PREFERRED RELIABILITY PRACTICES

IDENTIFICATION, CONTROL, AND MANAGEMENT OF CRITICAL ITEMS LISTS

Practice:

Initiate the preparation of Critical Items Lists (CILs) early in programs to identify and potentially eliminate critical items before the design is frozen and as an input to hardware and software design, testing, and inspection planning activities. Utilize CILs during the operational portion of the life cycle to manage failures and ensure mission success.

Benefits:

Early identification, tracking, and control of critical items through the preparation, implementation, and maintenance of CILs will provide valuable inputs to a design, development, and production program. From the CIL activity, critical design features, tests, inspection points, and procedures can be identified and implemented that will minimize the probability of failure of a mission or loss of life.

Programs That Certified Usage:

Rocket Solid Motor Booster (RSMB), Space Shuttle Main Engine (SSME), Solid Rocket Booster (SRB), and External Tank (ET).

Center to Contact for More Information:

Marshall Space Flight Center (MSFC)

Implementation Method:

I. Background

The Failure Mode and Effects Analysis (FMEA) is performed to identify failure modes. As part of this process, critical failure modes that could lead to loss of life or loss of mission are also identified. These critical failure modes are then placed into a CIL, which is carefully examined for programmatic control by implementing inspection requirements, test requirements and/or special design features or changes which would minimize the failure mode occurrence.

Failure Mode and Effects Analyses and resulting CILs can be used not only as a check of the design of systems for reliability, but also as main design drivers for the product or service. Reliability management is the activity

IDENTIFICATION, CONTROL AND MANAGEMENT OF CRITICAL ITEMS LISTS

involved in coordinating the reliability analyses of design, development, manufacturing, testing, and operations to obtain the proper performance of a given product under specified environmental conditions. Reliability management interfaces with the program management function, the design function, the manufacturing function, the test and inspection function, and the quality function.

Reliability management is approached through the formulation and preparation of reliability plans, the performance of specific product design analysis, the support of classical reliability analysis activities, and project/product team participation using concurrent engineering methodologies (see NASA Reliability Design Practice GD-ED-2204).

The FMEA/CIL Process (shown on Figure 1) plays a key role in reliability management. Principal outputs of the FMEA/CIL process are CILs (shown on the lower right-hand corner of Figure 1).

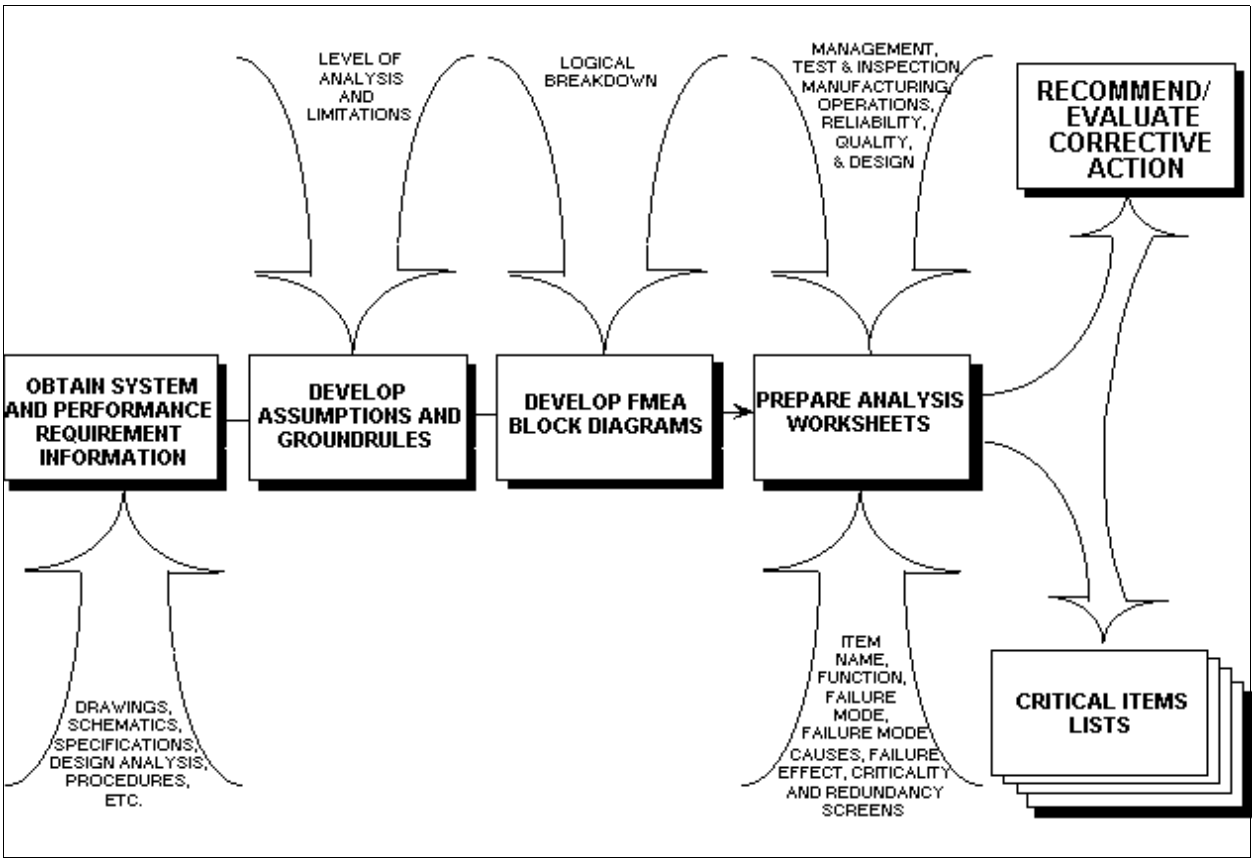

Figure 1. FMEA/CIL Analysis Process

IDENTIFICATION, CONTROL AND MANAGEMENT OF CRITICAL ITEMS LISTS

II. Critical Items Lists and Retention Rationale

Specific lessons have been learned that will change the value of preparing and maintaining (CILs) early in high-technology, multi-disciplinary aerospace programs and projects. Critical Items Lists are identified through the conduct of a Failure Mode and Effect Analysis (FMEA). The FMEA Process (see Practice No. PD-AP-1307) involves a bottom-up analysis of each hardware or software element in a complex system for each possible failure mode. The determination of the "worst case" effect of that failure on the system is then determined. If the item can fail in a mode which could result in the loss of life or vehicle or in loss of the mission, the item is placed on a Critical Items List. The FMEA, and resulting CIL, is most effective when it is performed concurrently with the design process and maintained throughout the life of a program or project. The FMEA results in the identification of single failure points (SFPs) and critical redundant items. A typical SFP is defined as a single item of hardware (usually at the component level) the failure of which could result in the loss of life, vehicle, mission, or damage to a vehicle system. It is the general policy of NASA not to permit the retention of single failure points in design unless special conditions prohibit designing it out, such as technology, operations or cost. Retention of a single failure point requires that a justification or rationale be prepared which describes actions taken, safety margins, failure prevention measures, tests, or inspections that will ensure that the critical item of hardware will not fail in the mode indicated in the FMEA.

Typical rationale for retention of hardware or software items on a project's Critical Items List includes information on design, testing, inspection, failure history, and operational use as described below:

1. Design Rationale: Design rationale identifies design features and/or margins that have been provided in the design of the hardware or software element which minimize or eliminate the probability of occurrence of the failure mode and/or reduction or elimination of the potential causes of the failure mode.

2. Test Rationale: Test rationale includes a description of specific tests that have been completed to detect potential failure causes during acceptance and certification tests.

3. Inspection Rationale: Inspection rationale addresses specific inspection methods, procedures, tools, and techniques that are used in the hardware or software manufacturing, assembly, and integration process to detect susceptibility to failure modes or to detect and assess the probability of encountering failure modes and their potential causes.

4. Failure History: Failure history and corrective actions are included as a part of single failure point critical items retention rationale to indicate that the reason for previous failures has been removed or reduced as a potential hazard, and to provide trend analysis.

IDENTIFICATION, CONTROL AND MANAGEMENT OF CRITICAL ITEMS LISTS

5. Operational Use: Special operational techniques that would either prevent the particular failure mode or mitigate its effect once it has occurred are included as part of the retention rationale. This rationale includes such factors as flight rules, crew procedures, such as emergency stop features or special crew training. It also includes contingency actions such as extravehicular activity and unplanned in-flight maintenance procedures.

The flow of these facets of retention rationale are shown on Figure 2.

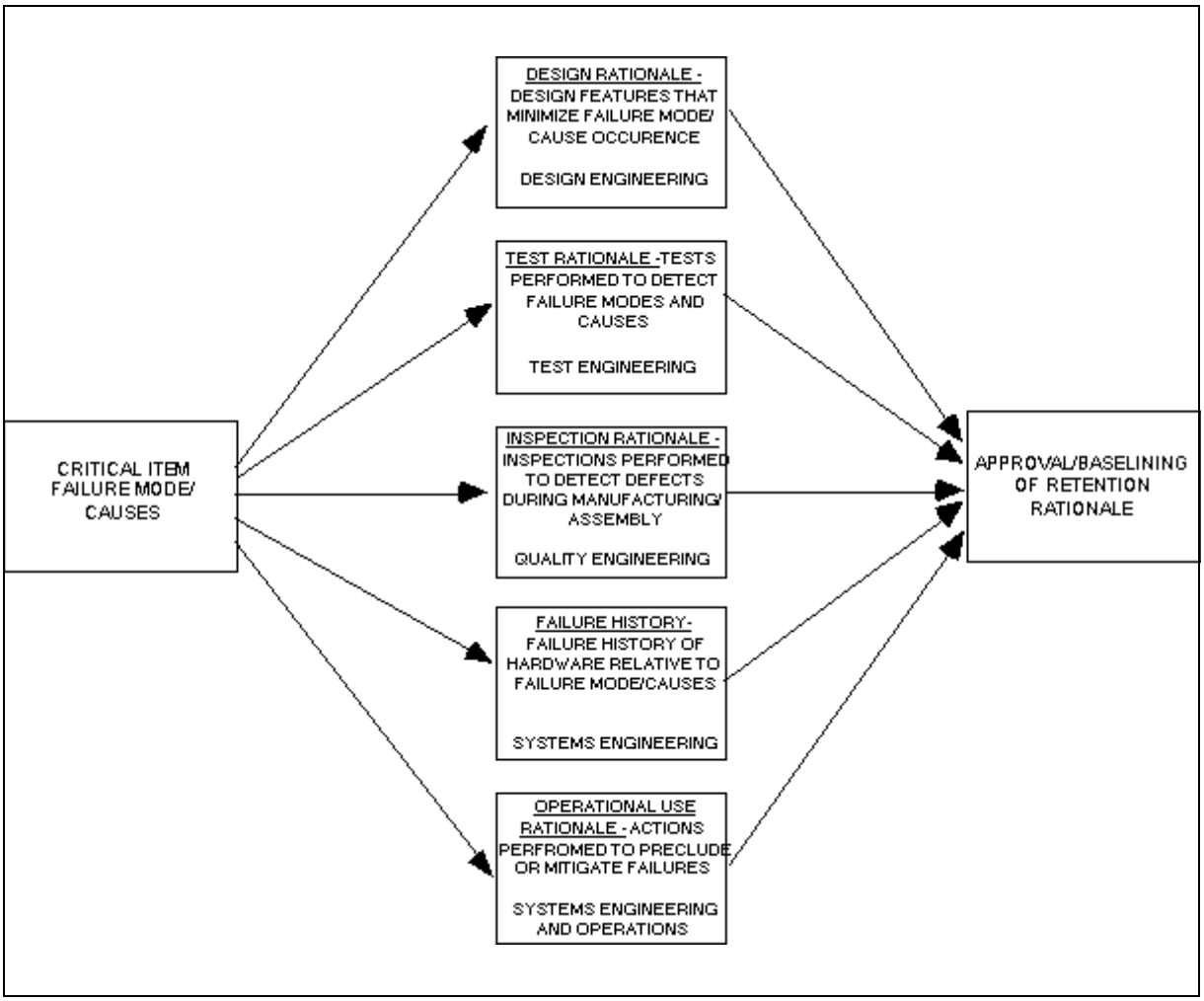

Figure 2. CIL Retention Rationale Process

III. Suggestions for Effective CIL Implementation

1. Correlation of FMEA Results with Fault-Tree Analyses and Hazards Analyses: The FMEA/CIL data can serve as an input to the hazard analysis process. The hazards

analysis uses fault trees and is basically a top down approach. It focuses on human errors and considers multiple unrelated failure modes which the FMEA/CIL ground rules out.

2. The Use of Probabilistic Risk Assessments: Probabilistic risk assessments have proven to be useful procedures in providing product development teams with an insight into factors of safety and to strengthen critical item or single failure point retention rationale. Margins of safety have a strong influence on the acceptability of retaining potential failure modes or critical items if it can be proven that risk of failure is reduced to an acceptably low level.

3. Process, Equipment, and Facility Critical Items Analyses: Failures in manufacturing, assembly, and test processes, equipment, and facilities have only an indirect effect on the freedom of flight hardware and software from mission or life-threatening occurrences. Nevertheless, the conduct of process, equipment, and manufacturing facility FMEAs can provide valuable assistance in identifying critical items whose failure could impact system performance or availability. Statistical process control methods, if used prudently in the manufacture of hardware can assist in the detection of conditions which could lead to impending failures affecting performance or schedule.

4. Computer-Aided Management of Critical Items: Common numbering systems coupled with the use of electronic data processing techniques, can speed up the CIL implementation and management process. Where failure modes or causes are identical or related for various system elements, these failure modes or causes can be referenced rather than repeated, reducing the volume of text in retention rationale. Critical item listings can be more easily referenced to corresponding information derived from fault-tree analyses and hazards analyses if there is a common numbering system.

5. CIL Retention Rationale as a Road-Map: Critical Item List retention rationale that is developed very early in hardware or software programs can be used as a road-map for development plans, tests, and inspections. Development program content, then, can be tailored specifically to prevent loss of mission, vehicle, and human life. This road-map could be used to identify inspection points and to help avoid too many series inspections of the same hardware.

Critical Items List should be worked in a way that would not impact important program milestones or create unnecessary work-around in the areas of cost, schedules, or performance. For example, processing methods are needed to quickly disposition discrepancies in critical items.

IV. Example Uses of Critical Items Lists

The uses of CILs are many. Among the more important uses are: (1) analysis of a product, process or project for reliability and failure avoidance before, during, and after the design process; (2) evaluation of the impact of design, material, or fabrication changes on reliability;

(3) assessment of failures experienced during testing; (4) recommendation of design changes that will avoid failure recurrences; and (5) determination of the risk of retaining mission critical or life endangering single failure points or redundant failure modes. Some specific examples of typical applications of the FMEA/CIL methodology as an aid to design follow:

1. Spacelab Recertification after the Challenger Incident

During the Spacelab recertification effort after the Challenger accident, the FMEA revealed a potential single failure point in the jettison circuitry of the Inertial Pointing System (IPS). A condition existed in which a short in the emergency arming switch could cause the firing of all four NASA Standard Initiators (NSIs). The analysis also revealed that the harness separator would not fire under these conditions. The detailed FMEA analysis of the wiring harnesses also revealed several mission critical wiring anomalies that had to be corrected. Additionally, the payload retention latch assembly was found to be in need of a redundant operational mode. As a result, redundant end switches were added.

2. Redesigned Solid Rocket Motor (RSRM) Project

During routine review and assessment of the CILs for the RSRM, it was observed that the specifications for the finish of the secondary sealing surfaces for nozzle joints three and four (inlet to throat joints) were inadequate to retain a 1R criticality ranking (which is a criticality 1 failure mode but with a second or redundant system). Defects of up to 50-mil depth were permitted on the secondary sealing surface while defects of only 3-mil depth had to be reworked for blending if they occurred in the primary seals. A CIL analysis indicated that actually a criticality 1 (potential loss of life) criticality ranking existed.

3. Space Shuttle Main Engine (SSME) Independent Risk Assessment Team

When contamination was discovered in the bearing cage of SSME No. 1209, a special independent risk assessment team was established to assess the problem and to determine if the engine was safe to fly. The team relied heavily on the FMEA/CIL analyses that had already been performed by NASA/MSFC and the SSME contractor personnel in order to understand the potential for failure and possible safety hazards. The team identified rationale for retention of the condition that caused the contamination, and the engine was judged safe to fly. This engine subsequently flew (many missions) successfully with no indication of potential failure.

Technical Rationale:

Extensive analytical work on existing and emerging programs relative to failure identification, management, and control has resulted in well documented, rigorous procedures for the treatment of critical items. Concurrent engineering approaches to program engineering and management have included attention to more details earlier in the design process and at a much lower level

IDENTIFICATION, CONTROL AND MANAGEMENT OF CRITICAL ITEMS LISTS

than previously attained. Assurance of success means the elimination or reduction of potential failure modes. Elimination or reduction of potential failure modes can only be achieved through the conscientious application of failure mode and effect analysis, critical item identification early in the concept/design phase, and prudent engineering management.

The advantages of the FMEA/CIL process are that it: (1) Systematically identifies all credible failure modes and causes; (2) permits a focus on critical single failure points and levels of redundancy; (3) provides risk acceptance rationale for critical failure modes/causes; (4) provides management control of critical items, associated procedures, specifications, and processes; and (5) provides a single, agreed-to listing of all critical items associated with a given project.

Impact of Nonpractice:

Failure to adhere to these guidelines could create operational schedule delays, increase operational costs, decrease the effectiveness of failure management, and could result in loss of the mission, loss of a vehicle, or loss of life.

Related Guidelines:

Practice No. PD-AP-1307, “Failure Modes, Effects, and Criticality Analysis”, Jet Propulsion Laboratory.

References:

1. Requirements for Preparation and Approval of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL), NSTS 22206, Revision D, Lyndon B. Johnson Space Center, Houston, TX, December 10, 1993.
2. MSFC Shuttle Elements Lessons Learned for the ASRM Project, George C. Marshall Space Flight Center, September 14, 1993.
3. Space Shuttle Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL) Groundrules, George C. Marshall Space Flight Center, November 5, 1986.
4. Payload and Experiments FMEA/CIL Groundrules: Marshall Space Flight Center, Report #CR5320.9, MSFC, Alabama.