GODDARD TECHNICAL HANDBOOK	GSFC-HDBK-8700
Goddard Space Flight Center Greenbelt, MD 20771	Approved: 09/13/2019 Expiration Date: 09/13/2024

GODDARD SPACE FLIGHT CENTER

GUIDELINE FOR FORMING AND OPERATING FAILURE REVIEW BOARDS AND ANOMALY REVIEW BOARDS

MEASUREMENT SYSTEM IDENTIFICATION:
METRIC/SI (ENGLISH)

THIS STANDARD HAS BEEN REVIEWED FOR EXPORT CONTROL RESTRICTIONS;
APPROVED FOR PUBLIC RELEASE
DISTRIBUTION IS UNLIMITED

NASA GODDARD SPACE FLIGHT CENTER
Greenbelt, Maryland 20771

Prepared By:

Original Signed By:
Jesse Leitner
Chief Engineer, Safety and
Mission Assurance Directorate
Goddard Space Flight Center

Approved By:

Original Signed By:
Steve Scott
Chief Engineer
Goddard Space Flight Center

Original Signed By:
Felicia Jones
Director of Engineering and
Technology
Goddard Space Flight Center

Original Signed By:
Dave Mitchell
Director of Flight Projects
Goddard Space Flight Center

Original Signed By:
Eric Isaac
Director of Safety and
Mission Assurance
Goddard Space Flight Center

DOCUMENT HISTORY LOG

Status	Document Revision	Approval Date	Description
Baseline		9/13/2019	Initial Release

FOREWORD

This handbook is published by the Goddard Space Flight Center (GSFC) to provide uniform engineering and technical implementation guidance for processes, procedures, practices, and methods that have been endorsed as standard for NASA programs and projects, including requirements for selection, application, and design criteria of an item.

This handbook defines a consistent approach for managing failure review boards and anomaly review boards at GSFC.

Requests for information, corrections, or additions to this handbook should be submitted via "Contact Us" on the GSFC Technical Standards website at http://standards.gsfc.nasa.gov.

Original Signed By James S. Milne For:
Josef A. Wonsever
Technical Standards Program Manager
Goddard Space Flight Center

TABLE OF CONTENTS

SECTION **PAGE**

1. SCOPE

1.1 Purpose

This handbook provides recommended guidelines for creating and conducting failure review boards (FRBs) and anomaly review boards (ARBs). This includes selecting the right supporting personnel, kicking off the investigation, identifying the undesired or unexpected event, flowing the logic from event to cause, characterizing and dispositioning the risk, and documenting the board activities. For the typical ARB or FRB, many of the formalities discussed herein are not required or are overly burdensome, so discretion should be used, particularly when dealing with failures or anomalies that are not particularly complex or impactful.

1.2 Applicability

The guidance set forth in this document provides a uniform approach for initiating, operating, and closing out ARBs and FRBs for GSFC projects in development, integration, and test. Formal ARBs and FRBs are typically only required for flight units, systems and interfaces, but each project sets the policy on extending ARB/FRBs to include engineering hardware and systems (e.g. prototype, breadboards, EDUs, ETUs, etc.).

This handbook may be cited in program, project, and other Agency documents to provide technical guidance.

2. APPLICABLE DOCUMENTS

2.1 General

Documents listed in this section contain provisions that constitute underlying requirements related to the implementation guidance provided in this handbook. When imposed, it is expected that the latest issuances of the cited documents will be used unless otherwise approved by the applicable Technical Authority (TA) as defined in NPR 7120.5. The applicable documents are accessible via the NASA Technical Standards System at http://standards.nasa.gov, directly from the Standards Developing Organizations, or from other document distributors.

2.2 Government Documents

GSFC-HDBK-8005	GUIDELINES FOR PERFORMING RISK ASSESSMENTS
GPR 5340.4	Problem Reporting and Problem Failure Reporting
NASA-HDBK-8739.18	Procedural Handbook for NASA Program and Project Management of Problems, Nonconformances, and Anomalies
NPR 7120.5	NASA Space Flight Program and Project Management Requirements

2.3 Non-Government Documents

None	

2.4 Order of Precedence

When applied internally, the technical requirements in NASA and GSFC directives (or other requirements documents) take precedence, in the case of conflict, over implementation guidance provided in this handbook.

3. ACRONYMS AND DEFINITIONS

3.1 Acronyms and Abbreviations

ARB	Anomaly Review Board
CND	Cannot Duplicate
CSO	Chief Safety and Mission Assurance Officer
EDU	Engineering Development Unit
ETU	Engineering Test Unit
FRB	Failure Review Board
GPR	Goddard Procedural Requirement
GSFC	Goddard Space Flight Center
I&T	Integration & Test
PDL	Product Design Lead
PFR	Problem Failure Record
PR	Problem Record
MSE	Mission Systems Engineer
SMA	Safety & Mission Assurance
SME	Subject Matter Expert
STD	Standard
TA	Technical Authority
UE	Unexpected Event
UVF	Unverified Failure

3.2 Definitions

Anomaly	An unexpected event, hardware or software damage, a departure from established procedures or performance, or a deviation of system, subsystem, or hardware or software performance outside certified or approved design and performance specification limits.
Anomaly Review Board (ARB)	A board formed in order to investigate an anomaly
Cannot Duplicate (CND)	A failure or anomaly that is not reproduceable within project resources.
Failure	The cessation of proper function or performance
Failure Review Board (FRB)	A board formed in order to investigate a failure
Issue or Problem	A risk that has been realized, whether or not the risk was known a priori.
Likelihood	The probability that a particular consequence will occur
Problem Failure Report (PFR)	A report generated in the PR/PFR database in response to the analysis of a PR that determines that there may be a significant risk to an aspect of mission success and that a project level review board is required for disposition. Examples of PRs that would be elevated to a PFR include: blown fuse; overvoltage; overcurrent; limit failure; connector mis-mate; change in hardware or software; hardware overstress; damage to flight or GSE hardware; personnel injury; safety violation.
Red-Flag PFR	A PFR for which (1) the root cause cannot be determined or corrected, (2) the failure or anomaly cannot be verified after the original occurrence (UVF), or (3) the failure or anomaly cannot be duplicated (CND).
Risk	The combination of 1) the likelihood (qualitative or quantitative) that a project, program, or organization will experience an undesired event such as cost overrun, schedule slippage, or failure to achieve a required outcome, and 2) the consequence or impact of the undesired event were it to occur.
Risk Assessment	The formulation of one or more statements of risk based on analysis of the supporting data associated with a concern.
Root Cause	The original event(s), action(s), and/or condition(s) generating an actual or potential undesirable condition, situation, nonconformity, or failure.
Unverified Failure (UVF)	A failure or anomaly that cannot be verified after the initial identification

4. GETTING STARTED

Problems will occur during development, integration, and test of space flight hardware. Upon identification of an anomaly or failure, it is required that the project follow the GPR 5340.4 procedural requirements on Problem Reporting and Problem Failure Reporting to document the issue. The involved personnel should stop work, preserve the configuration, and notify the project. Preserving the configuration means to record the state of hardware, software, GSE, test environment and test activity at the time of the event, including environmental conditions in the room, and not change anything (demate/remate a cable, change a software parameter, etc.). Troubleshooting is not allowed at this time. Failing to properly preserve the configuration may result in a potential UVF or CND. Photographs, telemetry records, and trending reports leading up to the anomaly or failure should be entered into the PR/PFR system.

Upon notification of the event, the project will make the determination if the anomaly or failure warrant a formal ARB or FRB. It is understood that some issues are straightforward in nature and have an obvious root cause and corrective action plan. If the Product Design Lead (PDL), Mission System Engineer (MSE), Project Manager, Principal Investigator, or Chief Safety and Mission Assurance Officer (CSO) determine an investigation board is needed, they will become a convening authority for the board. The convening authority may select a board chair at this time (typical for failures and anomalies with high impact to the project) or defer the selection to the board.

4.1 Create a Written Charter

The review board charter should be to objectively determine the causes and contributing factors that led to the unexpected event (UE), and to recommend corrective actions to prevent the UE from recurring in the future. There should be no speculation in defining the UE as it should be the specific outcome that triggered the need to form an investigation board. The charter should direct the board to ensure containment of the problem. Containment comprises the 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 involve steps taken to avoid creating an unverified failure or to avoid losing data essential to a failure investigation. The charter may also include such things as evaluating the possibility of existing items vulnerable to the same root cause. Finally, if root cause is not determined or cannot reasonably be eliminated, the board should assess and communicate the residual risk associated with a lingering problem. The scope of the investigation should be bounded by well-defined direction, which includes a process for expanding or reducing scope based on observations in the course of investigation.

4.2 Compose a Board

The project determines the minimum required participants in the Project PR/PFR Plan. In many cases it is advantageous to add expertise outside of the project to the investigation board. When selecting Subject Matter Experts (SME) to serve on an ARB or FRB, there are four primary considerations: (1) expertise in terms of direct subject matter or key engineering or safety and mission assurance disciplines, (2) objectivity of the members, (3) management of the investigation, and (4) legal or policy requirements such as insight privileges and required training. Expertise is the top priority, in both broad subject matter expertise for the technical area and in knowledge of the system design at hand. Objectivity is often stated as independence, but the real concern is whether there is at least one individual who is not biased by the design in hand or the potential outcomes of the investigation. Under consideration are, for example, whether an individual can be impartial about a particular design or product, or if there is a contractual relationship that creates a potential conflict of interest (or an appearance of conflict of interest). For investigations that have high visibility (e.g., relating to yellow or red risks, issues presented at GSFC monthly status reviews, directorate or Center “top ten” items, etc), objectivity by necessity takes the form of independence for one or more individuals, and in most cases, the investigation chair. Consider, as needed, the use of consultants that have a very focused expertise to aid with specific questions, but that are not needed for the day-to-day aspects of the investigation. A funding charge number (i.e. WBS) should be furnished by the financial sponsor of the ARB/FRB. Expectations for overall costs, path to completion, and time charging for individuals should be sent to the project’s resource manager for budget planning. It is common that the uncertainties around initial estimates are very large so one should be cognizant of this and communicate it.

When composing an investigation board, the following contains some examples of SMEs and sources:

Discipline experts:

- Individual with experience with systematic RCCA process
- Discipline division chief engineer
- Peer engineers on other projects with similar experiences
- Discipline specific engineering (Parts, Radiation, mechanisms, thermal, etc.)
- Well-known consultants within the discipline
- Risk assessment engineers

Sources of experts:

- Contact Code 500 respective branches or divisions for recommendations on engineering expertise
- Contact Code 400 divisions for recommendations on good review board chairs
- Contact Code 300 for experts in SMA (i.e. reliability, commodity risk assessment engineering, RCCA process, circuit boards, workmanship, etc.)

- Code 300 maintains a working list of discipline experts here: https://spaces.gsfc.nasa.gov/display/SMA300/GSFC+experts+for+consulting
- NASA Engineering and Safety Center

4.3 Hold an Initial Meeting

The chair should promptly schedule a time when key board members are available, preferably in person. The chair of the board should capture minutes and actions for all meetings related to this review board. The meeting should focus on the elements of the charter and ensuring everyone understands the UE, the information currently available, and the closure criteria for the investigation. Describe the specific designs and configuration, list the available telemetry and test records, identify the conditions present during the UE, and address any questions about the background. Questions that arise during this initial meeting may not immediately be answered but should be captured and prioritized as appropriate. The meeting should conclude with a documented list of actions and plan forward including when the board will meet again.

4.4 Negotiating a Draft Deadline

It is common for the convening authority to negotiate a release date for an initial draft report with the board chair. By defining this date, it sets expectations for urgency, provides visibility into the status of the investigation, and prompts feedback to the stakeholders. And because the report is a draft, it also carries lower risk that the findings will be construed as final. ARBs and FRBs have high visibility for flight projects in I&T, and further provide a message to the Center about when to plan for information on these high visibility events. Clear communication on progress, status, and updates is essential.

4.5 Be Open-minded

Stay open minded - many surprises appear in an investigation. Chances are fair that initial theories will not hold. Actively seek information that refutes or disproves the top explanation, because if it indeed is the explanation, it should fit all the data. The chair should request inputs from all members of the board. It is not uncommon for a subset of an investigation board to contribute the majority of discussion, however the quieter board members sometimes have invaluable thoughts or ideas that can send the review board into an entirely different direction of closure. The chair should be mindful of any board member that tries to force the data to fit their failure theory. A successful ARB/FRB will avoid misdirection from an individual that is having trouble hearing inputs from all board members. It is the review board chair's responsibility to create an open communication environment. Be sure that all members have a voice and be sensitive to all personality types. When a member feels that he/she is not being heard, it can widely erode trust and confidence in the investigation.

5. CONDUCTING THE INVESTIGATION

An investigation that relates to significant risk in a project or high visibility outside of the project may become a full-time activity for a period of time, especially when there are sufficient data to process, background research to conduct, models/analyses to construct, or tests to perform.

5.1 Brainstorming and Investigating

At the beginning there will be many suggested explanations for what caused the UE. Establish a logic flow approach upfront to trace from the UE down to the root cause and contributing factors. Examples of this logic flow approach include a cause-effect diagram (Ishikawa or fishbone), fault tree, or simple spreadsheet table (which would capture elements of the aforementioned approaches). The fishbone diagram is best suited to start with all identified possible outcomes and work down through a process of elimination to the most likely causes. This is the most common tool used for ARBs and FRBs. The fault tree is a top-down logical decomposition of the UE that steps down layer by layer, where each layer answers the “why” question for the layer above. The lowest layer is one in which there are no further questions to ask, or no further data available. This method is used most commonly for mishap investigations. When the eliminated blocks are removed, the remaining logic flow is called an event and causal factor tree. Project Reliability may have a fault tree already in hand that can be used directly or modified as appropriate. An existing Failure Modes and Effects Analysis may be a helpful starting point as well. There are many software tools available for fishbone and fault tree analysis, such as the NASA Root Cause Analysis Tool (which uses the fault-tree approach), but as mentioned above, the logic can be laid out in a spreadsheet as well. If a whiteboard can be maintained, keep the diagram up and use multi-color cross-outs to eliminate items. Regularly take photos of the board in case of accidental erasure, and for members to review when outside of board meetings.

The first step is to brainstorm proximate causes that led to the UE. A good practice is to have members generate their own lists of causes and bring to the meeting. Invite inputs from all board members and include in the logic diagram. Each of the proximate causes can then be flowed down into intermediate causes (at potentially multiple levels), and some will flow into (potential) root causes.

The goal of the investigation is to confirm or reject the prioritized list of possible explanations, including updates that occur during the course of the investigation. There are many paths an investigation can take based on the circumstances and complexity. The sequence should be based on risks involved (likelihoods and consequences), potential for (further) damage, reversibility, and resources available. Project systems engineering and reliability engineering should be engaged to help with likelihood calculations, either as part of the board or as an outside consultant. An approval process should be put in place before disturbing a critical item (such as entering a command into an orbiting spacecraft). In many cases, especially with an orbiting spacecraft that has very limited access, it may be very difficult to isolate a problem to a single explanation with high certainty. See section 6.3.3 for information applicable when this is the case.

5.2 Troubleshooting

The ARB/FRB should collectively decide what trouble shooting steps should occur, in what order they should occur, and when it is acceptable to break the configuration of the anomaly/failure due to no more information from the current configuration being able to establish cause. Further troubleshooting may then occur in a different configuration as approved by the ARB/FRB.

5.3 Outcomes

5.3.1 Determination of Root Cause

Root cause is the causal factor below proximate and intermediate causes for which there is no further "why" questioning that would be meaningful. If the root cause were not present, the UE would not have occurred, thus elimination of the root cause of the problem will prevent the UE from occurring again.

An example flow would be as follows: Consider the UE to be a board shutting down to a safe mode during ambient testing. The proximate cause was that a current limit indicator surpassed its red limit threshold of 5 Amperes. An intermediate cause was that a ceramic capacitor in the circuit lost insulation resistance. The intermediate cause below that was that the part was cracked with metal migration bridging the crack. The part had cracked due to a combination of the part having weak ceramic and the fact that the part had been manually touched up with a soldering iron. The root causes can then be determined to be a manufacturing process problem at the capacitor manufacturer and poorly-defined processes for manual touchup on center. This logic flow is illustrated in Figure 1.

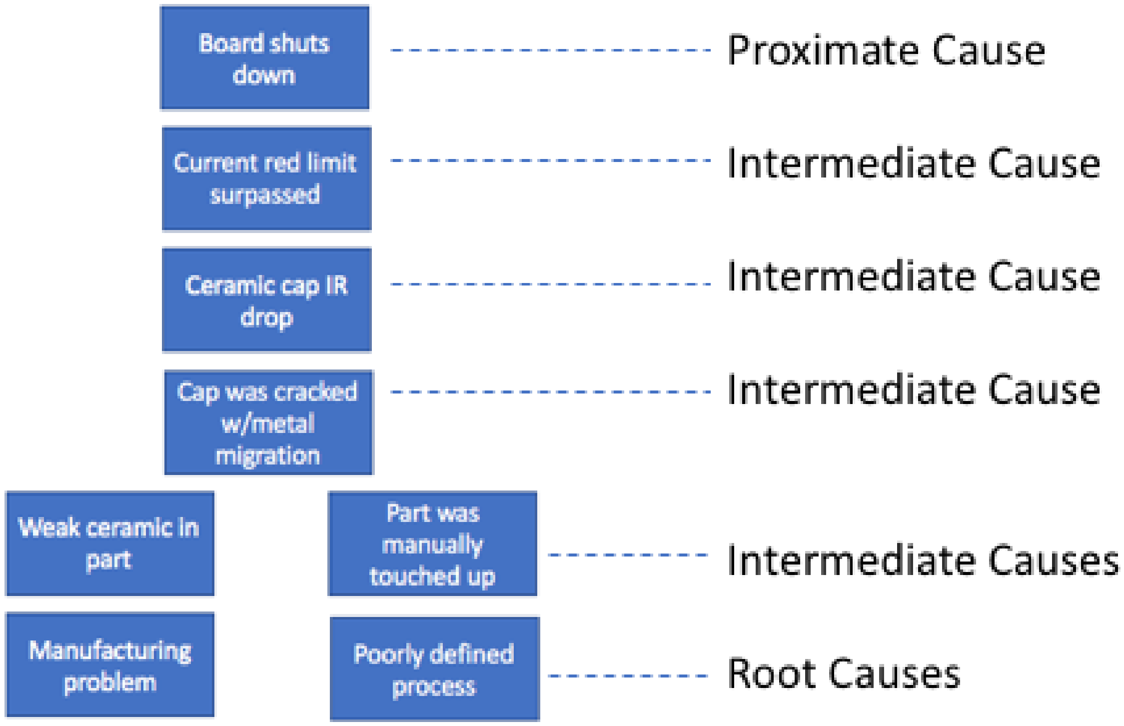

Figure 1. Fault tree representing logic flow for example

5.3.2 Root Cause and Corrective Actions Known

Once the causes are understood, corrective actions must be determined. The corrective actions should address the deepest concerns that can be addressed within project resources. When that is insufficiently corrective, such as when the corrective action ties to a management chain outside of the project's authority, the information should be provided to Engineering and Safety and Mission Assurance organizations for a higher-level disposition for acceptability and/or risk.

5.3.3 Red-Flag PFRs

There are three main classes of unresolved problems that constitute red-flag PFRs: those with unknown or uncorrected root cause, unverified failures (UVFs), and cannot duplicates (CNDs). Each of these conditions overlaps and in many cases, they represent the same condition. However, it is worth defining each as they all contain information to help indicate whether a problem has been resolved. A problem with unknown root cause is one in which either insufficient data or insufficient resources are available to reach the deepest underlying cause. A UVF is a failure for which there is no traceable evidence that it occurred beyond the initial observation. A CND is a failure or anomaly that cannot be reproduced within the project's resources. Each of these is important because it then becomes a candidate for a residual risk. In this section, we will not distinguish between these classes, but simply refer to red-flag PFRs.

5.3.4 Sufficient Uncertainty that the UE Occurred

In cases involving a red-flag PFR, the charter usually cannot be satisfied. In these cases, it is recommended: (a) to clearly state the reason for red-flag PFR (UVF, CND, root cause unknown or uncorrected), (b) capture or summarize the efforts taken in the report, (c) clearly state what the candidate explanations are at the time of the report (root cause, proximate cause, etc., are all acceptable), (d) clearly state that the charter cannot be satisfied, (e) clearly state the findings and corrective actions identified, if any, while the board was convened, and (f) clearly state whether the report does or does not submit candidate risk(s), if any, given the outcome. For item (f), it is commonly someone other than the ARB/FRB who would submit the risk, such as the PDL or MSE.

5.3.5 Risk

Risk should be the primary driver for the substance and recommended actions in the report. In the case where the risks or impact of correcting the causes preclude their implementation, then risk(s) should be captured. GSFC-HDBK-8005 can be a helpful tool for characterizing risk. The associated risk should be presented in the report, documented in the PFR, and subsequently brought to the project risk board for disposition.

Risk can also be a tool or element to optimize an ARB/FRB for time, cost, relevance to mission, or some other parameter. For example, ARBs/FRBs working close to a launch date are under unique pressure to conclude and report out results on a top-down schedule. Risk is an element that can be used to optimize for that deadline. The ARB/FRB should characterize and communicate risks to concur on a path forward.

5.4 The Report

The report is important not only for record to refer back to within the project, but also to help prevent recurrence of similar problems on other projects or inform parties who experience the same UE. The report is either attached or written in the PR/PRF system directly. It is a written record to characterize the outcome of the investigation, with sufficient information to assess the quality. In many cases, a briefing format is sufficient for the report, but it depends on visibility and how widely-applicable the problem may be. ARB and FRB reports are well suited to be "Chair's reports" and need not be "consensus reports". Given the tight constraints that exist on projects, consensus reports may not be worth the time required to bring them to closure. To solicit feedback while clearly communicating that the report is not final, use the "draft" label liberally in all versions of the report until the report is complete. In either case, the report should be centered on risks that remain in the project as a result of the anomaly, failure, or the actions taken to recover from the event.

5.4.1 Minority Report

When implementing a non-consensus, or minority report, such as a chair's report, invite and give heavy consideration to feedback and minority positions or reports. This can be a section on its own or part of a dissenting opinion section. This is the Chair's tool to get feedback from the board on a specific position drafted by the report. These are often invited in writing, and if still applicable at the time the report is declared complete, a discussion between the Chair and dissenting or minority member should take place to determine if they will be included with the report (oftentimes as an appendix). If objections are particularly strong, be prepared to handle dissenting options through the NASA dissenting opinion process per NPR 7120.5. The best way to engage in the dissenting opinion process is to thoroughly communicate, be well informed, and consider the alternate opinions. ARB/FRB outcomes do not need to be perfect but they should be the best practical.

At times, uncomfortable topics may arise in the investigation and necessitate inclusion in the report. Uncomfortable topics can range from a technical imperfection in units that cannot be corrected (such as orbiting spacecraft) to an insufficient process well outside the reach of the ARB/FRB and Project (such as an Agency process). In these cases, it is best to stick closely to the facts, such as design X is vulnerable to failure mode Y or process A does not address potential failure mode B.

5.4.2 Report Distribution and Approval

The distribution of a report should be commensurate with the importance of the affected system, subsystem, component, or part, but at a minimum should go to the PDL or component lead, the MSE, the FRB members, and the CSO. The convening authority is responsible for accepting the report and determining whether the ARB/FRB has fulfilled its duties. The convening authority is responsible for implementing a corrective action plan.