

# Failure Review Board Guidance Document

June 10, 2011

Thomas C. Hecht  
Systems Integration and Test Office  
Mission Assurance Subdivision

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: Engineering and Technology Group

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

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

# Failure Review Board Guidance Document

June 10, 2011

Thomas C. Hecht  
Systems Integration and Test Office  
Mission Assurance Subdivision

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: Engineering and Technology Group

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

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

# Failure Review Board Guidance Document

June 10, 2011

Thomas C. Hecht  
Systems Integration and Test Office  
Mission Assurance Subdivision

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

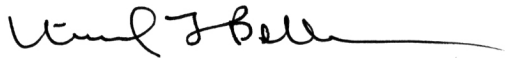
Authorized by: Engineering and Technology Group

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

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.


## Failure Review Board Guidance Document

Approved by:



---

Michael L. Bolla, Principal Director  
Mission Assurance Subdivision  
System Engineering Division  
Engineering and Technology Group



---

Malina M. Hills, General Manager  
MILSATCOM Division  
Space Programs Operations  
Space Systems Group

## Acknowledgments

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 U.S. 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:

Thomas C. Hecht, The Aerospace Corporation  
James C. Brosious, Lockheed Martin  
Dan Callan, Lockheed Martin Corporation  
Mary D'Ordine, Ball Aerospace & Technologies Corporation  
Mark Greby, ATK  
Daniel Gresham, Orbital Sciences Corporation  
Stephen M. Killman, The Boeing Company  
Jim Kinnison, Applied Physics Laboratory (The John Hopkins University)  
Bill McMullen, Northrop Grumman Aerospace Systems  
John McBride, Orbital Sciences Corporation  
Mark Porter, General Dynamics  
Albert (Ted) Ross, Raytheon Space and Airborne Systems  
Roger Valeri, Raytheon Space and Airborne Systems

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

Dan Callan, Lockheed Martin  
James C. Brosious, Lockheed Martin  
Thomas C. Hecht, The Aerospace Corporation

The Topic Team would like to acknowledge the contributions and feedback from the following organizations:

The Aerospace Corporation  
Lockheed Martin  
Ball Aerospace & Technologies Corporation  
ATK  
Orbital Sciences Corporation  
The Boeing Company  
Applied Physics Laboratory (The John Hopkins University)  
Northrop Grumman Aerospace Systems  
General Dynamics  
Raytheon Space and Airborne Systems

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

Bill Bjorndahl, The Aerospace Corporation  
Doug Addy, Ball Aerospace & Technologies Corporation  
Jack Harrington, The Boeing Company  
Alan Zoyhowski, ITT Corporation  
Chris Hersman, Applied Physics Laboratory (The John Hopkins University)  
Hugh (Andy) Penner, Lockheed Martin  
Paul Kruszewski (Alt), Northrop Grumman Aerospace Systems  
Mark Wroth, Northrop Grumman Electronic Systems  
Larry DeFillipo, Sam Travis (Alt), Orbital Sciences Corporation  
Tom Kmiec, Pratt & Whitney Rocketdyne (PWR)  
Steve Dunlap, Bill Luhrs, Raytheon Space and Airborne Systems  
Brian Hudson, United Launch Alliance, LLC (ULA)

A special thank you goes to Margaret K. States (The Aerospace Corporation) for her support as the Program Committee Liaison.

## Executive Summary

There is a significant benefit to having consistent Failure Review Boards (FRB) and processes across the space enterprise. Strong root cause determination and strong remedial actions that address the specific failure cause, other corrective and preventive actions to mitigate the likelihood of similar failures, as well as a common baseline failure review process and expectations benefit the entire industry base. While the desired, successful outcome of a failure investigation and FRB process is the conclusive determination of root cause and the implementation of effective and lasting corrective action, this guidebook also addresses the realities of complex system failures and technical and programmatic constraints in the event that root cause is not determined.

At a summary level the general FRB elements of this guideline include the following:

- **FRB Requirements:** Identify the primary purpose of the FRB, threshold for convening an FRB, and acknowledgement of secondary uses of FRBs.
- **FRB Organization:** Provide suggested leadership, membership, typical charter, authority, and accountability.
- **FRB Process:** Describe the end-to-end process from the time the failure occurs through failure closure, corrective action process, and potential broader implications of a specific failure.
- **FRB Interfaces:** Describe likely organizational and process interfaces including, but not limited to, Corrective Action Boards, program/customer elements, and other boards.

This document describes an FRB process that complements the MIL-STD-1543B process, but is focused on resolution of system or component failures. The overall intent of this guideline is to provide recommended common practices and terminology that can assist in bringing about more consistent and therefore more successful FRB practices across a wide variety of aerospace systems.





# Contents

Acknowledgments .....	iii
Executive Summary .....	v
1. Purpose and Scope .....	1
2. Failure Review Process Introduction .....	3
3. References and Definitions .....	5
3.1 References .....	5
4. FRB Requirements .....	9
4.1 Charter .....	9
4.2 Thresholds .....	10
5. FRB Organization .....	13
5.1 Constituency .....	13
5.2 Responsibility .....	13
5.3 Authority .....	15
5.4 Governance Processes (Responsibility, Authority, Administration) .....	15
6. FRB Process .....	17
6.1 Anomaly Observed: Anomaly Declared .....	17
6.2 Preliminary Investigation: Containment and Analysis .....	18
6.2.1 Additional Safeguarding Activities and Data Preservation .....	19
6.2.2 Configuration Containment Controls and Responsibilities .....	19
6.2.3 Failure Investigation Plan and Responsibilities .....	19
6.2.4 Initial Data Collection and Failure Analysis (Prior to Breaking Configuration) .....	20
6.3 Root Cause Investigation: Perform Root-Cause Test and Analysis .....	21
6.4 Root Cause Determination: Root Cause Determined or Undetermined .....	21
6.4.1 Root Cause Determined .....	22
6.4.2 Unknown Root Cause .....	22
6.4.3 Unverified Failure or Unknown Direct Cause .....	22
6.5 Remedial, Corrective, and Preventive Action Implementation .....	24
6.6 Closure: Close FRB Records .....	24
6.6.1 Entry Criteria (Pre-review Requirements) .....	24
6.6.2 Documentation (Typical Package Contents) .....	25
6.6.3 Exit Criteria .....	26
6.7 Enterprise Corrective Action Board: Possible Enterprise/Industry Alert Notification ...	27
7. Interfaces .....	29
Appendix A. FRB Template .....	33
Appendix B. Suggested Checklists .....	41
Appendix C. Suggested Root Cause Analysis Tools .....	49
Appendix D. Summary of Other Investigation Tools and Techniques .....	51

## Figures

Figure 1.	Failure review process flow.....	3
Figure 2.	Failure review process flow.....	17

## Tables

Table 1.	Common FRB Terminology.....	5
Table 2.	Levels of Causation and Associated Actions.....	8
Table 3.	Example of FRB Constituency at Various Levels of Failure Investigation and Suggested Escalation Criteria.....	14
Table 4.	FRB Closure Package Template.....	25
Table 5.	A Summary of the Other Typical Interface Relationships of the FRB.....	30
Table 6.	General Failure Assessment Tools and Techniques.....	51
Table 7.	Laboratory, Non-Destructive Evaluation (NDE) and Destructive Analysis and Component/System Test Tools and Techniques.....	52

## 1. Purpose and Scope

There is a significant benefit to having consistent Failure Review Boards (FRB) and processes across the space enterprise. Strong root cause determination and strong remedial actions that address the specific failure cause, other corrective and preventive actions to mitigate the likelihood of similar failures, as well as a common baseline failure review process and expectations benefit the entire industry base. Wide variability in the conduct of FRB activities across the space enterprise, in particular a lack of effective root cause determination and follow on corrective/preventive action implementation, has been a continuing concern that this guidebook is intended to help mitigate. A successful FRB depends upon several factors including a comprehensive, structured, effectively managed and well-documented investigative approach. A multi-discipline team composed of representatives from different organizations has developed the following industry best practices to provide guidance to the practice of conducting consistent and successful FRBs. While the desired, successful outcome of a failure investigation and FRB process is the conclusive determination of root cause and the implementation of effective and lasting corrective action, this guidebook also addresses the realities of complex system failures and technical/programmable constraints in the event root cause is not determined.

At a summary level the general FRB elements of this guideline include the following:

- FRB Requirements: Identify the primary purpose of the FRB, threshold for convening an FRB, and acknowledgement of secondary uses of FRBs.
- FRB Organization: Provide suggested leadership, membership, typical charter, authority, and accountability.
- FRB Process: Describe the end-to-end process from failure detection through closure, program unique corrective action, interface with enterprise corrective action process and potential broader implications of a specific failure. This will include administrative aspects, early engagement in failure containment, investigation oversight, root cause review and disposition, failure event closure, and follow-on activities.
- FRB Interfaces: Describe likely organizational and process interfaces including, but not limited to, Corrective Action Boards, program/customer elements, and other boards.

The overall intent of this guideline is to provide recommended common practices and terminology that can assist in bringing about more consistent and therefore more successful FRB practices across a wide variety of aerospace systems.

The emphasis of this guidance document is the execution of an FRB process focused on resolution of system or component failures. Whereas MIL-STD-1543B provides for an FRB as an element of a Failure Review, Analysis, and Corrective Action System (FRACAS) for gathering failure statistics used in reliability models, in design updates, and to demonstrate the effectiveness of corrective actions; the FRB described in this guidance document emphasizes the active management of failure investigations. MIL-STD-1543B does not explicitly require this in its description of an FRB although data reviewed at MIL-STD-1543B FRBs ideally represent outputs of high-fidelity root-cause investigations. Within the aerospace industry, there exists some confusion about the relative merits of these two types of FRBs. These two types of FRBs are actually complementary processes with somewhat different goals as opposed to a single process in different evolutionary stages. The confusion stems from the industry practice of calling both FRBs.

The different emphases of the two FRB types means that some space programs can benefit from a management approach that invokes both FRB types, and others may find regular application of only one of these processes necessary. Production programs consisting of many builds or designs that incorporate a large number of identical hardware components generate valuable trend data for use within MIL-STD-1543B FRBs. Among the various types of space programs, one-of-a-kind builds utilizing limited quantities of unique hardware types might not benefit as much from MIL-STD-1543B. These programs usually do not generate sufficient failure statistics to meet the intended goals of MIL-STD-1543B. They do, in contrast, stand to benefit substantially from the FRB process described within this document. This class of program will likely encounter specific, late-stage integration failures for the first (and possibly, only) time making active management of the root-cause, corrective-action steps essential to mission success. The use of this guidance-document FRB process reduces the risk of unfortunate surprises late in a program when the management of high-stakes, complex hardware failures involving multiple interfaces has the most programmatic impact. In general, factors favoring regular application of MIL-STD-1543B FRBs include (1) high production volume, (2) significant numbers of previous flight missions, and (3) failures previously documented in an existing database of well-understood root-cause and corrective-action events. The opposite considerations that favor this guideline FRB are:

- Low production volume.
- A first or early build with limited or no flight heritage.
- Builds with significant new hardware or software development.
- Limited history of root-cause, corrective-action resolutions.

In addition, this guideline FRB should be used to resolve failures with new or uncertain signatures occurring at an integrated level (see Section 4b) that meets the threshold for invoking this process. Regardless of the program type, outputs (i.e., root cause analyses) of this guideline's FRB investigations should always be provided to program reliability engineers even if sufficient data does not exist to effectively implement all elements of MIL-STD-1543B.

## 2. Failure Review Process Introduction

A generic failure review and root-cause investigative process as shown in Figure 1 provides the framework for the detailed discussion laid out in Section 6. The process begins with an anomaly triage decision to determine the necessity of resolving the issue within the FRB (see Section 4.b). For anomalies thus identified as requiring an FRB approach, the next steps involve a closed-loop root-cause investigation. The root-cause investigation nominally identifies the cause or causes of the failure as well as remedial, corrective, and preventive actions that the FRB implements or flows to enterprise-level boards. The FRB also has responsibility for closing the initial anomaly records and for addressing unverified and cause-unknown failures. Each of these elements is necessary to implement a closed-loop failure process that has the highest probability of isolating the failure root-cause and implementing effective measures to correct the present failure situation and prevent occurrence/recurrence.

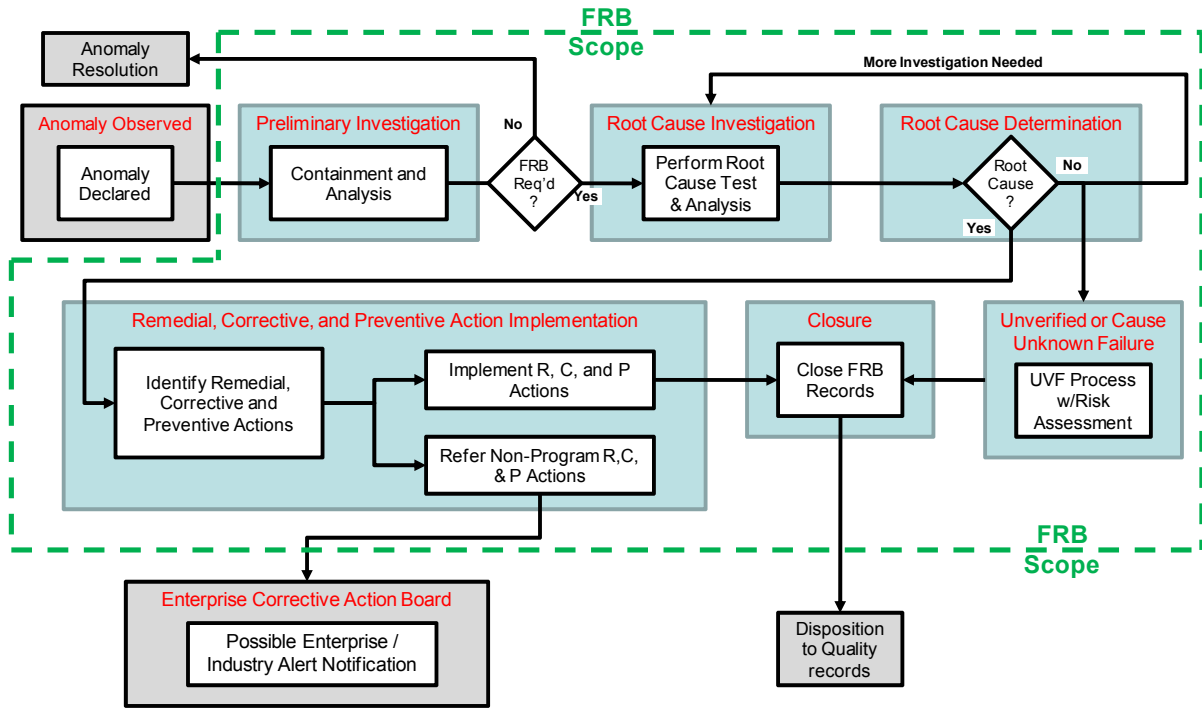


Figure 1. Failure review process flow.



### 3. References and Definitions

The following list of references and definitions is provided to assist the community in establishing a common terminology for the practice of conducting FRBs.

#### 3.1 References

MIL-STD-1543B	Reliability Program Requirements for Space and Launch Vehicles
Aerospace Report No. TOR-2007(8583)-6889	Reliability Program Requirements for Space Systems
ANSI/AIAA S-102.1.4.2009	Performance-Based Failure Reporting, Analysis & Corrective Action System (FRACAS) Requirements
ANSI/AIAA S-102.1.5, 2009	Performance-Based Failure Review Board (FRB) Requirements
MIL-HDBK-2155 11 December 1995	Failure Reporting, Analysis and Corrective Action Taken

A common lexicon facilitates standardization and adoption of any new process. The following list provides consistent terms used in this report to implement the FRB process. However, significant variability exists among the MAIW-participant contractors regarding terminology. Where this has occurred, emphasis is on consistency within this guideline as opposed to historical accuracy or otherwise rigorous definitions.

A glossary of FRB terminology is included below:

Table 1. Common FRB Terminology

Term	Definition
Acceptance Test	A sequence of tests conducted to demonstrate workmanship and provide screening of workmanship defects.
Anomaly	An unplanned, unexplained, unexpected, or uncharacteristic condition or result or any condition that deviates from expectations. Failures, nonconformances, limit violations, out-of-family performance, undesired trends, unexpected results, procedural errors, improper test configurations, mishandling, and mishaps are all types of anomalies.
Break In Configuration	Any change to the test configuration in which the Unit Under Test (UUT) experienced the anomaly of failure. This can include changes to the UUT as well as the support equipment or environments: power off/power cycling, SW reboot/reload, physically moving items, handling cables, changing temperature or vacuum conditions, demating connectors.
Component	A standalone configuration item, which is typically an element of a larger subsystem or system. A component typically consists of built-up subassemblies and individual piece parts.

Term	Definition
Containment	Appropriate, immediate actions taken to reduce the likelihood of additional system or component damage or to preclude the spreading of damage to other components. Containment may also infer steps taken to avoid creating an unverified failure or to avoid losing data essential to a failure investigation.
Contributing Cause	A factor that by itself does not cause a failure. In some cases, a failure cannot occur without the contributing cause (e.g., multiple contributing causes); in other cases, the contributing cause makes the failure more likely (e.g., a contributing cause and root cause).
Corrective Action	An action that eliminates, mitigates, or prevents the root cause or contributing causes of a failure. A corrective action may or may not involve the remedial actions to the unit under test that bring it into conformance with the specification (or other accepted standard). However, after implementing the corrective actions, the design, the manufacturing processes, or test processes have changed so that they no longer lead to this failure on this type of UUT.
Corrective Action Board	A group that oversees, within its defined area of responsibility, the Corrective Action Process. The board's scope does not need to be limited just to failure corrective actions.
Corrective Action Process	A generic closed-loop process that implements and verifies the remedial actions addressing the direct causes of a failure, the more general corrective actions that prevent recurrence of the failure, and any preventive actions identified during the investigation.
Direct Cause (often referred to as immediate cause)	The event or condition that makes the test failure inevitable, i.e., the event or condition event which is <i>closest</i> to, or immediately responsible for causing the failure. The condition can be physical (e.g., a bad solder joint) or technical (e.g., a design flaw), but a direct cause has a more fundamental basis for existence, namely the root cause. Some investigations reveal several layers of direct causes before the root cause, i.e., the real cause of the failure, becomes apparent.
Event	An event is an unexpected behavior or functioning of hardware or software that does not violate specified requirements and does not overstress or harm the hardware.
Failure	A state or condition that occurs during test or pre-operations that indicates a system or component element has failed to meet its requirements.
Failure Modes & Effects Analysis (FMEA)	An analysis process that reviews the potential failure modes of an item and determines their effects on the item, adjacent elements, and the system itself.
Failure Reporting, Analysis, and Corrective Action System (FRACAS)	The totality of closed-loop processes for detecting, reporting, analyzing, documenting, correcting, trending, preventing, and managing the system or component and software failures.
Failure Review Board (FRB)	Within the context of this guideline, a group, led by senior personnel, with authority to formally review and direct the course of a root-cause investigation and the associated actions that address the failed system.



Term	Definition
Government Industry Data Exchange Program (GIDEP)	A U.S. Government sponsored program that alerts and informs participating companies and corporations within the industry to specific parts and reliability issues and concerns for generic, common, or widely used items.
Material Review Board (MRB)	The MRB typically consists of individuals trained and certified to the MRB process. This is a cross functional group that normally reviews non-conforming materials, assemblies, or procured items prior to acceptance or system integration. The MRB can alert the FRB that anomalies that may require FRB attention have occurred. Subsequently, the MRB performs associated failure analysis and/or regression activities with FRB oversight. The MRB process includes the nonconformance database used to track and close the system or component anomalies.
Nonconformance	The identification of the inability to meet physical or functional requirements as determined by test or inspection on a deliverable product.
Nonconformance Database	A database (typically software) that records and tracks nonconformances to closure.
Overstress	An unintended event during test, integration, or manufacturing activities that results in a permanent degradation of the performance or reliability of acceptance, proto-qualification, or qualification hardware brought about by subjecting the hardware to conditions outside its specification operating or survival limits. The most common types of overstress are electrical, mechanical, and thermal.
Preventive Action	An action that would prevent a failure that has not yet occurred. Implementations of preventive actions frequently require changes to enterprise standards or governance directives. Preventive actions can be thought of as actions taken to address a failure before it occurs in the same way that corrective actions systematically address a failure after it occurs.
Probable Cause	A cause identified, with high probability, as the root cause of a failure but lacking in certain elements of absolute proof and supporting evidence. Probable causes may be lacking in additional engineering analysis, test, or data to support their reclassification as root cause and often require elements of speculative logic or judgment to explain the failure.
Qualification	A sequence of tests, analyses, and inspections conducted to demonstrate satisfaction of design requirements including margin and product robustness for designs. Reference MIL-STD-1540 definitions.
Remedial action	An action performed to eliminate or correct a nonconformance without addressing the root cause(s). Remedial actions bring the UUT into conformance with a specification or other accepted standard. However, designing an identical UUT, or subjecting it to the same manufacturing and test flow may lead to the same failure. Remedial action is sometimes referred to as a correction or immediate action.
Root Cause	The ultimate cause or causes that, if eliminated, would have prevented the occurrence of the failure.

<b>Term</b>	<b>Definition</b>
Root-Cause Analysis	A systematic investigation that reviews available empirical and analytical evidence with the goal of definitively identifying a root cause for a failure.
Root Cause Corrective Action (RCCA)	Combined activities of root cause analysis and corrective action.
Significant Failures	Test failures or potential overstress events occurring at or above a minimum level of integration (system or component level) for which a program's contract or company procedures requires FRB oversight.
Unit Under Test (UUT)	The item being tested whose anomalous test results may initiate an FRB.
Unknown Cause	A failure where the direct cause or root cause has not been determined.
Unknown Direct Cause	A repeatable/verifiable failure condition of unknown direct cause that cannot be isolated to the UUT or test equipment.
Unknown Root Cause	A failure that is sufficiently repeatable (verifiable) to be isolated to the UUT or the Test Equipment, but whose root cause cannot be determined for any number of reasons.
Unverified Failure (UVF)	A failure (hardware, software, and firmware) in the UUT or ambiguity such that failure can't be isolated to the UUT or test equipment. Transient symptoms usually contribute to the inability to isolate a UVF to direct cause. Typically a UVF does not repeat itself, preventing verification. Note that UVFs do not include failures that are in the test equipment once they have been successfully isolated there. UVFs have the possibility of affecting the flight unit after launch, and are the subject of greater scrutiny by the FRB.
Worst-Case Change Out (or Worst Case Repair)	An anomaly mitigation approach performed when the exact cause of the anomaly cannot be determined. The approach consists of performing an analysis to determine what system(s) or component(s) might have caused the failure and the suspect system(s) or component(s) is then replaced.

In particular, the terms “remedial action,” “Corrective Action,” and “Preventive Action” address three levels of causation as follows:

Table 2. Levels of Causation and Associated Actions

<b>Level of Causation (in order of increasing scope)</b>	<b>Action Taken to Mitigate Cause</b>	<b>Scope of Action Taken</b>
Direct Cause	Remedial Action	Addresses the specific nonconformance
Root Cause	Corrective Action	Prevents nonconformance from recurring on the program and/or other programs
Potential Failure	Preventive Action	Prevents nonconformance from initially occurring

## 4. FRB Requirements

### 4.1 Charter

The Failure Review Board (FRB) should be chartered by program management or Enterprise Governance documents to provide oversight, direction, and evaluation of failures detected during qualification, acceptance, system validation, or operational testing. The eventual outcome of the FRB is the return of the product to test, flight and/or operational readiness, and minimizing the effect of failures on delivered products while balancing the risk and impacts of action identified to address the causes of the failure. The process is applied to failures regardless of locations. The FRB serves as the governing board that steers the investigation efforts. The charter for the board for each failure should be clearly defined, stated and documented in the FRB meeting, and recorded as part of the FRB minutes. The FRB also provides an interim and is often the final forum for the investigation progress and results. Most requirements owners (i.e., customer) state only they have the authority to accept a failure or non-conformance to that requirement, usually via waiver or deviation process. The FRB may recommend to the program to accept the risk of the failure/nonconformance until the waiver/deviation can be processed. This is generally viewed as “temporary acceptance” of the failure. In the event root cause is not determined and/or the failure has significant mission implications, the FRB has the responsibility to ensure appropriate risk acceptance rationale is developed and escalation of the failure review to higher levels of internal and customer management is pursued. Subsequent sections of this document provide more detail on root cause determination and possible FRB escalation to higher levels of review.

This guideline addresses the application of FRBs in the context of test failures. However, use of the FRB process is encouraged to investigate and identify root cause and corrective/preventive actions for other anomalies that require a structured systems engineering approach to resolve.

The key elements and overall purpose of the FRB are:

- Integrate and direct the investigation effort to ensure an accurate, complete, and timely failure resolution.
- Minimize the occurrence of Unknown Cause failures by preserving failure evidence and preventing hasty changes in test configuration that may prevent root cause identification and verification.
- Provide visibility to the program and the customer of failure investigation planning and progress.
- Protect the system or component at higher levels of integration from failures occurring at lower levels, preclude propagation of the failure.
- Coordinate with management to ensure that the appropriate resources are made available to the investigation effort and are properly prioritized and focused.
- Coordinate with management and other enterprise-wide boards to address reach back (reactive), reach forward (proactive), horizontal (across adjacent products and programs), and reach across (spanning various Lines of Business within an Enterprise, or even across different companies and corporations within the industry) aspects and elements of the resultant actions and recommendations.

In every case, the primary goal of the FRB process is to ensure the reliability of space-flight hardware. FRBs conventionally accomplish this through the implementation of a closed-loop, root-cause, and corrective action approach. However, not all FRBs arrive at root cause, and FRBs must develop appropriate courses of action when circumstances make hardware reliability uncertain. Examples of the latter include unverified failures and potential overstress events. Secondly, an efficient FRB can help a program balance critical resources (e.g., staff and test sets) and priorities.

## 4.2 Thresholds

The threshold criteria for convening a Failure Review Board must be clearly defined and documented in the enterprise or program command media.

An FRB should be convened when:

- A failure is declared by the test conductor.
- An unexpected test event, or result, presents significant cost, schedule, and technical risk.
- A failure occurs during acceptance testing, qualification, or proto-qualification of a flight element, and the initial investigation of an anomaly has not isolated the cause to test equipment, test procedure, or operator error.
- Any change to the test configuration in which the UUT experienced the anomaly or failure; this can include changes to the UUT as well as the support equipment: power off/power cycling, SW reboot/reload, physically moving items, handling cables, and demating connectors.
- Any condition that creates possible overstress to the flight element(s).
- Systemic issues identified by the investigating team or lower level FRB determine cause that could affect other elements of the program.

By way of example, in failures related to electronic systems, mechanical or electro-mechanical systems, FRBs are traditionally convened when a failure occurs after first power is applied to the board, box, subassembly, assembly, or fully integrated flight system or component level for acceptance or qualification testing. In other systems such as structural, propulsion and thermal systems, FRBs are convened when the failure occurs after the formal commencement of test operations per the test planning documentation. In broader applications, FRBs may also be convened for anomalies that occur at any time during the development, integration, and testing of an aerospace program.

Other criteria or events may warrant an FRB, such as failures of units or subsystems after formal delivery (regardless of test type). An FRB may be convened at the discretion of program, technical management or the customer to address items that may influence mission success or need the FRB's expertise to adjudicate. The following are examples of other items that use the FRB for adjudication:

- Failures on subcontracted system or component with limited FRB capability at the subcontractor.
- Sibling failures (failures that occur on other programs using the same system or component) including sibling failures on subcontracted system or component.

- Software/Firmware failures.
- Out of family results based on trending or post-test data evaluations.
- Overstress that occurs during non-test stages of a program. For example, a transportation mishap that results in damage to a unit.
- Concerns raised by Subject Matter Experts:
  - Failures that occur during test phases outside of protoqual, qualification, or acceptance on flight HW, but have a direct impact on requirements or mission success.
  - Anomalies and or failures that occur on non-flight HW (i.e., engineering units), which have direct reach to the flight design.
  - Hardware/Software integration interactions that are producing unexpected/anomalous results and/or producing integration “features” or “signatures.” In some cases there is not a direct impact to requirements but could over time impact mission success.
- Unexpected results: Test results, including signatures and features, that deviate from what was predicted by models, documented by test procedures, or established in requirement documentation. A processor which is considered “fault tolerant” that “halts” would be considered an unexpected result. The temperature of hardware in TVAC, which is much higher than what was modeled, is an unexpected result.



## 5. FRB Organization

This section describes the FRB membership and those members' roles and responsibilities (see Table 3) providing a hierarchical view of the organization at various levels. The FRB's authority, administrative duties, and products will also be described at a high level with details provided in Section 6, "FRB Process."

### 5.1 Constituency

The FRB Chair for a given failure incident is assigned by Program Management or per Enterprise Governing Processes. The FRB Chair may be a member of the program team or from independent engineering, mission assurance, product, quality, or program organizations. The selection is often dependent on the company and/or program structure, available resources and the specific nature of the failure. The FRB chair should be a Senior Systems Engineer, Mission Assurance Engineer, or Chief Engineer. Recommended skills include in-depth system level familiarity with the unit under test, problem solving and root cause analysis, and leadership skills. FRB members should include the program's Systems Engineer, Mission Assurance and/or Quality Engineer Manager, Subject Matter Experts (SMEs) as needed, (e.g., a Safety Engineer for hardware lift or personnel safety issues, or a Reliability Engineer if electrical overstress is suspected), and the responsible engineer for the unit under test. Customer participation on the FRB varies depending on the contract, and ranges from a non-participating observer role to a full voting member on the board. It is strongly recommended that voting and non-voting members of the FRB be clearly defined and communicated in the FRB charter.

### 5.2 Responsibility

A standing FRB organization is not required but may be established if the program/enterprise warrants and is established in the appropriate program/enterprise command media. The intent of the FRB process is to establish an FRB that provides independent review of investigation results, direction of investigation, and ensures the processes themselves are rigorously followed. The FRB chair is responsible for guiding and approving the investigation activities and ensuring that effective remedial actions are executed to resolve the failure.

The FRB chair and members are responsible for ensuring the root cause and remedial actions identified are sufficient, and that any residual risk is identified and captured in the program's risk mitigation efforts. In many organizations, non-failure specific corrective actions are outside the scope of the FRB. Commonly, the dividing line is the direct cause and remedial actions are the domain of the program FRB, and broader corrective actions are the domain of the program or enterprise corrective action process as shown in the FRB flow in Section 2 in Figure 1 with additional detail present in Section 6.

Table 3. Example of FRB Constituency at Various Levels of Failure Investigation and Suggested Escalation Criteria

Failure Review Org	Criteria for convening	Authority	Suggested Key Members	Failure Disposition/ Review Escalation Decisions
Preliminary Review (prior to convening MRB or FRB)	Investigate and disposition test anomalies, but cannot disposition any remedial action of hardware or deliverable software. Dispositions are limited to troubleshoot, retest/re-inspect, no defect, and promote to MRB and/or FRB.	Test Engineer with concurrence from Systems Engineer/Quality Engineer	Candidates: Test Engineer (authority), Systems Engineer (interim concurrence), Quality Engineer (final concurrence), Responsible Engineer (hardware owner), SMEs (technical expertise), Reliability Engineer (failure assessment), Safety Engineer (as applicable)	1) MRB if needed (decision to convene FRB if FRB thresholds met or exceeded)
MRB	Convened to address all nonconformances including test failures per program nonconformance/ MRB plan requirements	Per Program Plan; Quality usually has final sign-off of disposition subject to engineering disposition	MRB Authority; Other Candidates include Quality Engineer, Responsible Engineer (hardware owner), Customer (if required by contract), SMEs (technical expertise), Reliability Engineer (failure assessment), Safety Engineer (as applicable), Test Engineer	1) Use as is and repair dispositions are assessed for residual risk & captured by program or determination if FRB thresholds are met or exceeded and FRB is required 2) Evaluation and initiation of corrective action process including enterprise/ industry notification assessment
FRB (Project/ Program Level)	Convened when preliminary review has determined that a failure of requirements has occurred or the system behavior is not understood without further investigation.	FRB Chair, with Program MA Manager concurrence preferred	FRB Chair candidates are often Senior Systems Engineer, program Mission Assurance manager, Chief Engineer or Senior Quality Engineer; other members may include but are not limited to Responsible Engineer (hardware owner), SMEs (technical expertise), Reliability Engineer (failure assessment), Safety Engineer (as applicable), Test Engineer, Quality Engineer (liaison to MRB), Customer representative as required by contract	1) Test failure dispositions are assessed and remedial actions implemented, residual risk; risk is captured on program risk list, determination if senior management review and further risk acceptance is required 2) Failure Review Escalation Decision 3) Evaluation and initiation of corrective action process including enterprise / industry notification assessment
Product FRB (Single Product line)	Convened when failures with significant residual risk with the failure resolution remains or when a product line is affected (> 1 program). When a product line is affected by a failure identified on a program, additional investigation is required to determine root cause and corrective action at the product line level.	Product FRB Chair with Mission Assurance/ Success concurrence (MA/MS may be replaced by an alternative enterprise level independent review function)	Product Area Management, FRB Chair product area MA/MS manager (concurrence), Responsible Engineer (hardware owner), SMEs (technical expertise), Reliability Engineer (failure assessment), Safety Engineer (as applicable), Test Engineer (if event occurred during test), Program MA Managers from affected programs (liaisons to programs)	1) Residual risk acceptance or 2) Failure review escalation decision 3) Evaluation and initiation of corrective action process including enterprise/industry notification assessment
Enterprise FRB	Convened when failures with significant residual risk with the failure resolution remains and high mission consequences or when > 1 program is affected and the issue is not limited to a product line.	Enterprise FRB Chair with Mission Success concurrence (MS is an enterprise level independent review function)	Enterprise Level Executive Management, FRB Chair, Mission Assurance / Success (concurrence), SMEs (technical expertise), Process owner(s) as applicable	1) Residual risk acceptance 2) Evaluation and initiation of corrective action process including enterprise/ industry notification assessment



Note that there are also broader containment actions beyond containment of the specific failure required when a failure is detected, which are detailed in Section 6.3. As soon as the FRB chair and supporting team is identified they should begin to provide oversight to these actions and communicate broader containment concerns as required. When containment actions cross program boundaries (i.e., failures common to re-used design, commodity product, or part) the FRB responsibility touches the interface with other parts of the organization (e.g., corrective action board [CAB], alerts [engineering], Government Industry Data Exchange Program [GIDEP] [parts or reliability]).

The FRB, as a team, should ensure the investigation team produces the required products:

- Problem statement
- Failure resolution goals directly corresponding to the FRB's scope
- Relevant information and generation of missing relevant data
- Root cause and contributing factors with supporting evidence
- Remedial actions
- Recommended corrective actions to address the root cause and contributing factors and prevent failure recurrence
- Preventive actions to mitigate the occurrence of the failure in the first place

Full review and concurrence with the results of investigation are the primary responsibility of the FRB including communication of any corrective/preventive action recommendations and follow-up as described in Sections 6.7 and 6.8 of this guideline. Full documentation (including meeting minutes) of the FRB effort and outcome is required.

### **5.3 Authority**

The FRB chair's authority should come from a higher level of enterprise governance such as a functional engineering or Mission Assurance vice president or director, or the program manager. The program manager empowers the FRB chair, the FRB team and provides the resources necessary for the investigation. The FRB chair's authority normally specifies responsibility for the execution of the FRB and determining whether the FRB has met its exit criteria. If the Material Review Board (MRB) and FRB share authority over system or component operations and remedial actions when the FRB is convened, the MRB members may typically be members of the FRB. This shared authority should be specified in enterprise command media and flowed down and expanded in program FRB requirements and plans.

### **5.4 Governance Processes (Responsibility, Authority, Administration)**

Programs, internal organizations or the customer should develop a governing FRB plan as part of the program documents, such as mission assurance plans. The FRB should develop an investigation plan consistent with the significance of the failure. The investigation plan should include problem statement, goal, approach, test and analyses requirements, program constraints (including cost, schedule, need dates, or milestones), and resource requirements. The plan should be drafted early in the investigation and updated as appropriate. The plan should identify investigation approach and problem solving tools such as process mapping, Failure Modes & Effects Analysis (FMEA), design of experiments, data analysis, test, and root cause analysis approach to a sufficient level of detail to

guide the investigation and address other affected system elements, product lines, and/or enterprise processes as required.

FRB administrative duties should include action item lists, meeting management and minutes, and interim investigation status reports. Ultimately, the FRB should present a formal failure report. Mission Assurance or Quality should maintain FRB supporting evidence and documentation.

Interfaces with other organizations, boards, and processes (e.g., test review boards, MRB, corrective action boards, and corporate FRBs) are discussed in Section 7, “Interfaces.” It should also be noted that FRB needs to forward all configuration issues to the Engineering Review Board (ERB)/Configuration Control Board (CCB) for resolution.

## 6. FRB Process

Section 2 introduced the failure review process at a summary level as shown in Figure 2 below. As referenced, the process consists of the following elements: Anomaly Observation; Preliminary Investigation; Root Cause Investigation; Root Cause Determination; Remedial, Corrective and Preventive Action Implementation; and Closure. Situational awareness of the need to escalate reviews to higher-level boards (e.g., in the case of an unverified or unknown cause failure) and address possible enterprise/industry failure notifications is also described. This section provides a more detailed description of each of these elements.

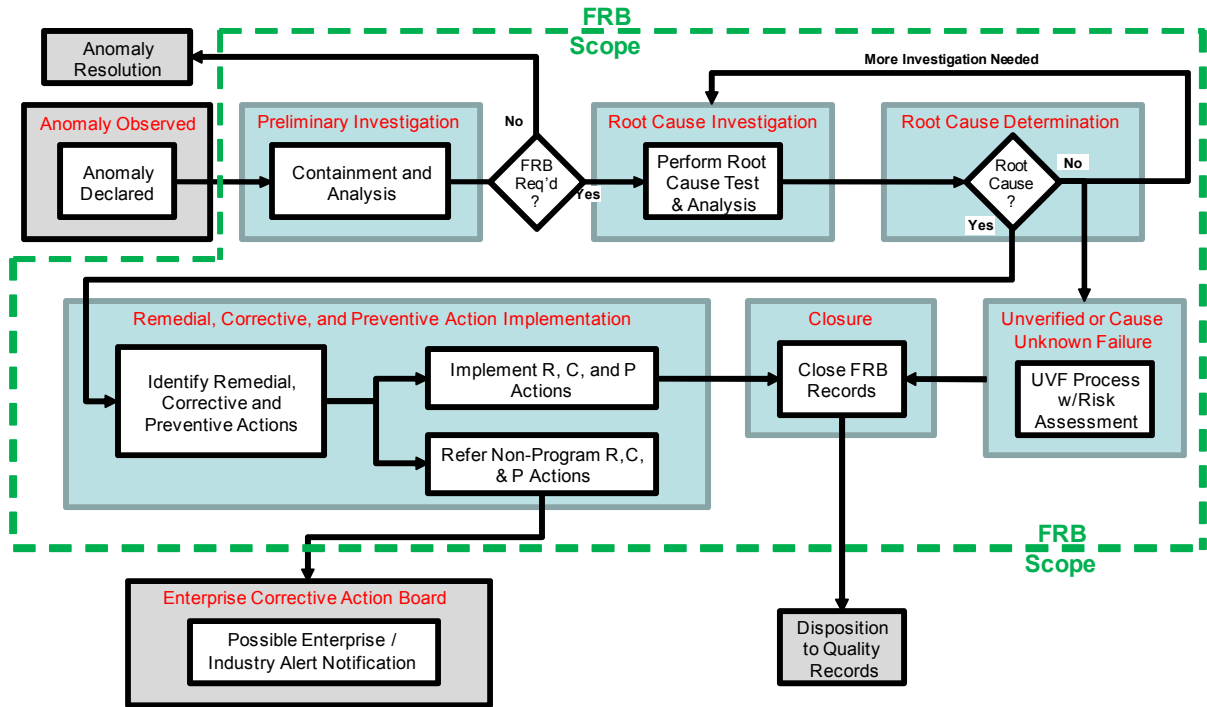


Figure 2. Failure review process flow.

### 6.1 Anomaly Observed: Anomaly Declared

The Anomaly Observed element represents the process used by personnel to identify that either an event or a failure has occurred. Once the anomaly has been defined as a failure the successful FRB process hinges on clear, well-reasoned guidelines regarding conditions requiring additional review at the Preliminary Investigation level, and test and quality personnel must recognize the need to assess failures and related issues that may lead to an FRB. Test personnel must also understand best practices for maintaining test configuration, as unauthorized changes to the Unit Under Test (UUT) or test equipment can compromise the future course of the investigation. Of course, immediate safeguarding of personnel and hardware is the first step after the occurrence of a system failure is suspected. Ensuring personnel safety should override hardware, support equipment, data, and potential investigation evidence safeguarding concerns.

At this early stage, personnel should document a potential nonconformance of a UUT and refer the matter to a Preliminary Investigation team. Examples include test failures (the UUT does not meet minimum performance requirements), test anomalies (unplanned or unexplained condition that deviates from expectations), and electrical, mechanical, and thermal overstress. In the latter case, an external agent has possibly overstressed the UUT in a manner that casts doubt on the UUT's ability to

subsequently perform reliably during its planned mission. Another class of anomaly warranting further consideration involves unintended breaks in configuration even when these do not involve a specific performance failure or overstress. Such breaks (e.g., of calibrated interfaces, changes in environment, removal of power, resetting or rebooting software.) can invalidate any remaining qualification or acceptance tests, and test personnel should escalate these to the Preliminary-Investigation level as well.

## **6.2 Preliminary Investigation: Containment and Analysis**

During the Preliminary Investigation, personnel carefully consider the implications of the perceived anomaly. If executed properly, this element continues to safe the UUT and preserve forensic evidence to facilitate the course of a subsequent root-cause investigation. In the event the nature of the failure precludes this (e.g., a catastrophic test failure), immediate recovery plans should be made. The FRB chair should be kept apprised of these activities by the investigation lead and have the opportunity to communicate any concerns that may compromise potential evidence or future investigation activities.

Some examples of seemingly benign actions that can be “destructive” if proper precautions are not taken for preserving forensic evidence include loosening fasteners without first verifying proper torque (once loosened, you’ll never know if it was properly tight); demating a connector without first verifying a proper mate; neglecting to place a white piece of paper below a connector during a demate to capture any foreign objects or debris.

A performance test failure that resulted from an incorrect test procedure or configuration also known to *not* have damaged the UUT may be dismissed with the appropriate justification and documentation including a Root Cause Corrective Action (RCCA) to prevent reoccurrence. However, if the Preliminary Investigation cannot definitively validate the physical integrity of the UUT, the matter definitely warrants additional investigation and analysis by the responsible/cognizant engineers of the Preliminary Investigation team.

At this point, it may also be important to consider hardware/software integration interactions that are producing unexpected or anomalous results. Emergent properties and behaviors at the System level are frequently a direct cause of hardware/software integration; it is especially important to consult with knowledgeable and cognizant software engineers, typically the software integrator.

In some instances, UUT behavior during test or operation may still be within performance requirements but determined to be sufficiently different from past performance (e.g., during recurring acceptance testing), that special attention to the results may be warranted. Terms such as “out of family” are often used to describe these types of events, and the necessity of calling an FRB to address this class of situation hinges to a great extent on the cognizant engineering leads’ familiarity with the system or component. An FRB process may be warranted to ensure that test or operational results are not providing an early indicator of an adverse trend or process related drift that needs attention.

When the Preliminary Investigation cannot definitively exonerate the system or component, or cannot definitively validate the physical integrity of the UUT, the team will elevate the issue to the appropriate authority specific to the company and program who will determine if an FRB should be convened.

Any Preliminary-Investigation activities subsequent to the initial ruling about the necessity of an FRB are performed under the direction of the FRB chairperson. The first investigative steps should attempt non-invasive troubleshooting activities such as UUT and test-set visual inspections and data reviews. Photographing the system or component and test setup to document the existing test condition or configuration is often appropriate. The photographs will help explain and demonstrate the failure to

the FRB. The investigative team should record all relevant observables including the date and time of the failures (including overstress events), test type, test setup and fixtures, test conditions, and personnel conducting the test. The investigative team then evaluates the information collected, plans a course of action for the next steps of the failure investigation, and presents this information at a formal FRB meeting. Noninvasive troubleshooting should not be dismissed as a compulsory, low-value exercise. During the first FRB presentation, the FRB will consider the Preliminary Investigation team's plans and recommendations for collecting additional data and either approve this course of action or modify it.

There are a broad range of "best practices" that should be considered and adopted during the Preliminary Investigation process. The Preliminary Investigation process can be broken down into the following sub-phases:

- Additional safeguarding activities and data preservation
- Configuration containment controls and responsibilities
- Failure investigation plan and responsibilities
- Initial troubleshooting, data collection and failure analysis (prior to breaking configuration) including failure timeline and primary factual data set related to failure event

### **6.2.1 Additional Safeguarding Activities and Data Preservation**

The actions of the Preliminary Investigation team should be to verify the immediate safe guarding actions taken earlier were done adequately. This includes verification of the initial assessment of damage and hardware conditions. This should also include verification of data systems integrity and collected data prior to, and immediately after, the failure event occurrence. Once the area and systems are judged secure, additional considerations should be given to collecting initial photographic/video evidence and key eyewitness accounts (i.e., documented interviews). When the immediate actions are completed, securing the systems and the test area from further disturbance finalizes these actions.

### **6.2.2 Configuration Containment Controls and Responsibilities**

Immediately following the safe-guarding and data-preservation actions, the Preliminary Investigation team, with help from the FRB and/or the program, should establish: area-access limitations, initial-investigation constraints, and configuration-containment controls. The organization responsible for this should be involved in any further investigation requirements that could compromise evidence that may support the investigation. While this is often assigned to the Quality or Safety organizations it may vary across different companies and government organizations.

### **6.2.3 Failure Investigation Plan and Responsibilities**

Overall responsibility for the investigation planning and execution is assigned by management. The lead investigator may or may not be part of the test team and should be intimately familiar with the test objectives, planning, and the system or component. Either a Chief or Senior Systems Engineer would be a suitable candidate for this role but other organizations may have special expertise in failure investigation that may warrant consideration for the leadership role. The team members should include the most knowledgeable of the UUT regardless of whether they are part of the UUT test team. The Systems Engineering and Quality organizations or their equivalents play an integral role in supporting the lead investigator throughout the investigation. Other key team members are dependent

on the system that failed and the nature of the failure but careful consideration of staffing the investigation team is important to the planning effort.

The plan should include initial FRB requirements and responsibility unless the program or company has a standing FRB organization in place. Concurrence with the investigation plan should include the lead investigator, or more commonly known as the FRB chair.

Unless the failure is clearly understood and/or the investigation plan is judged by the FRB and program management to be covered by existing procedures related to failure investigations, an independent investigation plan should be developed. The investigation plan should clearly identify the roles and responsibilities of the investigation team, resource requirements from the test team and supporting organizations and the details of inspection, test, analysis, and demonstration required to conduct the investigation and drive towards understanding and demonstrating root cause. The plan should be approved by program management.

An initial version of a root-cause-analysis tool assessment (e.g., a fishbone, truth table or fault tree) may be generated during the initial planning phase to help steer and substantiate the investigation requirements. The associated investigation-plan should be controlled so that misunderstandings among the team participants do not compromise or delay the investigation. One approach is to place the plan under configuration control. Alternatively, many contractors find it helpful to require FRB review of all investigation-plan changes. In that case, details regarding the plan are placed in FRB presentation packages. Depending on the agility of the contractor's configuration-management and FRB processes, the latter approach may reduce bureaucratic investigation delays. In either case, the goal is to enforce discipline on the investigation to maximize the likelihood of finding root cause and minimize opportunities for damaging hardware.

#### **6.2.4 Initial Data Collection and Failure Analysis (Prior to Breaking Configuration)**

The preliminary investigation team should establish a repository for archiving data related to the failure; non-invasive troubleshooting activities such as visual inspections or data review could aid in uncovering the cause of the anomaly. If necessary, photograph the hardware and test setup in order to document the existing test condition or configuration. Record all observables including the date and time of the failures, test type, test setup and fixtures, test conditions, and those involved with the test. In the event the nature of the failure precludes these types of non-invasive steps (e.g., a catastrophic test failure), immediate recovery plans should be made. The FRB chair should be kept apprised of these activities by the investigation lead and have the opportunity to communicate any concerns that may compromise potential evidence or future investigation activities. Typical data products of interest at this stage include failure timelines, initial efforts to replicate the failure, and preliminary analysis of test data (digital, analog, and imagery) that may affect or shape follow-on inspections, test, analyses, and demonstrations once the test configuration is broken.

Experience has demonstrated that at this point in the process, a common investigation database facilitates the timely flow of information among the FRB and investigation participants. The database is preferably electronic and accessible by all parties including the FRB. The structure of the database will vary and should be tailored to the specifics of the failure and the system involved but should be aligned with the investigation plan and the selected root-cause-analysis tool. As part of this database, the investigation team should begin to integrate and summarize information that will support the FRB presentation packages as described in Section 6, "FRB Meeting Closure." Caution should be used to segregate working database files from the investigation evidence as identified by the investigation team leadership.

### **6.3 Root Cause Investigation: Perform Root-Cause Test and Analysis**

As the Preliminary Investigation transitions to the Root-Cause-Investigation element, the investigative team accumulates enough data to begin hypothesizing about direct causes, contributing causes, and root cause. Interfaces and integration consistent with the investigation plan and a structured root cause analysis tool should be documented and maintained to drive investigation priorities and maximize the likelihood of ultimately determining root cause. The team may employ tools such as affinity diagrams, cause and effect fishbone diagrams, truth tables, 5 why's, process maps, fault tree analysis, timeline analysis, and brainstorming to manage the data-gathering and analysis processes. The investigative team may return to present results and plans to the FRB several times before closing a root-cause investigation. The FRB will generally manage complex and high-risk root-cause investigations by mandating conditions on the investigative team for returning to the FRB with new findings. At each meeting, the FRB will review the investigative team's recommendations for additional data gathering. The investigation should follow the facts and data in a systematic manner. Doing so will improve the chances that the investigation will lead logically to direct causes, contributing causes, and root cause and usually reduces extraneous activities that place unwelcome demands on program costs and schedule. Part of the FRB's role is to ensure any external/outside experts or independent review teams evaluate and weigh in on the relative merits of various troubleshooting activities and emerging conclusions. This is especially important when the investigative team determines that the root-cause activity requires invasive troubleshooting or breaks in configuration. Breaking configuration too early in a troubleshooting process may lead to an unverified or unknown direct cause failure, and invasive disassembly of the flight system or component may lead to unnecessary cost and schedule delays. The FRB can also allocate program resources (e.g., test sets, test beds, and key personnel) to more effectively address high priority investigations. The key output from this element is a systematic development and documentation of credible hypotheses based on evidence to drive towards determination of root cause.

The physical evidence process that is obtained by examination of the failed hardware is a key part of the root cause investigation. It can also be misunderstood. The physical examination (performed in a lab environment using the "Destructive Physical Analysis" tools identified in Table 7 in Appendix D) of the failed test article can provide key information that will direct the remainder of the investigation. The physical examination can explain "how" the failed test article failed. This is also termed as the "failure mechanism" being determined. This is an important differentiation to "why" the failed test article failed, which is root cause. It is important that the physical hardware steps will only provide failure mechanism (the "how"). It is review of other evidence (mostly supplemental analyses) that can lead to determination of root cause (the "why"). An example that illustrates these points is a fractured bolt. If the physical examination concluded the failure mechanism were ductile overload, the investigation would focus on means that applied the overload. If, however, the bolt broke in a brittle manner, the investigation would look at the material qualification or manufacturing process. In summary, the "how it broke" information helps lead to the "why it broke" determination.

Appendix C provides a summary of Root Cause Analysis Tools and Appendix D provides a listing and description of other root cause investigation tools and techniques that may be considered.

### **6.4 Root Cause Determination: Root Cause Determined or Undetermined**

The Root-Cause-Determination process element represents the formal review of data collected during the previous process element (Root-Cause Investigation) among the collective disciplines comprising the FRB. The FRB provides a high-level forum for the presentation of the hypotheses and supporting facts obtained in the Root-Cause-Investigation element. The FRB may either agree or disagree with its investigative team's root-cause analyses, and if in disagreement will often direct the team to gather more information or adopt alternative plans. In this manner root cause analysis and root cause

determination are typically an iterative process. Practical considerations may sometimes render a particular failure not amenable to a root-cause determination. This can lead to an alternate process that deals with unverified failures or unknown cause failures—the absence of the failure after implementing remedial actions does not prove the effectiveness of the actions. Sometimes programmatic considerations (cost, schedule, safety of the system or component or personnel) may limit the scope of an investigation and make an accurate determination of direct causes impossible. In either case, the absence of definitive information about direct causes makes subsequent analyses of root causes highly speculative and requires significant effort to determine risk of proceeding without a determined root cause. Appendix D provides a number of examples of tools and techniques that can be used to improve confidence an investigation ends with root cause determined or undetermined.

#### **6.4.1 Root Cause Determined**

The causes of many test failures will be isolated with certainty. A structured investigation process supported by a formal root cause analysis tool is critical in effectively capturing the necessary evidence to clearly demonstrate proof that cause has been identified and understood. This is the ideal outcome of a failure investigation as it allows for mitigation activity to be performed with confidence that the ending risk posture will be acceptable.

#### **6.4.2 Unknown Root Cause**

The direct causes of many test failures will be isolated with certainty. The failure investigation succeeds in determining the event or condition that is immediately responsible for causing the failure. As an example, the direct cause of a failure might be a bad solder joint. Digging deeper toward root cause, the investigation team might, for any number of reasons, not completely close on the reasons for this defect. Candidate contributing and root causes could include poor visual access to the solder joint (a design issue), technician and inspector training, and equipment malfunction (a failed soldering iron or power supply). Repairing the solder joint ostensibly brings the hardware into conformance with the relevant specifications, but the investigation cannot immediately prove the absence of additional solder-joint defects in this or other hardware built in the associated manufacturing area. The team will probably recommend inspecting the box for other defects during the repair operation. In addition, the team might interview the technician and inspector, evaluate these individuals' experience and past performance, and test the manufacturing equipment. Regardless of the outcome and additional risk-reduction activities associated with this part of the investigation, the team has already significantly reduced risk to the program by identifying the failed solder joint and thereby reducing the range of possible root causes to a manageable level. This contrasts significantly with an investigation that fails to identify the defective solder joint as the direct cause even though, strictly speaking, neither investigation identifies the ultimate root cause of the failure.

#### **6.4.3 Unverified Failure or Unknown Direct Cause**

When circumstances and supporting evidence prevent direct cause from being determined, three possibilities exist regarding knowledge as to the source of the failure.

1. It may be possible to determine the source of the failure is the support equipment.
2. It may be possible to determine the source of the failure is the flight system.
3. It may not be possible to determine if the source of the failure is the flight equipment or the support equipment.

Some failures provide sufficient evidence for the investigation team and FRB to determine the failure originated with the support systems. Such anomalies are effectively a “no failure” condition from a flight system perspective. While these “failures” are at least inconvenient, they may be determined to



not present a risk to the flight system as long as overstress conditions are properly addressed and applicable corrective actions that address the support system problem are effectively implemented.

Some failures provide sufficient evidence for the investigation team and FRB to determine the failure originated in the flight system. However, for technical or programmatic reasons, the troubleshooting is unable to determine the direct cause. The phrase “unknown direct cause” is sometimes used to describe failures isolated either to the UUT or the support equipment, whose direct cause cannot be found.

Some failures do not provide sufficient evidence for the investigation team and FRB to determine if the cause originates in the flight system or the support systems. These failures typically involve transient symptoms. For these failures, the symptoms usually “evaporate” before it is possible to isolate the source of the failure to the flight or support systems. The phrase “failure not verified” or “unverified failure” is sometimes used to describe this type of failure. After parsing the types of failures that resist direct cause investigations, two types remain that are threats to flight systems.

1. Failures that are known to originate in flight equipment (possibility 2 above)
2. Failures that may or may not originate in flight systems (possibility 3 above)

The discussion of UVFs and other types of failures in this section is intended to aid in understanding the subtleties of types of test failures, to aid in failure investigation approaches, and provide standard terms for communication. The range of test failures extends beyond this discussion. Other sections of this document advise extra scrutiny for “UVFs.” This discussion of failures that resist direct cause determination is not intended to mandate particular investigation processes for particular failures. Programs need to assess failures on a case by case basis, consistent with their risk tolerance, to determine how to conduct particular failure investigations.

In the event of an UVF, a wide range of understanding and supporting evidence can exist regarding failures where the cause cannot be definitively determined. Examples include failures that appear to “self heal” and are not repeatable, or when the majority of the evidence supports a “most probable” cause but confounding supporting evidence exists for other possible causes. In this event, the FRB emphasis on understanding the consequence and probability of the failure re-occurring is paramount. Confidence in remedial actions that address the potential failure, such as worst case change out of the failed systems, is integral to proceeding with an acceptable risk-based corrective action for the failure. The FRB is the first line element in the determination of risk based considerations for failure resolution. Program and/or enterprise/customer limits of authority should be imposed on FRB authority in the event of an unverified failure conclusion to an FRB and the related risk acceptance. It is highly recommended that these limits be clearly defined in program FRB requirements documents and procedures at the executive level of the organization for senior FRB processing to be in place to accommodate this category of outcome. Senior FRB members typically span the enterprise and consist of Chief Engineers, directors and/or company vice-presidents allowing for a broad experience base with access to personnel and resources outside that of the typical program FRB. Unless the failure is at a very low level of the system hierarchy and has very low consequences if it re-occurs a Senior FRB is considered a highly recommended best practice.

As mentioned, Appendix H.2 is offered as representative checklists or criteria to consider when a failure investigation ends without root cause being determined. Caution should be used when halting an investigation prior to determining root cause as it may become necessary to implement many other corrective actions to address all possible causes.

## **6.5 Remedial, Corrective, and Preventive Action Implementation**

Whether the Root-Cause-Determination step leads to a determined root cause, a set of validated direct causes and contributing factors, or an UVF; the FRB will generally implement remedial, corrective, and/or preventive actions associated with the root-cause investigation. At this stage, the FRB-mandates remedial actions that address the direct cause of the failure (e.g., replacing a failed component), corrective actions that address the root cause and contributing factors, and preventive actions that address the prevention of a failure (e.g., instituting effective part screens that eliminate the occurrence of flawed components in the system). The FRB should document evidence that the actions have had the desired effects on the UUT. As an example, an FRB may require retest of a reworked or repaired UUT, and the FRB records should contain the successful completion of the retest. This proves that the remedial actions have effectively addressed the direct causes of the failure. If an FRB mandated corrective action is not implemented by the program, then the FRB should provide the program the risk associated with not implementing the corrective action, which is then captured in the program's risk management process.

The FRB should document preventive actions and their outcomes as well, but preventive actions may sometimes have enterprise-wide implications. In these cases, programs may not be able, in a reasonable period, to include the outcome of preventive-action steps within FRB documentation. Nevertheless, it is a good practice to show, within the FRB documentation, how the preventive actions were flowed to the enterprise or beyond to correct generic flaws. Programs should document all available data concerning the corrective/preventive action process (e.g., remedial actions and their successful outcomes) in a closed-loop tracking tool such as a nonconformance database.

## **6.6 Closure: Close FRB Records**

This section summarizes the typical content of the FRB closure package. It is highly recommended that early in the investigation the investigation team adopts a working data package and continuously updates its contents. This summary data package can be supplemented by the necessary analysis, test, and assessment planning and results documentation as suggested in Appendix A. The content and amount of detail contained in successive versions of this summary data package can be tailored as required as the investigation matures. The remainder of this section is focused on the requirements of the final failure investigation FRB package as presented by the investigation team.

### **6.6.1 Entry Criteria (Pre-review Requirements)**

The decision to convene the final FRB meeting should be mutually agreed to by the investigation lead and the FRB chair. The suggested minimum entry criteria to the final FRB presentation include the following.

- Completion of the failure investigation plan
- Determination of root cause or the exhaustion of all reasonable efforts to determine root cause
  - Basis of investigation results documented via selected root-cause-analysis tool
  - Residual risk assessment developed commensurate with understanding and basis for failure cause
- Remedial actions and corrective actions

- Identification of potential impact to similar components, subsystems, and/or systems on the same and other programs
- Forward plans and actions
- Recommend corrective and/or preventive actions for enterprise consideration

### 6.6.2 Documentation (Typical Package Contents)

The following table is provided as a template for the content of the FRB closure package. The sequence and specific content may vary depending on the failure under review but it is recommended that each of the elements of this template be considered for inclusion in the FRB closure package.

Table 4. FRB Closure Package Template

Agenda Item	Description
Purpose of FRB	Briefing purpose and expectations
Summary of Failure Event and Pertinent Background	Summary description of failure event including high level system or component and test description, what requirement has failed (e.g., Spec/Req id number), Failure Timelines, Pertinent data related to failure
Impact Assessment/ Containment	Implications of failure event and current system or component containment status
Investigation Approach	Summary of failure investigation plan elements, key activities and investigation logic
Investigation Results	Key investigation findings, observations, analyses, test and other assessments
Root Cause Analysis and Contributing Factors	Root Cause Analysis approach, supporting data and results
Overstress Analysis	Should address mechanical and thermal overstress as well as electrical overstress
Disposition of Failed Hardware/Software	Recommended actions (remedial actions) that specifically address the nonconformance
Other Preventive/ Corrective Actions	Additional actions recommended to eliminate the possibility of recurrence and to prevent occurrence of other failures
Residual Risk Assessment	Risk remaining to system especially if root cause is not identified. See, for example, the discussion in Section 6.4
Scope of Failure/Other Affected Hardware/ Software	Impact to other similar and related hardware/software on this and other company programs, potential impact to programs outside the company
Recommendations to FRB/Path Forward	Summary recommendations and open work
Optional: Executive Summary	Prepared for FRB use to communicate failure results and recommendation to management/customer elements
FRB Caucus <ul style="list-style-type: none"> <li>• Open Actions</li> <li>• Constraints</li> <li>• Dissenting Opinions</li> </ul>	FRB assessment of investigation team's results and recommendations, identification of open actions/constraints and FRB poll

Agenda Item	Description
Back-up and Detailed Supporting Data	Supporting data as required

### 6.6.3 Exit Criteria

The exit criteria for the FRB meeting are based on the completion of the FRB assessment, open actions, constraints, and the final FRB poll. The possible outcomes of the FRB can be collected into two general categories.

1. Root cause is clearly understood and substantiated, disposition of the failed hardware/software directly addresses root cause and retest and other verifications are judged acceptable. Other corrective actions beyond the failure remedial actions are determined not to affect the system under review and are clearly stated with assigned responsibility to the interface organization (e.g., the CAB). The FRB would recommend closure to the program. Escalation of the failure review to a higher level of management is indicated if implementation of corrective actions is impossible or impractical and this leads to a high-risk that mission threatening failures may recur.
2. Root cause is not determined. The amount of underlying evidence supporting any proposed—albeit not proven—cause(s) can vary widely, thorough risk analysis definitively addressing mission risks is required.

The FRB may close if the analysis of the failure’s mission consequences proves acceptable to the program. This depends on program specifics but should consider some of the items discussed in Section 6.4. Escalation of the failure review to levels of management above the program leadership may be required if the risk analysis concludes that the failure may have significant mission consequences. All reasonable efforts to determine root cause have been completed.

FRB follow-on activities are shaped by the specific outcomes of the investigation including the investigation’s success in determination of root cause, the investigation team recommendations to address cause, assessment and acceptance requirements of remaining residual risk, and other failure related corrective actions. Section 7 provides more detail on some of the follow-on interface requirements of the FRB. The following list provides a summary of closure and follow on FRB requirements:

- Communication of FRB results to key stakeholders including, but not limited to, management and the customer
  - In the event of an undetermined root cause and/or significant residual risk ensuing from the failure investigation, the FRB and the investigation lead have the responsibility to communicate the risk and risk acceptance rationale to senior FRB as defined by enterprise governance procedures (see Section 6.4).
- Oversight and closure of specific actions and constraints identified in the final FRB review.

The FRB should provide a final report on the investigation outcome. The report may be a separate report or be comprised of the FRB presentation package supplemented by the results of the follow-on actions described above.

## **6.7 Enterprise Corrective Action Board: Possible Enterprise/Industry Alert Notification**

To the extent that FRB findings have implications to other programs and industry notification groups, the FRB will recommend actions to an enterprise-level corrective action board (CAB). This element includes the following:

- Communication of FRB results and oversight of responsibilities assigned to other program boards and organizations (e.g., corrective action, engineering and risk management boards, independent review teams and suppliers)
- Determination and assignment of responsibility for communicating FRB results that have implications to other program and industry notification groups as required by company procedures



## 7. Interfaces

The FRB has a number of interface responsibilities with other program boards, management and customer elements and external systems. A detailed discussion of the primary and most important interface relationships is defined below, while Table 5 provides a summary of the many other FRB interfaces. In each of the following discussions, the interfacing element is identified and a summary of the FRB relationship is included.

The following items are critical to an effective FRB and investigation team working relationship:

- Investigation Team Deliverables to FRB
  - Preliminary failure information including but not limited to a description of failure event including the system or component configuration, test objective and set-up, failure description and timeline/sequence of events, immediate containment measures, and preliminary data/findings
  - Detailed investigation plans for the FRB approval including investigation approach, responsibilities, techniques, tools, schedule, and internal/external communication plans
    - Updates as required
  - The failure investigation plan including root cause analysis
  - The FRB presentation package and input to the FRB's final report
  - A residual risk assessment as a standard part of any failure investigation. Note this standard practice becomes a critical element of forward plans if root cause remains undetermined
- FRB deliverables to the Investigation Team and Management
  - Review and approve (or modify) the investigation team's findings and recommendations including corrective actions and additional investigation
  - Provide a risk statement to the appropriate management and customer organizations
  - Provide results to affected interfacing organizations and notification systems as required
  - Prepare final report to include final failure results and recommendations documentation and ensure corrective actions/notifications are properly closed by the responsible organizations
  - Documentation of recommendations of FRB process lessons learned and best practices for incorporation into future FRBs

Table 5. A Summary of the Other Typical Interface Relationships of the FRB

Interfacing Element	Relationship to the FRB	FRB Inputs and Outputs
Corrective Action Board (CAB)	Evaluation, management and closure of failure investigation preventive actions	<ul style="list-style-type: none"> <li>• Recommended specific corrective actions. CAB may provide corrective action closure to FRB</li> <li>• FRB may perform CAB function if the corrective action is being implemented immediately (before the FRB closes).</li> <li>• FRB reports failure data to the CAB for trending and systemic corrective action.</li> <li>• FRB reports preventive actions to the CAB for evaluation and action.</li> </ul>
Program Management	Charters FRB, assigns FRB chair and provides investigation resources per specific contract provisions (if applicable) and enterprise governance	<ul style="list-style-type: none"> <li>• Regular investigation status and final recommendations including residual risk assessment</li> </ul>
Customer	This interface may be through program management or as a direct member of the FRB (depends on contract provisions)	<ul style="list-style-type: none"> <li>• Regular investigation status and final recommendations per program requirements including residual risk assessment</li> </ul>
Engineering Review Board/Change Control Board (ERB/CCB)	FRB forwards all configuration issues and appropriate recommendations to this board for resolution	<ul style="list-style-type: none"> <li>• Regular investigation status and final recommendations per program requirements</li> <li>• FRB reports applicable data for trending and systemic corrective action of items</li> </ul>
Independent Review Team (IRT)	Independent of program and typically performs technical oversight of investigation and FRB activities and recommendations.	<ul style="list-style-type: none"> <li>• Regular investigation status and final recommendations</li> <li>• IRT may request and/or perform unique investigation analysis, test or other assessments</li> </ul>
Material Review Board (MRB)	MRB will escalate to an FRB based on program FRB threshold criteria. MRB supports detailed investigation activities as required and may act as FRB agent in day to day investigation decision making and controls	<ul style="list-style-type: none"> <li>• FRB recommendations are subject to standard MRB disposition and documentation processes</li> </ul>



Interfacing Element	Relationship to the FRB	FRB Inputs and Outputs
Parts, Material and Processes Control Board (PMPCB)	Monitors FRB and investigation activity and dispositions FRB recommendations as they apply to PMPCB responsibility and documentation requirements	<ul style="list-style-type: none"> <li>FRB should issue alerts per company process to attain containment or if this action is restricted to PMPCB a closed-loop action should be assigned.</li> <li>FRB reports trend data for systemic corrective action of items</li> </ul>
Qualification Review Board (QRB)	Independent of program and performs technical oversight of qualification across the program engineering functions	<ul style="list-style-type: none"> <li>Interacts with the FRB on proto-qualification or qualification anomalies and failures.</li> </ul>
Risk Management Board (RMB)	Monitors FRB and investigation activity and dispositions FRB recommendations as they apply to risk management responsibility and documentation requirements. May develop specific or general program risk elements dependent on failure investigation progress and outcome.	<ul style="list-style-type: none"> <li>Regular investigation status and final recommendations including residual risk assessment that is then captured by the RMB</li> </ul>
Software Change Control Board	A designated group of engineering and other professionals who evaluate SW change requests to SW that is under configuration control and determining the design, code, and unit test requirements to implement them	<ul style="list-style-type: none"> <li>FRB may typically provide evidence and test data indicating failures that are a result of SW, or where SW changes are warranted to make the overall system more robust</li> </ul>
Suppliers and Subcontractors	Subject to specific program FRB plans and requirements. May conduct internal FRBs and report results and recommendations to prime contractor or prime contractor FRB process may supersede internal supplier/contractor FRB (program and failure significance dependent).	<ul style="list-style-type: none"> <li>May typically provide supplier/contractor FRB oversight and acceptance.</li> </ul>
Escalated FRBs (e.g., senior management, enterprise or corporate FRBs)	A higher level management, enterprise or corporate level of oversight and decision making that accepts the risk posture from the FRB recommendation	<ul style="list-style-type: none"> <li>Failure results outbrief, residual risk assessment of failure remedial actions and broader failure containment recommendations</li> </ul>
Other Program, Government and Industry Notification Systems	Failures are subject to internal company and program systemic issues database requirements as applicable. In the event failures are determined to potentially affect similar components, subsystems, and/or systems, appropriate steps should be taken to provide notification of failure to external notification systems	<ul style="list-style-type: none"> <li>FRB recommendations will address notification of failure and potential implications to similar components, subsystems, and systems per company and program contract requirements to internal and external tracking systems.</li> </ul>



## Appendix A. FRB Template

### A.1 FRB Outline

1. Purpose of Meeting
2. Background
3. Investigation: Process/Results
4. Fishbone Analysis
5. Root Cause
6. Overstress Analysis
7. Disposition of Hardware/Software
8. Path Forward/Plan
9. Scope of the Issue/Other affected hardware
10. Preventive Correction Action
11. Action Log/Authorizations
12. Closeout

### A.2 Purpose of Meeting

One sentence that communicates the desired outcome from the Failure Review Board; examples of single sentences that meet this intent are:

Obtain authorization to disassemble hardware to confirm that the most probable cause theory is the root cause (Preliminary or Interim FRB).

or

Obtain authorization to repair failed hardware to the provided plan (Preliminary or Interim FRB).

or

Obtain authorization to close the Failure Investigation (Final FRB).

### A.3 Background (1 of x)

- On \_\_\_\_\_, a failure was first observed on \_\_\_\_\_
  - Configuration of product
  - Test setup (schematic/block diagram) and location
  - What was observed? (should be vs observed)
  - What is the failure?
- On \_\_\_\_\_, a failure was confirmed on \_\_\_\_\_
  - Relevant fact
  - Fact
  - Fact
  - Schematic
  - Block diagram with interfaces defined
  - Picture
  - Drawing

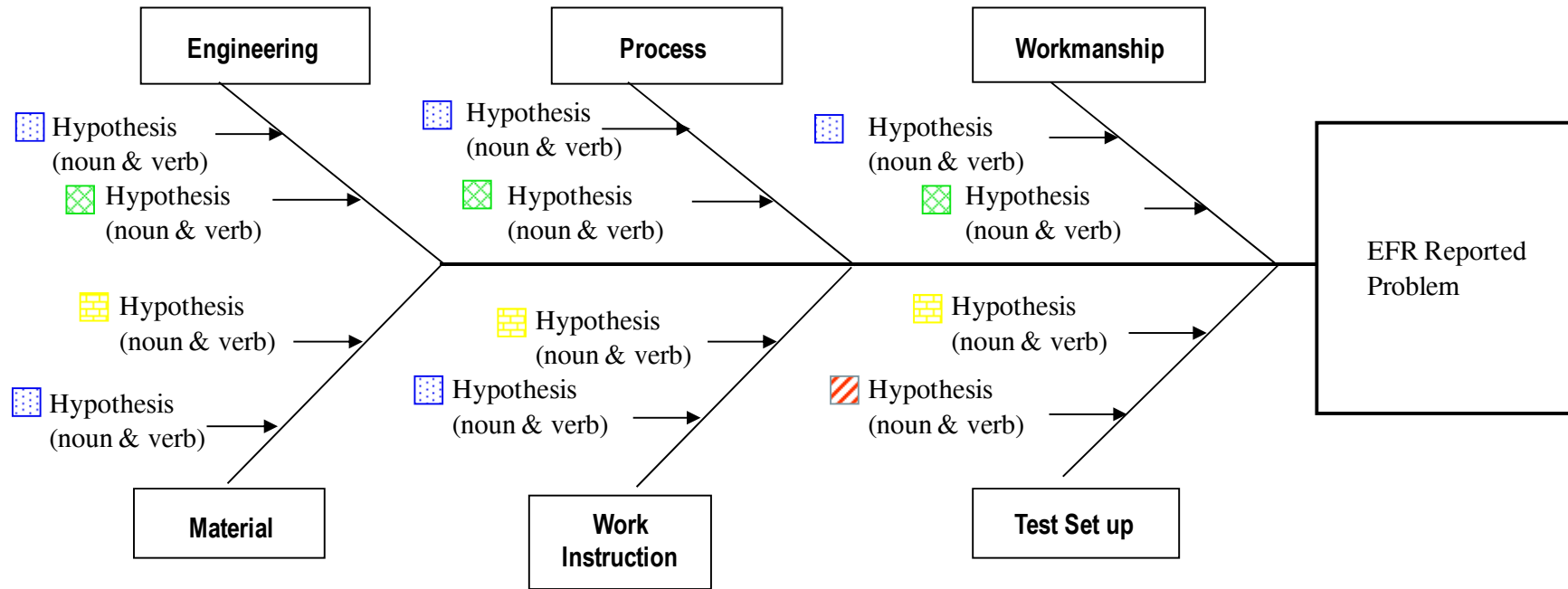
- References
  - TPs
  - STE liens
  - SRS (number and date); VDD (number and date)
  - Relevant SCRs (number and date)

#### **A.4 Investigation (1 of x) Note: Add Date(s) as Required**

- Summary of process/steps taken to find root cause
  - Summary timeline
  - Relevant configuration changes
  - Fact
  - Fact
  - Results
- Speculation as to root cause
  - What it is not...and why?
  - What it still could be...and why?
  - What is current theory on root cause or most probable cause

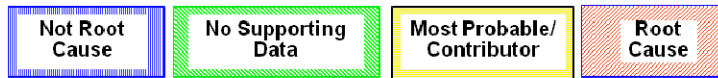
## A.5 Fishbone Analysis

(Sample Fishbone)



	<b>Color code</b>		<b>Blue</b>	: Proven not root cause
			<b>Green</b>	: No supporting data as root cause
			<b>Yellow</b>	: Suspect most probable/Contributing Factor
			<b>Red</b>	: Root cause

### A.6 Fishbone Disposition



Description (Hypothesis)	Not Root Cause	No Supporting Data	Most Probable/Contributor	Root Cause	Disposition (Supports or Refutes)

### A.7 Root Cause

- State the theory of root cause
- Document all supporting data to the root cause theory
  - Fact
  - Fact
  - Fact
  - Fact
  - Fact
- Document all of the data that still does not fit the theory (if any)
- Contributing Factors
  - i.e., Test and inspection did not detect problem

**We Have Determined The (Most Probable) Root Cause To Be ...**

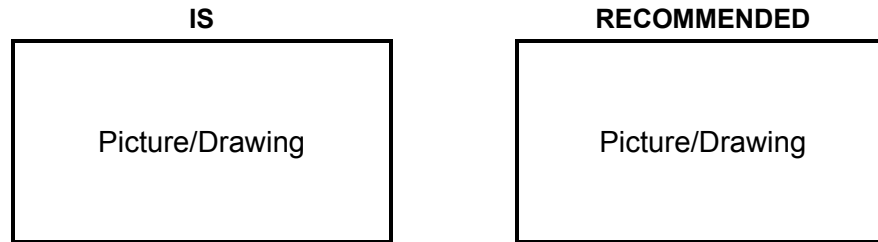
### A.8 Overstress Analysis

- Mechanical Overstress – None or Yes
  - Supporting data
- Electrical Overstress – None or Yes
  - Supporting data

- Hardware Safety – No Issues or Issue
  - Supporting data
- Test Validity – No Issues or Issue
  - Supporting data

### A.9 Disposition of Hardware/Software

- Describe the change to be or that has been incorporated



- Process Description
- Retest/Requalification
- How can we be assured this will not fail
  - Inspection/Retest
  - Qualification

### A.10 Path Forward/Plan Note: Add Date(s) As Required

- Plan
  - Key events (repair/rework, re-test, and penalty tests)
  - Key dates
- Actions taken or to be taken
  - Gates to assure success (changes in design, drawings, TPs, and Corrective Action Board inputs)

### A.11 Scope of the Issue/Other Affected Hardware

- Does the possibility of this failure exist anywhere else on this program
  - If not, why not: Prove it
  - If so, where: What are you going to do about it? When?
- Determine the possible reachback implications to Payload/Space Vehicle integration and test.
  - State any actions that must be taken

- Does the possibility of this failure exist anywhere else beyond this program?
  - If not why not: Prove it
  - If so where: What are you going to do about it?
    - GIDEP?
    - Customer alert?

**A.12 Corrective Action/Preventive Corrective Action**

- Corrective action
  - Supporting data
- Preventive action
  - Modify process
  - Modify procedure
  - Ensure compliance
  - Metrics on progress

Note: This escape caused significant impact to the program. What was the root cause? Immediate cause is NOT the same as root cause. What preventive corrective action is your company going to take to prevent recurrence of this type of failure in the future?

**A.13 Action Log/Authorizations**

- Date\_\_\_\_\_ Interim FRB 1
  - Action 1: \_\_\_\_\_ Status \_\_\_\_\_
  - Action 2: \_\_\_\_\_ Status \_\_\_\_\_
  - Action 3: \_\_\_\_\_ Status \_\_\_\_\_
- Date\_\_\_\_\_ Interim FRB 1
  - Action 1: \_\_\_\_\_ Status \_\_\_\_\_
  - Action 2: \_\_\_\_\_ Status \_\_\_\_\_
  - Authorization Provided \_\_\_\_\_
- Date\_\_\_\_\_ : Final



**A.14 FRB xxxxx Closeout**

Name	Title	Signature	Date
Your Name	Responsible Engineer		
IPTL's Name	IPTL		
Name	Reliability Engineer		
Name	System Engineering		
Name	Quality		
Name	Program Office / FRB Chairman		
Name	Customer FRB Representative, if appropriate		



## Appendix B. Suggested Checklists

The following Failure Investigation/FRB “checklists” are offered to provide additional guidance to the execution of the FRB process with respect to addressing root cause versus cause-unknown failures versus unverified failures and to guide escalation decision making.

### B.1 Criteria for Root Cause Acceptance and Closure

#### 1. Failure Review Board Responsibilities

- 1.1. Each member be adequately trained in several methods of formal root cause identification. This helps in discussions and understandings of what is a true root cause.
- 1.2. Test proposed root causes against the seven elements of technical rationale described below.
  - 1.2.1. ATK scores each of these as strong, medium, weak
  - 1.2.2. ATK realizes that there is seldom “Strong” justification in all elements, hence the need for a board to exercise judgment in accepting a root cause. However, by covering each of these items and a preponderance of evidence, a FRB can have a justifiable level of confidence in accepting a root cause.

#### 2. Seven Elements of Technical Rationale – Description

- 2.1. **Solid Technical Understanding:** A physics-based or root cause understanding of the issue exists (based on engineering data). Ask and answer questions such as:
  - 2.1.1. Do we know how/why this condition occurred (impact, scrape, ageout, moisture loss, and residual stress)?
  - 2.1.2. Did we use a fault tree?
  - 2.1.3. Do we understand the extent of the defect?
  - 2.1.4. Do we know what the foreign material is?
  - 2.1.5. What are the plausible contaminants and how could they be harmful?
  - 2.1.6. Do we understand how/why components with similar indications performed the way they did?
  - 2.1.7. Is there a fix/repair for this unit/article?
  - 2.1.8. Do we understand the repair process/condition?
  - 2.1.9. Are the generic design and process robust and in control?
- 2.2. **Condition Relative to Experience Base:** The condition is compared to the experience base. Ask and answer questions such as:
  - 2.2.1. Have we dealt with this problem before?
  - 2.2.2. How is this the same or different?

- 2.2.3. Do we have flight or test history with this defect?
- 2.2.4. With this repair?
- 2.2.5. Other motors or programs?
- 2.3. **Bounding Case Established:** The physics-based understanding is used to determine the bounding case. Ask and answer questions such as:
  - 2.3.1. What bounding scenarios (test and analysis) have been evaluated in the attempt to bound or envelope the issue (e.g., upper  $3\sigma$  loads, lower A basis allowables, a specific worse case system or component condition)?
  - 2.3.2. What assumptions were made?
  - 2.3.3. Where are they conservative? Not?
  - 2.3.4. Were all the failure modes addressed?
  - 2.3.5. Have we assessed the “what if we’re wrong” scenarios?
- 2.4. **Self Limiting Aspects:** Physical reasons exist that prevent the condition from getting worse than the bounding case or that show the part is fail-safe. Ask and answer questions such as:
  - 2.4.1. Physical reasons why the defect or condition will not get worse than current state or degrade.
  - 2.4.2. Why can the condition never exceed the bounding case?
  - 2.4.3. Is the system fail-safe or fault/failure-tolerant?
  - 2.4.4. Are there built in redundancies if the feature does fail?
- 2.5. **Margins Understood:** Adequate margins exist, ideally not substantially reduced from baseline. Ask and answer questions such as:
  - 2.5.1. What are the predicted margins for the discrepant or repaired part?
  - 2.5.2. Have they changed from baseline?
  - 2.5.3. What are the margins for the bounding case?
  - 2.5.4. Is the component/feature in an area of high or low thermal or structural margin?
  - 2.5.5. How far are we from a cliff?
- 2.6. **Assessment Based on Data, Testing and Analysis:** Final risk assessment is based on test data and analysis, not on gut feel or expert opinion. Ask and answer questions such as:
  - 2.6.1. Is the final assessment based on test data and analysis or on expert opinion and gut feel?
  - 2.6.2. Where do we actually have data?
  - 2.6.3. Where are we guessing?

- 2.6.4. Was the test/measurement/analysis technique standard and proven or new?
- 2.6.5. Do we understand all the assumptions that went into the assessment?
- 2.6.6. Does the analysis/assessment rely on a series of dependent assumptions (where an error could propagate) or are there independent elements or blocks?
- 2.7. **Interaction with other Elements/Conditions Addressed:** Interactions with other conditions (MRB, changes, technical issues) and system elements. Ask and answer questions such as:
  - 2.8. Are there any known, compounding interactions with other issues, components, and changes?
  - 2.9. How have the potential interactions been identified?
  - 2.10. How/when will they be addressed?

**B.2 Unverified Failure Checklist/Questions**

1	What was the nonconformance? Describe all significant events leading up to the occurrence. Describe the trouble shooting conducted and the results. Note: A Fishbone Analysis or FMEA is recommended as an aid in presenting this data. Describe how each possible source of the nonconformance was dispositioned. (attach to form if available)
2	What was the test hardware/software configuration at the time of the nonconformance (i.e., if at system test, were all flight items installed)? Were some non-flight items installed? If at subsystem or unit level, were all flight components installed?) Describe the level of any software in use at the time of the nonconformance, if applicable (i.e., was flight code installed at the time of the nonconformance)?
3	What test was in process and were multiple tests being performed simultaneously?
4	Did the nonconformance repeat or were there any attempts to repeat the nonconformance? If so, what was the result? Also, describe any troubleshooting performed while the nonconformance was present.
5	If the nonconformance cleared, what happened to cause the nonconformance to clear? What efforts were made to get the nonconformance to repeat? Were the hardware/software configurations identical to the original condition? If not, what were the differences, why were the differences necessary?
6	Was there any cumulative “nonconformance free” testing or re-testing that occurred after the event(s)?
7	Does a failure analysis of the problem clearly lead to assigning the nonconformance to a specific part or product? Was that part or product replaced? If so, when the part or product was fixed, was the problem cleared?
8	What would be required to perform a worst-case rework/repair? Was that performed? If not, describe the reason.
9	Did the nonconformance cause any overstress (consequential impact)? Is the overstress analysis documented? If not addressed, what was the rationale for not addressing the overstress issue?
10	Are there other relevant failures on other items or systems? If the failure is in a component/piece part, what is the failure history of that part? How many like units have been built and what is their performance record?

11	If the nonconformance was traced to a part, what were the results of the failure analysis/DPA (e.g., did destructive physical analysis [DPA] confirm the failure)?
12	Were any troubleshooting steps considered and not performed due to cost or schedule concerns? Could these troubleshooting steps determine the cause of the nonconformance. Describe the reasonableness/risk in performing this troubleshooting now.
13	Are there operational workarounds possible to mitigate the effect of this nonconformance? Could they be implemented within the mission?

### B.3 Checklist for Closure of Unknown Direct Cause Test Failures/Anomalies

Failure Report number: \_\_\_\_\_ Preparer: \_\_\_\_\_

Step No.	Step/Requirement	Program Name	Record specifics of this test anomaly or refer to attachment(s) with the appropriate specifics <sup>1</sup> . If a step is not applicable explain why.	Record Independent Review Participants	Signature, date, and Empl ID <sup>2</sup>
1	Test configuration a) Describe the test configuration. Include flight and/or test S/W versions in use. b) What aspects were different from flight configuration?				
2	Item <sup>3</sup> test history a) List and describe prior test occasions. b) Describe any troubleshooting done while the test anomaly was present. Describe conditions and actions immediately preceding and surrounding the test anomaly beyond the steps and conditions prescribed by the applicable operating instructions or test procedures. c) Describe other pertinent EFRs, reports, and bulletins. Did the test anomaly look like an existing report? d) Were there non-released instructions in use? e) Was there a technical review of the prior test data sheets after the anomaly occurred? Had the test been done previously? If so, when and what were the results?				
3	Causes considered at the time of the test anomaly List everything (including STE) that was considered as a cause.				

Step No.	Step/Requirement	Program Name	Record specifics of this test anomaly or refer to attachment(s) with the appropriate specifics <sup>1</sup> . If a step is not applicable explain why.	Record Independent Review Participants	Signature, date, and Empl ID <sup>2</sup>
4	<p>If the test anomaly cleared spontaneously:</p> <p>a) Describe what took place immediately prior to the clearing.</p> <p>b) Identify versions of S/W involved.</p> <p>c) If the item or STE was powered down, be specific about what was powered down and where in the troubleshooting sequence it occurred.</p> <p>d) Was the anomaly repeatable? If not, describe the attempts made to get it to repeat.</p> <p>e) List anomaly free testing/operating time that has accumulated since the test anomaly. Describe post-test anomaly testing; list all such test occasions.</p>				
5	<p>Internal failure mechanisms</p> <p>a) Consider what mechanisms internal to the item under test could have caused the test anomaly signature. Attach this analysis. An informal FMEA or a fishbone chart analysis would suffice but is not specifically required.</p> <p>b) Rank the identified possibilities by likelihood. Explain the ranking criteria?</p>				

Step No.	Step/Requirement	Program Name	Record specifics of this test anomaly or refer to attachment(s) with the appropriate specifics <sup>1</sup> . If a step is not applicable explain why.	Record Independent Review Participants	Signature, date, and Empl ID <sup>2</sup>
6	<p>Potential effects/impacts on higher levels of integration and mission</p> <p>a) Consider all possible impacts of the mechanisms identified in step 5 upon functions of higher levels of integration. What would be the consequences of recurrence (on the ground and/or during the mission)? Coordinate with engineering of higher levels of integration.</p> <p>b) Enter each effect into and attach an Impacts Table</p> <p>c) What function losses/degradations might have occurred during the anomaly but would not have been observed due to test configuration or test method?</p> <p>d) List any workarounds that could mitigate the impact of recurrence of this anomaly. Could they be implemented during the mission?</p>				
7	<p>Impacts of replacement</p> <p>a) List the impacts of replacement. Include technical and cost/schedule (ROM) impacts.</p> <p>b) What work has already been done?</p> <p>c) If the item were replaced, how could integration, test schedule, verification, and validation impacts be mitigated?</p>				



Step No.	Step/Requirement	Program Name	Record specifics of this test anomaly or refer to attachment(s) with the appropriate specifics <sup>1</sup> . If a step is not applicable explain why.	Record Independent Review Participants	Signature, date, and Empl ID <sup>2</sup>
8	<p>Impacts of rework/repair</p> <p>a) What work has already been done?</p> <p>b) Have all potential causes been reworked or repaired?</p> <p>c) What additional rework and/or repair would be required to remove all of the potential anomaly causes (identified in the analysis of step 5)?</p> <p>d) If rework or repair is chosen, list the impacts.</p> <p>e) How could integration, test, verification, and validation impacts be mitigated?</p> <p>f) What are the risks of such measures to the item to be reworked or repaired?</p>				
9	<p>Internal fixes</p> <p>a) If the analysis of step 5 identified components or subelements of the item that could have caused the test anomaly, were they replaced or fixed?</p> <p>b) List them in the order in which they were replaced or fixed.</p> <p>c) Did the test anomaly clear and, if so, after which fix?</p>				
10	<p>Overstresses</p> <p>a) List potential overstresses identified in the analysis of step 5.</p> <p>b) How were they addressed? List the pertinent steps taken for each.</p>				
11	<p>Off-program commonality</p> <p>a) Is the item common to other programs or systems with similar usage? List them.</p> <p>b) What is the off-program failure history of the item?</p> <p>Caution: Off-program confidentiality and/or security must be protected.</p>				
12	<p>If the test anomaly was traced to an electronic component, was a failure analysis or Destructive Physical Analysis (DPA) performed? Attach a summary of the results.</p>				

Step No.	Step/Requirement	Program Name	Record specifics of this test anomaly or refer to attachment(s) with the appropriate specifics <sup>1</sup> . If a step is not applicable explain why.	Record Independent Review Participants	Signature, date, and Empl ID <sup>2</sup>
13	Potential troubleshooting a) Were any troubleshooting steps considered but not performed due to cost, schedule, risk, or other concerns? List them. b) What is the likelihood for each that it would result in determination of the cause of the test anomaly? c) Explain the risks and problems in performing these steps and the rationale for not performing them.				
14	Describe any preventive actions that have been taken.				
15	Describe any planned troubleshooting (e.g., monitoring or testing) that will be performed to attempt to reproduce and/or isolate the anomaly.				
<sup>1</sup> Attachment(s) must be identified by the step/requirement number, signed with Employee ID, and dated. <sup>2</sup> Signature, date, and Employee ID are required for all items, including N/A items. <sup>3</sup> The term item used herein refers unit, subsystem, or system as is applicable to the test anomaly in question.					

Concurrence:

Independent Review Chairperson: \_\_\_\_\_

Chief Engineer, Space Systems: \_\_\_\_\_

Vice President, Engineering: \_\_\_\_\_

Vice President, Mission Assurance: \_\_\_\_\_

Vice President, "Product Area": \_\_\_\_\_

## **Appendix C. Suggested Root Cause Analysis Tools**

There are a number of well-established root cause analysis tools available to assist the determination of root cause. Each tool provides a structured methodology to identify possible causes, segregate improbable causes, and capture the failure investigation's inspection, test, analysis and demonstration evidence of cause in an organized structure. Early investigation adoption of a root cause corrective action (RCCA) tool also has high value in developing investigation plans and priorities. The selected RCCA tool is integral to the communication of cause to the FRB and subsequent management reviews if required.

The intent of this guideline is not to recommend one RCCA tool over the other as each has its merits and shortcomings. Organizational and customer preferences often influence selection of one tool over the other. Information on each tool is readily available within industry standards, public domain literature, and on the Internet. In addition, many companies that specialize in training and software application support in the use of these tools.

Fault trees, Fishbones, and Apollo root cause analysis tools are basically graphical representations of the failure cause domain. Each can also be viewed as an indented list as the diagrams may become very complex and difficult to manage in some failure investigations. An indented list also aids in aligning the investigation evidence against specific candidate causes as the investigation evolves and maintenance of an investigation database.

### **C.1 Fault Tree**

Fault tree diagrams are logic block diagrams that display the state of a system (top event) in terms of the states of its components (basic events). The failure event is represented as the top event. A fault tree diagram is built top-down and in terms of lower level events. It uses a graphic "model" of the pathways within a system that can lead to a foreseeable, undesirable loss event (i.e., a failure). The pathways interconnect contributory events and conditions, using standard logic symbols (AND and OR). The basic constructs in a fault tree diagram are gates and events.

### **C.2 Fishbone Diagram (Ishikawa Diagrams)**

Ishikawa diagrams (also called fishbone diagrams, cause-and-effect diagrams or Fishikawa) are diagrams that show the causes of a certain event—created by Kaoru Ishikawa (1990). Fishbone diagrams focus on identifying potential factors causing an overall effect in relation to the failure. Each cause or reason for imperfection is a source of variation. Causes are usually grouped into major categories to identify these sources of variation.

### **C.3 Apollo Root Cause Analysis**

Apollo root cause analysis focuses on identifying both conditions and actions that can lead to the problem outcome, and documenting evidence to confirm or deny each of them. This methodology takes into account the fact that a condition alone typically does not represent a cause, without the corresponding action that results from that condition and leads to the problem. Similarly, the action alone does not cause the problem unless the condition is also present. Ideally, improvement efforts should focus on eliminating the condition so that the related action never becomes a factor.

There are a number of other tools and methodologies related to or supportive of root cause analysis that can be found in the literature. Examples include the 5 why's, Failure Modes and Effects Analysis, various forensic engineering methodologies, techniques attributed to six sigma methodologies including Pareto and brainstorming diagrams and failure scenario development.



## Appendix D. Summary of Other Investigation Tools and Techniques

A successful FRB is highly dependent on the evidence the investigation team provides to the FRB supporting the understanding and demonstration of cause and effective mitigation of any remaining residual risks. In addition to the integrated root cause analysis tools there are a significant number of other investigation tools and techniques that can be employed in failure investigations. The most useful and critical techniques relate to replication of the failure either in the original test configuration or by use of physical or analytical simulators/modeling techniques.

It is highly recommended that additional tools and techniques be employed in identifying cause. While not exhaustive, the following list of additional failure investigation tools and techniques is offered to provide additional suggested methods that could be employed in a failure investigation.

Table 6. General Failure Assessment Tools and Techniques

Tool or Technique	Brief Description
Photographic and Video Evidence	Important in capturing physical conditions at time of failure and during subsequent physical assessments of failed systems. Easily obtained and catalogued with digital apparatus.
Failure Timeline Assessments	A detailed chronology of events prior to, during, and immediately after the failure. The timeline may be further expanded to capture important elements of the failed system or component life cycle history dating back to concept design and requirements development to aid root cause and corrective/preventive action understanding.
Supplier and Build Process Assessments and Outlines	Detailed assessments in outline form to understand the fabrication and assembly of the failed system or component and the supporting test equipment. May highlight out of sequence or position contributors to the cause of the failure. Useful in determining cause.
Supplier and Build Paper Interrogation	Similar to the processing outlines but usually consists of a Quality organization review of processing anomalies or nonconformances that may help explain the system or component failure.
Data Trending, Statistical Methods and Techniques Associated with Quality Management including Histograms, Pareto Diagrams, and the 5 Why's	Useful in determining if the system or component that failed had any "out of family" or out of tolerance performance or physical conditions that may have contributed to the failure.
Failure Scenario Development (Physics Based for Hardware Systems)	Useful in support of integrated root cause analysis tool assessments in analyzing failures where multiple causes/contributors are at play. For hardware systems assists in developing root cause test and analysis requirements/configurations and applicable failure environments.

<b>Tool or Technique</b>	<b>Brief Description</b>
Classical Engineering Methodologies including Failure Modes and Effects and Hazards Analysis	Classical bottom-up and top-down failure prediction/preventive cause methodologies sometimes helpful in developing root cause analysis tool structures and failure scenario development and assessment.
Classical Risk Methodologies	Necessary in providing structured risk assessments especially for FRB outcomes where root cause is not determined.

Table 7. Laboratory, Non-Destructive Evaluation (NDE) and Destructive Analysis and Component/System Test Tools and Techniques

<b>Tool or Technique</b>	<b>Brief Description</b>
Specialized Imaging Techniques including Thermography, Photogrammetric techniques, and various forms of X-ray NDE (conventional and nonconventional)	Techniques using specialized apparatus to enable detailed analysis of system or component elements without compromising integrity of failure units.
Shearography and Ultrasonics	Sonic based NDE system or component NDE techniques.
Eddy Current	Electrical based technique used for non-destructive testing of materials for geometry features, like micro-cracks.
Digital Logic Analyzer Assessment (e.g., Fire-inspector), and Time Domain Reflectometry	Families of specialized techniques used in the evaluation of electronic system failures.
Various Lab Tools including SEM, Auger, ESCA, N-RAY, and FTIR)	Various families of chemical analyses techniques useful in characterizing material properties conditions.
Destructive Physical Analysis (DPA)	Employed when non-destructive failure analysis methods have been expended. Structured dissection of system or component to interrogate possible failure causes.
Test or Analysis Based Failure Analysis and Simulation	Physical test or simulation modeling of the system or component behavior at the time of failure. Requires an understanding of the environments at the time of failure to accurately replicate the failure either physically or by computer analysis modeling applicable to the system or component under investigation.