GODDARD TECHNICAL HANDBOOK

GSFC-HDBK-8005

Goddard Space Flight Center
Greenbelt, MD 20771

Approved: 09-28-2017
Revalidation Date: 09/28/2022

GODDARD SPACE FLIGHT CENTER

GUIDELINE FOR PERFORMING RISK ASSESSMENTS

MEASUREMENT SYSTEM IDENTIFICATION: METRIC/SI (ENGLISH)

Prepared By:

Jesse Leitner
Chief Engineer, Safety and
Mission Assurance Directorate
Goddard Space Flight Center

Approved By:

for

Steve Scott
Chief Engineer
Goddard Space Flight Center

Felicia Jones-Selden
Director of Applied Engineering and Technology
Goddard Space Flight Center

Dave Mitchell
Director of Flight Projects
Goddard Space Flight Center

William Wrobel
Director of Wallops Flight Facility
Goddard Space Flight Center

Richard D. Barney
Director of Safety and
Mission Assurance
Goddard Space Flight Center

NASA GODDARD SPACE FLIGHT CENTER
Greenbelt, Maryland 20771

DOCUMENT HISTORY LOG

Status	Document Revision	Approval Date	Description
Baseline		09/28/2017	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 performing risk assessments in all discipline areas 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.

Josef A. Wonsever
Technical Standards Program Manager
Goddard Space Flight Center

TABLE OF CONTENTS

SECTION PAGE

1. Table of Contents

2. SCOPE

2.1 Purpose

This handbook provides a uniform approach for performing risk assessments across all discipline areas at GSFC, within the context of the continuous risk management process described in GPR 7120.4. This document may also be used to support projects under other risk management plans and procedures, and in such cases, the scales and likelihood and consequence definitions may differ from those in GPR 7120.4. This document does not supersede organizational or project/program usage of local risk management processes. The purpose of using a uniform risk assessment approach is that likelihood and consequence ranks used to estimate risks are derived consistently from a common reference. Commonly-derived basis ranks enable comparing risks consistently to provide engineers and managers more credible assessments for programmatic, safety, and technical decisions.

2.2 Applicability

The guidance set forth in this document provides the baseline approach for assessing and communicating risk, consistent with GSFC and NASA risk management policies and procedures.

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

The guidance provided in this document is based on extensive GSFC experience and those of its subcontractors.

3. APPLICABLE DOCUMENTS

3.1 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). 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.

3.2 Government Documents

GPR 7120.4D	Risk Management
NPR 8705.4	Risk Classification for NASA Payloads
GPR 8705.4	Risk Classification and Risk-based SMA for GSFC Payloads and Systems
300-PG-7120.4.2	Code 300 Risk Management Plan

3.3 Non-Government Documents

3.4 Order of Precedence

When applied internally or imposed by contract on a program or project, 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.

4. ACRONYMS AND DEFINITIONS

4.1 Acronyms and Abbreviations

BJTs	Bipolar Junction Transistors
CIL	Critical Items List
ECSS	European Cooperation for Space Standardization
EEE	Electrical, Electronic, and Electromechanical
ESD	Electrostatic Discharge
FI	Fastener Integrity
FMEA	Failure Mode & Effect Analysis

FMECA	Failure Mode & Effect Criticality Analysis
FRB	Failure Review Board
GIDEP	Government Industry Data Exchange Program
GPR	Goddard Procedural Requirement
GSFC	Goddard Space Flight Center
HVOCs	High Voltage Optocouplers
IAR	Internal Annual Ring
INST	Instruction
IPC	Institute for Printed Circuits
IR	Infrared
I&T	Integration & Test
LDC	Lot Date Code
LVPS	Low Voltage Power Supply
LxC	Likelihood and Consequence
MIL-PRF	Military Performance Specification
MIL-SPEC	Military Specification
MRB	Material Review Board
NPR	NASA Procedural Requirement
OHA	Operational Hazard Analysis
PCB	Printed Circuit Board
PRA	Probabilistic Risk Assessment
PSA	Parts Stress Analysis
SMA	Safety & Mission Assurance
STD	Standard

TA	Technical Authority
TSOP	Thin Small Outline Package
WCA	Worst Case Analysis

4.2 Definitions

Baseline Risk	The 'normal' level of risk generally considered unavoidable as a practical matter in the relevant activity (e.g., in developing and manufacturing a product). This risk level is accepted by a project or organization without requiring debate, additional analysis, or further tracking.
Concern	A logical determination that an undesired event may occur or that the protections against such an event may not be sufficiently well understood based on available data
Consequence	Foreseeable, negative impact(s) to meeting performance, programmatic, or safety requirements at the level of a project that is tracking the associated risk. A consequence ranking assessment can be quantitative and/or qualitative.
Credible Risk	A risk having a likelihood rank of at least "1" on the GSFC Risk Matrix Standard scale (Note: This risk scale has 5 likelihood ranks with rank 1 being the lowest likelihood.)
Hardware Safety	A condition of protection against threats to hardware under the ownership of a program or project
Hardware Safety Risk	Risk of damage to hardware that is under the ownership of a project or program. This is a subset of either technical or programmatic risk, depending on whether the threat is on-orbit or on the ground. This is not a subset of safety risk.
Institutional Risk	A risk involving a threat to institutional capabilities, infrastructure, or approval to operate. An institutional risk is generally a programmatic risk that pertains to the functioning of GSFC, as opposed to an individual project.
Intermediate consequence	The immediate, direct effect from a concern being realized
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
Programmatic Risk	A potential problem that involves the possibility of impact to development activities and / or the ability to deliver the required product within the allocated budget, schedule, and resources.

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 worst case 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.
Risk Classification	A stakeholder-assigned definition of risk-tolerance for a project. See NPR 8705.4 and GPR 8705.4.
Safety	A condition of protection against threats to (1) personnel, (2) the public, or (3) collateral damage outside of the ownership of a project or program.
Safety Risk	A potential problem that involves the possibility of personnel injury or death and/or damage to facilities or other property outside the ownership of a project or program.
Technical Risk	A potential problem that involves the possibility of impact to Flight / Ground segments during operations (i.e., "end products" performing their desired functions in their operational environments).”

5. UNDERSTANDING RISK

In performing any activity that has uncertainty in achieving an outcome, it is natural to have *concerns* that represent the things that can go wrong or the things that may not be well understood. These concerns may have a range of plausibility and uncertainty (e.g., occurrence of the event may be impossible, improbable, possible, probable, etc.) based on analysis, prior experience, observation, brainstorming, or even speculation. When a concern is placed into a context including an environment, operating regime, a required outcome, and supporting data, the concern can be couched as a *risk* by forming a condition statement and a threat to a technical, programmatic, or safety requirement. A *likelihood* and *consequence* (which may be preliminary) are then assigned to that risk. When a risk has been realized (happened), whether or not the risk had been identified previously, the risk then becomes an *issue or problem* (further references in this document will use only the term *issue*. The issue is that the consequence has occurred. Note that a risk and an issue can exist concurrently (e.g., an injury may have occurred, but the activity is still ongoing and the possibility of additional injuries remains).

5.1 Anatomy of a risk statement

Per 300-PG-7120.4.2, a risk statement is formed as follows:
“Given the [CONDITION], there is a possibility that [INTERMEDIATE CONSEQUENCE] will occur resulting in [CONSEQUENCE].” The condition must be a short and concise fact. The *intermediate consequence* is the immediate, direct effect from a concern being realized, and as such is an outcome internal to the project or organization that may have implications not immediately apparent to individuals outside the project and that may need further analysis to show its connection to higher level requirements. The *consequence* is a threat to project or organizational requirements that clearly communicates the impact to stakeholders and

individuals that may not have detailed knowledge of the project. For example, the intermediate consequence may be the failure of a capacitor in one of the instruments, and the consequence may be failure to meet the requirement of collecting short wave infrared imagery as stated in the project requirements documentation. The first part of the risk statement (condition that may lead to intermediate consequence) is used to establish likelihood, while the second part of the risk statement establishes the consequence to stakeholders at organizational levels above, including those outside, the project.

5.2 Categories of a concern

Concerns are categorized based on what can go wrong. A *technical* concern relates to a failure, anomaly, or performance problem with hardware or software. An example would be the possibility that a part or component may fail. A *programmatic* concern relates to the resources available supporting an activity. An example would be that a procurement may take longer than expected or that more labor effort, and hence more cost, will be required to complete a job. Another programmatic concern would be the availability of a facility to support an activity that is required to meet Center-level commitments. A *safety* concern relates to a threat of injury or death to a person or people, and can be expanded to include collateral damage to assets not owned by the project. For example, a rocket that runs astray, damaging a nearby road would be a safety risk realized, even without the presence of people.

5.3 Risk Categories

Risks are categorized in similar fashion to concerns (*technical*, *programmatic*, or *safety*), with the category being representative of the (ultimate) *consequence*. However, the risk category may be different from its underlying concern category. For example, while a part failure may be a technical *concern*, the *risk*, with its technical likelihood and consequence, of a part failure in the development phase most likely will be programmatic, (e.g., that the part will need to be replaced, which will take time and money) but a technical concern also may lead to a safety risk, (e.g., the part failure may result in a fire and/or someone may be injured). Likewise, a programmatic concern may lead to a technical risk, (e.g., a delivery may be delayed, reducing the amount of time available for environmental test, hence increasing the likelihood of an early failure on-orbit). A safety concern may lead to a programmatic risk, (e.g., insufficient definition of hazard controls early in the design process may require additional and costly safety measures late in the project and even threaten project cancellation).

A *concern* does not become a *risk* until *likelihood and consequence* are established for the risk.

Any of the concerns in 5.2 may lead to an *institutional* risk, which involves threats to institutional capabilities, infrastructure, or approval to operate.

5.4 Writing accurate and appropriate risk statements

There are three main attributes of a good risk statement:

(1) The consequence is written as a threat to the highest level in the organization that maintains the risk. For example, for a project risk, the consequence should be a threat to project requirements as follows:

> Given failures that have occurred with similar bipolar junction transistors, it is possible that one part will fail, subsequently taking out the short wave detector, resulting in loss of all short wave IR science data on-orbit. If the likelihood of a part failure is a "3" on the technical risk scale, then we would characterize this risk as 3x3 if the loss of short wave IR science data has a moderate impact on mission success.

A related example of a technical risk at the instrument level would be:

> Given failures that have occurred with similar bipolar junction transistors, it is possible that one part will fail, subsequently taking out the short wave detector, resulting in loss of the short wave IR instrument. At the instrument level, the loss of the part constitutes a total loss, so the risk at this level would be a 3x5.

(2) The risk has a single consequence. Multiple consequences generally have different consequence levels and different associated mitigations that might not be worked in parallel. Therefore, separate risk statements should be used to represent separate consequences unless the consequences seamlessly combine as a pair with the same (or combined) consequence level.

(3) The consequence is not another condition or another risk. The consequence must represent the specific impact to the project of the concern being realized, relative to the project's requirements.

6. Performing Risk Assessments

There are many purposes for performing a risk assessment. These include:

- To select among multiple options (e.g., trade studies, use-as-is, or fix a problem)
- To decide whether violation of low level requirements increases risk
- To prioritize activities
- To decide whether to discontinue a planned activity
- To complete a waiver, FRB, or MRB activity (which likely overlaps with one of the other purposes listed above)

6.1 Deciding on a category

The first step in performing the risk assessment is to determine which categories of risk apply (technical, programmatic, or safety). In most cases, this is straightforward. The following may be helpful to work through the nuances of categorizing a risk:

- Is the risk likely to be realized during ground testing [programmatic] or might it be undetected and subsequently occur on orbit (a latent defect) [technical]?
- Are normal downstream processes (for example, screening, testing, in-process controls, etc.) expected to mitigate or eliminate the risk [programmatic]?
- Is there a possibility that personnel are in danger or hardware can be damaged [safety]?
- Is it likely that a process or a waiver will not be approved or that controls will be put in place so late that further development or preparations for launch are prevented [programmatic]?
- Is there an expectation that the concern would most likely be realized in I&T, if ever [programmatic]?
- Is the consequence injury to personnel or the public, death, or destruction of property that is not owned by the project [safety]? (A threat to property owned by the project prior to launch would be captured in a programmatic risk because the ultimate consequence is that hardware would have to be repaired or replaced, as would happen with any type of test failure or anomaly.) Note that due to the very low thresholds for safety risks, safety concerns are generally handled via hazard reports and hazard controls to eliminate them or render them noncredible, and not typically by capturing risk statements.
- Is there **an expectation that the testing flow will not expose the intermediate consequence** [technical]?
- Have resources been exhausted trying to eliminate or mitigate a programmatic risk based on a technical concern [technical]?

Note that many risks in a project, even those based on technical concerns, will be programmatic until the available resources (e.g., cost/schedule reserves) used to resolve or mitigate the risk are expended or if there is early recognition that a risk can or will not be fully mitigated. This is because there is generally an expectation that with a thorough environmental test campaign and/or mission assurance program, most problems will be exposed before launch. For example, if there is a concern about a potential part failure because of a GIDEP alert, it would be natural to express a risk that a failure may occur in I&T. However, late in a project, if all of the concerns associated with the alert have not been addressed, a technical risk should be captured to represent the concern for an on-orbit failure. It should be noted that there are many risks that are inherent in a design, such as single points of failure, that are known up front, and that are likely to carry through as technical risks on-orbit. Risks associated with the design should get captured as technical risks early in the design process, so that the team appropriately balances the mitigation of these risks along with the programmatic risks during the development process.

6.2 Baseline risk

Baseline risk is the risk that exists as a result of implementing a collection of performance and assurance requirements used to guide the development, manufacturing, and integration of a product for a given risk posture. Note that this is entirely a subjective term and risk baselines often leverage off of widely recognized and standardized requirement sets at the individual technology discipline levels (e.g., EEE parts, environmental test, reliability, etc). However, it is important to note that baseline risk should always be viewed in the proper context for an area of concern and based on the technical area, it may not appear to align with the risk posture for the project. This view may lead to differing definitions of baseline risk for projects of different risk classifications or risk postures that may not be initially intuitive. For example, the baseline safety risk for a "Do No Harm" payload on the International Space Station may be lower than the baseline risk for a Class B free-flying spacecraft because there are more safety risks associated with the deployment and operation of the payload on ISS than on a free-flyer, and hence more safety-related risk mitigation activities will be required in order to protect ISS (and associated crew) as compared to those on a free-flyer.

The primary means of establishing baseline risk for a particular commodity area is through the use of requirements or specifications that have been proven to enable product development to an acceptable level of risk. In many cases, multiple alternative specifications have been analyzed and approved to establish baseline risk equivalently. For example, at the time of writing of this handbook, IPC 6012 DS, IPC 6012C 3/A, IPC 6012B 3/A, MIL-PRF-55110H, and ECSS-Q-70-10C all are acceptable at the same risk level for a Class A or Class B mission to establish baseline risk for rigid printed circuit boards. Another example of equivalent levels of baseline risk is in the specifications for mechanical fastener integrity. NASA-STD-6008 prescribes agency-level requirements, but GSFC uses its own 541-PG-8072.1.2, which is much more tuned to robotic (vs manned) missions, and GSFC's approach. Both of these specifications are considered to establish baseline risk for fastener integrity.

6.3 Credible risk vs possibility

A concern framed as a undesired event that has at least one realizable path, no matter how likely or unlikely, is a possibility. While it may be desirable to try to eliminate all possibilities of bad events occurring, allocated resources preclude doing so. Furthermore, actions taken to mitigate a given risk may create additional risks, so it is standard GSFC practice to establish a threshold above which risks should be formally managed for a project. In GSFC's risk management process per GPR 7120.4, this threshold is defined by a likelihood floor for each risk category as a likelihood "1" (out of the 5 likelihood levels). For GSFC-managed projects and programs, a risk whose likelihood is at or above the floor is defined as *credible*, and one with a likelihood below the floor is defined as *noncredible*. Note that noncredible risks may still be "possible" and may warrant further study and mitigation, especially when there is significant uncertainty in the likelihood.

6.4 Trade of programmatic and technical risk

Risk assessments performed during the development phase should facilitate project engineering and management decisions to advance mission success within cost and schedule constraints. It is important to recognize that many development activities involve undertaking programmatic risk to buy down technical risk.

One view of how risk management implementation trends for Class A to "Do No Harm" projects, as defined in GPR 8705.4, is that the ratio of programmatic to technical risk is very high for Class A decreasing to a very low ratio for a Do No Harm project. The programmatic risk being described is prompted by the extensive testing and preventive practices imposed that are intended to minimize technical risk that, however, come with cost and schedule demands that can be difficult to manage and satisfy. This intent to protect against a single or few defects significantly increases programmatic risks while the technical risk of an on-orbit failure is driven to relatively low levels.

6.5 Procedure

(1) Establish that there is elevated risk present, for example:

- Does the product not meet *any* of the approved specifications of the established risk baseline or equivalent? (Even if the product is purportedly *built* to one specification and is nonconforming to that particular specification, if the product is compliant to another approved baseline specification per GSFC or agency policy, then risk is not elevated. Note that crosscutting supplier concerns, such as the routine use of alternative technical standards, should be treated separately from the project-specific risk.
- Has there been a failure due to an unknown or uncorrected root cause or is it not feasible to duplicate or verify?
- Is the product out-of-family with other similar products without changes declared by the supplier that indicate the cause? Out-of-family is a subjective term that typically refers to products that have prior history and/or are produced in multiples, where the product meets the specification but has meaningful quality or performance attributes that differ from the general trend of other concurrent or prior units.
- Has a concern been identified through a hazard analysis, reliability analysis (e.g., FMEA, FMECA, WCA, PSA, PRA, CIL, OHA, etc), or systems engineering analysis?
- Is there a prior negative supplier quality trend that indicates an increased likelihood of delivery of defective units or significantly delayed deliveries?
- Is there an external warning that relates directly to components that are being used on the current project?
- Are there current supply chain issues that threaten the schedule?
- Has a schedule review identified unforeseen schedule threats?

(2) Identify the intermediate consequence. This is the direct effect associated with the concern. For example, if there is a concern associated with warnings (GIDEP Alerts,

NASA Advisories, other notifications, etc.), prior factual observations or findings, or an unresolved failure of a single part or component, the likely intermediate consequence is a failure of one or more instances of the particular part or component within the system.

(3) Identify the consequence at the level of the organization that is performing the assessment. For example, if the instrument team is assessing the risk of a particular concern on the instrument, then the consequence should be assessed to the instrument requirements. When the risk is elevated to the next indenture level (e.g., spacecraft), the risk statement and its consequence likely will change. Consider that there may be a range of consequences (e.g., degradation, brief outages, complete failure, etc.)

(4) Formulate a risk statement in the format described in Section 5.1.

(5) To the extent possible, use quantitative (statistical) methods to establish likelihoods for each of the intermediate consequences (there may be just one). Viable approaches include Weibull or other life data analysis, sampling statistics, Bayesian analysis, cumulative failure probability, engineering estimation, etc. [A project reliability engineer is trained to estimate the likelihood.] If the likelihood is below the floor of a "1" (out of 5) likelihood on the risk scale, then the risk is defined to be *noncredible* and the system is considered to be at baseline risk.

(6) Both likelihood (L) and consequence (C) are required to characterize the risk. In some cases it may be useful to capture two or more risks to cover multiple LxC pairs (e.g., low likelihood of a high consequence, or a high likelihood of a low consequence for the same concern), but a good approach would be to select the pair that represents the highest LxC (multiplicatively). The most important consideration is that the risk properly represents the concern.

6.6 Other considerations

The following should be considered when assessing risk:

- For programmatic risks (e.g., risks of loss of schedule and budget reserve from having to rework hardware to repair a failure), redundant elements increase risk likelihood because more opportunities for failure exist and, generally, a project will not launch with a nonfunctional or degraded side redundant element.

- For technical risks, redundancy reduces risk likelihood because at least two failures of less than 100% likelihood must occur and the likelihoods are multiplicative (when the failures are independent).

- *Hardware safety* almost always is associated with programmatic risks (commonly associated with lifting or the potential for overtest), but in some cases may involve a threat during pre-launch processing, launch, or commissioning.

- Be careful not to capture *hardware safety* risks as safety risks. Hardware safety risks are programmatic or technical. Otherwise, an *unbalanced* risk will result from prioritizing one risk over another that has the same outcome. Unbalanced risk is a situation where two different risks with comparable outcomes are judged using different scales, inappropriately making one higher priority than the other. Following the guidance in this document will prevent the proliferation of unbalanced risks.

- Safety risks are not common at GSFC because generally the approach is to eliminate any elevated threat to personnel or collateral damage.

- Once risks have been identified, they are managed per the risk management processes, prescribed in GPR 7120.4. Within a project, a risk that cannot be managed and mitigated at the component or subsystem level should be brought to the project risk board for disposition.

- While it is tempting to be "conservative" in assessing a risk, one should avoid biasing the assessment because management decisions, actions, and resources will be prioritized based on risk assessments. An overly conservative lower level assessment may lead to poor risk decisions at a higher level in a project. Assessments that are overly optimistic and that under-report a risk's likelihood and consequence can also lead to poor decision-making. Likelihood and Consequence numbers (ranks) should be derived from analysis and application of the criteria specified in GPR 7120.4, or as otherwise specified in a Project or Program Risk Management Plan. Likelihood and Consequence numbers (ranks) should never be arbitrarily inflated (or deflated) to emphasize (or de-emphasize) a specific risk.

APPENDIX A – Example risk assessments

Here we will provide some risk assessments performed for GSFC projects.

Example A1.

The first example is one where an issue was identified with how thin small outline package (TSOP) parts were installed on boards, causing concerns of future failures. The issue arose through inspections that identified cracks in the parts after installation. In all cases, the understanding of the problem and the testing performed indicated that the risk (related to functional failure of at least one part) would be realized in functional or environmental testing and that the technical risk was noncredible for a board to functionally survive through all of integration and test (I&T) then subsequently fail on-orbit. Therefore, risks associated with each of three options are programmatic.

Option 1: Vendor reworks the board using their own approach.

Given that the vendor will rework the board with encapsulated leads precluding further rework

There is a possibility that there will be other issues found with a flight board (part infant mortality) requiring replacement of a board late in the program

Resulting in significant cost and schedule expenditure

Likelihood 1 (2% - 10%). - *should substantiate with our knowledge of failures of these parts or parts in similar families*
Consequence 5 (unable to meet cost or schedule constraints within reserves) - *Note that the 2% - 10% likelihood is that failure will occur late enough that cost and schedule will increase outside of reserves. A lower consequence associated with this likelihood, for example 3 or 4, may be more appropriate, however, a lower consequence ranking depends on GSFC's prior experiences with these parts.*

And a second risk for this option is:

Given that the vendor will rework the board with a hard epoxy

There is a possibility that stress will transfer to the part body and cause part failure, requiring replacement of a board

Resulting in significant cost and schedule expenditure

This would be programmatic as well because likely GSFC will test the boards at more aggressive levels (I&T) than they will be subjected to in flight. This risk adds to the likelihood of

the first risk by adding another failure mode.

One factor that may reduce risk likelihood is that the vendor will be using an approach they are experienced and comfortable with.

Option 2: If the vendor were to do nothing (use-as-is)

Given that a TSOP thermal coefficient of expansion differential issue has been identified as a result of a failure (due to rework) on a different project,

There is a possibility that the TSOP parts may crack during the I&T flow,

Resulting in significant cost and schedule expenditure needed to replace the board.

This concern also is best framed as a programmatic risk and it is probably unlikely to manifest unless rework is performed on the board. Framing a technical risk would include a number of other factors that start with assuming no problems would be encountered or identified through I&T and then a problem appears after launch.

The two most pertinent scenarios would be (1) a failure is encountered late in I&T such that the project cannot resolve the problem and perform adequate regression testing using allocated resources and (2) a failure is encountered in environmental test at lower levels of assembly. The first (1) would have a very low likelihood and a very high consequence. Given the lowest likelihood for a programmatic risk (2-10%), the potential for a failure late in I&T without any earlier indications is below "1" on the programmatic risk scale. The catastrophic programmatic consequence of 5 thus can be deemed noncredible (that is, it is less than a 2% likelihood). At the likelihood of 2-10% ("1" on the programmatic scale), the failure is likely to be noted at lower levels of assembly, where the consequence would more appropriately be a 3 or 4. Since the problem is dominated by uncertainty about when a failure would occur or the resources required to overcome, a 4 is the more appropriate consequence choice.

Option 3: If the vendor were to follow GSFC's approach

Given that the vendor will follow GSFC's approach of applying coating only at the corners

There is a possibility that the unfamiliar rework will not be successful,

Resulting in significant cost and schedule to rework the board or replace the parts.

The approach is straightforward, and likely to be mastered in reasonable practice. However, this approach does not have a long history of successful implementation, so there may be limitations on its effectiveness. If the approach ends up being ineffective, the parts will likely exhibit cracks early at low levels of assembly, so a consequence of 3 is a reasonable estimate.

Given that all of the resulting risks are low, the project may choose the least costly option, or that which most closely reflects the developer's preferred approach. It should be noted that typically

directing the developer to use a different approach then they would choose means that the risk would be borne by GSFC. Therefore, aside from the cost implications, it may be best to take the higher risk option if it is the developer's choice.

Example A2.

A problem was discovered with JANS (level 1 equivalent MIL-SPEC, or Space Quality grade) bipolar junction transistors (BJTs) in packages with metal lids, characterized by an exhaustive, coincidental breakdown of processes that combined (1) overly deep laser marking into the parts' lids creating a hole and (2) ineffective fine and gross leak testing performed to screen out nonhermetic parts. Consequently, a very small percentage of JANS BJTs escaped the screening processes with holes in their lids. Ultimately, it was determined that while there were intermittently (with lot date code) increased occurrences (percentages), parts escaping the screen were miniscule. The overall average rate of parts escaping hermeticity screening was 13 parts per million. A lack of (or loss of) hermeticity in a part is not in itself a precursor to failure. However, it does elevate failure likelihood when other conditions exist, specifically corrosive substances either already inside of the part or pushed into the part through some entry path.

This GSFC failure involved one of the few parts having a laser hole that escaped the hermeticity screening process and then was installed into a flight assembly. This assembly was subjected to an aggressive cleaning agent prior to application of conformal coating. The part did not fail until tested for several hundred hours without incident. A thorough analysis revealed the nonconformance rates as a function of part types, packaging styles, and lot date code that provided the means to identify and screen suspect parts using x-ray radiography. However, the real concern associated with this type of problem is when parts have been installed, and in particular when the system has completed a substantial amount of testing and a risk-based decision must be made whether or not to replace the part. This example is representative of many instances that have occurred with GSFC projects.

The project scenario is as follows: A low voltage power supply (LVPS) board has 48 potentially affected BJTs in "small TO cans" from a 2007 lot date code (LDC). Each BJT is critical to board function (each suspect BJT is a single point failure for the board). There are two LVPS boards (one being redundant), only powered one-at-a-time as needed (i.e., standby redundant). A detailed reliability assessment based on re-inspections on tens of thousands of parts yielded a 63.7 parts per million nonconformance rate for small TO can BJTs from LDCs ranging from 0530-1013 (2005-2010). (In this case, "nonconformance" indicates the part has a laser hole through the part lid and it has escaped hermeticity screening tests.) The board assembly vendor used an aggressive water-soluble flux, albeit with proven, good board cleaning processes.

The project must make a decision about whether to replace the installed parts, use the boards as-is, , or perform other mitigations. To support this decision, at least two risk assessments should be performed.

Note that in this example, all potentially non-conforming parts in both redundant assemblies are from the same BJT population. The likelihood statistics (Ps's) were calculated based on the non-conformance proportions in the population (the 2005-2010 LDC range mentioned above), so the

common mode element across the two redundant assemblies already is considered by the nonconformance likelihoods for any part drawn from the population.

Option 1: Use-as-is. Use-as-is should always be the first risk to assess. Sometimes the risk is not readily apparent until a detailed analysis is performed. We will consider both the programmatic risk (for failure in I&T) and the technical risk (surviving through I&T and failing on-orbit).

Programmatic:
Given the use of 96 (opportunities for a part failure across both boards) BJTs in small TO cans affected by the reported laser etching concern
It is possible that one will fail in I&T

Resulting in significant resources to replace the part and regression test the board.

*First consider the likelihood of having a nonconforming BJT in one LVPS assembly. With 96 parts, the likelihood of a non-conforming part is: 96*63.7*1.e-6 = 0.0061 = 0.61%. For a nonconformance to progress to a failure, other events/conditions must occur. In this case, installed suspect BJTs must be exposed to a corrosive contaminant prior to conformal coating and that contaminant must be already present or forced into the package cavity. As these additional events are independent of the initiating event (the screening escape non-conformance), their probabilities are multiplicative. Thus any such events would reduce the combined likelihood if their chance of occurring is less than 1.0. Even if the additional events are assumed to occur definitely (Pocc = 1.0), the resulting likelihood will be less than programmatic risk threshold (<2%). Thus this programmatic risk is* noncredible.

Technical:
Given the use of 2 redundant boards, with 48 BJTs each in small TO cans affected by the reported laser etching concern

It is possible that two parts will fail (loss of one each side is required to lose function) on orbit after making it through I&T successfully

Resulting in loss of mission

*The likelihood of a nonconforming BJT on one side is 48*63.7*1.e-6 = 0.0031 = 0.31%. Even without considering the other events to prompt a failure from a nonconformance, the likelihood of two BJT failures due to this particular concern < 0.0031^2, which is far less than the floor of a technical risk (0.001). Therefore this risk is noncredible. At this point the risk assessment is complete. If credible risk were apparent here, then we would go on to perform similar risk assessments associated with the performance of rework. Rework almost always entails credible risks associated with: damage to the printed circuit boards, stress to components (e.g., ceramic capacitors), reduced testing levels and failure free hours.*

Example A3.

This is a simplified summary of a complex and multifaceted risk assessment performed for a mission that has been operating in space for well over a year prior to publication of this handbook. The probabilities are calculated using a mix of different statistical methodologies used over three independent, and unique, reliability assessments, and the details are beyond the scope of this handbook. However, there are good lessons of some key drivers for risk in space missions and it provides a nice example of a project where there was recognition well before launch that some risks would not be fully mitigated.

A GSFC project used a particular part type of high voltage optocouplers (HVOCs) throughout several high voltage power supplies in the spacecraft and instruments. Although there was some limited history in prior flights of these HVOCs, they had previously been used in quantities on the order of 10, at voltage levels typically of 1-3 kV (with some limited) examples up to 5 kV. The new application employed 300 of these HVOCs, with application to 6 kV and higher, and with much more aggressive switching operation in some of the power supplies than prior applications. The vendor typically produced these parts on the order of one every two weeks, while this project required them at a much faster pace. These particular specialized parts are not covered by standardized space-grade specifications and are not well-captured in GSFC's EEE-INST-002 EEE parts management instruction document. Not long into testing the project started to encounter problems with the parts in both parts-level testing and circuit-level testing. Ultimately many issues were discovered about the parts including, but not limited to, a fragile design of the part making it more susceptible to bondwire detachments, elevated likelihood of workmanship flaws due to the higher rate of production, and heightened sensitivities to both workmanship and material flaws due to the higher voltage and more stressing application. The early functional and screening test failures prompted a redesign of the part, making it less susceptible to the initially-discovered failure modes associated with the parts. However, the changes did not prepare the parts for the more aggressive operational stresses on the parts, and the arrival of the new parts exposed a brand new set of problems that were now more challenging, particularly those related to function in a complex high-voltage environment.

After a string of failures of the parts in project testing, the project captured a programmatic risk reflecting the potential recurrence of failures in I&T, generically stated as follows:

Given that the instrument developer has experienced HVOC anomalies during instrument board-level testing and that the results of the HVOC qualification tests are inconclusive

It is possible that further anomalies will be found during box-level or system-level testing requiring replacement of the suspect parts

Resulting in use of cost and schedule reserves.

At one point in time at one of the major milestone reviews, the failure history prompted a 1x2 risk, which assumed that the problematic parts would fall out sooner rather than later. There was a long history and evolution of this risk throughout the life of the project, including having the concern going back and forth between being characterized as a risk and then as an issue (i.e.,

where the risk had been realized), and then reverting back to a risk when it was assumed that the underlying causes were resolved.

Well over a year before launch the project and the GSFC organizations involved recognized that there would not be enough time or resources to eliminate all of the causes, nor would there be the resources or ability to remove all of the parts that had already been installed and that had some properties that were determined to be questionable based on recent reviews of screening and qualification data. At this point the project captured a risk that ultimately evolved into a technical risk at launch (denoted a *residual* risk), generically stated as follows:

Given that the instrument experienced HVOC anomalies late in I&T and root cause is not fully mitigated

It is possible that part dynamic failure leading to instrument degradation or part static failure leading to instrument spectrometer failure may occur.

Resulting in serious degradation of science objectives

The part dynamic failure above actually is a failure of 2 or more parts because of the fault-tolerance in the system. The consequence described above is not a total loss, but the degradation to the mission would be serious, defined as a "4" on the consequence scale. A reliability block diagram was generated that indicated the different combinations of part failures that could cause instrument failure (in some cases requiring 2 failures, in others more than 2). Three independent reliability assessments, each based on that reliability block diagram, were combined to estimate the most pessimistic reliability estimate (Ps) to be 87%. This estimate indicated a 13% likelihood of failure, defining a "2" likelihood on the technical risk scale.

It should be noted that upon making the early decision to acknowledge a technical risk, the project added a very aggressive testing campaign at the box level, aimed at fleshing out any remaining problematic parts. The project took further steps to reduce stress in operation of the affected instrument. At this point in time, not a single HVOC has failed in the mission, while at least 2 failures would be required to impact mission performance.

Example A4.

A common nonconformance situation encountered at GSFC is when a coupon representative of a printed circuit board (PCB) panel does not meet the specification indicated in the project's Mission Assurance Requirements. This example describes a case where a requirement in the drawing notes was violated in the coupon. The drawing notes specified a minimum internal annual ring (IAR) of 5 mil, however, the coupon revealed IAR measurements as low as 4.3 mil as shown in Figures A1 and A2.

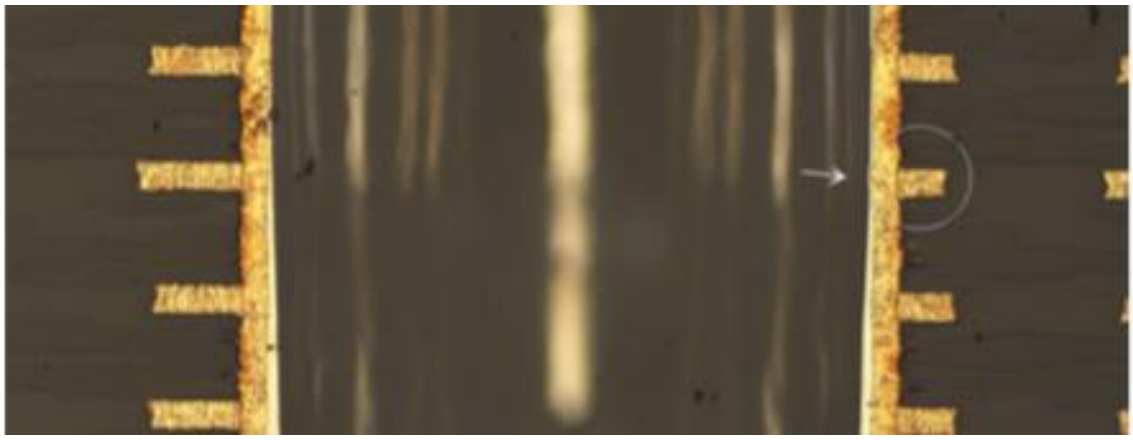

Figure A1: Plated throughhole in microsection

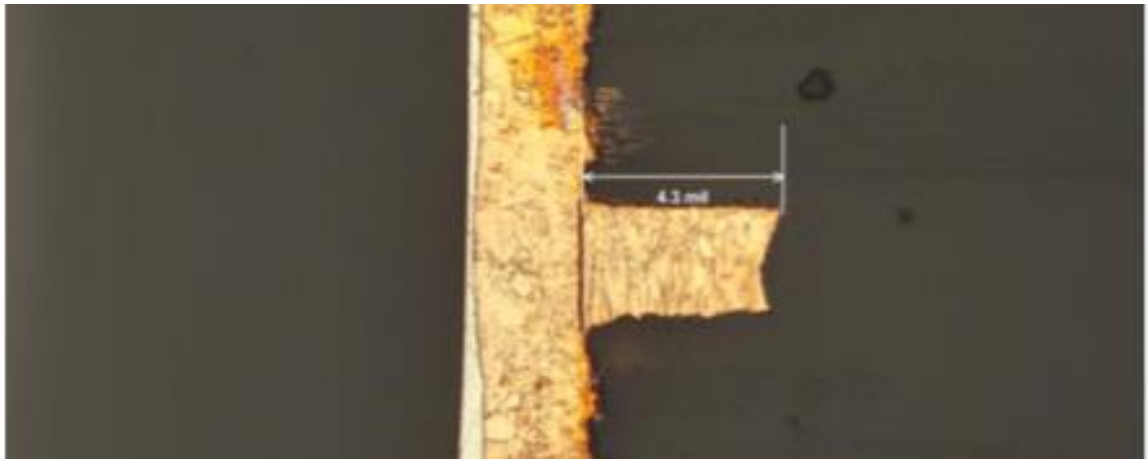

Figure A2: Close-up with internal annual ring measurement

The project had a C risk classification, per NPR 8705.4, and per GPR 8705.4, the guidance recommends IPC 6012D, Class 3, for rigid PCBs. IPC 6012D Class 3 specifies a minimum IAR of 1 mil. With no other nonconforming elements, the coupon meets the requirements of the spec pertinent to Class C, but violates the one requirement in the drawing. The next step is to understand what the basis is for the more stringent requirement for IAR in the drawing since there is no risk associated with the smaller dimension allowed by the specification. An investigation was performed into the source of the requirement and found that this was a requirement included in an old design predating the current specifications, and was scaled up to be conservative. Because insufficient IAR can indicate concern for a breakout condition on the board (where the IAR has insufficient contact with an active trace creating an open circuit defect), the coupon and design were reviewed for potential for breakout and there were no such conditions in place. Henceforth, there is no elevated risk in this case associated with the violation.

Example A5.

As a result of counterfeiting concerns that became apparent in the mid 1990's, GSFC began to impose requirements for fastener integrity to cover fasteners included in flight hardware and in critical ground support equipment. The requirements cover a range of different measures and protections to ensure quality, traceability, authenticity, hardness, and protection against stress corrosion cracking. GSFC considers such measures in defining baseline risk. A situation is encountered where an assembly in the launch vibration load path includes 24 bolts that secure a scanning assembly to an instrument. The instrument has been fully assembled and the bolts are in a location that is challenging to disassemble and reassemble. It was determined that a logistics error resulted in installation of fasteners that had been purchased for general ground use without meeting any fastener integrity (FI) requirements. It is also known that out of this batch of fasteners we have experienced 3 failures out of 1000 during torqueing operations and one failure out of 1000 in assembled hardware after successful torqueing. Consider the following two cases:

Case 1. Concern for failure in vibration test. In this case, we would formulate the following risk statement

Given that the scanning assembly interface is installed with 24 fasteners noncompliant to FI requirements with a prior history of post assembly failure of 1 in 1000

It is possible that a fastener will fail during vibration

Resulting in significant resources to replace the fastener

Since there is no detailed information about the prior failure, we can establish a failure likelihood of 24*1/1000 = 0.024, or 2.4%, which is likelihood of 1 on the programmatic scale. The impact of this occurring would impact schedule milestones, but is achievable within schedule reserves, while the cost can be handled within reserves, so according to GPR 7120.4D, the consequence is 3.

Case 2. Vibration test has occurred with no apparent failures after vibration test; concern for failure of three or more fasteners (one failure on its own would have no appreciable effect) in launch due to a latent defect. We assume that three adjacent fastener failures can initiate a zipper effect to cause failure of the entire interface. The risk statement would be as follows

Given that the scanning assembly interface is installed with 24 fasteners noncompliant to FI requirements with a prior history of post assembly failure of 1 in 1000

It is possible that three or more adjacent fasteners will fail during launch, causing the entire interface to fail

Resulting in loss of the scanning assembly

The likelihood of loss of a single fastener on its own is conservatively 1/1000. The loss of three fasteners is $(1/1000)^3$ = 1e-9. The fact that the fasteners made it through protoflight vibration levels without any modal changes or apparent losses of torque makes it less likely that there will be an on-orbit problem. With likelihood of this failure being << 1e-9, this technical risk is noncredible.

Example A6.

An incident that occurred in an office at GSFC involved a smoke alarm that caught fire due to an internal short circuit. After analyzing the problem, it was discovered that there is a flaw in the circuitry for an affected class of units that would cause 1 failure per 7 years for 1% of the class of units. Between 200 and 400 of the offices and facilities at GSFC have a unit in the affected class. It is estimated that it would take a month to replace all affected units using the standard replacement process. It is necessary to determine the risks both to facilities and personnel of proceeding with the nominal (i.e., non-emergency) replacement process.

Programmatic Risk to facilities:

A facility assessment established that all smoke alarm installations of affected alarms are known to be within fire retardant ceiling tile, with a minimum of 1 ft radius of each other. In case of a characteristic fire, the probability of catching neighboring materials on fire, including sparks going to the carpet prior to self-extinguishing is determined to be 1/3 for "moderate" damage, consequence "3". A pertinent risk statement is:

Given the use of fire alarms affected by a systemic flaw, **it is possible that** one catches fire during the month it takes to replace them all, **resulting in** moderate damage to facilities

The likelihood is 0.01*(1/7)*(1/12)*(1/3)*400 = 1.58%, assuming all 400 offices are affected. The programmatic risk scale begins at 2%, so this risk is noncredible. Being close to the threshold may prompt an accelerated process. First we will consider the safety risk.

Personnel Safety Risk:

The safety risk will build upon the previous programmatic risk, but safety becomes an issue prior to moderate damage, so a ½ is used as the probability of toxic smoke or other fire danger if the unit catches fire. The threats that the local area will catch fire without a functioning fire alarm include smoke inhalation, explosion, and trapped personnel. Furthermore, there is also a threat that toxic smoke will affect personnel prior to detection and warning by functional fire alarms.

A pertinent risk statement is:

Given the use of fire alarms affected by a systemic flaw, **it is possible that** one catches fire during the month it takes to replace them all, **resulting in** in serious injuries due to fire

The likelihood is 0.01*(1/7)*(1/12)(1/2)*400 = 2.38%. This results in a 4x4 safety risk using GSFC's risk scale. This red risk will prompt emergency action to replace the smoke detectors or perform other mitigations.

Example A7.

In the Sounding Rocket Program, one of the variants of sounding rockets had experienced some failures due to an engine combustion instability problem. The longstanding successful rocket experienced this problem due to a design change related to the nozzle. Given that there was no way to revert back to the original design, the process of redesigning, reviewing, and qualifying the new design on one of the main "workhorse" sounding rockets, gave rise to safety concerns and threatened the schedule for the sounding rocket program.

First, consider a range safety risk:

Given the combustion instability problem experienced on several sounding rocket missions, **it is possible that** one fails in flight, **resulting** in threats to the nearby population.

This risk is the first consideration in dispositioning the concern because range safety is paramount for sounding rocket flights. Analysis was performed that placed an error ellipse on the sounding rocket related to the potential effect of the engine problem if it manifested itself and combined this with the capabilities of the flight termination system. This analysis determined that the likelihood of a condition associated with the engine problem that could not be arrested by the flight termination system within the hazard zone is far less than 1.e-6. Therefore the safety risk is not credible.

The pertinent risk is programmatic:

Given that the design problem with the new nozzle may not be resolved in a timely manner, **it is possible that** delivery of new motors could be delayed, **resulting** in a negative impact on the launch schedule for the next year's launch campaign.

The risk as written, based on the most prevalent concern is best aligned with a programmatic consequence of 3. Given a remaining 6 key design issues and a need to qualify the new design once complete, a likelihood of 40-50% is determined to impact the launch schedule. Subsequently we have a likelihood of 3 for this programmatic risk.