PREFERRED
RELIABILITY
PRACTICES

Identification, Control, and Management of GSE Critical Items

Practice:

Identify potential critical items early in projects for Ground Support Equipment (GSE) as an input to hardware and software design activities. Perform Failure Modes and Effects Analysis (FMEA) for "as built" configuration GSE identifying Critical Items. Prepare Critical Items Lists (CIL's) and present the resulting risks to management for acceptance. Use CIL's to initiate control of the risks associated with the critical items and to request a waiver or deviation from program requirements.

Benefits:

Early identification of potential critical items will provide valuable inputs to design engineering for their avoidance and/or elimination. Critical Items Lists provide management with design acceptance rationale for those critical items which could not be eliminated, and identify test and inspection controls to minimize the probability of a failure.

Programs That Certified Usage:

All programs at the Kennedy Space Center

Center To Contact For More Information:

Kennedy Space Center (KSC)

Implementation Method:

Background

GSE at KSC includes equipment and facility systems used to test, checkout, process, handle, and transport Space Shuttle flight hardware at the launch and landing sites. Equipment used at other sites that is common to that used at the launch and landing sites is also included.

Prior to conducting the FMEA a criticality assessment is performed to assess each system function. If loss or improper performance of the function, without regard to available redundancy, could result in loss of life/vehicle or damage to a vehicle system the system is assessed as critical. FMEAs are performed on the hardware associated with the critical functions. The only exceptions are functions assessed as critical due to failure of passive components, such as certain types of structural components.

The FMEA is performed at the lowest level necessary to identify: 1) Single Failure Points (SFP's) which if failed could cause loss of life/vehicle or damage to a vehicle system; 2) The combined effect of two like or unlike redundant items which could result in loss of life/vehicle; 3) SFP's in safety or hazard monitoring systems whose failure modes assume the hazardous condition being monitored or combated has already occurred.

The FMEA and resulting CIL can be used not only as a check of the systems design for reliability, but can also be used as a driver for the systems design to reduce or eliminate critical items and/or implement value added maintenance design features.

The FMEA/CIL process plays a key role in reliability management. Reliability management is the activity involved in assuring that proper performance of the system/equipment and completion of maintenance procedures will minimize the risks associated with the identified failure modes. Reliability management coordinates the analysis of design, development, manufacturing, testing, maintenance, and operations to assure that the system output will support the prescribed program interface/function.

Reliability Management is accomplished through the formulation of reliability plans, the performance of system/equipment design analysis, the support of classical reliability analysis activities, and project/system team participation using concurrent engineering methodologies.

The principal outputs of the FMEA/CIL process are the CIL's.

Critical Items and Retention Rationale

Specific lessons have been learned that will enhance the value of identifying potential critical items early in high-technology, multi-disciplinary aerospace programs and projects. Critical items are identified through the conduct of a FMEA.

The FMEA process involves the analysis of each active component (hardware or software element) in a complex system to a specified level, for each possible failure mode. The determination of the "worst case" failure effect of that failure on vehicle systems and/or personnel safety is then determined. If the item could fail in a mode which could directly result in loss of life/vehicle and/or damage of a vehicle system, the item is designated as a critical item and categorized according to the severity of the failure effect. SFP's in designated safety or hazard monitoring systems, whose failure modes assume the hazardous condition being monitored or combated has already occurred, are also identified as critical items.

The FMEA is most effective when it is performed concurrently with the design process and maintained throughout the life of a program or project. It is the policy of NASA not to permit the retention of SFP's in design unless special conditions result in the application and approval of a waiver or deviation from the Space Shuttle Program (SSP) Configuration Management

Requirements.

Retention of a SFP requires that a CIL sheet be prepared which identifies the item, Criticality Category, Function, Failure Mode, Failure Cause(s), Failure Mode Number and Failure Effect. The CIL sheet also provides the Acceptance Rationale which describes the components design, test, inspection, failure history, and operational use. The elements of the Acceptance Rationale, as described below, include safety margins, prevention measures, and maintenance/operational procedures which will ensure that the critical item will not fail in the critical failure mode. The Acceptance Rationale forms the basis for management acceptance of GSE which contains critical items.

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 specific tests which are accomplished to detect failure modes and/or causes during acceptance and periodic certification. If turnaround checkout testing is accomplished via Operational and Maintenance Instructions (OMI's) the details of the test, frequency, and OMI number are included.

3. Inspection Rationale: Inspection rationale addresses specific inspection methods, procedures, tools, and techniques which are performed on a pre-operational and/or post-operational basis to determine whether or not the critical failure modes have occurred. Inspections which minimize the probability of encountering failure modes and their potential causes are also included. Tear-down analysis is excluded as a means for inspection.

4. Failure History: Failure history includes data on previously reported failures and corrective actions for the critical item in the critical failure mode(s) as found in the Problem Reporting and Corrective Action (PRACA) database. Reference is also made to the PRACA database for current data on test failures, unexplained anomalies, and other failures experienced during ground processing activities.

5. Operational Use: Corrective action that would either prevent the particular failure mode or mitigate it's effect once it has occurred is included as part of the retention rationale. The time required to take the corrective action (timeframe) is also provided.

The CIL sheet is presented to project management for approval/acceptance of the risk associated with the critical items and subsequently to the Program Requirements Control Board (PRCB) with the waiver request (CR). The waiver request identifies the failure modes which do not meet

the fail safe requirement from NSTS 07700, Volume X. The fail safe requirement specifies that all GSE (except primary structure and pressure vessels) shall be designed to sustain a failure without causing loss of vehicle systems or loss of personnel capability.

Suggestions for Effective CIL Implementation based on KSC experience

1. Correlation of FMEA results with Fault-Tree Analyses and Hazard Analyses: The FMEA/CIL data can serve as an input to the hazards 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. Use of the CIL sheets to initiate risk management controls: Preparation of the CIL sheet can be used as an opportunity to coordinate with the cognizant engineering organizations to develop and agree upon appropriate maintenance procedures and operational processes to assure control of the risks associated with the critical items. Subsequently the CIL can be used to initiate closed loop tracking of the test and inspection controls.

3. Use of FMEA/CIL to develop test and checkout procedures: FMEA/CIL developed early in design projects can be used as input to develop test procedures, inspection requirements, operational procedures, and trouble shooting guides. The component level analysis performed in the FMEA and the detailed reporting of critical items provides specific information regarding failure scenarios with defined system reactions and expected personnel corrective action.

CIL's should be implemented in a way that would not impact important program milestones or create unnecessary work-around in the areas of cost, schedules, or system performance.

Example Uses of FMEA / CIL

1. Use of FMEA for early identification of critical items: The design process for the 325 Ton Bridge Crane installed in the Vehicle Assembly Building at KSC utilized the FMEA process to identify potential critical single failure points in both hardware and software systems. As potential single failure points were identified the reliability engineer coordinated with the NASA and vendor design engineers. The design engineers were made aware of the failure effects, alternative designs were considered, and solutions were implemented. The FMEA process continued through test and acceptance of the equipment with the resulting design having no single failure points.

2. Use of CIL sheets to identify risk to management: The CIL process was utilized during the analysis of the extensible and auxiliary access platforms in the VAB. The analysis was initiated by a design study that indicated that a substantial number of platforms were equipped with hinges that may fail under dynamic loading. Reliability engineering analyzed

the systems and identified critical single failure points which, if failed, could allow a platform to fall causing a cascading effect of one platform upon another and resulting in the overloaded hinge scenario as described in the design study. The CIL sheets were used to advise management of the risks associated with platform operations. During presentation of the CIL sheets, Reliability Engineering also made recommendations for alternative fail-safe equipment. Management was able to assess the risks, accept interim controls and identification of new CIL items, and initiate implementation of corrective action.

3. Use of CIL sheets to initiate test and inspection controls: The CIL process has been used at KSC to manage the risks associated with cranes and hoists which, if failed, could cause loss of life or vehicle. CIL sheets for critical gear systems/components identify test and inspection requirements which are performed in a close-looped tracking operations and maintenance process. Performance of a periodic load test at rated load, verifies the operational integrity of the gear system and periodic ferrographic analysis of the gear lubricant is used to document wear trends and to assist in predicting future 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 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 FMEA, critical item identification, 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 SFP's and levels of redundancy; (3) provides management with risk acceptance rationale for critical failure modes/causes; (4) initiates control of critical items, associated procedures, 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 for ground processing operations could create operational delays, increase operational costs, decrease the effectiveness of failure management, and could ultimately lead to a system failure which could result in loss of life/vehicle or damage to a vehicle system.

Identification, Control, and Management of GSE Critical Items

References:

1. National Space Transportation System Critical Items List, Shuttle Program Critical Items List, Kennedy Space Center Ground Support Equipment, NSTS 08399, Book 4, Revision A, Lyndon B. Johnson Space Center, Houston, TX, November 28, 1988
2. Problem Reporting and Corrective Action System Requirements, NSTS 08126, Lyndon B. Johnson Space Center, Houston, TX, April 7, 1994
3. Requirements for the 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
4. Space Shuttle Flight and Ground System Specification, FMEA/CIL Deviation and Waivers, NSTS 07700 Volume X, Book 5, Revision K, Lyndon B. Johnson Space Center, Houston, TX, October 9, 1992
5. Space Shuttle Program Configuration Requirements, NSTS 07700 Volume IV, Lyndon B. Johnson Space Center, Houston, TX, November 23, 1994
6. NASA Reliability Preferred Practice PD-ED-1240, Guideline for the Identification, Control and Management of Critical Items