AEROSPACE REPORT NO.
TOR-2013-00293

Mission Assurance Practices for Satellite Operations

June 3, 2013

K. Rex Childers
SATCOM Operations Support
MILSATCOM Division

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

Authorized by: Space Systems Group

Developed in conjunction with Government and Industry contributions as part of the U.S. Space Programs Mission Assurance Improvement workshop.

AEROSPACE
Assuring Space Mission Success

AEROSPACE REPORT NO.
TOR-2013-00293

Mission Assurance Practices for Satellite Operations

June 3, 2013

K. Rex Childers
SATCOM Operations Support
MILSATCOM Division

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

Authorized by: Space Systems Group

Developed in conjunction with Government and Industry contributions as part of the U.S. Space Programs Mission Assurance Improvement workshop.

AEROSPACE
Assuring Space Mission Success

AEROSPACE REPORT NO.
TOR-2013-00293

Mission Assurance Practices for Satellite Operations

Approved by:

Russell E. Averill

Russell E. Averill, General Manager
Systems Engineering Division
Engineering and Technology Group

Jacqueline M. Wyrwitzke

Jacqueline M. Wyrwitzke, Principal
Director
Mission Assurance Subdivision
Systems Engineering Division
Engineering and Technology Group

Executive Summary

Mission Assurance for Satellite Operations is focused on two higher level areas of concern: preventive and recovery. The preventive section addresses the considerations necessary to reduce satellite operations risks by ensuring that process steps and products necessary for operations are ready to support, while the recovery section addresses the structure and process required to facilitate effective responses to satellite operational issues.

Development of operations products seeks to address the preparatory products required prior to any launch considerations. Measures are described to ensure readiness assessment of products such as command and telemetry databases as well as the structure to determine anomalous conditions that require actions. Operational manual structure and content are highlighted with best practice suggestions listed along with command procedure development, validation, and maturity assessment. Human machine interface suggestions are made to facilitate development, evaluation, and testing of the products that the operations team will utilize on a daily basis to understand and control the space asset.

Training is another broadly covered preventive topic with multiple facets addressed with suggested best practices to be applied by the stakeholders. The training topics cover the requirements development that encompasses the scope and standards that are necessary to meet the mission objectives. Roles and responsibilities are laid out and provide an actionable roadmap focusing on the requirements of each role enabling all personnel to clearly understand what is expected of them prior to, during, and after operations. The section covers all the steps for achieving an operations ready team. The areas covered are initial certification of the team, guidance for proficiency training of the operators all the way through stress inducing training, and personnel error recovery actions. Recovery training and capability documentation is also addressed with best practices woven within the section. The section identifies the ultimate goal of having capable, certified operators ready for all imagined, planned, and out-of-plan actions. All of the above training topics are addressed and envelope the section focusing on the rehearsal aspects of operations for the operators. This bottom up approach is designed to provide for the best possible approach to operator readiness.

Preventive measures describe the execution aspects of nominal and contingency operations and the products and processes associated with the baseline planned operations. Development of the commands themselves, the validation of the command string generated, as well as the expected result of the configuration change, are all addressed. Trending is covered highlighting the need for development of trending data points of interest along with tools necessary to provide the proper insight necessary to understand if actions need to be taken to prevent anomalous outcomes. Reach-back for assistance is covered both in the preventive and recovery sections as is the configuration management of the operations products as this is critical to preventing unintended consequences from impacting operations as the space asset ages. The preventive section also discusses self-assessment and feedback to ensure that the operations team is constantly seeking to improve performance and prevent failures, operational errors, and process escapes.

Recovery measures describe the process and best practices that are associated with recovery operations during a satellite's life in orbit. The topics covered within the recovery section are anomaly definitions and associated terminology, immediate response operations, description and processes associated with investigation and recovery, and finally review and disposition of the issues for historical and configuration control purposes.

It was deemed critical that our team seek to provide definition for the common terms utilized in satellite operations and this document accomplishes that objective. Anomaly categories and

classification definitions are represented and closely align with both government operations and commercial space operations ground terminology. What is designated as a common fault versus what needs to be classified as a satellite emergency are critical to understanding the process by which specific actions are to be implemented. These definitions also seek to provide guidance for structuring the reach-back and feedback format through clarification of events and their impacts on the space asset.

Immediate response is addressed such that this document outlines the responses required and the personnel roles and responsibilities. The operations crew and their actions are clarified such that the purpose of their actions is mandated and not subject to interpretation until the spacecraft is in a safe configuration. After the spacecraft has achieved a safe configuration the next step is to transition the operations team and the support functions into the investigation and recovery phase. Assembling the Anomaly Response Team (ART) to organize, investigate, evaluate, address and assess risk to future actions is detailed. Real roles and responsibilities are defined and highlighted such that the roles are interchangeable insofar as the "who does what" is not as important as the "what needs to get done." Assembling the team of subject matter experts to develop the investigation plan and evaluate the findings is paramount to resolving the space assets issue long term. The next step detailed is the process by which the same ART evaluates the risks associated with planned actions as well as consequences of those planned actions. Within this subsection the utilization of trade matrices and Ishikawa Diagrams to work through the probable causes necessary to focus the team on the solution is described and detailed.

The next step in the evolution of spacecraft anomaly operations is to review and disposition the next steps required to place the spacecraft into a safe, and mission-oriented configuration. This task falls to the Anomaly Review Board (ARB) with its members crossing from the ART investigation role to providing long term disposition and possible configuration directions. The ARB ensures anomalies are documented, investigated, and resolved. The ARB is responsible for making program level decisions which support the program mission in the best way possible. Additionally, the ARB approves non-nominal configuration changes. As other subsections roles and responsibilities are detailed, the process for review and final disposition is also presented.

The document is meant to provide guidelines for implementing mission assurance practices in mission operations from prelaunch through decommissioning. The inclusion of best practices is meant to provide guidance for future operations and assist teams in constructing and outlining processes necessary to increase mission success and minimize on-orbit risks. It is meant to provide a framework by which adherence to the described processes seeks to prevent operational errors, minimize the impact of degrading performance, and effectively review and resolve observed anomalies. This document does not require any specific skill set to provide to the role of gatekeeper, it simple needs to reflect the roles and responsibilities and best practices that are recommended for safe and effective satellite operations.

Acknowledgement

This document has been produced as a collaborative effort of the Mission Assurance Improvement Workshop. The forum was organized to enhance Mission Assurance processes and supporting disciplines through collaboration between industry and government across the US Space Program community utilizing an issues-based approach. The approach is to engage the appropriate subject matter experts to share best practices across the community in order to produce valuable mission assurance guidance documentation.

The document was created by multiple authors throughout the government and the aerospace industry. We thank the following contributing authors for making this collaborative effort possible:

Karl Arunski	Raytheon Intelligence, Information and Services
Derrell Brayton	Orbital Sciences
Linton Honda	The Boeing Company
Jay Landis	Space and Missile Systems Center
Tom Wunderlich	The Boeing Company
Rob Zmarzlak	Northrop Grumman Aerospace Systems

A special thank you for co-leading this team and efforts to ensure completeness and quality of this document goes to:

Rex Childers	The Aerospace Corporation
Rick Krause	Ball Aerospace and Technologies Corporation

The topic team would like to acknowledge the support, contributions, and feedback from the following organizations:

The Aerospace Corporation
Ball Aerospace and Technologies Corporation
The Boeing Company
Johns Hopkins University Applied Physics Laboratory
Northrop Grumman Aerospace Systems
Orbital Sciences Corporation
Raytheon Intelligence, Information, and Services
Raytheon Space and Airborne Systems
Space and Missile Systems Center (SMC)
Space Systems Loral

The authors deeply appreciate the contributions of the subject matter experts who reviewed the document:

Ed Fleming	Orbital Sciences Corporation
Mike Freeze	Johns Hopkins University Applied Physics Laboratory
Vince Heeg	Northrop Grumman
Brian Kosinski	Space Systems Loral
Ed Lesnansky	Raytheon Space and Airborne Systems
Steven Pereira	Johns Hopkins University Applied Physics Laboratory
Dave Pinkley	Ball Aerospace and Technologies Corporation
Lisa Talley-Nelson	Orbital Sciences Corporation
Paul Woznick	Ball Aerospace and Technologies Corporation

THIS PAGE INTENTIONALLY LEFT BLANK

Contents

Figures

Tables

1. Introduction

Mission assurance is the disciplined application of proven scientific, engineering, quality, and program management principles toward the goal of achieving mission success. It follows a general systems engineering framework and uses risk management and independent assessment as cornerstones throughout the program life cycle.

The Mission Assurance (MA) for Satellite Operations topic team was chartered for the 2012-2013 Mission Assurance Improvement Workshop (MAIW) cycle. The MAIW was formed in 2007 by the U.S. space community to develop and codify the best practices to meet key challenges to U.S. Space Program mission assurance. Each year subject matter expert topic teams are formed to work on key topics. The teams typically produce or enhance guidance documents that may evolve into written standards, best practice guides, and/or contractual compliance documents. Significant contributions to this product were provided by members of the team from industry and government.

In the beginning, the Satellite Operations topic team decided to approach mission assurance for satellite operations on two fronts: preventive and recovery. Preventive measures focus on producing high quality operations products, processes, and training to achieve the goal of mission success, e.g., command procedure development and command verification. Recovery measures focus on safely and effectively restoring service in the event of satellite and ground system issues and/or operational errors that even the best use of preventive measures cannot eliminate. The team first developed, and then added to, a list of both preventive and recovery tasks to be discussed. The team then drafted and refined guidance for each task from industry and personal experience. Per the normal MAIW process, other industry experts then reviewed the draft document and provided further guidance and comments that were adjudicated at the 2013 MAIW.

In describing the best practices for mission assurance for satellite operations the team sought to provide guidance that could be applied as appropriate to all phases of operations from pre-launch readiness to end-of-life disposal for all types of satellite programs.

The document provides guidance:

1. to organizations for effectively assuring mission success in satellite operations.
2. to be tailored to each individual program's overall operational concept, and therefore, is not prescriptive in nature.
3. to be applied by the operations and operations support teams and does not necessarily recommend that there be a dedicated mission assurance organization for satellite operations.

The responsibility for mission assurance in satellite operations lies with the entire operations team, although specific responsibility for each of the measures discussed can be assigned within the team.

1.1 Problem Statement

- Mission assurance standards are not well defined for satellite operations.
- Mission assurance standards that are defined are not consistently applied to on-orbit operations.
- Gaps in ops processes can force detrimental real-time decisions.

- On-orbit lessons learned are not consistently fed back to future development or operations efforts.

1.2 Background (how did we get to this point)

The following are some examples of where more robust application of mission assurance (MA) discipline could have prevented major on-orbit problems:

- Mission X encountered degraded performance of momentum wheel. Engineering team decided to attempt to re-power, but there was subsequent hard failure. The team used contingency procedures to reconfigure for operation without the faulty wheel. Participation was limited to customer/user, engineering, and program management (no MA).
  - No failure documentation in the prime contractor Quality Management System (QMS)
  - No quality process (risk assessment, procedure evaluation, investigation plan, contingency plan, etc.)
  - No cross program coordination
  - No failure containment
  - No root cause, corrective action
- Mission Y encountered a problem with a receiver, did not engage the prime contractor or unit subcontractor, switched to a redundant unit, and issued a customer anomaly report. Years later it was discovered that the original problem was caused by command error. A defective software patch had been uploaded and caused loss of vehicle later in mission.
- Mission Z had an incident where a command was sent to the wrong operational vehicle. The command sent to "wrong vehicle" was due to use of an incorrect operator console in the satellite operations center.

1.3 Scope

- Preventive
  - Minimize occurrence of operations errors
  - Maximize ability to predict and minimize impact of performance degradation and/or impending satellite hardware failures
  - Maximize operational availability
- Recovery
  - Maximize ability to detect and diagnose unforeseen failures/errors
  - Maximize ability to safely prevent further impact and recover from unforeseen failures and/or errors
  - Minimize recovery time so that customer service is minimally interrupted by the outage

1.4 Applicability

This document is intended to be used as a suggested guide in the development and implementation of mission assurance processes designed to assure successful satellite mission operations. It is assumed that every operations team is different and it is also assumed that each operational issue is different.

Based on these assumptions this document was written with the understanding that discipline-specific individuals must assume the various mantles of responsibility. This document does not seek to provide direction other than to define what roles and responsibilities must be followed to provide the best results. Specifically, this document does not necessarily advocate the need for a dedicated mission assurance person(s) for satellite operations. Every member of the satellite operations team must take ownership in adherence to the actionable steps described in this document. It is the responsibility of all team members to ensure that the processes are followed if best practice lessons learned are to be applied to future operations. The applicable phases of this document are as follows:

- Prelaunch development and exercise of operations processes
- Post launch execution
- On-orbit lessons learned feedback to future development

1.5 Intended Audiences

- Program management (mission assurance manager)
- Mission operations manager
- Engineering and manufacturing
- Operations teams
- Government stakeholders

1.6 Implementers

- Acquisition teams
- Operations teams

THIS PAGE INTENTIONALLY LEFT BLANK

2. Definitions

The following definitions are used throughout this document to represent the elements of operations. Individual programs may use different terms to represent these elements and functions.

- **Anomaly**: An anomaly is a system event which either threatens system safety or causes degraded performance. An anomaly may also refer to nonconformance to expected performance that may require reconfiguration to resolve.
- **Discrepancy or Nonconformance**: A condition of hardware or material where a characteristic does not meet requirement.
- **Discrepancy Report (DR)**: Documents satellite or ground system problem (hardware, software, procedural, etc.) failing to meet a documented specification or otherwise requires attention.
- **Disposition**: The direction for correcting an unexpected result or non-conformance.
- **Fault Management**: The satellite automated response to a specific fault.
- **Hazardous/Restricted Commands**: Commands that can cause serious impacts on the satellite if sent inadvertently. These commands generally require two steps (i.e., enable and execute) to accomplish the required action.
- **Operations Concepts**: Define how various aspects operations will be performed as well as roles and responsibilities of the various organizations and personnel involved
- **Preventive Action (PA)**: Action taken to eliminate similar occurrences of the issue.
- **Reach-back**: The ability to access the factory subsystem and system experts to support the planning and execution of complex activities, the diagnosis and mitigation of adverse trends, and the diagnosis and recovery from anomalous situations.
- **Satellite**: The combination of the spacecraft bus and the payload.
- **Watch Item**: A watch item is something that the engineering and operations teams want to monitor for further change.

THIS PAGE INTENTIONALLY LEFT BLANK

3. Target Processes

This section describes the critical activities and processes required to prevent and recover from operational issues.

Preventive processes provide a standardized set of steps to ensure repeatability across the team for specific functions with the goal of minimizing the occurrence of operations issues. Preventive processes are used to minimize the occurrence of operational errors and to improve the ability to predict future performance and determine possible actions to reduce the impact of hardware degradation and/or failures. Preventive processes are grouped into:

1. operational product development
2. training
3. mission execution
4. trending, identification, compilation and analysis
5. reach-back
6. self-assessment and feedback, and
7. configuration management

Recovery processes provide a standardized set of steps to ensure repeatability across the team for specific functions with the goal of efficiently and safely recovering from operational errors and/or hardware and software performance issues.

3.1 Preventive

3.1.1 Development of Required Operational Databases and Products

Two critical elements to the successful operation of an on-orbit satellite are the ability to "see" what the satellite is doing and to "tell" the satellite what to do. Another critical element is what the satellite can do to self-protect from hardware or software issues. The majority of this section is written with the assumption that the Spacecraft Provider knows and understands that there is a set of products required to exit from an Operational Readiness Review. These products might have subtly different names depending on the Satellite Provider but the content of each product is assumed to be similar. The information will cover command and telemetry handbook requirements and development, operational product requirements and development, and the development of the human machine interface (HMI). Mission assurance practices for the development and verification of all these critical elements are described below.

3.1.1.1 Development and Readiness Assessment of Command and Telemetry Database

The purpose of command database development is to provide detailed command descriptions for hardware and software commands, internal commands, and Ground Support Equipment commands. Similarly, the purpose of telemetry database development is to provide detailed telemetry descriptions for the hardware and software across all subsystems based on information taken from the equipment specifications and flight software. The development process is used to generate telemetry and command databases adequate to execute the mission. The telemetry database should contain alarm limits to notify the operations staff of off-nominal conditions and the command database must define all required arguments for each satellite command. The telemetry database may contain multiple sets of limits to account for different operating environments throughout the life of the vehicle, for example: launch and ascent, transfer orbit, and on-orbit. The command database must define all required arguments for each satellite command. There may be multiple variations of the command database where some commands are not accessible during test or specific or mission phases for safety reasons. If the command database includes hazardous commands they should be clearly identified. The development process also ensures that all on-orbit commands are executed and verified to the maximum extent possible during ground testing on the flight hardware along with the associated telemetry measurands. It is desirable to test the commands at the highest level of simulation and/or system integration possible.

Roles associated with Operations Product Development usually fall to the following disciplines:

1. subsystem engineering
2. systems engineering
3. flight software engineering
4. ground software engineering
5. operations engineering
6. mission assurance
7. quality engineering

The responsibilities are not limited to subject matter experts from any specific discipline, but rather any individual capable or assigned to perform to the roles identified above.

Subsystem engineers define the basic commands and telemetry points and verify that they are as expected during unit and subsystem test. Systems engineers capture the specific data passed between the ground spacecraft and payload into the appropriate interface control documents (ICDs) and verify these requirements during system level test.

Flight software engineers implement the software for formatting the subsystem telemetry and processing and routing commands received from the ground system to the destined subsystem hardware. The flight software engineers also implement the automated fault management software to take the defined actions based on the real-time monitoring of vehicle telemetry.

Ground software engineers ensure that the command and control software generates commands and processes and displays telemetry using the applicable ground databases.

Mission operations engineers participate in the review of:

1. related requirements
2. commanding scripts
3. display definitions and
4. other operational products providing feedback on how the satellite will be operated.

Readiness assessment entrance criteria should include:

- Telemetry measurands defined along with qualification and acceptance values, acceptable ranges (red and yellow limits), and units of measure. This list may include software data points that indicate version and check sum health status.
- Hazardous/restricted commands identified.
- Commands defined along with all argument values.
- Each command/argument executed elicits correct telemetry response.
- Applicable interface control documents to sufficient level of maturity.
- Ground command and control subsystem verified.
- Subsystems and satellite verified.
- Satellite simulator verified.

It is assumed that products will include documented command and telemetry databases and other operations products. Command database documentation provides detail command descriptions for hardware and software commands, internal commands, and ground support equipment commands. This document contains information that is taken from the equipment specifications of the subsystems. Similarly, telemetry database documentation provides detailed telemetry descriptions and alarm limits for the hardware and software across all subsystems based on information taken from the equipment specifications and flight software.

Best Practices:

- Using the same command and control database and software/hardware for vehicle integration and test (I&T) and ground system significantly reduces schedule and cost associated with syncing the two separate databases. Separate databases limit the interleaving of operations products and satellite I&T tasks against the flight hardware and/or system simulation due to the configuration lag between I&T and ground systems development. The test regime should also include a "commands not sent" test to verify commands not covered in other test cases. Using the flight database during test is consistent with a Test-Like-You-Fly approach.
- Implement controls during I&T to ensure that potentially harmful commands cannot be sent to the satellite.
- Ground systems testing should be completed using the interface identical to that used on-orbit to verify perfect functionality before launch.
- The fidelity of the satellite simulator is of upmost importance in verifying the command and telemetry databases; the higher the fidelity, the lower the risk of not testing groups of commands on the integrated satellite.

3.1.1.1.1 Command Database Description

This document should contain all necessary commands required to provide operational command capabilities to the satellite. These commands will need to be capable of modifying configurations as well as commanding for recovery. It is assumed that an operations manual is delivered as part of the satellite operations products containing all commands. An operations manual is generally designed to provide reference material necessary for satellite operators to control the satellite.

3.1.1.1.2 Telemetry Database Description

This document should contain all necessary telemetry points, including derived telemetry, required to provide health and status of the satellite as well as provide information necessary to act on anomalous conditions. The telemetry database should meet trending informational requirements as well as document the assumptions and/or coefficients necessary to convert the data to easily understood engineering units.

3.1.1.1.3 Anomaly Detection and Resolution System Description

This document or compilation of documents must contain all necessary information required to both detect anomalous conditions during operations as well as facilitate immediate ground operations responses. One example of a document that fits within this construct is the Satellite Engineering Handbook (SEH). The SEH should contain information with respect to each subsystem on the vehicle, and may even contain information detailing individual elements of any subsystem. This product is used by the operations engineering support team for the mission and anomaly response efforts to provide information necessary if/when configuration changes are required or anomalous conditions are observed. All products within this section are to be organized in a hierarchy to ensure detection and response takes into account dependencies between components, subsystems and data paths.

3.1.1.2 Development of Operations Products

The satellite development team has the responsibility, in concert with the operations team, to develop an operations manual (OM) detailing how to operate the satellite in both normal and contingency situations. This operations manual should include mid-level descriptions of all subsystems (to include the ground systems and remote ground facility) and functions so the operations team has a resource to help them fully understand how the satellite operates. This should be detailed enough to be used for training products development as well as for systems engineering reference. The operations team should be included in the review of this document since it has the task of developing the operations concepts, command procedures, and telemetry displays for the applicable ground systems to implement the operations manual. Mission assurance practices for the development and verification of these products are described below.

3.1.1.2.1 Operations Manual

The satellite operations manual provides users with the detailed information required to operate the satellite to include normal operations, launch operations, and early orbit operations, and special and contingency operations. It is constructed with inputs from experienced subsystem engineers, systems engineers, flight software engineers, ground software engineers, and operations engineers.

Hardware, software, and systems engineers provide an overview and define the basic, complex, and contingency procedures for the satellite and subsystems. Ground and operations engineers ensure that the procedures can be understood and implemented on the target ground system. Basic sequence definitions should include commands and associated telemetry responses, logic flow, and constraints that accomplish the required action correctly with off ramps for erroneous responses.

3.1.1.2.2 Command Procedures

Each satellite should go through the process of developing individual command procedures based on the operations manual tailored to the specific ground system(s) that will be controlling the satellite.

Command procedures as used herein include both paper and on-line command procedures, aka scripts. This development usually falls to operations engineers, ground systems engineers, subsystem engineers, systems engineers, and flight software engineers. Operations and ground system engineers develop each command procedure based on the operations manual and tailored to the specific ground system. Full participation of the cognizant systems and subsystem engineers is absolutely essential for the operations team to successfully create and validate operations procedures.

The following are absolutely required to ensure upcoming operations are successful:

- Sufficiently mature draft of the relevant procedures as defined in the operations manual
- Mature command and telemetry databases installed on the target ground system
- Satellite training on all operations products
- The developed command procedures accomplish the required action correctly and have appropriate off ramps for erroneous responses.
- Sufficient access to the satellite and other high fidelity simulation sources so that all procedures can be exercised and validated

In order to consider any command procedure complete it must be configuration controlled. Although a verified operations manual is the ideal entry criteria, program schedules may necessitate starting development of command procedures when drafts of the operations manual procedures are available.

Verified command procedures should be placed under configuration management control. Procedures fall into the following categories:

- Released procedures are signed off but require further input such as command parameter definitions and specific telemetry responses defined by engineering prior to execution
- Contingency procedure is a pre-planned response and recovery procedure for a specific spacecraft (S/C), payload (PL), and/or ground anomalies and/or faults.
- Pre-authorized contingency procedures are a subset of contingency procedures which may be executed by the operations crew immediately when entry conditions are met.

Tools to import procedures from the operations manual can significantly reduce development time. Tools that can access both the command and telemetry databases, import procedures from the operations manual, and create procedures in a standardized format can significantly reduce development time. A standardized format can potentially be imported into a tool for development of command procedures for a specific ground system. In this case only the ground system specific steps need be added. In addition, tools that can build complex procedures from building block procedures may also reduce development time and can potentially be used in real-time operations to build new contingency procedures. Command procedure verification should include both subject matter expert review and simulator or satellite in factory runs. If simulator or satellite runs are not possible, subject matter expert review is absolutely essential. However; the fidelity of the satellite simulator must be considered, the higher the fidelity, the lower the risk of not testing procedures on the integrated satellite.

Best practices include using the same command and control database and software/hardware for vehicle integration and test and ground system test to significantly reduce schedule, cost, and risk associated developing and verifying command procedures. System procedures used in I&T should reflect on-orbit scenarios and use of operational commands sequences to implement test-like-you-fly practices. Operational tests should be scheduled such that operational procedures can be verified against the actual satellite. The goal during procedure verification should be to get as close to “test like you fly” as possible.

3.1.1.2.3 Command and Telemetry Human Machine Interface (HMI)

Human factors engineering considers the functions that have been allocated to system operators and users, how much time is allocated for these tasks, what information is required, what level of proficiency is needed, and how the system operators, maintainers, and users will interact with and use the new system. Implicit in readiness planning are a series of analyses and simulations to:

1. capture requirements decomposition and allocation for human activity
2. conduct work flow analyses and simulations
3. conduct throughput analyses and simulations
4. determine the number, location, proficiency, and certification required of operators and users
5. determine system-provided status and product information formats, content and timeliness
6. assess and document decisions made by the system operator and user
7. evaluate the maintenance and calibration operations concept in light of availability requirements

The goals are to have operations and ground system engineers develop HMI to comprehensively and logically enter and verify commands and review subsystem telemetry to determine the status and state-of-health. Command and telemetry displays are developed for use by the operations team to configure the ground system, command the satellite, and determine the state-of-health of the satellite. The displays are usually created by operations engineers, ground system engineers, subsystem engineers, systems engineers and flight software engineers. As appropriate operators, subsystem engineers, systems engineers, flight software engineers review and approve the displays to ensure the data being displayed is accurate.

A sufficiently mature draft of the relevant operations manual should be used as a basis for the HMI design. Sufficiently mature command and telemetry databases should also be installed on the target ground system.

The developed HMI should display all telemetry accurately with proper units or states and limits. These new displays will be critically reviewed and ultimately modified as they will likely benefit from interface tests, multiple rehearsals, and other training exercises conducted prior to satellite launch operations. HMI verification should include both subject matter expert review and simulator or satellite in factory runs. The fidelity of the satellite simulator must be considered, the higher the fidelity, the lower the risk of not testing HMI on the integrated satellite.

3.1.1.2.4 Operations Concepts and Processes

The identification, development, and documentation of operational concept and processes is focused on improving the overall control and understanding within the operations and operations support teams. Operations concepts describe the scope of a particular activity, how it is to be conducted, and the roles and responsibilities of the participants. Operations processes detail the step by step process for accomplishing the activity within the scope of the operations concept. The main roles involved in the development of additional operational products should be the operators, operations engineers, ground engineers, satellite subsystem engineers, systems engineers, and management.

Operations engineers are generally charged with the responsibility of developing an operations concept or process related to flight and ground system operations. The remainders of the participants review and provide feedback to the development as appropriate to their role in the defined concept or process. A sufficiently mature draft of the operations manuals needs to be completed prior to the first team exercise or rehearsal so that any need for modifications can be gleaned and scheduled for incorporation. Determination by the operations team or others that a concept or processes needs to be defined and then fine tuned is required to produce a useful, efficient, and accurate product.

A small group of experienced operations engineers develops the concept or process, seeks to obtain community buy-in and feedback, and then executes and refines the concept or process through exercise and real-life use. Operations concepts and processes serve as guidelines but should not take the place of sound engineering judgment. Flexibility to handle unplanned or unforeseen situations must be a key consideration when developing concepts and processes.

3.1.2 Training

3.1.2.1 Ground Operations Training

- **Training Requirements**

  The ultimate goal of training is to ensure mission success and vehicle safety through development of a knowledgeable and disciplined operations team. Training also minimizes the risk of personal errors. The development of training and certification plans should be given careful consideration for every operational program. Standardized training plans establish the minimum level of knowledge that is required for every operations team member and mission support personnel such as systems engineers and operations managers to successfully complete their expected tasks. Everyone involved in supporting the daily operations of the satellite should have training commensurate with their position. To effectively create such a training plan all operations tasks (i.e., subsystems trending, mission planning, pass-plan execution, etc.) need to be well understood and in most cases defined in procedures. The training plans should include definitions for individual/positional roles and the required tasks that a team member is expected to accomplish proficiently. This ensures key knowledge is held by more than a single team member and helps establish standardized processes by which the task is performed. This also prevents personnel from becoming indispensible as their knowledge is contained within the procedures and processes that all team members use on a daily basis during operations.

  Training should be accomplished to an accepted standard, and once completed the team member is held accountable to that standard. A set of typical roles for operations generally include trending, orbit analysis, real-time commanding, and mission planning, but may include others depending on the mission. Non-typical tasks such as orbit raising, unplanned payload maintenance or ground systems maintenance should also be included. Prior to launch a formal document should be developed that contains a certification plan for each position. Additional areas to be considered are those that affect day to day operations and may include system administration, software development, and hardware maintenance. Individualized training and certification plans should be developed as required for each subject area that the trainee is expected to be proficient in. Personnel may become certified in multiple areas, however; each certification should exist as a stand-alone subject area. For example, it’s not uncommon for systems engineers to become certified as satellite operators so they fully understand how the ground system interfaces with the spacecraft as well as how the command and control functions are performed.

- **Training Scope**

  The scope of a training plan typically includes a list of recurring tasks that the person is expected to perform regularly as well as some non-recurring tasks that the person may need to perform in non-nominal situations such as a contingency procedure. Formal training is then planned and performed for the purpose of certifying personnel to conduct satellite operations. Training for the launch and early orbit and checkout team should, when possible, be performed according to a set program schedule and integrated with standard pre-launch events such as exercises, thermal vacuum, and compatibility testing. Training during system integration and testing is preferred for the systems engineering staff and console team that will support mission operations. Training will naturally occur through the development of procedures and participation of operations personnel in exercises and rehearsals but should also include standardized classroom training. If the program is assigned permanent systems engineering support, those engineers should also be trained in accordance with acceptable minimum standards which will enable them to perform their tasks proficiently.

  The same can also be said for operations management personnel. They require a broad knowledge of the spacecraft, ground system, remote ground facility, and the tasks that each team member has to accomplish. This is critical because ultimately the operations manager is accountable for mission assurance and should have a very good understanding of what is taking place on a daily basis.

- **Training Standards**

  Standards establish a level of proficiency that is required for consistently safe satellite operations. All standards that are established should be developed with vehicle safety and mission success in mind. The standards for each position should be developed by subject matter experts in that area.

- **Training Roles and Responsibilities**

  Ideally, each satellite program should have a person designated to administer training and produce training material. In cases where budgets may restrict staffing to fund a designated training person the shift supervisor could be given the role of trainer for their shift. Program managers may have to assign extra duties to crew members to create training material when they are not assigned to support a satellite contact or other activity.

  The roles and responsibilities for each position should be clearly defined and trained. The expectation of each position should be known by all persons to instill good situational awareness and discipline. The goal is to ensure that all daily tasks required to accomplish safe satellite operations are conducted without compromise. No one should ever have to wonder if and by whom a critical task is being accomplished, or if a task is being executed correctly.

  The roles needed to operate a satellite vary greatly depending on the mission and personnel. Budgets limit the number of personnel a program can afford, so the number and type of tasks a person should be assigned to do may vary. Programs should work to ensure that persons are not over-tasked which could lead to errors and potentially mission failure.

- **Initial Certification and Recertification**

  Once the roles are defined, a certification standard should be developed for each position required to operate or provide engineering support to the satellite. Subject matter experts in each position are best equipped to develop that standard.

Certification should occur after a thorough training plan is completed; a written test is administered that tests the person's knowledge in all common and positional tasks as well as an on-console observation covering a select number of basic tasks the person should be proficient in. It is highly recommended that the tasks covered include all of the nominal tasks required to complete a contact but should also include an anomaly to measure the proficiency of the persons response to that scenario. It is highly recommended that the observation be performed in a simulator so that vehicle safety is not jeopardized by a new operator under the duress of an observation. Some programs may wish to institute a question and answer session (sometimes known as a Mission Brief) with the operations manager prior to certification. Since the manager is ultimately accountable for mission assurance of the program this gives them an opportunity to assess if the new operator is truly ready to be certified on their program.

Depending on the manning and daily battle rhythm of a program, certification of systems engineers and other supporting cast should be considered. Some programs do not have any dedicated systems engineering support while others have at least one engineer assigned to the programs to complete daily trending and to generate payload maintenance command procedures among other things. Examples of engineering task required for certification might be in tools such as Systems Toolkit (formerly Satellite Toolkit), MatLab or your ground system (e.g., OS Comet, Epoch, AstroRT etc). It is also recommended that if there is a dedicated systems engineer they should be certified in a flight operations position as well.

Recertification may be required for individuals or the entire operations crew as a result of operational errors, long absences, major ground system changes, or the addition of new satellites. Recertification follows the same principles as initial certification but may be more limited in scope.

- **Proficiency Training**

  Proficiency is mastered through practice. Simulations and rehearsals of routine and contingency operations are highly recommended as a way to prepare a team's proficiency for handling various situations they may encounter during a shift. This is especially important for missions that are unique and require specialized training to ensure the team is proficient in all required tasks. Proficiency leads to discipline which decreases risk to the mission and vehicle. Periodic recurring training on critical tasks is recommended to maintain proficiency for long duration missions. At a minimum, proficiency training should focus on:

  - Changes to procedures or to the ground system
  - Tasks that do not occur on a fairly regular frequency (e.g., contingency operations)

- **Operational Errors**

  When operational errors occur there should be a thorough investigation that includes interviewing everyone involved, aimed at determining the root cause of the error, and what actions need to be taken to prevent the error in the future. Focus areas should be:

  - Operations environment
  - Operator training/experience
  - Unclear processes/procedures/documentation
  - Ground system/tools

Corrective actions may include:

- Individual retraining and recertification
- Team training
- Process/procedure change and training
- Ground system/tools change and training

- **Intervention (out of plan)**

  Out-of-plan intervention should not be taken lightly. It is a serious matter when an operations team encounters situations that may require manual commanding that has not been pre-planned. Some programs may allow persons to respond to predetermined anomalous conditions by allowing approved contingency commanding if certain conditions present themselves. This out-of-plan intervention is rare but can be used if thoroughly trained and evaluated for proficiency.

  It is recommended that out-of-plan activities be developed to ensure the activity can be effectively executed by the operations team. During the development of these out-of-plan contingency procedures it is imperative that they be tested on a simulator to ensure that the operations team can perform the procedure. There may be constraints (such as time) that will prevent the operations team from executing the procedure. These type of nuances need to be flushed out before the procedure is approved and passed to the training staff for implementation.

- **Training Documentation**

  Well written documentation is the foundation for an effective training program. Programs that lack good documentation put their systems at risk due to the potential for ambiguous interpretations of how the system works. The end goal for documentation should be to ensure that the entire program team is operating from the same reference source documents to ensure vehicle safety and mission assurance. These documents should also be managed under configuration control to maintain currency and correctness.

  As mentioned earlier, programs should develop detailed operations manuals for satellites and ground systems. These documents should be written with enough detail to allow operations personnel to use them to develop their personal knowledge of the systems, and create effective tests and training plans. For example, if the operations team or systems engineers will be performing pre-launch ground to satellite compatibility testing, they will need documents that they can reference that are written with enough detail to fully understand how the satellite and ground systems interface with each other so that the system can be properly tested. This also allows the operations team to develop well referenced procedures for various satellite operations activities.

  Development of training materials such as slides and handouts should be developed covering all subsystems of the satellite and ground systems. The slides should summarize details in the comments section of each slide.

  Tests and observations should be developed from the approved operation manuals. It is not recommended to expect persons to use ambiguous knowledge to answer test questions. Each question should have a well documented reference from an operations manual.

All program members (flight operations team, engineering, management, etc.) should have full access to all approved training material and operations manuals. This ensures that everyone can reference the same documentation when questions arise and they all should get the same answer.

- **Training and Certification Records**

  Documentation of each operations team member's training should be kept on file for the duration of their tenure on the program. These records are critical to managing the proficiency of the team and should be complete and accurate. Records should document initial training, certification tests, and observation results, as well as all recurring training activities.

  Records are useful if a person commits a personal error to determine whether or not they were properly trained and proficient in the task. Records should include a master task list which lists all of the tasks the person is expected to perform proficiently and include a reference document/paragraph so the person can easily find the learning material they need to train for the task. Once the person is confident that they can proficiently execute the task they should sign off on that task after they have been tested or observed completing the task proficiently by a subject matter expert/observer. The subject matter expert/instructor or lead should also verify the person can proficiently execute the task and sign off on the record.

- **Training Resources**

  Resources to help train the team should be identified and scheduled early as the program develops. Here is a list of suggested resources:

  - Lectures provide a professional training environment for personnel.
  - Satellite integration and test offers hands-on opportunities for the team to actually see the hardware and help test the vehicle. This is a critical part of the program development and is invaluable in making sure the team thoroughly understands the satellite.
  - Simulators are not always budgeted for, but are highly recommended. Ideally, a high fidelity simulator is desired which allows trainers to introduce anomalies and allows persons to analyze telemetry; send commands; and practice routine, as well as new command files to ensure they understand what to expect each time the command file is used in real time.
  - In addition to the operations manuals, it is recommended to have the "as built" documents available for the team in the event they have questions that are not covered in the operations manuals.

- **Recurring Training**

  Recurring training:

  - is critical to maintaining proficiency.
  - ensures that the team is exposed to non-routine and/or contingency activities that do not happen often but may require a proficient response at anytime.
  - should be considered an ongoing process that is routinely scheduled and administered.

The following are specific times when ad-hoc recurring training is recommended:

- When an operations team member or engineer commits a critical error, the entire operations team and systems engineering team may need to be trained on what happened and how to prevent it from happening to them.
- Anytime a change to the system is made. Personnel should receive training on anything that the operations team or systems engineering will use that has changed. Hardware upgrades, software changes, new procedures, command files are all example candidates for recurring training.

3.1.2.2 Exercises, Simulations, and Rehearsals

Exercises, simulations, and rehearsals of the entire operations team, or even part of it are powerful tools for ensuring readiness to accomplish launch and early orbit activities as well as other complex activities throughout the life of the mission. Exercises are typically less formal events focusing on a particular function or interface of the overall mission with just a portion of the operations team. They are used to assist in definition of operations concepts and procedures. Rehearsals and simulations are more formal events with the goal of running sections of each mission phase with a full team focusing on the integrated activity. Final launch rehearsals with the launch vehicle provider may be very formal with the goal of validating the launch countdown and early orbit timelines and demonstrating that the operations teams are ready for these events.

Rehearsals and exercises accomplish the following objectives:

- Focus the operations team, including any participating engineering support and mission management, on the activity to establish/practice team roles and responsibilities – basically "practice makes perfect."
- Validate and/or determine required changes or limitations to processes, operations tools, operations products, procedures (both normal and contingency), operations concepts, and HMI.
- Verify/establish timelines for accomplishing the activity during real-time contacts and series of contacts as needed to run mission operations.
- Reduce on-orbit risks by exercising and enhancing the satellite, ground system, and operations and engineering teams that will be supporting the mission.

A minimum of two exercises and/or rehearsals is the best practice for launch and early orbit operations, especially if this is the first vehicle for an operational system. The second exercise or rehearsal provides an opportunity to practice any changes made as a result of the first exercise or rehearsal. The last simulation or rehearsal should be held within 30 days of launch. At least one event should include anomalies and contingency operations with the goal of exercising the processes and operations concepts.

As much as possible during exercises and rehearsals, the operations team should utilize the actual operations concepts, products, processes, and procedures that are or will be used on-orbit.

For other complex events one exercise should be sufficient unless the team determines significant rework is required.

Each rehearsal or exercise should have a clear set of objectives established by leadership and provided to the team responsible for developing and presenting the event. In the case of launch and early orbit the objectives of a single event should stem from the objectives of the overall readiness campaign. The operations team should also establish a process for the capture, review, and disposition of observations from the event. Some observations may need to be corrected during the event whereas others can wait until after. The team may also want to conduct a review of the event with the participants immediately post event, as practical, to capture feedback through open discussion.

If at all possible the highest fidelity simulation available should be used. Exercises and rehearsals should also be accomplished in as near real-time as possible. However, time jumps may be necessary to accomplish all of the objectives. In addition, when using simulation, the introduction of anomalies should not be announced allowing the team to discover the anomaly as they would on-orbit. This provides the best environment to validate command procedures and HMI. The event development team should, if at all possible, dry run the event to include contingencies with the simulator to ensure that the execution of the event will be as smooth as possible.

3.1.3 Command Planning and Execution

Two critical operations processes are command planning and command execution. Command planning involves defining on-orbit activities to be performed then generating and verifying the commanding products needed to execute those on-orbit activities. Command execution is the real-time process of transmitting commands or uploading data to the satellite. Best practices for command planning ensure that the planned procedures and commands contained therein will accomplish the required objective. Best practices for command execution ensure that the commands that are sent to the satellite are correct and in the proper sequence.

3.1.3.1 Command Planning Process

- **Purpose**: Critical to command planning is ensuring that the commands and command sequences planned will accomplish the desired outcome whether it is for a routine activity or for a critical or anomaly resolution activity. The majority of command procedures should be predetermined and developed even before launch while others may need to be developed quickly to diagnose or resolve unexpected issues. Command planning ensures that the commands to be used are appropriate for the situation.
- **Roles**: Operations engineer, ground system engineer, subsystem engineer, systems engineer, flight software engineer.
- **Responsibilities**: Operations engineers and satellite engineers determine the command procedure or sequence of command procedures and command parameters needed to accomplish a specific objective. These may be prescribed in the operations manual, developed as part of the near-term planning process, or determined in real-time as in the case of unforeseen anomalies. Operations and satellite engineers verify procedures and commands via simulator or in factory satellite.
- **Entry Criteria**: A commanding activity is required.
- **Inputs**: Satellite current configuration, activity to be accomplished, desired outcome of activity, potential contingency off-ramps.
- **Exit Criteria**: Prior to accomplishment of a specific activity, verify that the selected command sequence and required command parameters will achieve the desired outcome. Ensure the command sequence is reviewed and approved by relevant subject matter experts and operators. Some activities may require combining several individual command

procedures and individual commands in proper sequence. This overall sequence should be treated as if it is a single command procedure for purposes of review and approval:

- In cases where commanding is to diagnose and/or resolve an on-orbit anomaly; assess the risk to the satellite or mission to understand how the commanding could adversely affect the situation.
- Select commands and/or command sequences that have the highest likelihood of achieving the desired outcome.
- If possible, include recovery contingencies that can re-configure back to the initial configuration.
- Document and control the overall sequence if the activity requires combining several individual command procedures and/or commands.
- Commands with variable parameters should be independently verified against the approved command procedure prior to execution.
- Verify command sequence and contingencies through testing unless a time-critical response limits the time and resources available.
- Automated sequences should be verified through testing using the same degree of automation that will be used in operations.

Approval to accomplish the command sequences should be received from the appropriate level of management applicable to the situation. For example, normal command sequences may be approved by the operations lead on-shift, whereas a new contingency command sequence may require approval by an anomaly review board and operations configuration control board.

- **Outputs**: Approved and verified command procedure and verified command builds.
- **Best Practices**: The operations team follows a planning and approval process for each satellite commanding contact. The degree of review by subject matter experts and testing via simulator is defined in the process based on the nature of the activity from routine to complex and anomaly resolution.

  Command sequences for all known routine, complex, and contingency operations are defined by developers and operators, documented in formal controlled documents, and verified via testing.

  - Activity examples: routine state-of-health, deployment of wings and antennas, anomaly resolution.
  - Document examples: On-Orbit Handbook, “pre-canned” command procedures.
  - Testing examples: simulator and in factory satellite.
  - After development and test and before use on an on-orbit satellite ensure documents and command procedures are under configuration management control. Establish a change control process.

  For all but the most routine commanding at least two knowledgeable operators or operations engineers should verify command builds. Verification should be documented.

Ensure a process is in place for review and approval of near-real-time and real-time changes (red lines) to command procedures.

Ensure post execution review of results and determine need for further commanding.

- **Special Considerations**: In addition to fidelity, the availability of a simulator in a time critical situation may prevent use of the simulator to verify a command procedure before it is needed. Even if the simulator does not provide full command verification it may still be of value just to verify the command is accepted.

3.1.3.2 Command Execution Process

- **Purpose**: Verify that the commands to be transmitted match the approved command procedure and are sent in the approved order.
- **Roles**: Operator, operations engineer.
- **Responsibilities**: The operator is responsible for transmitting the required commands to the satellite. The operator, operations engineer, and/or supporting engineering team should verify that the commands execute properly on the satellite in real-time or are stored onboard for later execution.
- **Entry Criteria**: Approved command procedure is available and satellite contact is scheduled.
- **Inputs**: Approved command procedure with variable command parameters defined. Commands with variable parameters built and verified.
- **Exit Criteria**: Commands have been uploaded and verified according to approved command procedure. The approved command procedure has been executed successfully.
- **Outputs**: The planned activity has been successfully executed and the satellite is in the desired state.
- **Work Instructions**: During execution of non-automated procedures verify that the commands or command names entered by the operator match those in the approved command procedure. If variable parameters are entered in real-time, they should be verified prior to transmission as well. Independent real-time review and approval to transmit is best practice. Complex/Critical activities may require real-time review and approval by subject matter experts prior to transmission to ensure proper timing and functionality of commands.

  Ensure verification of command functionality and logic flow are followed in accordance with the approved command procedure. In some cases functional verification of each command after it is transmitted may not be appropriate or possible and verification must wait until a specific sequence is completed.

  Ensure commanding activities can be completed in the time frame of the scheduled contact. In some cases, such as low-earth orbiting satellites, there is a small window to accomplish commanding operations and the operator must be focused on completing commanding objectives as efficiently as possible.

- **Best Practices**: Complex and/or critical command sequences should require two-person integrity to verify the correct command or command sequence is being executed prior to transmittal.

Documentation of the contact execution is important to clarify which commands were successfully uploaded and which were not.

- **Special Considerations**: Automated command sequences may prevent two-person integrity prior to transmission of each command. In this case the initiation of a command sequence may require two-person integrity.

3.1.4 Trending Identification, Compilation, and Analysis Process

Satellite telemetry data is routinely collected to evaluate the onboard performance of flight hardware, software, and instruments.

- What trending information is required to assess vehicle health and performance prior to launch?
  - Development of pre-launch trending information is critical to ensuring the readiness of the satellite for launch. It is important to construct a perceptive list of critical items to be trended during ground test operations. The spacecraft manufacturer usually adopts a standard list of trending data points for the satellite during development and test and updates this list for on-orbit operations. The satellite contract may also call out specific requirements for trending to be tracked and passed along to operations. This list is then used to transfer useful trend information from ground observations to post launch commissioning and all the way through vehicle on-orbit operations.
- What trending information is required to assess vehicle health and performance post-launch?
  - Development of post-launch trending information is critical to ensuring the performance of the satellite. It is important to construct a perceptive list of critical items to be trended during acquisition, commissioning, and nominal mission operations. During first acquisition and commissioning the correlation of trend data back to the pre-launch trend data must remain consistent in order to provide an insightful data set required for nominal operations commencement.
  - It is suggested that analytical tools be developed and packaged as part of ground based controller concept of operations (CONOPs) to monitor these trend points with a focus on predictive capabilities. Using pre-launch data coupled with post-launch data should afford the operations team the insight into both current and potential long-term health of operations capabilities.
- What trending information is required to assess vehicle health and performance after an anomaly has been observed and the satellite has recovered?
  - The application of additional trending data post-anomaly investigation is critical to future post recovery efforts. The data added should consist of any data not already identified on the trending schema identified during pre-launch and post-launch operations. This data should be specific to provide additional insight into any areas that might provide recovery information in addition to predictive insight.
  - If a satellite were to experience an anomaly requiring change to nominal operations established in the baseline CONOPs, the configuration changes required to facilitate return to mission operations need to be identified. These identified critical telemetry points should correlate with data useful to the operations team, controllers, and subject matter experts that are responsible for evaluating operational capabilities post-anomaly.
- How often should satellite trending data be reviewed by an engineering team?

  - Trending data should be reviewed by an engineering team on a periodic basis, as determined by the type of data, to confirm trends are as expected. When unexpected trends are identified the engineering team can begin looking at additional satellite data to understand the cause and determine whether it could be an early sign of a hardware failure. The sooner the unexpected trend is discovered and the cause determined, the sooner the discussions can begin on whether mitigation steps or operational workarounds need to be taken to minimize on-orbit risk to the mission. The engineering team can also start investigating options and steps that can be taken in the event of a true hardware failure; thus increasing the likelihood that the satellite can be recovered faster. Recovery time may take longer if an engineering team is not available to review data on a periodic basis because they will need to come up to speed and perform a detailed data review when an unexpected trend does occur.

- **Purpose**:
  - Baseline trending data for the satellite are collected to support the analytical assessment of the satellite. Trending data can be compared to specific component or subsystem models and simulations to evaluate effects of the space environment. Analyses that draw upon the archived trend data are performed to support the investigation of anomalies and to investigate health and safety data that trend beyond expected limits (particularly if it threatens satellite health/safety).
  - Initial values for satellite trending are obtained during I&T and initial on-orbit checkout. Thereafter, the baseline satellite trending data are established through periodic collection and archive of selected satellite data. Initial parameters for payload trending are established during I&T and checkout of each payload. Thereafter, baseline payload trending data are obtained through routine maintenance and calibration of the payloads, according to test sequences specified in the operations procedures.
  - Collection of baseline trending parameters for the satellite continues throughout Initial on-orbit testing. At the conclusion of early orbit testing, the satellite baseline trending will be evaluated and will be the point of departure for future day-to-day and periodic trending. Baselines for seasonal trends will also be captured and evaluated throughout the programs on-orbit life span.

- **Roles**:
  - The satellite contractor should play the primary role in the development of the trending information. This information needs to be compiled from existing experiences on other satellites as well as trending information specific to any recent changes to heritage trending telemetry. The end users will also play a role in the development of trending information specific to long-term insight focused on nominal operations and preventive rich information gathering.

- **Entry Criteria**:
  - Suggested criteria definition should fall to items defined as required telemetry data points to trend and should include critical perceptive telemetry that has both a high real-time sample rate in addition to having a heavy diagnostic focus.
  - Examples (bus current, motor current, motor torques, battery cell voltages, limited life items must always be included in trending data)

- **Exit Criteria**:
  - A standard set of trending reports are identified and provided and reviewed at regular intervals during on-orbit operations. Ground tools should be capable of generating the routine trend data reports and they should be made available for easy review by the operations and engineering teams.
- **Tools**:
  - Tools should be specific to the vehicle and the contractor developing that vehicle, but may fall into two specific categories. Category one would be the monitoring and collection tools required to gather trending data. Category two would be the analysis tools utilized to provide predictive inputs to the operations team capable of providing insight into coming problems.
- **Special Considerations**:
  - Every organization will approach trending in subtly different ways, and these differences will require oversight and agreement between the vehicle manufacturer and the end users.
  - Long-term management and archival of satellite data is a requirement that needs to be fully verified prior to launch. Having quick access to data for on-going trending as well as in the event of an anomaly can help to reduce on-orbit risk for a mission. If the tools are not well engineered or if they are not thoroughly tested before launch, issues can result for the operations teams. For example, if the archive data is deleted or the engineers are unable to get to it, this increases the mission's on-orbit risks. Since an on-orbit anomaly can manifest quickly and require a timely response, the ability to access critical satellite data quickly and generate new data plots becomes critical to making a timely and accurate response.

3.1.5 Reach-back

Reach-back is defined as the ability to access the factory subsystem and system experts to support the planning and execution of complex activities, the diagnosis and mitigation of adverse trends, and the investigation and recovery in anomalous situations. Although reach-back applies to both the preventive and recovery processes of satellite operations, it is primarily a preventive measure. Reach-back ensures the availability of factory satellite experts to safely plan and execute actions when accomplishing complex satellite operations or anomaly recovery. Reach-back can significantly reduce operational risk, and therefore improve mission success.

The program should ensure that there is a contractual vehicle for retaining and/or recalling factory experts to support operations when required. Factory experts are critical to failure diagnosis and development of further data gathering and recovery actions in unforeseen anomalous situations.

The operations team developing operations concepts and processes should define the roles and responsibilities of the factory experts in all applicable concepts and processes. This should include the method(s) of engagement such as working group participation, real-time execution support, and recall as appropriate.

Factory experts may be called upon to help develop and review operations products and even to directly support the execution of certain operations. If the factory experts are to support the execution of operations they should participate in any exercises or rehearsals of that activity.

3.1.6 Self Assessment and Feedback

- **Purpose and description**:

  Self assessment is the process by which an operations team reviews their performance in the execution of almost any activity and determines what worked and what did not. The emphasis in self assessment is on improving process execution and team coordination and decision making.

  Feedback is the process by which lessons learned in operations are fed back to the developer or other operations teams. The emphasis here is on capturing fixes or improvements to satellite and ground systems as well as processes.

  Self-assessment and feedback each have a twofold purpose:

  - Performance/process improvement
  - Future failure and/or error prevention

Each process includes:

  - Capturing lessons learned
  - Dissemination of lessons learned as appropriate
  - Modifying operations products as appropriate
  - Planning and execution of necessary improvement/preventive actions

  Self-assessment can be thought of as the tactical feedback loop where lessons learned are captured by the operations team and folded back into operations team process improvements and/or corrections. Self-assessment should be applied real-time and post-activity. In some cases preventive and corrective actions need to be taken on in-progress satellite operations. The operations team may even schedule semi- or regular- review sessions to review operations performance.

  Either through the self-assessment process or through root cause investigation of an anomaly lessons learned applicable to the developer are captured and fed back to the developer to determine and implement the required product or process changes. The organization must have mechanisms for capturing and disseminating the lessons learned for other on-going and future operations.

  The feedback loop may also apply at the enterprise level to ensure that the lessons learned are disseminated to other programs within the enterprise and even beyond.

- Inherent in these processes is that the root cause of an anomaly, or operational error, is understood before any preventive or corrective actions are taken. It is also a good practice to maintain all analyses for later comparison to new faults. There are cases where the root cause may be masked (such as two timers with incorrect values and only one are seen).

  Organizations will have multiple learning loops, as shown in the example in Figure 1, ranging from immediate, tactical learning within the current operations (Loop 1) to enterprise-level process improvements (Loop 4). This integrated process should ensure that lessons from anomaly investigations are integrated proactively with lessons developed through other independent or process assessments.

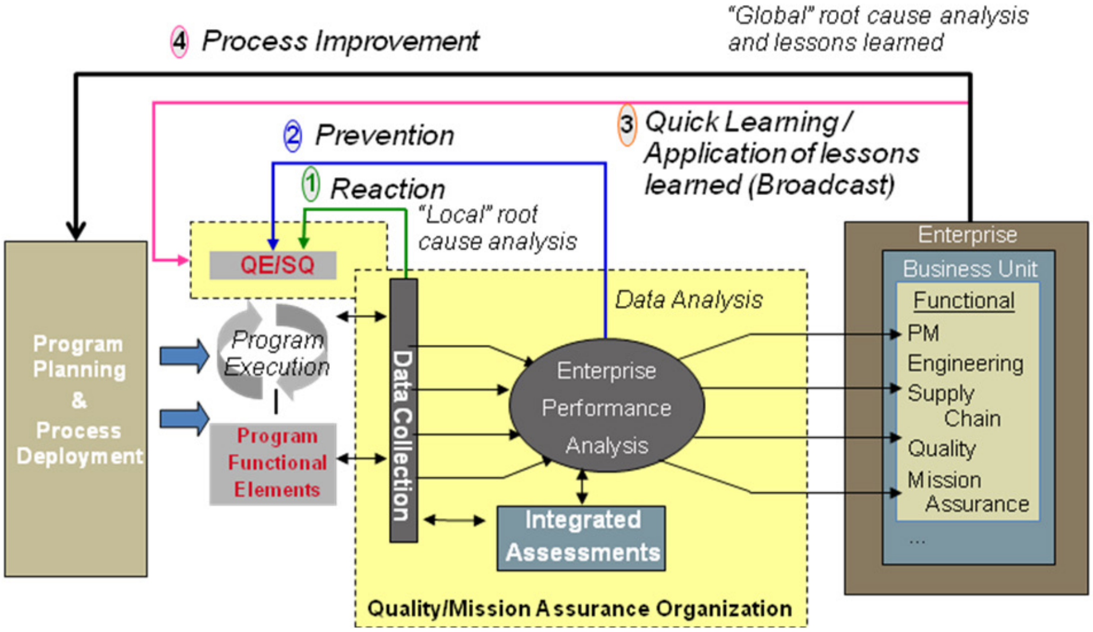

4 Process Improvement
"Global" root cause analysis and lessons learned
2 Prevention
3 Quick Learning / Application of lessons learned (Broadcast)
1 Reaction
"Local" root cause analysis
QE/SQ
Data Analysis
Program Planning & Process Deployment
Program Execution
Program Functional Elements
Data Collection
Enterprise Performance Analysis
Integrated Assessments
Quality/Mission Assurance Organization
Enterprise
Business Unit
Functional
PM
Engineering
Supply Chain
Quality
Mission Assurance
...

Figure 1. Self assessment and feedback process.

- **Process Flow**:
  - Several formal and informal mechanisms are used to flow operations lessons learned, both negative and positive, to the appropriate receiver.
  - The feedback loop starts with the record keeping. The operations team is responsible to document all aspects of the activity. This includes:
    - What happened
    - What the telemetry looked like, if applicable
    - How long it took
    - Impact anomaly, error, or positive action
    - Decisions made and steps taken to correct an issue or implement an action
    - Possible steps to take or not to take next time
    - Who was involved
    - What the issue or positive action was
    - How it was resolved or implemented
  - In the case of operational errors or actions the operations team then assesses the relevancy of the lesson learned to operational processes. If they determine changes are required then the appropriate change process is used to make and implement the change. The operations team, with assistance from the development team, also determines the relevancy of the lesson learned to developer processes.
  - In the case of a lesson learned that applies to a development process, such as database development, the developer determines if a change is required, and if so, flows the appropriate process to make and implement the change.

- In the case of an anomaly, the appropriate customer and or program processes should be followed to:
  - Determine, approve, and implement changes to the satellite, program fleet, or ground systems as appropriate.
  - Notify component vendors and/or other customers as appropriate and approved by the customer. Ensure approved notifications/alerts flow through formal channels and in line with legal and industry standards.
- In reality, there are multiple paths into and out of each leg of the feedback chain as shown in the example below. Which ones are used depends on the timing and severity of the anomaly. For example, an anomaly on a spinning satellite may not make it to the product line or program office if the company no longer builds them. On the other hand, if an operating procedure is found to be deficient, all legs of the feedback may be used.

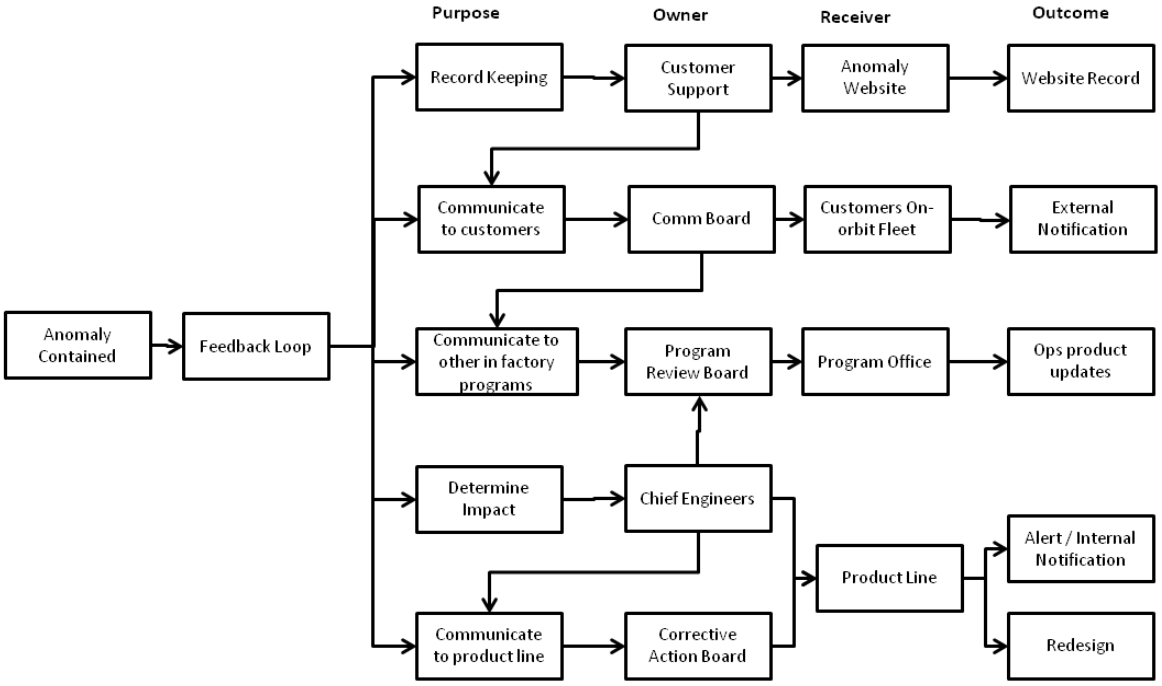


Figure 2. Typical feedback loop.

3.1.7 Configuration Management

- **Purpose**: Configuration Management (CM) is a critical aspect of satellite operations due to the complex, distributed, and redundant nature of space systems; coupled with their heritage that will typically include both new and legacy hardware and software, commercial and government off-the-shelf hardware and software; and complex interfaces to systems that may not be under local configuration control. The purpose of configuration management, then, is to have strategies and processes that identify and manage all configuration items in a system over the lifetime of a program. Configuration control must encompass satellite hardware and software, ground hardware and software, and operations products. Changes may be both planned (scheduled maintenance/updates uploads) and unplanned (corrective/anomaly responses). Any change to any of these components, regardless of whether they are planned or unplanned must be done under CM control and be pre-validated. The CM system must be both disciplined and flexible, to ensure consistency across all program elements, to accommodate simultaneous operations and development and multiple levels of access to the system hardware and software.

- **Roles**: Operations, sustainment, engineering, quality, and supply chain management all participate in a configuration management strategy that is developed and owned by a configuration management manager or organization.
- **Responsibilities**: Configuration management has the primary responsibility for establishing a CM strategy, captured in a CM plan, which encompasses the system lifecycle from development through operations and system retirement. Engineering will normally establish the development and sustainment environments in which the system is developed and operated. Supply chain management has the responsibility for ensuring adherence to the CM rules and deployment of the environment across the development and operations teams.
- **Entry Criteria**: A critical entry criteria is a hardware\software baseline that comprises the system hardware and software and all potential uploads to the satellite. Well-defined rules for validating any and all changes to satellite instruments, busses, or other elements must be in place across the enterprise.
- **Inputs**: Program plans, including incremental builds, early deliveries, concurrent operations; organizational and industry CM standards and best practices.
- **Exit Criteria**: Approved Change Requests.
- **Outputs**: CM plans, processes, training, audits, and budgets that accommodate concurrent development, operations, and sustainment across the enterprise.
- **Tools**: Configuration management tools can be commercial off-the-shelf or program developed but need to manage change requests that capture changes to the satellite, ground system, ops product, the impacts, testing results, and list of approvers.
- **Techniques**: Configuration management processes can be extremely formal or informal depending on the size and complexity of the mission. A periodic CM control board meeting may be needed to establish a routine where this is required or it may be scheduled only when needed. A real-time process needs to be defined to facilitate real-time changes that cannot wait until the next meeting time. The real-time process needs to include critical personnel, for example, operators, engineers, and management personnel, that are on-call to support a time-critical change decision.
- **Best Practices**:
  - A CM database should be created and maintained for the duration of the program so that all changes are documented and accessible in one place.
  - CM plan and/or crew procedures should provide procedures for how the crew should implement a mission critical change required outside of normal, day-staff duty hours.

3.2 Recovery

This section is organized into four main topics:

- Anomaly definitions and terminology
- Immediate response (Operations Crew)
- Investigation and recovery (Anomaly Response Team)
- Review and Disposition (Anomaly Review Board)

3.2.1 Anomaly Definitions and Terminology

- **Anomaly:** A system event which either threatens system safety or causes degraded performance.

  Anomalies may be discovered by noticing a deviation from established trends, a telemetry limit threshold is exceeded, a fault management action, by observing payload and S/C telemetry, or by a reported issue from the mission user.

- **Anomaly Classification**: Define the urgency of response required for an anomaly.

  Each program can tailor anomaly classifications based on program specific needs. This document provides a recommended approach based on NASA and USAF Space Command best practices. There are three anomaly classes ranging from A to C; A being the worst case and C being the most benign.

  Class A: The technical implications of the anomaly are not immediately known and a safe satellite cannot be declared.

  Class B: The anomaly represents a potential threat to mission operations and/or the life expectancy of the satellite.

  Class C: The anomaly represents no significant risk to satellite and has minimal impact on the mission.

Table 1 provides a description of the satellite status for each class of anomaly and examples.

Table 1. Anomaly Classes

Anomaly Class	Satellite Status	Examples
Class A	Unsafe satellite (or unknown status)	Satellite bus voltage below critical limit and decreasing. Any other safe satellite criteria are violated. Loss of communications to the satellite for an extended period of time as defined by the mission requirements.
Class B	Unexpected mode change Potential unit or assembly failure	Satellite transition to safe survival mode. Payload transition to Off.
Class C	No mode change No apparent unit or assembly failure	Single bit error repeating in same memory location. Thermistor failure.

- **Anomaly Review Board (ARB)**: Management group responsible for approving Anomaly Response Team recommended actions and anomaly closure.
- **Anomaly Response Team (ART)**: The group of technical experts that investigate and resolve satellite anomalies.

- **ARB Action Item**: Generally associated with long-term responses to prevent future instances of the anomaly. ARB Action Item (AI) closure is not required to restore the satellite to an operational configuration. ARB AIs are generated after ART closure or are adopted as part of ART closure. ARB AIs are managed to closure by an anomaly lead (AL) or coordinator.
- **ART Action Item (AI)**: Generally associated with short-term responses in order to restore the satellite to a sustainable state of operation. ART AIs are generated and managed to closure by the ART as part of a specific anomaly investigation.
- **Contingency**: As used herein, refers to satellite or ground anomalies/faults for which a pre-planned response is prepared .
- **Faults**: As used herein, refers to specific Level 1, 2, or 3 faults as defined in section 8.2.3 satellite faults.

  Satellite faults are detected and responded to by on-board fault managment (FM) software, provided that the FM is enabled to monitor and respond. Appropriate FM is either enabled autonomously by flight software or by ground command. The ground system may also detect satellite faults and in some cases command a fault response.

  Satellite faults include spacecraft bus and payload faults. Satellite faults can be detected either during real-time contacts (latched fault flags in telemetry), or by playback of recorded data.

  The most important initial step for the operations crew is to assess and ensure that the satellite is safe, and if not, to take action to save the satellite. In most cases, the on-board fault management software algorithms will have taken the appropriate actions to safe the satellite; the initial response for an on-duty engineer or crew member is to notify the lead engineer, confirm satellite health and safety, and after ensuring that the satellite is safe, attempt to determine the cause of the fault (Fault Level and Fault Title are latched and in real time telemetry). These activities generally will include downloading stored data from spacecraft recorders and/or dumping predefined spacecraft processor memory regions.

- **Initial Response**: The immediate actions required and taken in order to safe the satellite.
- **Off-nominal Condition**: An off-nominal condition is a phenomena, behavior, or condition which imposes no immediate danger or degradation to the satellite and may need further study. Further study, if warranted, will determine if the off-nominal condition should be a watch item, is an unexpected result, is a maintenance issue, is an anomaly, or is not a concern.
  - Ex: temperature higher than expected but below red limit

  If the off-nominal condition becomes a watch item, an Ops Alert should be generated to provide the operations team with instruction.

- **Probable Cause(s)**: The most likely event(s), as determined by data and analysis, which could have caused the problem.
- **Problem Statement**: The active failure (or fault response) resulting in the anomalous/unexpected indications.
- **Recovery**: Configuration changes made to restore normal operations after the satellite is considered safe and stable.

- **Recurring Anomaly**: An event or condition which has been previously experienced and analyzed by an ART. The primary cause (active failure) of a recurring anomaly has been determined and no further corrective action is planned. The anomaly documentation has been completed and closed. The ART or ARB has authorized specific actions in response to the recurring anomaly so an ART or ARB is not required to approve executing the authorized response. The entry conditions into the anomaly response are specific and documented from ART or ARB.
- **Root Cause**: The event, as determined by data and analysis, that ultimately caused the problem. Eliminating the event would prevent the problem from occurring.
- **Satellite Emergency**: Unexpected or serious situation that will, without prompt action, result in mission loss or degradation of the satellite. This includes impending loss of the satellite and/or permanent loss of the satellite's primary payload.
- **Unexpected Result:** An unexpected result is a condition or behavior of the system, hardware or software, that causes a failure or degradation in performance.

  Unexpected results can be described and defined a priori for each program and documented in the system on-orbit handbook during design and test for use by the operations crews after launch.

- **Ground System Technical Issue:** A ground system technical issue is an issue which is known to be related only to ground equipment. The satellite may not be at risk although there may be a temporary loss of command and/or telemetry capability due to ground problems. Planned/scheduled operations may be disrupted and may need rescheduling.

  Ground system technical issues may be identified during routine scheduled ground system maintenance, deviations from established resource trends, real-time observations, or analysis and investigation related to other issues.

  The process for handling ground system technical issues is to first confirm the issue is a true ground-related issue. Ground communication, telemetry, cryptographic gear and telemetry display system functionality is confirmed through the use of ground operations procedures. If the issue is isolated to the ground system (including ground terminal site issues whether organic or shared) versus an aberration (such as a temporary telemetry drop-out), it should be determined if the issue presents a near term impact on planned satellite operations; if so, it should be immediately reported so that management can assess the impact to planned activities, reschedule as necessary, and remedy the issue.

  Any ground system technical issue should be assessed as to whether it requires additional investigation, reconfiguration, or maintenance, or is simply an issue to watch for further change. There can also be components of the ground that service the "mission" of the satellite and operate far from the operations staff in a "lights out" facility. Remote telemetry from the facility can inform the operations personnel of pending problems where corrective action (such as switching to a backup on the ground) can be taken.

  Most systems have a process for capturing ground system technical issues; e.g., problem reports if the issue causes an interruption in operations. It is important for the operations crew to document and trend issues so that corrective and preventive actions can be identified and implemented.

3.2.2 Immediate Response: Operations Crew

- **Purpose:** Define the conditions and procedures to diagnose an issue and/or establish a safe satellite configuration in the event of unexpected indications or inadvertent actions.
  - Define indications of a safe satellite that operations crews can confirm and monitor during satellite contacts.
  - The basic six criteria for assessing if a satellite is safe are:
    - Good telemetry downlink
      - In view: telemetry believable and updating correctly
      - Out of view: no faults indicating telemetry will not be available at next contact
    - Good command uplink
      - In view: command link verified
      - Out of view: no faults indicating command capability will not be available at next contact
    - Rates and attitude errors understood and under control
    - Power understood and under control
    - Thermal within limits or exceptions understood
    - Payload(s) is safe: the criteria for verifying a safe payload are:
      - Power understood and under control
      - Thermal within limits or exceptions understood
      - Other system unique safe payload mode factors should be added as applicable to the specific mission requirements
  - Additional elements can be added to safe satellite checklist based on unique subsystem/payload requirements.
- Identify necessary telemetry for future investigation
- Establish notification requirement protocols
- Define pre-authorized crew actions for immediate response to an anomaly to confirm/establish a safe satellite and to collect data to support the anomaly investigation. At a minimum, these procedures should cover:
  - Entry criteria for pre-authorized response actions – safing. These should be as unambiguous as possible to preclude inadvertent/incorrect response.
  - Actions to accomplish if entry criteria are met.
  - Initial data gathering actions – downloading stored state-of-health data ASAP.
  - Criteria for declaring a satellite emergency.
  - Actions for responding to a satellite emergency.
- Define reconfiguration actions operators should initiate based on observed telemetry (this may include actions for non-anomalous conditions to include unexpected results or observed trends/non-alarm events as preventive and/or precautionary measures (i.e., re-orienting the vehicle for specific points-of-interest demands just received or because there is some action

to be taken as a result of anomalous conditions on another vehicle, in response to trending analysis)

- **Roles**: Operations crew, satellite engineer (for case of observed deviations from established trends)
- **Responsibilities**:
  - Verify safe satellite
  - Exonerate ground system as applicable
  - Execute authorized procedures to safe satellite and/or reconfigure as necessary
  - Declare a satellite emergency as applicable (this declaration can be used to alert other agencies/users to a mission impact and also raise priority of support for ground terminals and/or space communication relay providers)
  - Initiate the anomaly call-in process
- **Entry Criteria**:
  - Satellite or ground system issue
  - Observed deviation from established trends
  - Observed red alarm limit
  - Others as defined by each program
- **Inputs:**
  - Real-time telemetry displays
  - Archived telemetry
  - Operations manual
  - Operations procedures
- **Exit Criteria**:
  - Anomaly notification complete
  - Safe satellite established
- **Outputs:**
  - Command and telemetry logs
  - Down-linked recorded telemetry and processor memory data
  - As-executed operations procedure checklists
- **Work Instructions**:
  - Verify telemetry link
  - Verify nominal attitude control
  - Verify nominal power profile
  - Verify nominal thermal profile
  - Verify command link (most commonly by sending a no-op command to the satellite)
  - Verify payload health and safety

  - Dump recorded telemetry and on-board processor memory
  - Activate notification process and convene ART
- **Tools**:
  - Automated scripts to be run at the start of contact and/or periodically when in contact to verify telemetry for safe spacecraft/payload. This is intended as a job aid for the operations crew and not a replacement of visually monitoring telemetry. Because there are many telemetry points across multiple pages, this aid can expedite the determination of safe spacecraft/payload.

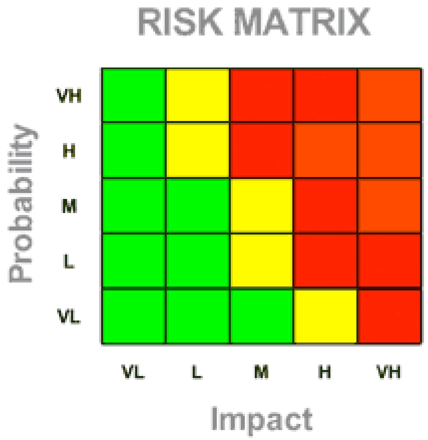
3.2.3 Investigation and Recovery: Anomaly Response Team (ART)

Investigative flow for anomaly response does not need to be heavily prescriptive, and is likely a similar flow to a pre-launch Failure Review Board structure employed by the satellite contractor. There are items and decisions points, however, that are to be considered required. An example of this type of item is the application of an Ishikawa Diagram (fishbone) to identify issues and determine root cause through interpretation of items categorized as part of the Ishikawa Diagram development process. Another example is the evaluation of telemetry to assess pre- during- and post- anomaly observed/measured information. Examples of decision points is determined by the operational construct and operation control authority, but should include authority to investigate, change satellite configuration, and implement suggested actions as well as development of a trade matrix illustrating recovery actions against impacts.

Participants will be determined by operational authority and will likely follow the construct of specific command authority. The participants should include as voting/decision authority ART lead, technical lead, mission assurance manager, command lead and/or customer representative. Participants that are necessary, but are not granted voting authority, would include factory and operations team subsystem subject matter experts, controllers, customer technical representatives, and command personnel.

Documentation should include, at a minimum, Ishikawa Diagrams, an investigative documentation package (used to capture any/all discussions and directions relating to investigation), ART meeting minutes, trade matrices (used to capture all the actions being traded for impacts to satellite) and configuration change instructions.

Risk determination is another process that can be used as a tool during anomaly investigations conducted on a satellite. This tool provides the probability and impacts possible for all prescriptive actions taken to both recover from the anomaly and re-establish nominal operations. The risk assignment method should align with whatever methodology and/or product is used by the satellite control organization. Levels assigned to facilitate risk ratings should be prescribed by the satellite customer/owners. The most common format for risk evaluation and assignment is a 5 by 5 Risk Matrix (see Figure 3) and serves to associate a numeric value to probability and impact.



Probability \ Impact	VL	L	M	H	VH
VH	🟩	🟨	🟥	🟥	🟧
H	🟩	🟨	🟥	🟧	🟧
M	🟩	🟩	🟨	🟥	🟧
L	🟩	🟩	🟨	🟥	🟥
VL	🟩	🟩	🟩	🟨	🟥

Figure 3. Risk matrix.

- **Purpose**: Provide a systematic approach for investigating anomalies to determine probable cause, preventive and corrective actions, and subsequent recovery steps for returning to full or degraded mission operations.

  The ART is a tactical technical team with a focus of restoring the satellite's operational capability. The ART will determine the cause of the anomaly and will generate briefings to document and report to the ARB. The ART will confirm restoration of satellite operational capability once recovery has been approved and implemented. The ART will recommend closure of Class A and B anomaly to the ARB once cause has been determined and the anomaly no longer impedes satellite near-term operations.

  The satellite Fault Management (FM) design is such that most satellite anomalies will manifest as level 1, 2, or 3 faults or as payload faults. Once the operations crew detects fault occurrence, they will determine the level and/or severity of the fault from telemetry.

  When formalizing/documenting ART findings, fault diagnosis, and the recovery plan, the anomaly lead will get concurrence from each ART team member present, or note any member's lack of concurrence or concerns, before proceeding with recommendations/findings to management. Actions directed to the operations crew will be documented in the appropriate form for requesting the action of the crew. Concurrence may be gained verbally in order to act quickly. Such action will be followed up by documenting the agreement.

  The ART develops a recovery plan after the anomaly is understood to the point where a course of action can be developed. The intention of the recovery plan is to restore the satellite to normal operations to the extent possible, as soon as possible, and when safe to do so. Any configuration changes to a safe and stable satellite must be approved by the ARB. The ART recovery plan may also include recommendations regarding long-term operations of the satellite. Goals of these recommendations are to minimize impact of the anomaly on mission performance, reduce satellite risk, and maximize satellite life.

  The recovery plan must be comprehensive, including any process or documentation changes required. If a faulty component has been identified as the cause of the problem, then the recovery plan will exclude the use of this component in the future. Any flight software or on-board stored command sequences that call, use, or configure faulty equipment will need to be modified to use non-faulty equipment.

After the ART has received approval, the recovery plan and associated products must be simulated and/or tested as required. Testing should be accomplished using the highest fidelity venue available. Initial conditions should be modeled as closely as possible to the actual satellite conditions. Initial conditions should include the following, as applicable:

- Flight software
- FM detect and response status
- Payload software configurations
- Equipment status
  - Attitude and navigation
  - Power
  - Thermal
  - Propulsion
  - Payload
  - COMMS
  - Other

New products should be CM controlled. Training packages should be generated and instruction and simulation provided to the operations crews.

The recovery plan and/or procedures should be rehearsed if time permits. Resources such as personnel, contacts, external resources (e.g., ground terminals, space communications relays) must be scheduled.

Direction to the operations crew to implement recovery action, after approval by the ARB approver delegates, is documented in a procedure and/or applicable crew direction/information form.

The ART should also consider the possibility of reach-across (and vendor notification), that is a similar or identical failure occurring on any “sister” satellites (i.e., a “systemic” failure). If this is a credible possibility, the ART should issue a preliminary alert to the operations team to warn of possible problems with the “sister” satellite and recommend possible preventive action or mitigation. This information must also be captured in lessons learned and fed back to concurrent and/or future block developments of the system as a preventive action.

The anomaly lead proposes closure of the ART once the satellite has returned to “operational” usage for the immediate future and all associated reporting and documentation has been completed. The ART may be closed with liens, such as closure of outstanding issues and action items to be dealt with in the Anomaly Review Board (ARB) closeout package.

- **Roles**: Spacecraft and/or payload lead, satellite systems engineering lead, and subsystem experts meet with the ART. Reach-back to factory subsystem subject matter experts is critical in most cases to determining what the most likely cause is and how to go about resolving. The program needs to ensure that there is a means to expedite factory subject matter expert engagement when the situation warrants.

- **Responsibilities**:

  Anomaly lead duties:

  - Track status of all anomalies and technical issues
  - Maintain an anomaly log, official list of all anomalies by number
  - Track technical progress of anomaly resolution teams (ART)
  - Track ART schedules for resolving anomalies
  - Ensure that ART generated material is maintained
  - Ensure schedules/milestones for report generation are met
  - Track author's report generation progress
  - Review anomaly reports, subsystem reports, cover letters and briefings for completeness, consistency, clarity, format, signature requirements, etc.,
  - Develop/update anomaly closeout package for ARB
  - Manage distribution of anomaly reports for those anomalies closed by ARB
  - Update anomaly log; post to shared data center
- **Entry Criteria**: The observation and/or identification of an unexpected or non-nominal state
  - Red Limit Responses
    - Data points that exceed critical limits are monitored in telemetry by ground software and displayed on-console.
    - The operations team will have predefined actions for key red limits. Most of the responses will be one of the following:
      - Execute a specific procedure
      - Expect a specific response and monitor (ex: Do nothing, and expect a level 3 failover to occur autonomously.)
      - Contact a technical specialist
  - Satellite fault identification
    - Satellite faults are detected by on-board flight software monitors and responded to by on-board Fault Management (FM) or by ground command. Each system will have a series of increasingly more severe fault levels. An example of a 3 fault level system follows:
      - Level 1 faults
      - Level 2 faults
      - Level 3 faults
    - The Level 1, 2, and 3 faults are briefly described in the next section. Crew procedures should include authorized contingency procedures to respond to Level 1, 2, and 3 faults.

    - Level 1 Faults:

      Level 1 fault conditions have minimal or no permanent impact on satellite health and generally allow the satellite to continue operations in support of mission objectives. Mechanisms exist on-board either to fix or workaround the condition and provide a status indicator to ground operations that the condition occurred.

      The majority of Level 1 fault flags are intended to be "FYI" regarding a transient condition; and for many Level 1 faults, if the transient condition persists, the fault becomes Level 2 or 3.

    - Level 2 Faults:

      Level 2 fault conditions do not impact the power, thermal, or stability conditions enough to endanger the satellite, but may be severe enough to require reconfiguration of on-board equipment. The Level 2 FM response may place the satellite in a safe state, but the satellite will remain in normal operational attitude configuration (e.g., Nadir pointed).

    - Level 3 Faults:

      Level 3 faults conditions may result in the loss of the satellite if not commanded to a safe state by FM or by ground command if FM is not enabled. Upon detection of a Level 3 fault, FM may sequence the payload into a standby or safe powered-off configuration. The Level 3 FM response may also trigger partial or full load shed depending on the situation.

      For non-geosynchronous spacecraft, it is more likely that satellite anomalies will occur out of view due to the limited amount of time spent in view. Therefore the team may have to respond to a failure to acquire the satellite when it should be in view. First actions upon failure to acquire signal should be to exonerate the ground system and communications path between the ground station and the spacecraft.

- Payload Anomalies

  Most payloads have FM capability which monitors and autonomously safes payload boxes when critical out-of-limit (OOL) conditions are detected. Established contingency operations procedures should allow the ground operators to disable payload functions and safe the payload via ground commanding when an issue occurs that does not trigger an automated FM response or where FM fails to respond as expected.

- Deviations from established trends

  Deviations from established telemetry trends might be identified over long periods of time. Discussion between support engineers and operators takes place once a deviation is identified.

  A deviation should be classified as an anomaly if the deviation affects satellite health and safety or the mission (i.e., degradation of performance).

  It is particularly important to recognize deviations from nominal trends for parameters which are approaching a critical OOL condition. Mitigation by ground intervention may be possible and should be investigated if it is apparent a critical OOL condition may occur in the future.

Deviations from established trends should be logged and kept on a watch list. They should also be assessed by technical specialists as to severity and potential impact to normal and test operations. The deviation should be briefed at crew changeover to ensure continued vigilance. Operators or satellite engineers may be specifically tasked to monitor the deviation, and subsystem engineers should be updated as to status.

If it is determined by the appropriate technical specialists that the deviation does not affect satellite health/safety or mission performance, then the investigation may be closed and documented.

- **Inputs**:
  - Satellite processor memory dumps and telemetry archives
  - Subsystem design manuals
  - Satellite/payload wiring diagrams
  - Command logs
- **Exit Criteria**:
  - Understanding of the sequence of events pre- during- and post anomaly
  - Recovery plan tested and executed
  - Mission restored to the extent possible
  - ART Action Items disposition
  - Lessons learned captured
  - ART package ready to close out to Anomaly Review Board (ARB)
- **Outputs**:
  - Interim and final paths forward
  - Completed ART package ready for submittal to ARB
    - Fishbone diagrams
    - Timeline
    - Anomaly summary
    - Completed Action Items
    - Path forward results
    - Future actions beyond the immediate scope of this anomaly
  - Recovery plan products
  - Lessons learned
  - Updated constraints as applicable
  - Required updates to operations procedures identified
  - Post recovery dissemination

- **Work Instructions**:
  - Assemble time line of events associated with anomaly
  - Write summary of anomaly
  - Capture investigation summary
  - Conduct fishbone analysis
  - Identify gaps in data and develop actions to fill gaps
  - Establish primary cause of anomaly
  - Identify corrective and preventive actions
  - Develop and test recovery actions and products
  - Identify other affected systems/subsystems
  - Establish potential reach across to other satellites, components, etc.
  - Track and close out of Action Items
  - Develop and present anomaly close-out package to the Anomaly Review Board (ARB)
- **Tools**:
  - Fishbone Diagram: Used to decompose and isolate root or probable cause for the anomaly by providing an organized method for categorizing subcomponents and/or factors based on observed data. The process also provides insight into areas where additional information is required to further the investigation.

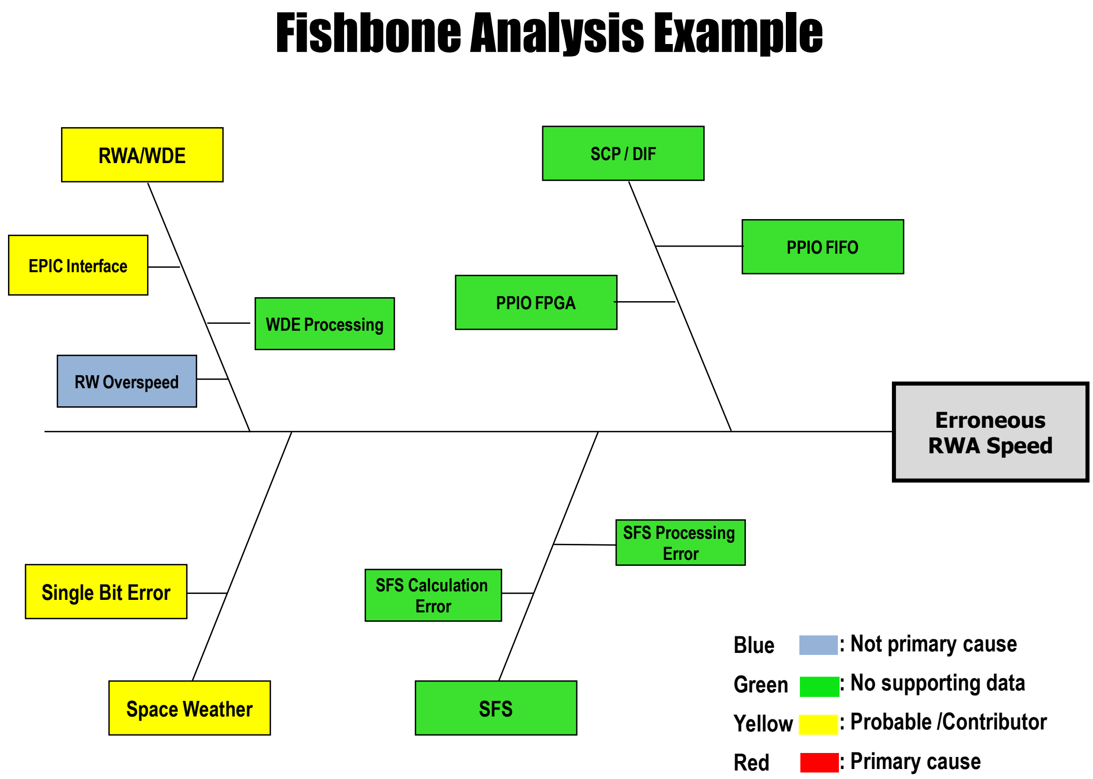


Figure 4. Fishbone analysis example.

- **Off nominal checklist**: A checklist executed by the ART to collect the data for determining probable/root cause, the specific checklist actions are:
  - Verify support for subsystems affected
  - Start timeline
  - Interview system and subsystem engineers
  - Interview operators
  - Generate overall timeline
  - Generate screen shots (real time or playback)
  - Key questions to address:
    - Are there any urgent commands?
    - What actions can we take to gather more information?
    - Do commands need to be in specific order (to preserve data)?
    - Was the spacecraft being commanded immediately before or during the anomaly?
    - What were the conditions of the space environment before or during the anomaly?
    - What is path forward?
    - What other subsystems may be affected?
    - What other activities may be affected?
    - Consider reach-across to other satellite?
- **Techniques**:
  - Anomaly Data Sharing: Post and update documents in an electronic share center accessible by all stake holders if available. The shared folder area should be read only to maintain configuration of the anomaly products. Primary and alternate MA personnel should be members of the anomaly team and take responsibility for posting the files into the shared area swiftly upon their generation. The data file names should include date time information for easy identification of which files are the most current.
- **Post Investigation Recovery Direction**
  - Recovery/mitigation products should take on two specific and unique flavors of information dissemination. The first being satellite control directions associated with operational reconfiguration. These documents should consist of the following parts: the change to be implemented; how the change is to be executed (baseline recovery commanding, satellite reorientation, software patch uploads, etc); what configuration does the satellite need to be in to kick-off the recovery/mitigation operational reconfiguration; how the requested reconfiguration was verified safe for execution; and authorization signatures.
  - Prior to execution of recovery/mitigation the actions to be executed should be verified as capable of achieving the desired result and are safe to uplink to the satellite. It is recommended that the highest fidelity test venue be employed for this testing and that multiple branches be considered and tested to cover potential contingencies that may occur when executed on-orbit. (Reference section 8.1.4.1 Command Application Verification).

- **Best Practices**:
  - Posted files are read only, QA/MA personnel have write privileges for configuration control.
  - Use of video or audio teleconference capability for any meetings to include geographically dispersed participants.
  - Edit recommended path forward in real time as team and polling decision authority determine changes are required.

- **Special Considerations**:
  - Consider test bed operating concepts and limitations when defining tests for updated/new flight software or other operations products to determine effectiveness of the test. Augment limitations with domain expert peer reviews and identify risks and mitigation plans accordingly.

3.2.4 Review and Disposition: Anomaly Review Board (ARB)

The Anomaly Review Board (ARB) provides a systematic approach for reviewing anomalies to determine completeness of the actions and resolution. Determine any subsequent actions that need to occur, ensure that reach-across and lessons learned are complete and disseminated appropriately. The ARB is also responsible for approving long-term reconfiguration actions to the satellite, and the modification of satellite memory actions that are outside the immediate scope of ensuring the satellite is safe or are beyond the set of preauthorized actions identified in the on-orbit handbook and existing operations procedures.

The ARB will approve the anomaly closure packages for Class A and B anomalies. Class C anomalies are closed and documented through the ART team once consensus has been reached to do so.

- **Purpose**
  - The ARB ensures anomalies are documented, investigated, and resolved. The ARB is responsible for making program level decisions which support the program mission in the best way possible. Additionally, the ARB approves non-nominal configuration changes.

- **Roles**:
  - The ARB has a chair, coordinator, voting members, reviewing members, ARB approver delegates, and supporting members.

- **Responsibilities**:
  - The ARB chair leads the ARB meetings, assigns actions, and votes on ARB decisions.
  - The ARB coordinator schedules the meetings, sets the agenda, and facilitates discussion.
  - The ARB reviewing members are responsible for reviewing ARB and ART documentation. It is recommended that ARB reviewing members attend all ARB meetings, but it is not required.
  - The ARB approver delegate members are responsible for reviewing and approving ART path forward and documentation. It is recommended that ARB reviewing members attend all ARB meetings, but it is not required.

- The ARB supporting members attend ARB meetings as requested, execute actions, and provide status on actions.
- ARB voting members:
  - Attend ARB meetings.
  - Assign action items.
  - Vote on board decisions.
  - Ensure that lessons learned are captured and fed back to the factory.
  - Approve closure of the anomalies and ARB Action Items associated with the anomaly.
  - Approve cause determination and ensure cause has been pursued to the appropriate depth.
  - Approve post issue dissemination and reach across adequacy.
  - Direct further ART actions as they deem appropriate.

- **Entry Criteria**:
  - Non-authorized configuration change required (including reviewing of emergency configuration changes implemented by ART team to establish a safe satellite)
  - Interim ART reviews as necessary (can be initiated by either ART or ARB members)
  - Final ART package ready for review

- **Inputs**:
  - ART packages
  - Configuration change requests
  - Test execution summary and results for requested changes
  - ARB Action Item status

- **Exit Criteria**:
  - ARB approval to close out anomaly
  - Approved configuration changes

- **Outputs**:
  - Approved ARB packages
  - Lessons learned database

- **Work Instructions**:
  - The ARB members are briefed by the ARTs in order to approve actions recommended in response to anomalies.
  - During the ARB closure meetings, the ART delegate presents a summary of the cause, actions taken, and recommendations implemented.

- **Techniques**:
  - Post Issue Dissemination
    - It is critical that while investigating an on-orbit anomaly, the team also allocate an individual or group of individuals responsible for constructing products necessary to communicate recovery methodology and future operations concept changes (if required). These configuration controlled products should include documentation of changes to all pre-anomaly baselines. These products should also afford the controllers and subject matter experts a clear identification of what has changed and what the effects are. The documented changes need to be captured in easily retrievable locations readily accessible to operations personnel. This information also needs to be fed back to the satellite contractor in the form of lessons learned.
    - The package should contain a description (unclassified version if applicable) of the anomaly observed, investigation findings, root or probable root cause determination recovery actions directed, trending items added for predictive capabilities, and finally, operational status/results of directed actions. This package should carry some level of formality and be viewed as critical to adaptation, modification, and product improvement in order to mitigate similar anomaly on similar products manufactured by satellite contractor.

- **Best Practices**:
  - The ARB is co-chaired by the customer and contractor and consists of voting members, reviewing members, and supporting members as defined by the program to include customer technical support contractors or other senior independent subject matter experts.
  - ARB members are identified in the anomaly response summary.
  - ARB Board Quorum: The chair or delegate and voting members or their delegates must be present to hold an ARB meeting. An ad hoc ARB meeting may be held for time critical issues as a group or with the chair and each voting member individually.
  - ARB meetings are scheduled as needed.

- **Special Considerations**:
  - It is in the best interest of the end user that lessons learned be flowed back into future designs of this or other systems, thus ensuring a substantive improvement in future products.

4. Example Applications

4.1 Example 1: Preventable Commanding Error

4.1.1 Summary:

Commercial satellite command error led to damaged flight hardware and reduction in mission capabilities

4.1.2 Detailed Description:

During orbit raising maneuvers and shortly after solar array deployments the operations team determined that additional thruster firings were required to remain in prescribed attitude for next stage of orbit raising operations. The health and status of the vehicle was collected and reviewed, confirming that all parameters were nominal. The Attitude Control Systems subject matter expert determined that one out-of-sequence thruster firing was required to re-orient the satellite to the desired positional attitude. Being an out-of-plan thruster, firing the length of burn had to be calculated as did the thruster burn sequences. After the firing sequence and duration were calculated the operations team had to construct a command string with the desired burn parameters. This was accomplished by building the command by hand and having the Attitude Control Systems subject matter expert verify the string structure and upload the command.

The satellite burned considerably longer than planned and on two aft thrusters only, not at all as had been planned. The spacecraft began to tumble and quickly entered into autonomous control safe mode stabilizing itself with thruster firing and momentum wheels spin up operations. Upon stabilization equalization it was discovered that one solar wing was not pointed toward the sun as commanded. The team determined that within the command string constructed for the burn an alpha capital “O” had been mistakenly entered for a numeric “0.” The resulting violent maneuver had most likely broken the yoke interface to the solar wing drive mechanism.

4.1.3 Mission Assurance Shortfall:

This operational error and permanent degradation of mission objectives could have been prevented if a few factors had been considered and steps taken prior to command execution. The first preventive consideration would have been to pre-construct and verify thruster burn scripts that could be easily modified to allow the operators to fire in any selectable sequence and burn for any selectable duration. This would have been implemented during the pre-launch command script generation phase. The next preventive consideration would be to implement a series of gates requiring verification of the command string format prior to execution. This could have been accomplished by something as simple as command compiler execution, which would have caught the alpha-numeric mistake. Another preventive consideration option or additional option would have been to execute the command on a spacecraft simulator to determine if the desired result would be achieved.

Had the operations team exercised appropriate mission assurance measures in the upfront planning and execution of the out-of-plan commands, this degradation of mission objectives would never have happened. The application of mission assurance principles is made more critical in the planning and execution of previously unplanned activities.

4.2 Example 2: Lack of Feedback

4.2.1 Summary:

Satellite operator did not notify prime contractor of anomaly leading to incorrect root cause and correction analysis (RCCA)

4.2.2 Detailed Description:

A satellite ground operating system indicated a spacecraft control processor (SCP) variable went into an alarm state. The operator notified the on-call systems engineering staff which concluded that the anomaly was due to a single event upset (SEU). The operator sent the command to put the SCP in the correct configuration. An internal anomaly report was generated, but the prime contractor of the satellite was not notified.

Several months later, during the summer solstice season, the satellite power subsystem dropped onto battery control, using battery power. The customer notified the prime contractor and reported that the solar array power degradation was much greater than predicted and assumed it was due to radiation environmental effects. The prime contractor asked for solar array current data going back one year. The data showed that the solar array panel shunting current dropped suddenly several months prior to the summer solstice, equivalent to a loss of several solar strings in one moment. When the satellite history was reviewed for that day, it was noted by the customer that there was an SEU at the same moment the solar array current capability dropped. Upon further review of other subsystem data, it was noted that the spacecraft angular momentum and attitude had changed.

The prime contractor concluded that a meteoroid struck the satellite, causing the spacecraft attitude and angular momentum to change and the sudden loss of several solar array strings. In addition, the more likely cause of the SCP upset was an electrostatic discharge event.

4.2.3 Mission Assurance Shortfall:

The lesson learned by the operation staff was that when an anomaly occurs, plots should be made for all subsystems to determine if there was a change during the time frame of the anomaly. The absence of alarms does not mean that the other units or subsystems were not affected by the anomaly.

Another lesson learned is that the prime contractor should be notified of all anomalies, even ones seemingly benign as an SEU, for two reasons. The prime contractor keeps statistics for these types of events across all satellites in the fleet and they may not concur with the RCCA of the operation staff. Without this feedback, opportunities for product improvement will be wasted and may lead to incorrect state-of-health assessments for the fleet.

Had there been a more rigorous recovery process with associated feedback to the factory the root cause would have been determined immediately and dealt with more efficiently.

5. Summary of Recommendations

5.1 Product Implementation

5.1.1 Utilization

- Guide for current operations teams to assess their current operations practices and potentially improve their mission assurance posture
- Guide for new operations teams to follow in developing their operations practices for launch, early orbit, and on-orbit operations

5.1.2 Recommendations

- Include operations team in the development process for space systems as early as possible
- Industry should assess these best practices against their command media and incorporate process improvements
- Government should do the same as industry for government run satellite operations
- Acquirers should consider incorporating these best practices when establishing requirements for future missions

5.2 Potential Follow-on Topics

Best Practices for Mission Systems Engineering

Best Practices for Ground Systems Architecture and Evolution