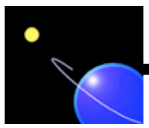

SPACE ENVIRONMENT TECHNOLOGIES

Space Research *Space Operations* *Space Standards*

DRAFT

Critical Item Risk Management (CIRM) Process

Command Media

Written by:	Reviewed by:	Reviewed by:
Electronically Signed	Electronically Signed	Electronically Signed
Pat Branch	Tyrone Jackson	James E. French

Approved by:	Approved by:	Approved by:
S. Dave Bouwer	Rian Shelley	W. Kent Tobiska

SPACE ENVIRONMENT TECHNOLOGIES

Space Research *Space Operations* *Space Standards*

Critical Item Risk Management (CIRM) Process

ORGANIZATIONAL MISSION ASSURANCE STANDARD (TIER 3)

Draft Revision: 0 Release: 04-15-2011 Effective: 04-15-2011

CORPORATE STANDARD

OBJECTIVE

This Standard defines *SET's* approach for implementing a Critical Item Risk Management (CIRM) Process. Through the interpretation and implementation of this Standard, *SET* projects will tailor the set of CIRM Process activities to be commensurate with the unit-value/criticality of their development products. At the time this Standard was written, *SET* did not develop any very-high or ultra-high unit-value products.

Note: Guidance for product unit-value/criticality determination is found in Figure 1.

APPLICABILITY

This Standard applies to all present and future *SET* sites/facilities, programs/projects, business lines/services, functional organizations/working groups, and employees/subcontractors, regardless of whether a CIRM Process has been contractually imposed.

Note: The terms and acronyms used in this Standard are defined in Section 3.

TABLE OF CONTENTS

FIGURES

TABLES

1. INTRODUCTION

This Standard establishes uniform requirements and criteria for the performance-based Critical Item Risk Management (CIRM) Process. The performance-based aspect of this Standard requires that the organization's CIRM capability be rated according to predetermined criteria for process capability and data maturity. The Space Environment Technologies (*SET*) uses the CIRM Process to control the development of hardware and software items that impact safety-critical and mission-critical functions and have a high or serious risk of failure. Safety-critical and mission-critical items whose failure risk is high or series require special quality processes to ensure they are safe and reliable for operational usage.

1.1 Scope

This Standard applies to all present and future *SET* sites/facilities, programs/projects, business lines/services, functional organizations/working groups, and employees/subcontractors regardless of whether a CIRM Process has been contractually imposed. Although it is a common industry practice for CIRM to involve the use of software tools, this Standard does not mandate the application of any particular computerized risk management methodology.

1.2 Purpose

The CIRM Process is implemented to control the development of critical items that exhibit high or series risk. These critical items are identified using Hazard Analysis, FMECA, or equivalent fault/failure analysis methodologiess. The provisions for controlling and testing each critical item is identified in the Critical Items List (CIL) or the Critical Item Document Tree (CI Doc Tree), which is generated to document the hardware and software items which require "special attention" during development. This "special attention" includes verifying that special quality processes are established, or equivalent quality processes are in place, to ensure likelihood of affecting system safety, mission success, maintainability, monitoring capability, and life cycle support cost are minimized. Periodically, project reviews are conducted to determine if additions or deletions to the CIL or CI Doc Tree and its associated control plans are warranted, and to assess the effectiveness of the critical item controls and tests.

When the CIL or CI Doc Tree is created or modified, the hardware and software configuration items identified in that document are considered critical until designated otherwise by the appropriate risk acceptance authority. An item may exit this process only when it is determined the item is no longer critical. This process applies to identified critical items from initial design or acquisition through delivery of the end product.

1.3 Applicability

SET established and maintains an enterprise-wide CIRM Process that is based on AIAA Standard S-102.1.6. This process is used to identify, control and test critical items from initial design through delivery of the end product. This Standard ensure that all affected personnel, such as, design, purchasing, manufacturing, inspection, and test, are aware of the essential and critical nature of each critical items. Each critical item control plan and test method is subject to on-going review and evaluation by the contractor and acquisition authority

2. REFERENCES

2.1 Normative References

The following reference documents of the issue in effect on the date on invitation for bid or request for proposal form a part of this Standard to the extent specified:

AIAA S-102.1 Mission Assurance Management

1) AIAA S-102.0.1 (Draft)	Mission Assurance Program General Requirements
2) AIAA S-102.1.1 (Draft)	Mission Assurance Program Planning Requirements
3) AIAA S-102.1.2 (Draft)	Subcontractor and Supplier Mission Assurance Management Requirements
4) AIAA S-102.1.3 (Draft)	Mission Assurance Working Group (MAWG) Requirements
5) AIAA S-102.1.4 (Released)	Failure Reporting, Analysis and Corrective Action System (FRACAS) Requirements
6) AIAA S-102.1.5 (Released)	Failure Review Board (FRB) Requirements
7) AIAA S-102.1.6 (Draft)	Critical Item Risk Management (CIRM) Requirements
8) AIAA S-102.1.7 (Draft)	Project Mission Assurance Database System Requirements
9) AIAA S-102.1.8 (Draft)	Quality Assurance (QA) Requirements
10) AIAA S-102.1.9 (Draft)	Critical Item Risk Management (CIRM) Requirements
11) AIAA S-102.1.10 (Draft)	Environmental Safety Assurance Requirements

AIAA S-102.2 Mission Assurance Engineering and Analysis

12) AIAA S-102.2.1 (Draft)	Functional Diagram Modeling (FDM) Requirements
13) AIAA S-102.2.2 (Released)	System Reliability Modeling Requirements
14) AIAA S-102.2.3 (Draft)	Component Reliability Predictions Requirements
15) AIAA S-102.2.4 (Released)	Product Failure Mode, Effects and Criticality Analysis (FMECA) Requirements
16) AIAA S-102.2.5 (Draft)	Sneak Circuit Analysis (SCA) Requirements

17) AIAA S-102.2.6 (Draft) Design Concern Analysis (DCA) Requirements

18) AIAA S-102.2.7 (Draft) Finite Element Analysis (FEA) Requirements

19) AIAA S-102.2.8 (Draft) Worst Case Analysis (WCA) Requirements

20) AIAA S-102.2.9 (Draft) Human Error Predictions Requirements

21) AIAA S-102.2.10 (Draft) Environmental Event Survivability Analysis Requirements

22) AIAA S-102.2.11 (Released) Anomaly Detection and Response Analysis Requirements

23) AIAA S-102.2.12 (Draft) Maintainability Predictions Requirements

24) AIAA S-102.2.13 (Draft) Operational Dependability and Availability Modeling Requirements

25) AIAA S-102.2.14 (Draft) Hazard Analysis (HA) Requirements

26) AIAA S-102.2.15 (Draft) Software Component Reliability Predictions Requirements

27) AIAA S-102.2.16 (Draft) Process Failure Mode, Effects, and Criticality Analysis (FMECA) Requirements

28) AIAA S-102.2.17 (Draft) Event Tree Analysis (ETA) Requirements

29) AIAA S-102.2.18 (Draft) Fault Tree Analysis (FTA) Requirements

30) AIAA S-102.2.19 (Draft) Fishbone Analysis Requirements

31) AIAA S-102.2.20 (Draft) Similarity and Allocations Analysis Requirements

32) AIAA S-102-2.21 (Draft) Component Engineering Requirements

33) AIAA S-102.2.22 (Draft) Stress and Damage Simulation Analysis Requirements

AIAA S-102.3 Mission Assurance Testing

34) AIAA S-102.3.1 (Draft) Environmental Stress Screening (ESS) Requirements

35) AIAA S-102.3.2 (Draft) Reliability Development / Growth Testing (RD/GT) Requirements

36) AIAA S-102.3.3 (Draft) Reliability, Maintainability, and Availability Demonstration Testing Requirements

37) AIAA S-102.3.4 (Draft) Reliability Life Testing Requirements

38) AIAA S-102.3.5 (Draft) Design of Experiments Requirements

39) AIAA S-102.3.6 (Draft) Ongoing Reliability Testing (ORT) Requirements

40) AIAA S-102.3.7 (Draft) Product Safety Testing Requirements

Corporate References

41) Reliability Design Rules (Draft)

42) Joint Services Software Safety Design Rules (Released)

2.2 Relationship to Other Corporate Standards

This Standard falls under the *SET* Corporate Standard for the Quality Assurance (QA) Program, and is aligned with the *SET* Corporate Standards for the System Safety Program and the Reliability, Maintainability, Availability & Dependability (RMAD) Program, all of which fall under the *SET* Corporate Standard for the Mission Assurance Program. This Standard defines the sets of activities that are used to control and document changes to products under development, in a manner that is commensurate with each product's unit-value/criticality.

3. TERMINOLOGY

3.1 Terms and Definitions

acquisition authority
an organization (Government, contractor, or subcontractor) that levies requirements on another organization through a contract or other document

ad hoc
for a particular end or case at hand without consideration of wider application

ambiguity group
the expected number of items in the set of items to which a failure can be detected and isolated

anomaly
apparent problem or failure affecting a configured product, process, or support equipment/facilities that is detected during product verification or operation
NOTE: Anomalies are distinguished from discrepancies, product defects which do not violate project requirements which may or may not be documented in the FRACAS.

approximation[1]
a value that is nearly but not exactly correct or accurate

audit[2]
an independent examination of accounts and records to assess or verify compliance with specifications, standards, contractual agreements, or other criteria

authorization
the act of establishing by or as if by authority

baseline process
the minimum set of functions that constitute a specific type of process

baseline program
the minimum set of functions that constitute a specific type of program

capability[2]
one or more processes or activities that describe how SR&QA programs are used, treated, or developed within an organization

capability-based system safety program
the set of processes that assesses and controls product deficiency risk at one or more predefined capability levels

[1] Definition source: IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*

[2] Definition source: IEEE 1624-2008, *IEEE Standard for Organizational Reliability*

capability level
measure of the ability of a system safety process, as specified by a set of activities, to address the pertinent system safety needs of a systems engineering process

capability level growth
a measurable improvement (e.g., an increase in resources, scope of effort, or maturity of input data) in the ability of a system safety process to support the system safety needs of a systems engineering process

chaos
the random occurrence of unpredictable and unrelated events

control
a method used to reduce the consequences, likelihood, or effects of a hazard or failure mode
NOTE: Controls include special design features, procedures, inspections, or tests.

credible failure mode or hazard
a failure mode or hazard with a probability of occurrence greater than $1.0E^{-6}$, 0.000001, or one in a million

critical item
an item that requires additional precautions or special attention because of complexity, application of state-of-the-art techniques, or because a failure of the item would significantly affect product performance (such as single point failure modes)

engineering judgment
a properly trained engineer's technical opinion that is based on an evaluation of specific data and personal experience
NOTE: Engineering judgments are a reality that cannot not be avoided when insufficient time, data, or funding are available to perform a detailed quantitative analysis.

environmental safety assurance
appropriate consideration of potential environmental impacts prior to beginning any action that may significantly affect the environment

estimation
a tentative evaluation or rough order magnitude calculation

failure
termination of the ability of a unit to perform its required function
NOTE: A fault may cause a failure.

failure mode
consequence of the mechanism through which a failure occurs, or the manner by which a failure is observed

fault[3]
[1] [Software reliability] a manifestation of an error in software; [2] [Hardware reliability] any undesired state of a component or system; [3] [Components] a defect or flaw in a hardware or software component; [4] [Human reliability] procedure (operational or maintenance) or process (manufacture or design) that is improperly followed;
NOTES: [1] An accident may cause a fault; [2] A fault may cause a failure; [3] A fault does not necessarily require failure.

hazard
a condition that is prerequisite to a mishap and a contributor to the effects of the mishap
NOTE: A single point failure mode (SPFM) item is a hazard with respect to its potential to lead directly to loss of a safety-critical or mission-critical system function.

maturity level
measure of the degree of accuracy of a data product, as developed using a specified set of input data, in relation to what is considered the best achievable results

method[4]
a formal, well-documented approach for accomplishing a task, activity, or process step governed by decision rules to provide a description of the form or representation of the outputs

mishap
an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment

mission
the purpose and functions of the space system (sensors, transponders, boosters, experiments, etc.) throughout its expected operational lifetime, and controlled reentry or disposal orbit time period.

NOTE: A space system may have multiple missions, i.e., primary mission, ancillary mission, and safety mission.

mission assurance
the program-wide identification, evaluation, and mitigation or control of all existing and potential deficiencies that pose a threat to system safety or mission success, throughout the product's useful life and post-mission disposal

NOTE: Deficiencies include damaging-threatening hazards, mission-impacting failures, and system performance anomalies that result from unverified requirements, optimistic assumptions, unplanned activities, ambiguous procedures, undesired environmental conditions, latent physical faults, inappropriate corrective actions, and operator errors.

mission capability
purpose and functions of the space system (sensors, transponders, etc.) throughout its intended system mean mission duration (the expected life of the space vehicle).

---

[3] Definition source: IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*

[4] Definition source: IEEE 1220-1998, *Standard for Application and Management of the Systems Engineering Process*

NOTE: Ref. AFMAN 91-222 SUPL1

mitigation
(1) a method that eliminates or reduces the consequences, likelihood, or effects of a hazard or failure mode; (2) a hazard control

modeling
act of producing a representation or simulation of one or more items

non-credible failure mode or hazard
a failure mode or hazard with a probability of occurrence equal to or less than 1.0E-6, 0.000001, or one in a million

NOTE: In Systems Safety Engineering, the qualitative probability values of an improbable hazard and a non-credible hazard are equivalent.

plan
a method for achieving an end

practice[5]
one or more activities that use specified inputs to develop specified work products for achieving specified objectives

process
a sequence of tasks, actions, or activities, including the transition criteria for progressing from one to the next, that bring about a result

NOTE: A process can be unmanaged or managed. An unmanaged or "free" process does not have its inputs or outputs controlled. The rain and melted snow that replenishes a lake is an example of an unmanaged process. A managed or "controlled" process has its inputs and outputs controlled. An electrical power station is an example of a managed process.

process-based lesson learned
important information created, documented, and retrieved according to a process or procedure descriptor

product-based lesson learned
important information created, documented, and retrieved according to a system or device life cycle specific functional or physical descriptor

program
[1] the managed collection of an organization's practices that is structured to ensure that the customers' requirements and product needs are satisfied (Ref. IEEE Standard 1624-2008); [2] a defined set of managed processes conducing to an end under a single plan

NOTE: A program does not have to consist of related, managed processes. Compare with definition of *"system"*.

[5] Definition source: IEEE 1624-2008, *IEEE Standard for Organizational Reliability*

quality
a measure of a part's ability to meet the workmanship criteria of the manufacturer

NOTE: Quality levels for parts used by some of the handbook methods are different from quality of the parts. Quality levels are assigned based on the part source and level of screening the part goes through. The concept of quality level comes from the belief that screening improves part quality

reliability
probability that an item will perform its intended function for a specified interval under stated conditions

residual risk
risk associated with significant failure modes or hazards for which there are no known control measures, incomplete control measures, or no plans to control the failure mode or hazard

root cause(s)
most fundamental reason(s) an event might or has occurred

root cause analysis
a process for identifying the fundamental cause of an event or failure

safety
freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment

safety critical
a term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe system operation or use; e.g., safety critical function, safety critical path, safety critical component

specialty engineering
a subgroup of the engineering processes that make up the Mission Assurance Process

NOTE: Traditionally, this subgroup includes Reliability, Maintainability, PMP, Survivability, and Supportability

system
[1] a defined set of related processes [2] elements of a composite entity, at any level of complexity of personnel, procedures, materials, tools, equipment, facilities, and software, that are used together in an intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement

NOTE: A system that consists of one or more unmanaged processes is susceptible to becoming "unbalanced" and changing over time (e.g., an ecological system). For a system to maintain stability, it must be "balanced" and consist only of managed processes.

system safety
the application of engineering management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system lifecycle (Ref. MIL-STD-882C)

systems engineering
An interdisciplinary approach encompassing the entire technical effort to evolve and verify an integrated and life-cycle balance set of system product and process solutions that satisfy customer needs. (Ref. MIL-STD-499B Draft)

tailoring
process by which the individual requirements (tasks, sections, paragraphs, words, phrases, or sentences) of a standard are evaluated to determine the extent to which each requirement is most suited for a specific system acquisition and the modification of these requirements, where necessary, to ensure that each tailored document invokes only the minimum needs of the customer

timely
performance of a task, subtask, or effort when planning and execution results in the output being provided with sufficient time for management, if need be, to identify and implement cost-effective action
EXAMPLE: An action that avoids or minimizes schedule delays and cost increases.

validation
the act of determining that a product or process, as constituted, will fulfill its desired purpose

verification
the process of assuring that a product or process, as constituted, complies with the requirements specified for it

3.2 Acronyms

A_O	Availability Analysis
CA	Criticality Analysis
CIRM	Critical Item Risk Management
CN	Criticality Number
DCA	Design Concern Analysis
D_O	Dependability Analysis
ECP	Engineering Change Proposal
EOLP	End of Life Plan
ESS	Environmental Stress Screening
ETA	Event Tree Analysis

ETC	Estimate to Complete
FDM	Functional Diagram Modeling
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FRACAS	Failure Reporting, Analysis, and corrective Action
FRB	Failure Review Board
FTA	Fault Tree Analysis
HA	Hazard Analysis
HW	Hardware
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
LLAA	Lessons Learned Approval Authority
LOE	Level of Effort
MAP	Mission Assurance Program
	Mission Assurance Process
MAPP	Mission Assurance Program Plan
	Mission Assurance Program Planning
MCLP	Multiple Capability Level Process
O&SHA	Operating and Support Hazard Analysis
PMP	Parts, Materials & Processes
PoF	Physics of Failure
QA	Quality Assurance
R&M	Reliability and Maintainability

RD/GT	Reliability Development/Growth Testing
RMAD	Reliability, Maintainability, and Availability Demonstration
	Reliability, Maintainability, Availability and Dependability
SCA	Sneak Circuit Analysis
SCLP	Single Capability Level Process
SEC	Standards Executive Council
SEMP	Systems Engineering Management Plan
SPFM	Single Point Failure Mode
SR&QA	Safety, Reliability & Quality Assurance
SSP	System Safety Program
SW	Software
SSWG	System Safety Working Group
TAAF	Test, Analyze and Fix
TPM	Technical Performance Metrics
V&V	Verification & Validation

4. GENERAL REQUIREMENTS FOR CIRM PROCESS

Critical items, once identified, are evaluated for appropriate controls in accordance with the system requirements and this Standard. The control methods include cause-effect analysis, root cause analysis, reliability life testing, qualification testing, stress analyses, and other techniques as required to reduce the risk of failure to an acceptable level. The design engineers are required to examine the Critical Items List and make appropriate recommendations for additions and deletions with supporting rationale.

The project's Quality Assurance (QA) Program is the owner of the CIRM Process for that project. Modifications to the CIRM Process are coordinated thru the project's QA Program Lead. In all cases, the capability level of the CIRM Process will not be lower than the unit-value/criticality category of the product that it is applied to. The unit-value/criticality categories for sample products are defined in Figure 1.

Figure 1. Product Unit Value/Criticality Categories for Sample Products.

Unit Value/Criticality Category 5	Unit Value/Criticality Category 4	Unit Value/Criticality Category 3	Unit Value/Criticality Category 2	Unit Value/Criticality Category 1
• Defense satellites • Launch vehicles • Long-range missiles • Short-range missiles/rockets • Passenger aircraft / helicopters • Military aircraft / helicopters • Military drones / unmanned vehicles • Naval vessels • Nuclear weapons • Nuclear power plants • Cyclotrons	• Commercial / communications satellites • Fossil fuel / hydro-electric power plants • Oil tankers • Field / off shore oil rigs • Water filtration plants • Explosive devices • Passenger trains / buses • Cruise liners • Satellite ground control stations • Safety-critical hardware / software equipment / components • Safety-critical equipment testing/	• Science satellites • Cargo ships • Mobil / mechanized weapons • Freight trains • Amusement park rides • Elevators / escalators • Small private aircraft / helicopters • Automobiles / trucks / motorcycles • Farm equipment • Construction / demolition / excavation equipment • Factory machinery • Fire arms	• Industrial electronics • Motorized / manual hand tools • Mission-critical hardware / software equipment / components • Industrial computers / peripherals • Satellite communications relay stations • Laboratory / research equipment • Communications / utility equipment • Mission-critical equipment testing/ monitoring apparatus • Computer operating system software • Large Batteries	• Consumer electronics • Household appliances • Small Batteries • Battery operated toys • Infant/ children toys • Computer application program software • Personal computers / peripherals

5. DETAILED REQUIREMENTS FOR CRITICAL ITEM RISK MANAGEMENT

5.1 Perform Critical Item Identification

The CIRM Process begins with the designation of a configuration item as being safety-critical or mission-critical with an unacceptable probability of occurrence. When this occurs, the QA Program independently monitors the item from its initial design or procurement through its delivery as a component in the end product. The QA Program Lead is responsible for ensuring the project's engineering disciplines identify the items whose failure can affect system safety, mission success, maintainability, monitoring capability, and life cycle support cost. A hardware or software configuration item will be designated as a critical item if one of the following characteristics is met as a result of its failure, malfunction, or absence:

(1) Can item lead to a catastrophic or critical mishap either directly or in conjunction with another failure?

(2) Can item cause system reliability, dependability, or availability to fall below required value?

(3) Can item lead to loss of ability to meet key project objectives, including performance, system safety, mission success, cost, and schedule?

(4) Can item cause extensive/expensive maintenance and repair[6]?

(5) Can item cause death or permanent disability to the operator or bystander?

(6) Can item lead to exposure of personnel to hazardous materials, radiation, or laser energy, which can cause long term disability or death?

(7) Can failure of item lead to loss of a system valued at $2M or more?

Can item prevent receipt of data to evaluate system safety, availability, mission success, or need for maintenance or repair?

(8) Does item have an unsatisfactory operating history?

(9) Does item have a stringent performance requirement in its intended application relative to state-of-the-art techniques for similar items?

(10) Does item have insufficient operational or test history, or insufficient similarity with other items with sufficient operational or test history, to provide confidence in its reliability?

(11) Is item difficult to procure and/or manufacture relative to state-of-the-art techniques?

(12) Is item stressed during operation in excess of recommended derating criteria?

(13) Does item have a limited operating life, shelf life, or susceptibility to environmental hazards, such as, vibration, high temperature, thermal cycling, propellant, etc., which warrants controlled surveillance under specified conditions?

(14) Is item known to require special handling, transportation, storage, and/or test precautions?

[6] High unit-value/criticality items are mission-critical for design-to-life-cycle cost.

(15) Does item have a failure history or processing deficiency that warrants traceability?

(16) Does item have redundant hardware or signal paths that provide a safety-critical or mission-critical function, but cannot be checked out prior to use?

(17) Is item safety-critical or mission-critical and cannot be isolated to Ambiguity Level 1 or 2 when failed?

(18) Is item mechanical hardware that is to be deployed, reconfigured, or in motion during use?

Exposure of personnel to hazardous material refers to any material where the Material Safety Data Sheet (MSDS) limits are exceeded and credible likelihood exists for personnel disability or death to occur. Exposure of personnel to radiation refers to nuclear radiation material, ionization radiation material, or radio frequency (RF) radiation levels. Laser energy refers to blinding potential as well as burning potential.

Software components may be designated as critical items based on the results of a software hazard analysis that is performed at the computer configuration item (subroutine) level or at the block level in a logic flow chart. A software hazard analysis shall be performed for all software configuration items to identify software critical items.

In cases where operator training is necessary to properly operate safety-critical or mission-critical equipment, the training manual and plan are considered critical characteristics of the item, and are included in the CIL or CI Doc Tree for tracking.

SET requires all of its suppliers to clearly identify the critical characteristics of their products in the specifications, installation and assembly drawings, and other documents provided to *SET* for review. If an *SET* project cannot verify that a critical item was inspected at the supplier's facility, then incoming inspections will be conducted to ensure the item's critical characteristics are acceptable.

Items that meet the critical item classification criteria due solely to the potential of Foreign Object Damage (FOD) occurring during operation will not be designated as critical items. Instead, the QA Program will focus on minimizing the likelihood of FOD affecting the item during its operation.

5.2 Collect Critical Item Information

The identification of a critical item is followed by the collection of pertinent information about that item. The type of information collected includes, but is not limited to:

(1) performance requirements,

(2) functional and physical drawings/schematics and narratives;

(3) indentured parts lists;

(4) wire lists and interconnect drawings;

(5) design specifications;

(6) manufacturing assembly drawings;

(7) test plans;

(8) operating plans;

(9) descriptions of the mission phases and environments,

(10) all normal, degraded modes that are applicable to each mission phase; and

(11) failure history.

If a Capability Level 3 or higher CIRM Process is required, sufficient information will be entered in the FMECA/Hazard Analysis database to allow cross-referencing the identified critical items with /approved design drawings and parts lists.

5.3 Monitor Critical Item Development

If a Capability Level 4 or higher CIRM Process is required, the QA Program Lead will ensure each stage of the development cycle of the critical item is evaluated to identify procedures used to detect deficiencies that affect the item's form or function. This evaluation includes estimating the failure coverage of each deficiency detection method. All critical items whose failure coverage during development is less than 99% will be reported to the project manager.

5.4 Perform Critical Item Control

Critical items will be controlled by either eliminating them from the design or reducing their likelihood of failure to an acceptable level. All evaluations of proposed design changes or alternative operating modes to either eliminate a critical item or reduce its likelihood of failure will consider the affects of those changes on both operational effectiveness and life cycle cost of the end product. For example, if adding redundancy is necessary to reduce failure likelihood, then it must be justified in terms of what it will cost and what it will buy over the life cycle of the product's inventory. All process controls proposed to reduce the likelihood of damage to a critical item during product development, test, integration, handling, transportation, storage, or operation will be validated prior to their use. All methods proposed to detect damage to a critical item during product development also will be validated prior to their use. The SET Critical Item Control Plan Worksheet is provided in Annex A.

The QA Program shall maintain a record of all the processes applied to each critical item during its development cycle, which includes design, manufacture, quality screening, integration, and functional testing. The critical item's operating time will be recorded and included in its risk acceptance documentation. The critical item control methods will be implemented in accordance with the end product's requirements and this Standard, which includes the applicable control methods in Table 3.

Table 1. Critical Item Control Methods.

Critical Item Control Methods	Description of Failure Control Method
Risk Management	• Develop documentation that provides clear evidence all required process controls were peer reviewed and correctly applied (Capability Level 4)

Critical Item Control Methods	Description of Failure Control Method
Requirements Tracing	• Develop documentation that provides clear evidence all functional performance requirements were properly developed and flowed down (Capability Level 1) • Develop documentation that provides clear evidence approved waivers were provided for all contract-specified functional performance requirements that were not met (Capability Level 1) • Develop documentation that provides clear evidence all configuration requirements were properly developed and flowed down (Capability Level 2) • Develop documentation that provides clear evidence approved changes were provided for all contractor-specified configuration requirements that were not met (Capability Level 2)
Manufacturing, Test, Packaging, Handling, Transportation, and Storage Records	• Develop documentation that clearly describes the item's functional test history (Capability Level 1) • Develop documentation that clearly describes the item's power-off test and physical inspection history (Capability Level 2) • Develop documentation that clearly shows functional test data were subjected to trending analysis (Capability Level 3) • Develop documentation that clearly describes the item's complete build history (Capability Level 3) • Develop documentation that clearly describes the item's complete operating history (Capability Level 3) • Develop documentation that clearly describes the item's complete rework history (Capability Level 3) • Develop documentation that clearly describes the item's storage history (Capability Level 4) • Develop documentation that clearly describes traceability of the item's lower level parts and materials (Capability Level 4) • Develop documentation that clearly describes the complete test and inspection history of the item's lower level parts and materials (Capability Level 4) • Develop documentation that clearly describes the physical and chemical analysis history of the item's lower level materials (Capability Level 5)

Critical Item Control Methods	Description of Failure Control Method
Configuration Control	• Develop documentation that clearly describes the item's as-built configuration (Capability Level 2) • Develop documentation that clearly describes the evaluation and resolution of differences between build-to and as-built configurations (Capability Level 2)
Failures / Discrepancies Evaluation	• Develop documentation that shows clear evidence all functional test and analysis discrepancies for the item were evaluated appropriately (Capability Level 1) • Develop documentation that shows clear evidence all power-off test and physical inspection discrepancies for the item were evaluated appropriately (Capability Level 2) • Develop documentation that shows clear evidence all functional, physical, or logical discrepancies for lower level parts and materials were evaluated appropriately (Capability Level 5)
Quality Records	• Develop documentation that provides clear evidence all of the project's quality records were properly filled out (Capability Level 1)
	• Provide clear evidence all of the project's quality records can be retrieved using database software (Capability Level 3)
Mission Assurance	• Develop documentation that provides clear evidence all required product specifications, drawings, and plans were reviewed to assure they meet the needs of the Systems Engineering Process (Capability Level 3) • Develop documentation that provides clear evidence Failure Mode, Effects and Criticality Analysis (FMECA), worst case analysis, parts stress analysis, thermal analysis, and all other applicable casual analyses were performed to the appropriate level of detail (Capability Level 1) • Develop documentation that provides clear evidence the Lessons Learned Process was implemented in accordance with the enterprise's command media, and that lessons learned were documented and shared with Risk Management and other disciplines (Capability Level 3)

Only the development processes that impact the critical characteristics or critical components of the critical item are required to be controlled. An item's critical designation does not necessarily extend downward to every characteristic and component of that item. Instead, the critical item

designation extends only to those characteristics and components that have been determined to be relevant to failure of the item. For example, if the hardness of an item is its only critical aspect then only the hardening process for that item need be controlled. Figure 2 shows the *SET* hardware development process, and Figure 3 shows the *SET* software development process.

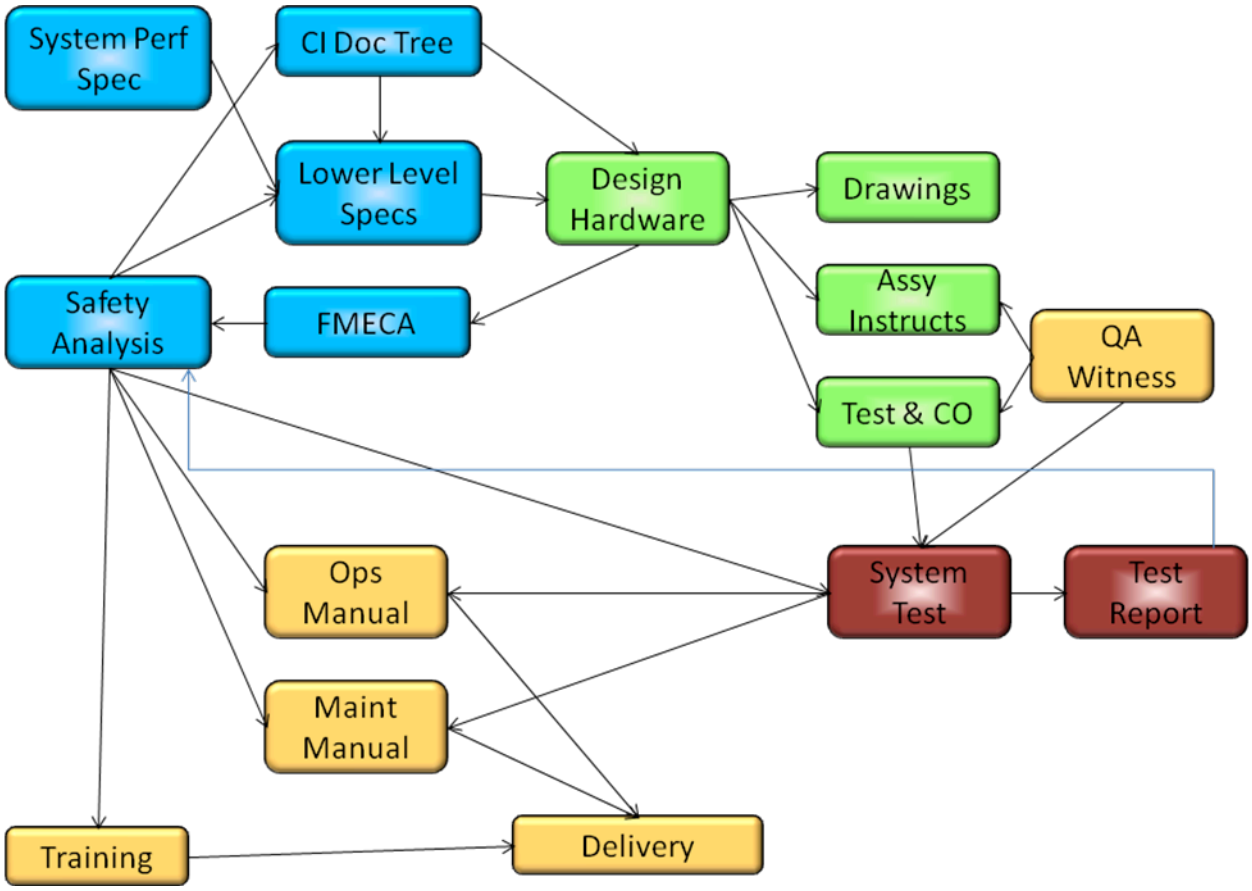

Figure 2. *SET* Hardware Development Process.

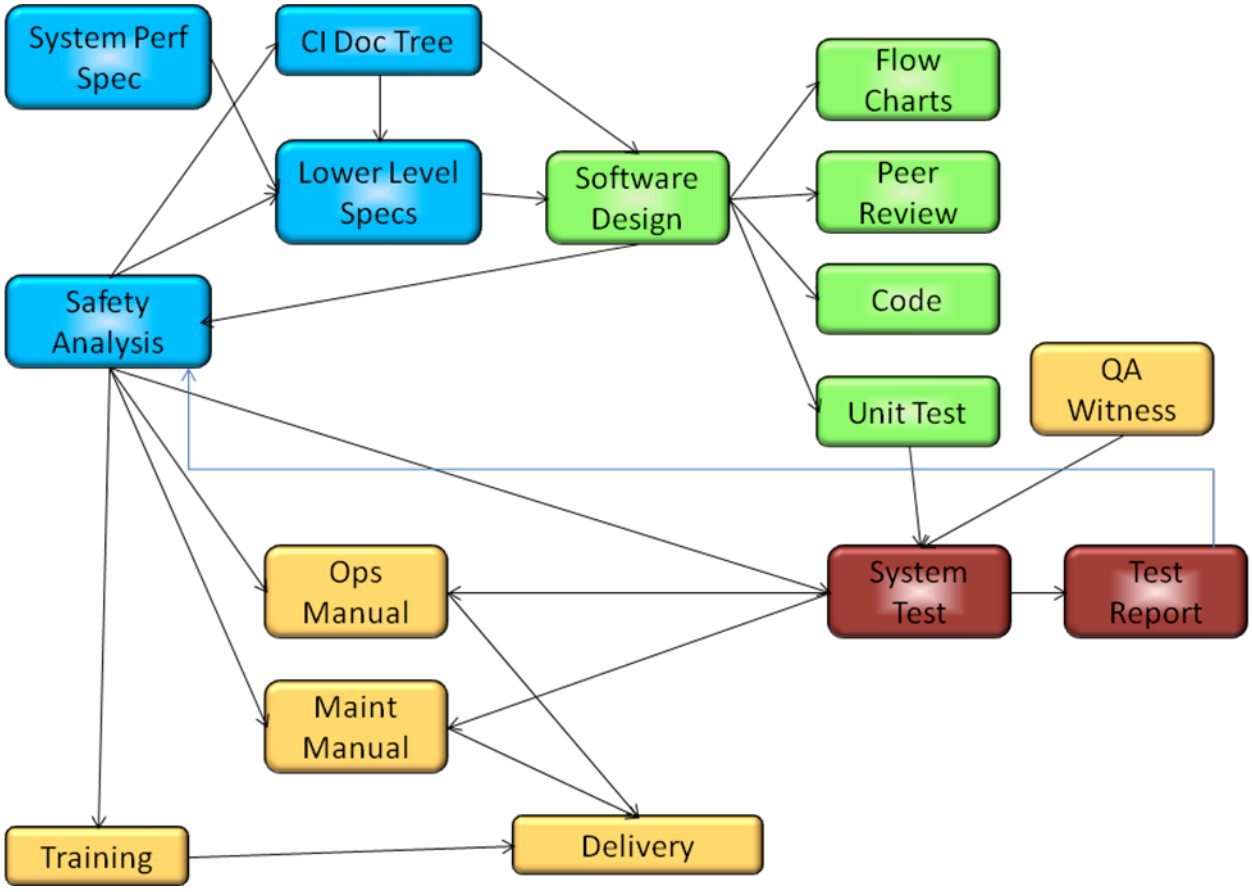

Figure 3. *SET* Software Development Process

Latent safety-critical or mission-critical failure modes and faults that cannot be isolated to an Ambiguity Group 1 or 2 during operation may require regular inspections, preventive maintenance, or periodic replacement to control their risk of failure.

When there is more than one CIRM control method to choose from, the disposition is for the project to follow the MIL-STD-882C risk mitigation method order of precedence, which is defined as follows:

(1) Eliminate faults through design selection. Ideally, the risk of a failure mode should be eliminated. This elimination is often accomplished by selecting a design alternative that removes the fault altogether;

(2) Reduce risk through design alteration. If the risk of a failure mode cannot be eliminated by adopting an alternative design or alternative material, consider design changes that reduce the severity and/or the probability of a failure mode;

(3) Incorporate engineered features or devices. If the risk of a failure mode is unable to be eliminated or adequately mitigated through a design alteration, reduce the risk using an engineered feature or device. In general, engineered features actively interrupt the failure mechanism sequence and devices reduce the risk of a failure mode;

(4) Provide warning devices. If engineered features and devices do not adequately lower the risk of the failure mode, include a detection and warning system to alert personnel to the presence of a faulty condition or occurrence of an undesirable latent event. Develop procedures and training.

(5) Where other risk reduction methods cannot adequately mitigate the risk from a failure mode, incorporate special procedures and training. Procedures may prescribe the collection of diagnostics or prognostics data. Warnings, cautions, and other written advisories shall not be used as the only risk reduction method for high and serious initial risk levels.

5.4.1 Risk Management

The Failure Severity Classification for each identified critical item will be defined, and qualified or rated based on the worst case end effects on the product or mission. Definitions for severity classifications are based on the specific analytical objectives, such as, performance, system safety, mission success, availability, etc. Table 1 provides the AIAA Standard S-102.0.1 Failure Severity Classification Criteria. If a Capability Level 3 or higher CIRM Process is required, a Fault Tree Analysis or equivalent analysis methodology will be performed to verify all safety-critical functions are dual fault tolerant.

Table 2. AIAA S-102 Failure Severity Classification Criteria.

Failure Severity Classification	Failure Effect Description
Catastrophic	Failure would cause loss of life or total disability to personnel, or Failure would cause identifiably catastrophic damage to system and repairs that are beyond the capability of the user or contractor to resolve the effects
Critical	Failure would cause severe disabling injury or severe occupational illness to personnel, or Failure would cause identifiably critical damage to the system and extensive repairs to resolve the effects
Marginal	Failure would cause minor injury or minor occupational illness to personnel that may require hospitalization, but failure is not disabling, or Failure would cause identifiably marginal damage to the system and acceptable level of repairs and downtime to resolve effects
Minor	Failure would cause minor injury to personnel but those injuries would not require hospitalization, or failure would cause minor occupational illness, or Failure would cause identifiably minor damage to the system and minor repairs and short downtime to resolve effects
NEGLIGIBLE	Failure would cause less than minor injury and no occupational illness, or Failure would cause negligible damage to the system and insignificant or no downtime to resolve effects, or Failure is not credible

The Failure Likelihood Classification for each identified critical item will be defined based on a quantified or qualified estimate of the probability of occurrence of the worst case effects of failure on the end product or mission. The failure likelihood estimate will include probability of damage being induced or escaping during development or procurement of the critical item, and will be based on credible causes only, such as, characterized weaknesses and faults in development, test, and integration processes. Failure likelihood will be estimated by using Component Reliability Predictions (Reference 14), Product FMECA (Reference 15), Software Component Reliability Predictions (Reference 26), Process FMECA (Reference 27), Similarity Analysis (Reference 31), or an equivalent methodology. Table 2 provides the baseline AIAA Standard S-102.0.1 Failure Likelihood Classification Criteria. If a Capability Level 4 or higher CIRM Process is required, the probability of damage occurring during development will be estimated using a prediction method that provides at least a 90% lower-bound confidence. For

cases where the critical item is known to be affected by unplanned events during development, test or integration, the estimated likelihood of failure will include probability of unplanned events.

Table 3. AIAA S-102 Failure Likelihood Classification Criteria.

CLASSIFICATION	LEVEL	QUANTIFICATION	DESCRIPTION
FREQUENT	A	($X > 10^{-1}$)	Likely to occur frequently
PROBABLE	B	($10^{-1} > X > 10^{-2}$)	Will occur several times in the life of an item.
OCCASIONAL	C	($10^{-2} > X > 10^{-3}$)	Likely to occur some time in the life of an item
REMOTE	D	($10^{-3} > X > 10^{-6}$)	Unlikely but possible to occur in the life of an item
IMPROBABLE	E	($10^{-6} > X$)	So unlikely, it can be assumed occurrence may not be experienced

The project will translate the critical item risk matrix that is based on the MIL-STD-882D system safety methodology, or any other risk assessment methodology, to the format of the conventional 5x5 risk matrix shown in Figure 3.

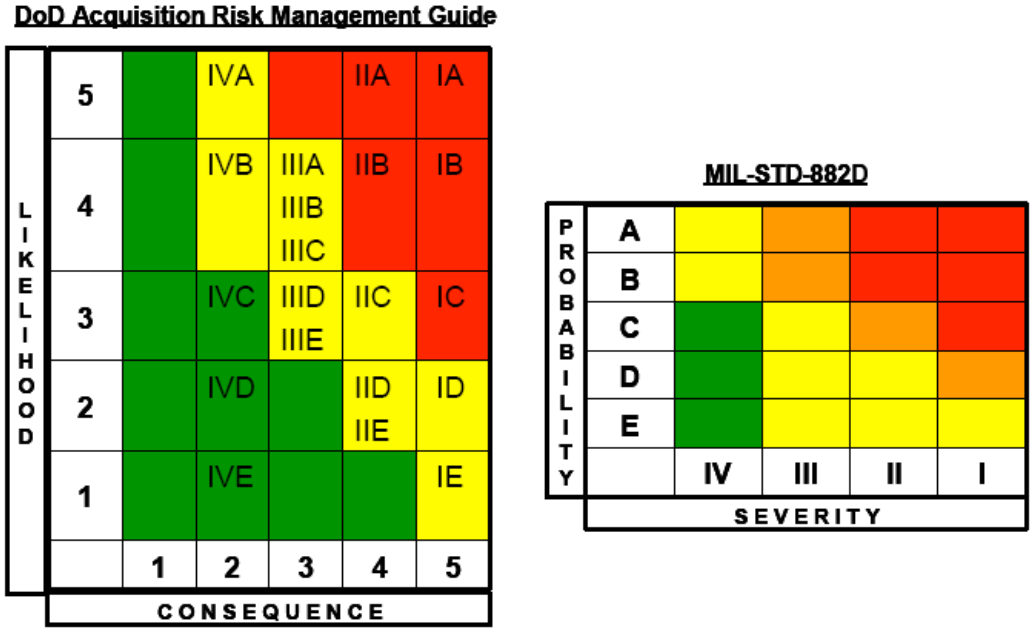

Figure 4. Translation of MIL-STD-882D Risk Matrix to Conventional 5x5 Risk Matrix.

The QA Program Lead will ensure the responsible Product Engineer reviews all project documents that cite a critical item, including specifications, parts lists, drawings, allocations, test plans, test reports, failure reports, QA inspection procedures, hazard analysis, FMECA reports, reliability prediction reports, and training manuals.

5.4.2 Requirements Tracing

During the early phases in the project's Systems Engineering life cycle, specifications are written and the requirements are flowed down to the configuration items that make up the product. Bi-directional tracing of requirements among specifications will be performed. Metrics which show requirement coverage between specifications will be collected and maintain. The System Safety Program and the Reliability, Maintainability, Availability, and Dependability (RMAD) Program will generate their respective Minimum Equipment List (MEL). The MEL will identify all equipment required for system safety and mission successs. Safety and reliability design requirements will be allocated to the items on the MEL. The MEL should also identify mission scenarios and the critical equipment for each scenario.

The Requirements Tracing will identify the Qualification Test events for all critical items. A Qualification Test (QUAL TEST) is testing performed on the first article to verify the design meets all design requirements. The Requirements Tracing also will identify Acceptance Testing events for all critical items. Acceptance Testing are tests performed on every article to verify the manufacturing processes were followed properly. The results of Requirements Tracing will be documented in the test procedures and in the product specifications. Metrics from Requirements Tracing will be used to uncover any requirements that are not completely verified.

When there are conflicting mission assurance requirements involving a critical item, the disposition is for the project to follow the AIAA Standard S-102.0.1 mission assurance requirements order of precedence, which is defined as follows:

(1) System safety requirements

(2) Mission success requirements

(3) Dependability/availability requirements

(4) Reliability requirements

(5) Maintainability requirements

(6) Testability requirements

5.4.3 Manufacturing, Test, Packaging, Handling, Transportation, and Storage Records

Specific manufacturing steps that can affect the characteristics of a critical item will themselves be identified as critical items on the manufacturing/assembly drawings.

All critical items will be serialized and tracked throughout the life of the end product. This includes the ability to trace the lower level parts and materials. For a Capability Level 4 or higher QA Program, this traceability will include the processes and chemical analysis of the raw materials.

All safety critical and mission critical manufacturing processes for critical items will have QA inspection procedures identified in the QA Program Plan. All test procedures will show how compliance with all safety design requirements are verified. The QA inspection procedures which involve critical items will be identified in the QA Program Plan.

5.4.4 Configuration Control

SET's Configuration Control Command Media will be followed for all critical items. Specifically, all changes to approved configurations involving critical items will be submitted and approved thru the Engineering Change Request (ECR) process. When new or multiple versions of software exist, configuration controls will be implemented which identify hardware and software compatibilities. This configuration management process shall prevent unsafe configurations from being delivered.

5.4.5 Failure/Discrepancy Evaluation

All critical item test failure will be documented, tracked, and classified through the project's Discrepancy Reporting process. Discrepancy reports that expose a safety-critical or mission-critical problem will require immediate notification of all customers that have the affected item in their system. Metrics will be collected on discrepancy reports, including the criticality of the reported failure and the level of testing the failure occurred.

5.4.6 Quality Records

The QA Program will document and retain the following records of each critical item:

(1) qualification test records

(2) acceptance test records

(3) build history

(4) rework history

(5) operating history log book

(6) maintenance history log book

Periodic inspection audits of the QA records will be performed. Any differences between the build-to and the as-built configurations will be identified and resolved thru the Discrepancy Reporting process. QA records will be retained for the life of the product and will be electronically retrievable.

5.4.7 Mission Assurance

The responsible product engineer will recommend the preferred method to control the critical item during its development, and provide rationale for each recommendation. The QA Program Lead will ensure these recommendations undergo peer review prior to approval by the project manager. Metrics will be collected and shared on the peer review findings.

Structural design of the critical items, for which fracture is a critical failure mode, will ensure a factor of safety of at least four (4) or the item will be tested to two (2) lifetimes.

The QA Program Lead will ensure that industry acknowledged hardware and software design standards are followed for all critical items. In addition, the QA Program Lead will ensure a *SET* approved or industry acknowledged software coding specification is followed for all software critical items.

Modification of a software critical item requires a minimum set of regression testing as specified in the test process. Software can be reused for critical software functions if a safety hazard analysis of the usage is performed to determine testing requirements.

Both a Product FMECA and a Process FMECA will be performed on all critical items. The Process FMECA will include possible human operational errors and maintenance errors in addition to manufacturing and test equipment induced failure modes. In addition, an Operations and Support Hazard Analysis (O&SHA) will be performed on all manufacturing and testing process involving critical items. If the Process FMECA or O&SHA identify components, processes, tests, or maintenance procedures as critical items that were not previously identified then the CIL or CI Doc Tree, drawings, assembly instructions, and test procedures will be updated to include the critical processes.

Certain maintenance procedures may be identified as critical items. For example a non-redundant connector if not connected properly could vibrate lose and cause a catastrophic hazard. If the hardware designer, system tester, or safety analyst determines that a preventive maintenance procedure is safety-critical in this case, then QA inspection procedures will be identified for that procedure.

A Lessons Learned process will be used to provide feedback of all critical item controls. This feedback will be provided after every major product release. The lessons learned database will be shared across projects. Internal data users will be surveyed about the control methods and data products with recommendations for continuous process improvements. This survey will be conducted by the QA Program Lead after every major product release. The continuous improvement process and lessons learned process will include annual goal setting and outside evaluations of the project.

Critical items that pose a health or injury risk when damaged or past their useful life will be shipped with warning labels to notify users of the potential dangers and instructions for proper replacement or disposal. These critical items require feedback from the customers to ensure they are used in a safe manner. This only applies to items where the critical characteristic is associated with proper operation or maintenance. For Capability Level 4 or 5 QA programs, procedures will be established to provide feedback from customers of critical item field operations and failures.

5.4.8 Improving the CIRM Process

When improvements in the CIRM Process are necessary, *SET* handles them as would any other changes. In every case, the approval of all stake-holder organizations is obtained prior to implementing a change in the CIRM Process.

6. CRITICAL ITEM RISK MANAGEMENT (CIRM) PROCESS EVALUATION CHECKLIST

This checklist assists SET projects in establishing an effective CIRM process. If a question cannot be answered affirmatively, the product stake-holder should carefully examine the situation and take appropriate action.

Process Management

___Was documentation provided that shows clear evidence item's data is maintained in a project-wide database, e.g., a Reliability or Quality Records Database? Level 3

___Was documentation provided that shows clear evidence that implemented processes are controlled? Level 4

Requirements

___Was documentation provided that shows clear evidence requirements were properly developed and flowed down? Level 1

___Were approved waivers provided for all contract-specified functional performance requirements that were not met? Level 1

___Was documentation provided that shows clear evidence the contractor had specified the necessary configuration requirements? Level 2

___Were approved changes provided for all contractor specified configuration requirements that were not met? Level 2

Manufacturing, Testing, and Handling

___Was documentation provided that describes functional test history of item? Level 1

___Was documentation provided that describes power-off test and physical inspection history of item? Level 2

___Was documentation provided that shows functional test data was subjected to trending analysis? Level 3

___Was documentation provided that describes complete build history of item? Level 3

___Was documentation provided that describes complete operating history of item? Level 3

___Was documentation provided that describes complete rework history of item? Level 3

___Was documentation provided that describes complete storage history of item? Level 4

___Was documentation provided that describes traceability of lower level parts and materials in item? Level 4

___Was documentation provided that describes complete test and inspection history of lower level parts and materials? Level 4

___Was documentation provided that describes physical and chemical analysis history of lower level materials? Level 5

Design Engineering

___Was documentation provided that describes as-built configuration of item? Level 2

___Were all differences identified, evaluated, and resolved between (1) the build-to and as-built configurations of item, and (2) the qualification test and acceptance test items? Level 2

Failure Reporting, Analysis, and Corrective Action

___Were item's functional test discrepancies evaluated appropriately? Level 1

___Were item's power-off test and physical inspection discrepancies evaluated appropriately? Level 2

___ Is Failure Mode, Effects and Criticality Analysis (FMECA) for item accurate, is it comprehensive, and is it performed to the level of detail necessary to identify all unique functional failure modes? Level 4

___Were functional and physical discrepancies of lower level parts and materials in item evaluated appropriately? Level 5

Engineering Analysis

___Were all concerns identified in FMECA, Worst Case Analysis, parts stress analysis, and thermal analysis resolved appropriately? Level 5

Lessons Learned

___Were any lessons learned created as a result of processing the item and were those lessons learned documented and distributed? Level 5

ANNEX A

SET CRITICAL ITEM CONTROL PLAN WORKSHEET

1. ITEM: _____
2. PART NUMBER: _____
3. MANUFACTURER: _____
4. CRITICAL FACTORS: _____
5. Identify primary factors which cause the item to be designated as a critical item:

   _____

6. CONTROLS: Detail the specific controls which will be implemented for the item including (as applicable):

   _____

7. Design Controls: _____
8. Manufacturing Controls: _____
9. Test Controls: _____
10. Assembly/Integration Controls: _____
11. Contamination Controls: _____
12. Packaging/Handling Controls: _____
13. Inspection Controls: _____

APPROVED:

_____ _____

Responsible Product Engineer Date

ANNEX B

SET CAPABILITY-BASED CRITICAL ITEM RISK MANAGEMENT PROCESS

General Requirements (normative)

B.1 The Capability Level 1 Critical Item Risk Management shall include the following tasks:

B.1.1 Timely establishment of the requirements and implementation ground-rules for the CIRM process (This is a process validation activity when it includes evaluation of the appropriateness of the CIRM process prior to it being used to identify and control safety-critical and mission-critical items during product development.);

B.1.2 Timely establishment of CIRM Technical Performance Metrics (TPMs);

NOTE: Example TPMs include completed versus required specification traces, performed versus planned subsystem hazard analyses, convened versus scheduled peer reviews, and logged versus adjudicated discrepancy reports (DRs).

B.1.3 Timely collection and evaluation of sufficient system design, analysis, manufacturing, and test information needed to identify critical items in accordance with the system requirements and AIAA Standard S-102.1.6. The system information collected shall include, but not be limited to:

(1) functional and physical drawings/schematics and narratives;

(2) indentured parts lists;

(3) wire lists and interconnect drawings;

(4) design specifications;

(5) manufacturing assembly drawings;

(6) test plans/reports;

(7) operating plans;

(8) descriptions of the mission phases and environments;

(9) all normal, degraded, and contingency system modes that are applicable to each mission phase;

(10) minimum equipment list (MEL).

B.1.4 Timely assessment of the system design to identify hardware items that support functions which are safety-critical, mission-critical, or neither, in accordance with the system requirements and AIAA Standard S-102.1.6. The identification of hardware critical items shall be based on the following criteria:

(1) A specific failure mode of the item would cause death to the operator or bystander;

(2) A specific failure mode of the item would cause permanent disability to the operator or a bystander;

(3) A specific failure mode of the item would expose personnel to hazardous material, radiation, or laser energy which can cause long term disability or death;

(4) A specific failure mode of the item would lead to loss of an irreplaceable system, e.g., research spacecraft and experimental aircraft;

(5) Failure of the item would critically affect system safety, cause the system to become unavailable or unable to achieve mission objectives, or cause extensive/expensive maintenance and repair[7];

(6) Sole failure of the item causes system failure. In other words, the item is a Single Point Failure Mode (SPFM);

(7) Failure of the item will prevent obtaining data to evaluate system safety, availability, mission success, or need for maintenance/repair;

(8) The item has exhibited an unsatisfactory operating history.

(9) The item has stringent performance requirements in its intended application relative to state-of-the-art techniques for similar items;

(10) The item does not have sufficient operational or test history, or sufficient similarity with other items with sufficient operational or test history, to provide confidence in its reliability;

(11) The item is difficult to procure and/or manufacture relative to state-of-the-art techniques;

(12) The item is stressed in excess of recommended derating criteria;

(13) The item has a known operating life, shelf life, or environmental exposures such as vibration, thermal, propellant, or a limitation which warrants controlled surveillance under specified conditions;

(14) The item is known to require special handling, transportation, storage, and/or test precautions;

(15) The item's history, nature, or processing has a deficiency that warrants traceability;

(16) The item is redundant hardware or signal paths that provide a mission-critical function, but which cannot be checked out prior to use;

(17) The item is mechanical hardware that is to be deployed, reconfigured, or in motion during use.

B.1.5 Timely qualification or rating of the severity for each critical item based on the worst case end effects on the system or mission, e.g., software hazard analysis report (SHAR);

B.1.6 Timely qualification or rating of the likelihood of process-induced failure for each critical item based on the worst case end effects on the system or mission, e.g., SHAR

[7] High unit-value items are reliability-critical for design-to-life-cycle cost.

B.1.7 Timely generation of the CIRM Report[8] to document the control methods for all hardware critical items, in accordance with the system requirements and AIAA Standard S-102.1.6. The hardware critical item controls shall include, but not be limited to, the following:

(1) Develop documentation that provides clear evidence all functional performance requirements were properly developed and flowed down;

(2) Develop documentation that provides clear evidence approved waivers were provided for all contract-specified functional performance requirements that were not met;

(3) Develop documentation that clearly describes the item's functional test history;

(4) Develop documentation that shows clear evidence all functional test and analysis discrepancies for the item were evaluated appropriately;

(5) Develop documentation that provides clear evidence all of the project's quality records were properly filled out;

NOTE: Quality control guidelines should be followed to prevent damage and deterioration of the part during its manufacturing, assembly, and testing processes. Examples include (1) a recommended temperature profile, (2) cleaning agents, (3) adhesives, (3) moisture sensitivity, and (4) electrical protection. As new technologies emerge and products become more complex, quality control guidelines become more important to ensure the required quality and reliability of the parts and the product is met.

(6) Develop documentation that provides clear evidence Failure Mode, Effects and Criticality Analysis (FMECA), worst case analysis, parts stress analysis, thermal analysis, and all other applicable casual analyses were performed to the appropriate level of detail.

B.2 The Capability Level 2 Critical Item Risk Management shall include all the minimum tasks in the Capability Level 1 CIRM plus the following:

B.2.1 Timely development, documentation, and flow down, as appropriate, of a CIRM Plan that is based on industry-accepted concepts for performance-based practices and is an integral part of the Mission Assurance Program Plan. The CIRM Plan shall describe the objectives, analytical ground-rules or scope, assumptions, activities or approach, performance metrics, data products, and the organizational elements responsible for generating and processing the CIRM data products;

B.2.2 Timely control of hardware critical items in accordance with the system requirements and AIAA Standard S-102.1.6. The hardware critical item controls shall include, but not be limited to, those described in Section B.1.4, plus the following:

(1) Develop documentation that provides clear evidence all configuration management requirements were properly developed and flowed down;

[8] The CIRM Report is equivalent to the Critical Items List (CIL) described in MIL-STD-785B and ANSI/GEIA-STD-0009.

(2) Develop documentation that provides clear evidence approved changes were provided for all contractor-specified configuration requirements that were not met;

(3) Develop documentation that clearly describes the item's power-off test and physical inspection history;

(4) Develop documentation that clearly describes the item's as-built configuration;

(5) Develop documentation that clearly describes the evaluation and resolution of differences between build-to and as-built configurations;

(6) Develop documentation that shows clear evidence all power-off test and physical inspection discrepancies for the item were evaluated appropriately.

B.3 The Capability Level 3 Critical Item Risk Management shall include all the minimum tasks in the Capability Level 2 CIRM plus the following as a minimum:

B.3.1 Timely identification of software critical items in accordance with the system requirements and AIAA Standard S-102.1.6. The identification of software critical items shall be based on the following criteria:

(1) A specific fault of the software module would cause death to the operator or bystander;

(2) A specific fault of the software module would cause permanent disability to the operator or a bystander;

(3) A specific fault of the software module would lead to loss of an irreplaceable system, e.g., research spacecraft and experimental aircraft;

(4) A specific fault of the software module would critically affect system safety, cause the system to become unavailable or unable to achieve mission objectives, or cause extensive/expensive maintenance and repair;

(5) A sole specific fault of the software module causes system failure. In other words, the software module is a SPFM;

(6) A specific fault of the software module will prevent obtaining data to evaluate system safety, availability, mission success, or need for maintenance/repair;

(7) The software module has exhibited an unsatisfactory operating history;

(8) The software module has stringent performance requirements in its intended application relative to state-of-the-art techniques for similar software modules;

(9) The software module does not have sufficient operational or test history, or sufficient similarity with other software modules with sufficient operational or test history, to provide confidence in its reliability;

(10) The software module is difficult to program relative to state-of-the-art software programming techniques'

B.3.2 Timely control of hardware and software critical items in accordance with the system requirements and AIAA Standard S-102.1.6. The hardware critical item controls, and software critical item controls where applicable, shall include, but not be limited to, those described in Sections B.1.4 and B.2.2, plus the following:

(1) Develop documentation that clearly shows functional test data were subjected to trending analysis;

(2) Develop documentation that clearly describes the item's complete build history;

(3) Develop documentation that clearly describes the item's complete operating history;

(4) Develop documentation that clearly describes the item's complete rework history;

(5) Provide clear evidence all of the project's quality records can be retrieved using electronic records software;

(6) Develop documentation that provides clear evidence each required plan was reviewed to assure it meets the needs of the Systems Engineering Process;

(7) Develop documentation that provides clear evidence the Lessons Learned process was implemented in accordance with the enterprise's command media, and that lessons learned were documented and shared with Risk Management and other disciplines.

B.3.3 Timely development and maintenance of a Product FMECA/Hazards Analysis/CIRM database that allows: (1) cross-referencing identified critical items with official/approved design drawings and parts lists, (2) automatic generation of part of the CIRM Report, and (3) an authorized person to indicate particular data is a lessons learned candidate;

B.3.4 Timely utilization of the Product FMECA/Hazards Analysis/CIRM database to the greatest extent practical by project activities, such as, System Safety and Logistics, and R&M Program tasks, such as, FRACAS, Component Reliability Predictions, and Maintainability Predictions, to aid in assessing the criticality of critical item failure modes as part of the integrated efforts of risk management and mission assurance;

B.3.5 Timely collection and review of existing CIRM lessons learned that are: (1) derived from sources internal to the enterprise, and (2) relevant to the system being developed. The objective of this activity is to identify needed CIRM process improvements;

B.3.6 Timely evaluation of all aspects of the CIRM process, including its implementation and data products, to identify candidate product-based and process-based candidate lessons learned. Evaluate these lessons learned for quality, prioritize them, and forward them to the Lessons Learned Approval Authority (LLAA) for appropriate action;

B.3.7 Timely development and documentation of sufficient detailed information in the CIRM Report to allow independent evaluation of the comprehensiveness of the process.

B.4 The Capability Level 4 Critical Item Risk Management shall include all the minimum tasks in the Capability Level 3 CIRM plus the following:

B.4.1 Timely control of hardware and software critical items in accordance with the system requirements and AIAA Standard S-102.1.6. The hardware critical item controls, and software critical item controls where applicable, shall include, but not be limited to, those described in Sections B.1.4, B.2.2, and B.3.2, plus the following:

(1) Develop documentation that provides clear evidence all required process controls were correctly applied;

(2) Develop documentation that clearly describes the item's storage history;

(3) Develop documentation that clearly describes traceability of the item's lower level parts and materials;

(4) Develop documentation that clearly describes the complete test and inspection history of the item's lower level parts and materials.

B.4.2 Timely development and maintenance of a Product FMECA/Hazard/CIRM database that is a part of, is integrated with, or interfaces with the Project Mission Assurance Database, all of which must comply with S-102 Mission Assurance keyword data element description (DED) requirements;

B.4.3 Timely evaluation of the CIRM process in accordance with the project's Risk Management Plan and AIAA Standard S-102.1.6 (This is a process verification activity in so far as it qualifies the uncertainty associated with the process);

B.4.4 Timely exchange of LLAA-approved CIRM lessons learned with other projects throughout the enterprise. Review lessons learned received from other projects to identify CIRM process improvements that should be implemented, such as, improvements in automated tools or training materials.

.

B.5 The Capability Level 5 Critical Item Risk Management shall include all the minimum tasks in the Capability Level 4 CIRM plus the following:

B.5.1 Timely control of hardware and software critical items in accordance with the system requirements and AIAA Standard S-102.1.6. The hardware critical item controls, and software critical item controls where applicable, shall include, but not be limited to, those described in Sections B.1.4, B.2.2, B.3.2, and B.4.1, plus the following:

(1) Develop documentation that clearly describes the physical and chemical analysis history of the item's lower level materials;

(2) Develop documentation that shows clear evidence all functional, physical, or logical discrepancies for lower level parts and materials were evaluated appropriately.

B.5.2 Timely development and implementation of a structured review process[9] (Peer Review, Independent Review Team/Panel, Independent Technical Assessment, etc.) that draws heavily on the CIRM experiences of other projects to aid the implementation or evaluation of the CIRM process of concern, as appropriate, in all product life cycle development phases;

B.5.3 Timely establishment of a process for the continuous improvement of the enterprise-approved documented CIRM practices and training materials. This activity includes annual goal setting and periodic independent evaluations of the organization's progress toward those goals.

B.5.4 Timely collection and review of CIRM lessons learned that are documented by outside organizations to identify significant recommendations that should be implemented by the project. Share CIRM lessons learned that are not subject to proprietary or legal constraints with external organizations through established channels, such as, the Government-Industry Data Exchange Program (GIDEP) or a non-profit research and development (R&D) consortium. (This activity requires establishing appropriate safeguards for security-classified, ITAR-restricted, and proprietary data).

[9] The development and implementation of a comprehensive review checklist facilitates a structured review process.