to predict what events will and will not occur that may have an adverse effect on communications. Rather than trying to design a system that responds in a predefined manner to a given set of failures, we can look at designs that choose from among several alternatives, using information about the system and environmental state to find the response that has the highest probability of maintaining or restoring communications. Providing this kind of information to an FDIR system might allow a higher degree of reliability than has been previously achievable in communications control systems.

REFERENCES

[1] McDonnell Douglas Aerospace, *Flight System Software Requirements (Communications and Tracking System Software)* SSP 30606, Volume II Revision B (April 5, 1993).