**Department of the Air Force**
**HQ AEDC (AFMC)**
**Arnold AFB, TN 37389**

# Safety, Health, and Environmental Standard

**Title**: **SYSTEM SAFETY**

**Standard No.:** A4

**Effective Date:** 07/30/2009

The provisions and requirements of this standard are mandatory for use by all personnel engaged in work tasks necessary to fulfill the AEDC mission. Please contact your safety, industrial health and/or environmental representative for clarification or questions regarding this standard.

Approved:

Contractor/ATA Director
Safety and Health Group

Air Force Functional Chief

## Record of Review/Revision

| Date/POC | Description |
|---|---|
| 7/20/09<br>Jennings | Added Inherent Risk to paragraph 4.9.2.5.11. Inserted paragraph 4.9.3.12 for pressure testing. |
| 06/04/08<br>A. Jennings;<br>M. Johnson | Revised the requirement for 2 year approval of BSR's. Revised section 4.11.1. Revised Annexes E, G, and H. Made changes throughout text to reflect current organizations and references. |
| 05/04/07<br>Jennings | Added paragraphs 4.2.7, 4.3.6, 4.3.7, 4.5.7, and 4.6.8 to clarify government approval requirements for RPC 3. Revised section 4.21 to remove Contractor Quality audit responsibility and expand Contractor Safety audit responsibilities |
| 01/18/07<br>M. Johnson<br>/A.Jennings/<br>J.Watts/L.Davis | General revision and rewrite; read entire standard.<br>Reorganization for clarification, addition of AF organizations, and clarification of MatrixOne processes. |
| 06/10/05<br>Environmental | Updated page 1 of Annex A to incorporate current Environmental requirements. |
| 04/28/05<br>Jennings/<br>Watts/Davis | Revisions made by J. Watts, A. Jennings and L. Davis to incorporate the use of MatrixOne, BSR, PSR requirements. |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

**Department of the Air Force**
**HQ AEDC (AFMC)**
**Arnold AFB, TN 37389**

**Effective** 07/30/09
**Std. No.** A4

# Safety, Health, and Environmental Standard

## SYSTEM SAFETY

## 1.0 INTRODUCTION/SCOPE/APPLICABILITY

1.1 This standard describes the tasks, activities and actions required under the area of system safety at AEDC. The standard implements the six steps of the Air Force Operational Risk Management process within the test and industrial areas of AEDC. The system safety process is an analytical decision making tool, which when properly applied can protect personnel, equipment and facilities, reduce resource losses, eliminate the need for crisis management, and maximize mission success. System Safety is also a preventive action tool used to reduce the probability and severity of risk. Risks treated under this standard include those related to operations, maintenance, design projects, test safety, explosive safety, industrial safety, industrial hygiene, and environmental protection.

1.2 This standard applies to all AEDC personnel, including Air Force, Navy, US Army Corps of Engineers, and Contractors (including subcontractors) at the Tennessee location and all remote locations assigned to AEDC and to operations conducted by AEDC personnel or Contractors outside the confines of Arnold AFB.

1.3 This standard shall be considered to be the Contractor-developed System Safety Program Plan and ensures that the requirements and objectives of a System Safety Program are implemented at AEDC.

1.4 All new or revised system safety analyses must comply with this standard.

## 2.0 BASIC HAZARDS/HUMAN FACTORS

The AEDC mission – testing – can be extremely dangerous. Tremendous amounts of energy in the form of electricity, jet and rocket fuel, gunpowder, X-rays, lasers, and high-pressure fluids are routinely used to satisfy customer requirements. Aging facilities and equipment are often pushed to their limits.

## 3.0 DEFINITIONS

Active Test Unit – Any test unit having had operation within the past two years.

Ameliorator - Countermeasures that usually apply to downtime and control severity after an undesired event has begun, but they do not prevent the event from occurring. Downtime Ameliorators include spare parts, length of time to repair/replace, backup power supplies, etc.

Barrier Analysis- An analysis of all potentially harmful energy sources within the system, together with an assessment of the adequacy of safeguards for each to afford protection against unwanted release.

Baseline Hazard Analysis (BHA) – An analysis used to document known hazards concerned with the normal day-to-day operation and maintenance of a system, subsystem or facility.

Baseline Safety Report (BSR) – A compilation of the entire baseline hazard analysis for a test unit, plant operation, utility, etc. The BSR allows the individual hazard analyses that make up the baseline to be evaluated in a comprehensive package and thus shows the interaction of the systems and interfaces.

Cause – A deficiency the correction, elimination, or avoidance of which would likely have prevented or mitigated the mishap, damage and/or injuries. The circumstance or action ("mechanism") that leads to the hazard's occurrence. It may be a failure mode, operator error, or out-of-limit condition.

Confined Space – See AEDC Safety, Health, and Environmental (SHE) Standard B5 for definition.

Contractor – Term used to identify the AEDC Operation, Maintenance, Information Management and Support Contractor.

Countermeasures – Actions taken to reduce risk to a lower level by reducing the severity and/or probability of occurrence of the hazard, cause, or effect. Countermeasures may be measures that prevent occurrence or reoccurrence, or steps that reduce the effect if the mishap scenario should occur.

Critical Effect – An effect that has been reduced from a risk priority code (RPC) 1 or 2 to a RPC 3 via the application of countermeasures.

Data Compromise – A mishap that results in data that are inaccurate, lost, or otherwise corrupted.

Downtime – Time that a system or test facility is unavailable to support its intended function.

Effect – The "outcome" to be avoided. It identifies who or what resources will be injured, damaged, or destroyed if the hazard occurs.

Hazard – Any real or potential condition ("source") that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment, or property; downtime, data compromise, or damage to the environment.

Hazard Analysis – An analysis performed to determine how a device, task, location, system, etc. can cause hazards to occur and then to reduce the risk of occurrence to an acceptable level. A hazard analysis includes a risk assessment before and after countermeasures are implemented. Hazard analyses are categorized as baseline, test, or barrier and maybe further broken down as system, subsystem, or operational and support.

Hazard Probability – The likelihood, expressed in quantitative or qualitative terms, that a hazard would result in a mishap of given consequence. (See Annex A.)

Hazard Severity – An assessment of the consequences of the most credible mishap that could be caused by a specific hazard. In this specific application "worst credible mishap" is defined to mean a hypothesized mishap that is reasonable or has historical precedent. (See Annex A.)

High Accident Potential (HAP) Event (Near Miss, Significant Event) – Any hazardous occurrence that has a high potential for becoming a mishap, but does not meet mishap reporting injury or property damage criteria.

High Level of Protection Countermeasure – Actions taken to reduce the risk of occurrence of a hazard from RPC 1 or 2 to RPC 3 and/or

- Significantly reduces probability (2 or more levels) and/or
- Reduces severity by one or more levels and/or
- If the ending RPC is a 1 or a 2.

In addition this could be an engineering judgment that the level of protection should be High, depending on the criticality of the Hazard, Countermeasure and Effect.

Life Cycle – All phases of the system's life including design, research, development, test & evaluation, production, deployment, operations and support, and disposal. The phases through which a system, test, project, facility or product passes during its lifetime.

Mishap —An unplanned occurrence, or series of occurrences, that result in damage or injury and meets Class A, B, C, or D criteria identified in AFI 91-204.

Mission Phase – Activities during specific phases of the lifecycle of a system for which a hazard analysis is being performed (i.e. operations, maintenance, preops, postops, etc.). Mission phases are used to organize a hazard analysis into the logical processes being evaluated.

Operating and Support Hazard Analysis (O&SHA) – A risk assessment that includes hazards arising from subsystem failures, interfacing system operation, and human involvement in operations and maintenance activities in the operating environment.

Operational Risk Management – The process of detecting, assessing, and controlling risk to enhance total organization performance. The process involves six steps: Hazard identification, risk assessment, analysis of risk control measures, risk control decisions, risk control implementation and supervision and review. (See AFD 90-9 and AFI 90-901.)

Preliminary Hazard Analysis – An analysis performed to identify safety critical areas within a system, identify and roughly evaluate hazards, and begin to consider safety design criteria. (See Annex B.)

Probability Interval – The period for which a system is evaluated for the occurrence of potential hazards. (See Annex C.)

Project Safety Report (PSR) – A process used as a means to provide an overall risk assessment and to inform and obtain management concurrence regarding the safety and risk of a project. The PSR contains a BSR and a test hazard analysis; these documents comprise the project Safety Plan.

Risk – An expression of the degree of risk in terms of severity and probability. Risk Assessment Matrix – A tool that uses severity and probability to determine a Risk Priority Code. (See Annex A.)

Risk Priority Code (RPC) – A numerical value from the Risk Assessment Matrix that defines relative risk levels. (See Annex A.)

Safety Plan – The approved BSRs and/or PSRs.

Safety Review Board (SRB) – Representatives of the DoD & Contractor who meet to review test or work operations risks. Test sponsors and customers may also participate. (See Annex D.)

Subsystem – A grouping of items satisfying a logical group of functions within a particular system.

System – An integrated composite of people, product, and processes that provide a capability to satisfy a stated need or objective.

System Safety – The application of engineering and management principles and techniques to achieve acceptable mission risk, within the constraints of operational effectiveness, time, and cost throughout the system's lifecycle.

System Safety Assignee – Person responsible for performing a hazard analysis on a system.

System Safety Engineering – An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mission risk.

System Safety Evaluator – Senior level individual responsible for assuring adequate hazard analysis and implementation of system safety requirements in a given area (turbines, aircraft, utilities, etc.).

System Safety Management – All plans and actions taken to identify, assess, mitigate, and continuously track, control, and document environmental, safety, and health mishap risks encountered in the development, test, acquisition,, use, and disposal of DoD weapon systems, subsystems, equipment, and facilities.

System Safety Working Group (SSWG) – A formally chartered group of persons organized to achieve system safety objectives.

Target – Asset affected by the particular mishap scenario under consideration. Targets considered at AEDC are Personnel Injury/Loss (P), Equipment Loss (E), Environmental (V), Test Unit Downtime (DT), and Data Compromise (DC).

Test Hazard Analysis (THA) – An analysis performed on hazards that are in addition to those covered in the BHA. These analyses are performed on hazards specific to a particular test article, maintenance of the article, transportation of the article, special handling or equipment hazards dealing with the test article, etc. In this definition the test article can be a system undergoing test at AEDC or a system undergoing installation/modification or a system being developed that will become an AEDC asset. Therefore, test peculiar hazard analyses also apply to special activities such as the activation of new or modified systems, return to service from major maintenance or repair, or unique operations. These constitute activities that are outside "normal" day-to-day operations.

## 4.0 REQUIREMENTS/RESPONSIBILITIES

### 4.1 AEDC/CC:

4.1.1 Approves all Hazard Analyses, BSRs, and PSRs that have an RPC of 1

4.1.2 Chairs, or designee, an SRB for every BSR/PSR that has an RPC of 1.

4.1.3 Contacts AFMC/SES in the event that a BSR/PSR that has an RPC of 1.

### 4.2 704th MXG/CC:

4.2.1 Approves all BHAs and BSRs that have an RPC of 2. (See Annex E.)

4.2.2 Approves all PSRs for maintenance/return to service that have an RPC of 2.

4.2.3 Assures all MXS Facility Managers receive System Safety Training.

4.2.4 Chairs, or designee, SRBs for every BSR or PSR that have an RPC of 2.

4.2.5 For BHA, BSR and PSR with an overall RPC of 3, government approval is required by the appropriate AEDC Squadron Commander, or asset manager if so delegated.

### 4.3 704th TG/CC and Geographically Separated Unit (GSU) Directors:

4.3.1 Approves all THAs and PSRs for test projects that have an RPC of 2. (See Annex E.)

4.3.2 Assures all TS Project Managers receive System Safety Training.

4.3.3 Chairs, or designee, SRBs for every PSR that has an RPC of 2.

4.3.4 For THA and PSR with an overall RPC of 3, government approval is required by the appropriate AEDC Squadron Commander, GSU director, or asset manager if so delegated.

4.3.5 For BSRs and BHAs with an RPC of 2 or 3 at GSU locations, GSU director approval is required.

**4.4 AEDC/SE:**

4.4.1 Manages the AEDC System Safety program per MIL-STD-882D.

4.4.2 Provides system safety training for AEDC DoD personnel.

4.4.3 Reviews all BSRs/PSRs and BHA/THA with an RPC of 1 or 2. (See Annex E.)

**4.5 704th TESG/CC (Investments):**

4.5.1 Approves all THAs, BSRs and PSRs for Investment Projects that have an RPC of 2. (See Annex E.)

4.5.2 Assures that all TESS Project Managers receive System Safety Training.

4.5.3 Chairs, or designee, SRBs for every PSR for Investment projects that have an RPC of 2.

4.5.4 For BHA, BSR and PSR with an overall RPC code of 3, government approval is required by the appropriate AEDC Squadron Commander, or asset manager if so delegated.

**4.6 704th MSG/CC:**

4.6.1 Approves all BSRs, BHAs, THAs, and PSRs for base infrastructure that has an RPC of 2. (See Annex E.)

4.6.2 Assures all MSG Project Managers receive System Safety Training.

4.6.3 Assures that requirements identified in this standard are incorporated into the AEDC Civil Engineering processes and policies.

4.6.4 Assists in the Information Technology and Support (IT&S) part of the System Safety process.

4.6.5 Chairs, or designee, SRBs for every BSR or PSR for infrastructure that has an RPC of 2.

4.6.6 For BHA, BSR, THA and PSR with an overall RPC of 3, government approval is required by the appropriate AEDC Squadron Commander, or asset manager if so delegated.

**4.7 AEDC Operation, Maintenance, Information Management and Support Contractor (Contractor):**
**NOTE:** See Contract F40600-03-C-001 Operation, Maintenance, Information Management, and Support of AEDC, Performance Work Statement Section 4.2.2:2.3 and Data Item Description DI-SAFT-80101B, System Safety Hazard Analysis Report (SSHA) for requirements.

4.7.1 Contractor Safety:

4.7.1.1 Trains Contractor personnel on system safety.

4.7.1.2 Reviews all hazard analyses, BSRs and PSRs before transmittal to Contractor management and AF.

4.7.2 System Safety Assignees and Evaluators:

4.7.2.1 Assignees (preparers) and evaluators shall be appointed by their respective organizations with the responsibility for preparation and review of hazard analyses.

4.7.2.2 Assignees and evaluators shall receive training in system safety by Contractor Safety prior to performing system safety tasks.

4.7.2.3 Evaluators shall be appointed according to their field of technical specialization, project responsibilities and training in system safety, and shall be current in technical aspects of testing in their area of responsibility.

**4.8 System Safety Process**

4.8.1 The System Safety Process consists of analyzing for risk, documenting that analysis, reviewing the analysis, and approving the analysis. The main elements of the process are BHAs, THAs, BSRs, PSRs, and SRBs. The process shall begin with the earliest initiation of work and continue through all phases of the life cycle. It shall include an in-depth analysis of subsystems, systems and operations, to identify hazards, assess risk, and eliminate/control hazards.

4.8.2 System safety engineering techniques and principles shall be applied where possible to reduce mission risk.

4.8.3 System safety shall be used where possible to identify design requirements.

4.8.4 System safety methods shall be used to protect Information Technology resources per Annex F

4.8.5 System safety management processes shall be applied throughout the System Engineering Process.

**4.9 Hazard Analysis**

**4.9.1 Hazard Analysis Types and Methods**

The selection of specific methods and techniques for performing a hazard analysis should be based on the level of complexity of the system being evaluated, the extent of development, and existing analyses for the same or similar projects. As a minimum, a hazard analysis or Risk Assessment shall be performed, documented, reviewed, and approved per the requirements of this standard. For Other System Safety tools see System Safety Analysis Handbook located in the AEDC Technical Library TA169.7 S96. Analyses such as preliminary, subsystem, or system hazard analyses should be considered for applicable stages of the systems engineering process. Analyses shall provide continuity through the system's life cycle and interface the results of analyses of interconnected systems. Guidance for different life-cycle Hazard Analyses is located in the Air Force System Safety Handbook (SSH).

4.9.1.2 Three types of O&SHA are required per this standard:

4.9.1.2.1 BHA – Section 4.12.1,

4.9.1.2.2 THA – Section 4.12.2,

4.9.1.2.3 Barrier Analysis (BA) – Section 4.12.3.

**4.9.2 Hazard Analysis Format**

4.9.2.1 Hazard analyses shall be prepared using the eMatrix® hazard analysis preparation process. Preparation of hazard analyses using Form GC-215, System Safety Hazard Analysis and Risk Assessment may be approved by AEDC/SE in cases listed below:

4.9.2.1.1 If a short hazard analysis is required in an emergency or extremely time sensitive situation or,

4.9.2.1.2 A Hazard Analyses if required for entry into confined spaces on an emergency or time critical basis,

4.9.2.2 Tunnel 9 and the NFAC facilities should use the GC-215 form.

4.9.2.3 The hazard analysis shall be written in sufficient detail such that reviewers with minimal or no knowledge of the system, test, or process can understand the potential mishaps and risk mitigation.

4.9.2.4 All hazard analyses shall include the following documentation as an attachment (as applicable):

4.9.2.4.1 A system block diagram and/or some form of graphical presentation (i.e. pictures, schematics, flow charts, etc.) to assist in review of the system(s) and subsystems.

4.9.2.4.2 Stress analysis.

4.9.2.4.3 SRB or Test Readiness Review (TRR) information (briefing charts, memos, etc.).

4.9.2.4.4 Any other documentation relative to the system, test article, process, etc. (e.g. MSDS, explosive classifications, X- rays, etc.).

4.9.2.5 Each hazard analysis shall be developed in accordance with the following format as a minimum:

4.9.2.5.1 Title. The title should be easily searchable in eMatrix®, and shall describe the system or process analyzed. The title shall include the asset for baseline hazard analyses.

4.9.2.5.2 Description. The description shall include the system, test, or process being evaluated including the purpose, major system components, energy sources, interfaces (system and human), operating location and environment. Assumptions shall be clearly stated. Revisions to an approved document shall include a summary of the revision.

4.9.2.5.3 Mission Phase. Mission phases shall be used to break the analysis into sections such as pre-ops/post-ops, operations, maintenance, handling operations, installation, etc that are analyzed separately because they

have different potential mishaps. The Mission Phase description shall include enough information to explain the activity being analyzed.

4.9.2.5.4 Probability interval or duration of exposure. (See Annex C.)

4.9.2.5.5 Hazard. Hazards shall provide an adequate explanation and description of the hazard, and shall be applicable to the mission phase being analyzed.

4.9.2.5.6 Cause. A hazard may have multiple causes and each must be identified. Causes shall provide an adequate explanation and description of the cause, and shall be applicable to the mission phase being analyzed. Each cause shall be listed and analyzed separately unless the causes can be controlled or eliminated via the same countermeasures.

4.9.2.5.7 Effects and Targets. All applicable effects and targets related to the hazard and cause shall be identified. The effect description shall provide an explanation of the damage or loss in quantifiable terms. Targets to be considered are P, E, V, DT, and DC.

4.9.2.5.8 Countermeasures. Countermeasures shall be applicable to the mission phase being analyzed and shall be described in sufficient detail in the hazard analysis such that reviewers may evaluate the effectiveness of the countermeasure. Each countermeasure shall be listed separately and identified with the hazard/cause/effect that it eliminates or reduces. All work instructions used as countermeasures to mitigate hazards shall be identified, approved, and kept on site. Procedures used to mitigate all severity I hazards (and severity II hazards to personnel) shall be formal written work instructions that comply with Contractor policies and procedures. High level of protection countermeasures shall be identified in the analysis.

4.9.2.5.9 Severity. Severity of the potential mishap shall be assessed both before and after implementation of countermeasures. (See Annex A.)

4.9.2.5.10 Probability. See Annex A. Probability of the potential mishap shall be assessed both before and after implementation of countermeasures.

4.9.2.5.11 Risk Level. (Same as Risk Priority Code.) Risk level shall be assessed both before and after implementation of countermeasures via the use of the Risk Assessment Matrix (Annex A). The RPC before countermeasures is known as the "Inherent Risk." The RPC after countermeasures is known as the "Residual Risk."

4.9.2.5.12 Recommendation. Recommendations shall be provided if risk level after implementation of countermeasures remains an RPC 1 or 2. Recommendations may include an ECD (Estimated Completion Date), cost estimate, and OPR (Office of Primary Responsibility) if known. If recommendations do not exist that would reduce the risk (i.e. the risk is inherent), then the recommendation shall state that fact.

**4.9.3 Hazard Analysis Application**

Hazard analyses shall be prepared for normal and high-risk operations (i.e. high energy source checkouts, major modifications, high risk operations to personnel), or those that results in a new facility/system or change to an existing facility/system including but not limited to the following:

4.9.3.1 Test projects.

4.9.3.2 Explosives and propellant handling or use. (See SHE Standard E15)

4.9.3.3 Confined space entry. (See SHE Standard B5.)

4.9.3.4 Investment Projects, for the following phases; Design, Execution/Construction, checkout as determined by Contractor Safety and/or AEDC/SE, and Baseline Operations. (See Annex B.)

4.9.3.5 Maintenance and Repair projects (as required). (See Annex B.)

4.9.3.6 Chemicals stored or used in excess of the threshold quantities. See 29 CFR 1910.119 and 40 CFR 68.

4.9.3.7 Off-site operations involving hazardous or dangerous conditions.

4.9.3.8 Significant post-maintenance checkouts.

4.9.3.9 Significant system activation or reactivation.

4.9.3.10 Support Facility Operations and Maintenance.

4.9.3.11 Utility Facility Operations and Maintenance.

4.9.3.12 Pressure Testing (See SHG Standard D2.)

4.9.3.13 Interface between systems.

4.9.3.14 As directed by the Contractor Safety and Health Office, Environmental Office, or the DoD.

### 4.9.4 Hazard Analysis Preparation, Review, and Approval

4.9.4.1 The hazard analysis shall be prepared by the Contractor system safety assignee and reviewed by the Contractor system safety evaluator. Contractor Safety and Health shall review all hazard analyses. Hazard analyses involving occupational health, environmental hazards, or quantities of chemicals in excess of the threshold quantities shall be submitted to Contractor Safety and Health and/or Environmental Offices for review. The requirement for Contractor management approval of the analysis shall be determined by the preparer's organization.

4.9.4.2 Architect/engineering firms working on Corps of Engineer projects shall perform a hazard analysis per this standard during design and construction, and deliver the analysis to AEDC as a submittal under the Military Construction Project.

4.9.4.3 No unnecessary risk shall be accepted. **Approval shall not be granted for personnel hazards with an RPC 1 or 2.**

4.9.4.4 A guideline for requirements and review of hazard analyses is found in Annex G. Other methods or techniques may be applied as necessary.

4.9.4.5 The Contractor approval cycle for hazard analyses shall be at the Contractor's discretion, however, as a minimum the analysis shall be reviewed by a system safety evaluator and the Contractor safety office. Government approval for all hazard analyses is required. The Contractor shall route all hazard analyses to the appropriate government asset, facility, or project manager.

4.9.4.6 Hazard analyses must be approved and the countermeasures in place prior to the work, activity or test commencing. If any analyses are allowed to expire, they are no longer approved; therefore, the safety plan is no longer valid. The hazard analysis will be defined as 'Overdue' in eMatrix® if the HA has passed the expiration date. This means that the associated test/activity shall no longer have an approved safety plan and cannot continue until the analyses are approved.

4.9.4.7 If hazard analyses are applied to a system or activity that affects another organization or test, the implementing DoD organization shall coordinate with the affected DoD organization. This is accomplished in the ITIS system by selecting the affected DoD official to review the hazard analysis. The implementing organization shall show the affected organization the hazard analysis results and the countermeasures implemented. This shall be documented and approved by both parties through an SRB, TRR, or other organized meeting.

4.9.4.8 All hazard analyses shall be revised to reflect any changes or modifications to the subject of the analysis after initial approval.

4.9.4.9 See Annex G for review and approval flowcharts.

## 4.10 Hazard Analysis Types

### 4.10.1 Baseline Hazard Analyses (BHA)

4.10.1.1 An approved BHA shall exist for each active test unit, plant facility, and utility operations, process, or system.

4.10.1.2 The 704$^{th}$ MSG/CC would approve HA with an RPC 2 and 704th CES/CC or 704th CS/CL would approve RPC 3s.

4.10.1.3 The 704 MXG or 704 MSG asset manager and AEDC/SE shall determine if a BHA is not required for an active asset. This decision shall be documented in the BSR description.

4.10.1.4 Systems or groups of systems identified for purposes of hazard analysis shall be chosen strategically to yield an adequate assessment of hazards affecting the mission. It is recommended that the BHA align with the AEDC asset listing; however similar systems may be combined. If this approach is taken, it shall be clearly stated in the BHA description and the description in any associated BSR.

4.10.1.5 A BHA shall cover applicable mission phases, but as a minimum shall include normal operation and maintenance activities. If maintenance is not included, the BHA description shall include an explanation of the reason for exclusion.

4.10.1.6 Specific areas to be analyzed in the BHA include:

4.10.1.6.1 Hazards that components may impose on the system.

4.10.1.6.2 Hazards that may be imposed on the system by interfacing systems.

4.10.1.6.3 Hazards that the system may impose on interfacing systems.

4.10.1.6.4 Hazards that may be imposed on the system by operators or maintainers.

4.10.1.6.5 Hazards that may be imposed by the system or environment that may affect operators or maintainers.

4.10.1.6.6 Hazards that the system may impose on the environment.

4.10.1.6.7 Hazards that result in data compromise or downtime.

4.10.1.7 The BHA shall include a description of the system being evaluated including block diagrams, pictures, one-line schematics and other documentation necessary to convey the major components, interfaces and operation of the system to the reviewer.

4.10.1.8 Confined space hazard analyses and mitigating procedures used as countermeasures shall be submitted for initial review/approval prior to being released for routine use by entering personnel. Subsequent modifications to the hazard analysis and procedures affecting the safety and health of personnel shall also be submitted for review/approval prior to release. See SHE Standard B5, Annex A.

4.10.1.9 The responsible engineer and system safety evaluator shall conduct a review and revision of the BHA at least every 24 months. If the system, process, or activity is inactive and is projected to be inactive for at least the next 24 months at the required time of review, no review and revision is required and the applicable Air Force Asset Manager will promote the analysis to the 'inactive' state in eMatrix®. In the event that the system, process, or activity is re-activated, a complete review and revision of the hazard analyses shall be accomplished at that time. This review shall include a review of hazards, causes, effects, and countermeasures for any changes or additions. The review shall also include verification that all counter-measures are current and active. The BHA shall be revised to maintain accuracy of the hazard analyses.

4.10.1.10 Revisions to the BHA shall be delivered to the government a minimum of 15 government working days before the expiration date of the BHA.

4.10.1.11 BHAs shall be reviewed and updated if any of the following projects change hazards, causes, effects, or countermeasures for a test facility, plant, etc:

4.10.1.11.1 Investment.

4.10.1.11.2 Civil Engineering.

4.10.1.11.3 Maintenance and Repair.

4.10.1.11.4 Improvement and Modernization.

4.10.1.11.5 Construction Support.

**4.10.2 Test Hazard Analyses (THA)**

4.10.2.1 THAs are required for all test projects. 704$^{th}$ TG, 704$^{th}$ TESG, 704$^{th}$ MSG and the GSU Directors are the approval authority for THA for which they are the asset owner.

4.10.2.2 THAs shall also be required for special activities such as the activation or checkout of new or modified systems; return to service from major maintenance or repair; unique or high risk operations; or activities not included in or in conflict with a BHA. These constitute activities that are outside of "normal" day-to-day operations that would normally be analyzed in a BHA.

4.10.2.3 The THA shall be used to identify the hazards associated with the tests and the actions necessary to minimize or control them. These are prepared during the test planning phase and finalized during the PSR.

4.10.2.4 Specific areas to be analyzed in the THA include:

4.10.2.4.1 Hazards that the facility may impose on the test or test article hardware/software.

4.10.2.4.2 Hazards that AEDC or User personnel may impose on the test and test article hardware/software.

4.10.2.4.3 Hazards that the test and test article hardware/software may impose on the facility.

4.10.2.4.4 Hazards that the test and test article hardware/software may impose on AEDC or User personnel.

4.10.2.4.5 Hazards that the test article hardware/software and test may impose on the environment.

4.10.2.4.6 Hazards that the environment may impose on the test article hardware/software.

4.10.2.4.7 Test-peculiar hazards that may result in data compromise or loss.

4.10.2.4.8 Hazards that the test article brings to AEDC, in maintenance procedures, handling procedures associated equipment and or personnel.

4.10.2.4.9 Unique aspects of the test not covered in, or are in conflict with, the BHA for the facility to be used.

4.10.2.5 The THA is part of the safety plan and shall be attached (linked) to the PSR for the test and delivered to the Government for review and approval a minimum of 10 government working days prior to the associated activity.

4.10.2.6 THA may be presented to an SRB to reflect a particular configuration or operation.

### 4.10.3 Barrier Analysis (BA)

4.10.3.1 A Barrier analysis (GC-1806) is a specialized analysis that is required for all Investment, Maintenance and Repair, and Military Construction Projects for the following phases; Design, Execution/Construction, and Checkout as determined by Contractor and/or AEDC/SE, and the 704 MXG or 704 TESG.

4.10.3.2 The BA is not a substitute for a formal O&SHA, but rather is a tool to identify hazards and risk mitigation early in the design process.

4.10.3.3 A BA shall cover applicable mission phases:

4.10.3.1 Specific areas to be analyzed in the BA include:

4.10.3.3.2 Hazards that the activity/components may impose on the system.

4.10.3.3.3 Hazards that may be imposed on the system by interfacing systems.

4.10.3.3.4 Hazards that the system may impose on interfacing systems.

4.10.3.3.5 Hazards that may be imposed on the system by operators or maintainers.

4.10.3.3.6 Hazards that may be imposed by the system or environment that may affect operators or maintainers.

4.10.3.3.7 Hazards that the system may impose on the environment.

4.10.3.4 Annex H contains a hazards checklist.

4.10.3.5 The BA shall be attached to a THA for construction/execution or checkout phase of the project as determined by Contractor Safety, AEDC/SE, or the AF project manager. BA shall be approved by the Contractor project manager, AF project manager, and Contractor Safety.

### 4.10.4 Other Hazard Analyses

Situations may arise where neither a BHA nor a THA seems applicable, but a hazard analysis is warranted. In such cases a hazard analysis shall still be prepared using the eMatrix® hazard analysis system. AEDC/SE shall determine the appropriate review cycle for the analysis.

## 4.11 Safety Reports

### 4.11.1 Baseline Safety Report (BSR)

4.11.1.1 The BSR provides a tool for the review and approval of all anticipated normal facility operations and maintenance proportional to the risk involved. The BSR is a compilation of BHAs that constitutes the hazards associated with the specific operation of a facility, or utility and includes a BHA for all systems to be operated or maintained. Approval of the BSR constitutes approval of the safety plan for the normal

operation and maintenance of the facility. The BSR is documented in an electronic database as part of the eMatrix® application.

4.11.1.2 Approval of the initial release and any revisions to the BSR shall be by the appropriate level approval authority based on the RPC. Delivery to the government of the initial BSR and any revision shall be a minimum of 15 working days before intended operation of the facility.

4.11.1.3 A review of the BSR for the operation and maintenance of a plant, facility, utility, or system shall occur at least every 24 months. This review will be conducted by the preparer/owner of the BSR and approved by the appropriate Air Force Asset Manager. Delivery of the review shall be to the Air Force Asset Manager 15 days prior to the two-year anniversary. The review process will consist of an automatic email sent to the Air Force Asset Manager and the ATA preparer/owner. The preparer/owner will review the BSR and if no changes are required update the 'reviewed date' field. eMatrix® will then send an email to the Air Force Asset Manager that there is a BSR waiting for his approval. Approval will consist of the Asset Manager changing the approval date.

4.11.1.4 A revision to the BSR shall be required whenever: a) An attached BHA is revised and the overall RPC is decreased (BHA risk is higher). If an attached BHA is revised and the overall risk has not increased, the BSR does not have to be revised. b) If a new BHA is connected to the BSR and its RPC is lower (BHA risk is higher). For example, the RPC of the BSR is 3 and a new BHA is an RPC2, then a revised BSR is required. c) When requested by Air Force Asset Owner, Air Force Safety, ATA Management, or ATA Safety. This request may be made if new BHA is added to the test unit, plant, utility, etc covered or if significant changes are made to existing systems and the BHA is revised accordingly. Whenever a BHA is connected or disconnected from a BSR, an email notification shall be sent automatically to the Air Force Asset Manager, Assignee and ATA Safety Reviewer.

4.11.1.5 The Summary Description shall include as a minimum a brief description of the facility/utility covered by the BSR.

4.11.1.6 BSRs shall include documentation of BHA, SRBs, and other safety related information. Attachments shall include as a minimum, a block diagram showing the systems that comprise the BHA and interfaces.

### 4.11.2 Project Safety Report (PSR)

4.11.2.1 The PSR provides the documentation of the safety review, approval, and test safety planning process. The approval of the PSR constitutes approval of the safety plan and an assessment/assumption of the overall safety risk level of the test/activity. The PSR is documented in an electronic database as part of the ITIS. The PSR is a "cover sheet" for the attached hazard documentation (i.e.; Test Hazard Analyses, Baseline Safety. The PSR must document the hazards of the test series/activity, configurations, and scope.

4.11.2.2 PSRs are required for the following activities:

4.11.2.2.1 Test.

4.11.2.2.2 Technology.

4.11.2.2.3 Return to Service.

4.11.2.2.4 Major Maintenance and Repair.

4.11.2.2.5 Construction support (per AEDC/SE direction).

4.11.2.2.6 Other activities at government project manager or AEDC/SE direction.

4.11.2.2.7 Investment projects at government project manager or AEDC/SE direction.

4.11.2.3 PSRs shall include documentation of THA, SRB, BSR, and other safety related information. Prior to coordination and approval of the PSR, all documentation must be verified by the review chain.

4.11.2.4 The purpose of the Summary of Risk section is to provide the reader with an overview of what is contained in the attached safety documents. Therefore, the Summary of Risk section of the PSR shall provide as a minimum a brief description of the test or activity (sufficient to give the reader an indication of what the test article is and if this test is "standard" or has some unique properties). It shall also provide a brief summary of the risk from the test peculiar analyses. The Summary of Risk shall also explain the validity of the BSR as it relates to the test. If test-peculiar hazards are addressed in the baseline, this shall also be noted.

4.11.2.5 Special attention must be given to communicate newly identified hazards and countermeasures to exposed workers. Supplemental analyses shall be performed, as appropriate, for projects involving hazardous materials or operations if hazard risk was not assessed in the initial or phase-reviewed analysis.

4.11.2.6 If a series of tests is going to be performed on the same type of engine, rocket motor or test article (i.e. test conditions/parameters), only one PSR shall be required as long as the hazards associated with the test remain the same. If the tests are going to be performed outside parameters for which the original PSR was prepared, a new PSR shall be required. If, during the test/activity anything changes from the original scope described, a new PSR is required. The dates of the tests shall be clearly stated in the PSR.

4.11.2.7 Annex G contains the guidance for the PSR.

4.11.2.8 The RPC for the PSR shall be that of the THAs as a minimum. If THAs are not included in the PSR, the RPC shall be that of the BSR as a minimum.

4.11.2.9 The Contractor shall deliver a PSR to the government approving officials at least 10 working days from the test/activity start date for review and coordination. At the time of delivery to the government, all associated THA and BHA must be approved at least by all required Contractor personnel.

**4.12 Safety Review Board (SRB)**

4.12.1 The purpose of the SRB is to brief the safety plan to the appropriate DoD chairperson. The SRB should convey the inherent and mitigated risks of the test/operation/activity and thoroughly explain the risk reduction methods (countermeasures). The SRB shall follow the requirements established in this standard; AFI 99-103, paragraph 6.9.2; and AFMCI 99-103.

4.12.2 The SRB is convened to accomplish the following:

4.12.2.1 Review the safety plan for the project/activity and to ensure the associated hazards/causes/effects are identified; that risk is properly assessed; and that risk is eliminated, minimized or controlled to an acceptable level via the implementation of adequate countermeasures.

4.12.2.2 Establish the overall risk level.

4.12.2.3 Recommend approval/disapproval of the project or activity safety plan to the approval authority.

4.12.3 The SRB shall be held when safety documentation is sufficient to adequately evaluate the hazards. In most cases, the SRB should be convened after formal delivery of the final safety plan (THA, BHA, BSR) to the government and prior to approval by the DoD. This will allow any action items or revisions to the safety plan identified at the SRB to be included before approval.

4.12.4 SRBs may be convened for all activities at AEDC at the discretion of the Commander or appropriate Group or Squadron Commanders; DoD Program Manager or higher authority at Tunnel 9 and NFAC. SRBs may be held for the review of a BSR, or an individual hazard analysis or collection of analyses.

4.12.5 An SRB shall be required for the following:

4.12.5.1 Projects, activities, and facility baselines with an RPC 2 or 1.

4.12.5.2 Projects, activities, and facility baselines with an RPC 3, by discretion of the appropriate Squadron Commander.
**NOTE:** If an SRB is not held, this shall be noted by memorandum attached to the PSR or BSR as appropriate.

4.12.5.3 All initial Facility BSRs.
**NOTE:** Subsequent SRBs for BSR revisions may be held at the discretion of the approval authority.

4.12.6 The SRB chair shall serve as AEDC/CC (or designee) for an RPC 1; the appropriate Group Commander (or designee) for an RPC 2; and the appropriate Squadron Commander (or designee) for an RPC 3. As a minimum, three voting members shall participate in the SRB. Voting members shall be the Chair, appropriate government personnel (as determined by the Chair), and Air Force Safety or Contractor Safety. The Chair may add other voting board members. SRB attendees shall include independent technical and operations representatives, maintenance experts, safety experts, the test manager/planner, and other personnel directly involved in the test to provide insight into the risk assessment.

4.12.7 The AEDC operating Contractor shall have responsibility to brief the SRB voting members on the safety aspects of the project/activity.

4.12.8 The recommended formats for the SRB meeting for BSR's, PSR's and PSRs held concurrently with TRRs are provided in Annex D:

4.12.9 The recommended SRB Meeting Summary Memorandum is provided in Annex D.

4.12.10 The recommended SRB Record for PSRs and/or BSRs is provided in Annex D.

4.12.11 The results of the SRB shall be documented in the eMatrix® database and attached to the PSR or BSR. This documentation shall include the slides, action items, and minutes of the SRB.

4.12.12 The status of the Safety Plan implementation shall be a mandatory agenda item at the TRR.

**4.13 Safety Plan**

After an AF Class A or B recordable mishap, or as directed by AEDC/SE, a revised hazard analysis shall be submitted to the Safety Investigation Board (SIB) for approval. This revised safety plan shall be reviewed and approved by the SIB prior to continuation of work or testing via a BSR or PSR as appropriate. (See AFI 91-204.)

**4.14 System Safety Working Group**

See AEDCI 90-902 Operational Risk Management

**4.15 Training**

4.15.1 Initial training shall be required and shall be provided to Contractor personnel directly involved in the system safety process, including, preparers, system safety assignees, system safety evaluators, SSWG members, reviewers, and approval authorities.

4.15.2 DoD Project Managers shall receive system safety training provided by AEDC/SE or Contractor Safety.

4.15.3 System safety training shall include instruction in the identification of hazards; assessment and reduction of risks; the Safety Review Process; and preparation, review and approval of hazard analyses.

4.15.4 At a minimum, refresher training shall be conducted for personnel directly involved in the system safety process, including, preparers, system safety assignees and system safety evaluators.

**4.16 Inspection/Audits**

4.16.1 Contractor Safety shall conduct an independent audit of selected hazard analysis as directed by AEDC/SE.

4.16.2 Audits shall consist of at least the following:

4.16.2.1 Verification that work instructions used as countermeasures are current, relevant, and in use such that hazard mitigation occurs.

4.16.2.2 Verification that systems used as countermeasures are functional.

4.16.2.3 Verification that hazard analyses are prepared according to this standard and have been reviewed and approved by the system safety evaluator, Contractor Safety, and others as required.

4.16.2.4 Verification of training records to assure that system safety practitioners have been adequately trained according to the requirements of 4.15.

4.16.3 Written results of hazard analysis audits shall be submitted to Contractor Safety Director and AEDC/SE

4.16.4 Non-conformances requiring corrective action shall be tracked using the Contractor corrective action system. Revisions to hazard analyses required as a result of the audits shall be submitted to the government for review and approval not later than 30 days from the time the audit is conducted.

**5.0 REFERENCES**

AEDC Contract F40600-03-C-001: Operation, Maintenance, Information Management, and Support of AEDC: Attachment 8, Performance Work Statement (PWS)Data Item Description DI-SAFT-80101B, System Safety Hazard Analysis Report (SSHA) (Required by the AEDC Contract F0600-03-C-001 PWS)

AEDCI 90-902, Operational Risk Management

AFI 90-901, *Operational Risk Managemen*t

AFI 91-202 AFMC Sup1 - I, *US Air Force Mishap Prevention Program* (Chapter 13)

AFI 91-202 AFMC Sup1, *US Air Force Mishap Prevention Program* (Chapter 13)

AFI 91-202, *US Air Force Mishap Prevention Program* (Chapter 9)
AFI 91-204, Safety Investigations and Reports
AFI 99-103, Capabilities Based Test and Evaluation
AFMCI 99-103, Test Management
AFPD 90-9, *Operational Risk Managemen*t
AFPD 91-2, *Safety Program*s
MIL-STD-882D, *Standard Practice for System Safety*

**ANNEXES**

A. Risk Assessment Matrix
B. Investment Project Hazard Analysis Requirements
C. Probability Interval Guidelines
D. Recommended Format for Safety Review Board Meetings
    1. Project Safety Reports
    2. Baseline Safety Reports
    3. Project Safety Reports Held Concurrently with Test Readiness Reviews
    4. Sample SRB Meeting Summary Memorandum
    5. Project Safety Report/Baseline Safety Report
E. Approval Flow Charts:
    1. Project Safety Report for Maintenance Group Projects
    2. Baseline Safety Report for 804th MXS/Baseline Safety Report for 704th MXG
    3. Project Safety Report for 704th Test Group Projects
    4. Project Safety Report for 704th Test Systems Group Projects
F. IT&S Guidelines for BHA Development
G. Hazard Analysis/Project Safety Report Review Guideline
H. Barrier Analysis

## ANNEX A

## RISK ASSESSMENT MATRIX

| | | | POTENTIAL CONSEQUENCES | | | | | PROBABILITY | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | A | B | C | D | E |
| | Category | Descriptive Word | Personnel Injury/Illness | Equipment Loss | Test Unit Downtime | Data Compromise | Environmental | Frequent | Reasonably Probable | Occasional | Remote | Extremely Improbable |
| SEVERITY | I | Catastrophic | Fatality or Permanent disability | >$1,000,000 | > 4 Months | Data not recoverable or primary program objectives lost | ‣ Regulatory non-compliance and definable immediate danger to environment<br>‣ Release not captured prior to compliance point with biological impact (flora or fauna) NOV with fine > $10K<br>‣ Remedial actions >$500K | 1 | | | | |
| | II | Critical | Severe injury, Severe occupational illness | >$200,000 to $1,000,000 | >2 Weeks to 4 Months | Repeat of test program | ‣ Release in excess of CERLA/EPCRA/RCRA quantity reportable (RQ)<br>‣ Release not captured prior to compliance point without biological impact NOV with compliance order or fines up to $10K<br>‣ Remedial actions $25K - $500K | | 2 | | | |
| | III | Marginal | Minor injury, minor occupational illness | $10,000 to $200,000 | 1 Day to 2 Weeks | Repeat of test period | ‣ Release of non reportable quantity; captured prior to compliance point<br>‣ Administrative NOV without fines<br>‣ Remedial actions $5K to <$25K | | | 3 | | |
| | IV | Negligible | Less Than minor injury or illness | <$10,000 | <1 day | Repeat data point or data requires minor manipulation or computer rerun | ‣ No Federal or State permit violations<br>‣ Release contained at site of release<br>‣ Remedial actions <$5K | | | | | |

| **PROBABILITY** | | | |
|---|---|---|---|
| **Level** | **Descriptive Word** | **Definition** | **1 Failure in # Cycles** |
| A | Frequent | Likely to occur repeatedly during the life cycle of the system (test/activity/operation) | <10 |
| B | Reasonably Probable | Likely to occur several times during the life cycle of the system (test/activity/operation) | 10 - 99 |
| C | Occasional | Likely to occur sometime during the life cycle of the system (test/activity/operation) | 100 - 999 |
| D | Remote | Not likely to occur during the life cycle of the system (test/activity/operation) | 1000 - 999999 |
| E | Extremely Improbable | Probability of occurrence cannot be distinguished from zero | 1M – 100M |

| **RISK PRIORITY CODE (RPC)** | | | |
|---|---|---|---|
| **Code** | **Risk** | **Contractor Action Required** | **DoD Action Required** |
| 1 | **High** | Imperative to suppress risk to lower level before operation | Imperative to lower risk if possible<br>AEDC/CC approval required<br>Coordination with AQEDC/SE and 3-letter office |
| 2 | Medium | Operation may require written, time limited waiver endorsed by Contractor management | AEDC Group Commander approval required as applicable<br>Coordination with SE and Squadron Commander |
| 3 | Low | Operation permissible | AEDC Squadron Commander approval required as applicable. Coordination with SE |

## ANNEX B

## INVESTMENT PROJECT HAZARD ANALYSIS REQUIREMENTS

System safety requirements for investment projects are based on the philosophy that safety will be considered from the conception phase through execution of the project. Modification of existing analyses will be the responsibility of the Investment Project Manager for only that part of the analysis affected by the project. It is expected that Investment Projects will not fund complete baseline hazard analysis updates unless the entire system is affected by the project, or updates unrelated to the project are added to the scope of the effort. See AEDC-STD-SE-1 Systems Engineering for further information.

| PROJECT TYPE | ANALYSIS TYPE | PROJECT PHASE | COMMENTS |
|---|---|---|---|
| High Risk Projects * | | | Completed by |
| Design phase | Preliminary SSHA, Preliminary SHA, Preliminary BHA, Preliminary BA, Preliminary THA as required. | PDR | Contractor Project Engineer responsible for requesting assignment and completion of preliminary analysis at PDR |
| Construction/Execution Phase | BA, and/or Approved THA. BSR and PSR as required. | CDR (Note: A SRB may be required) | Contractor Project Engineer responsible for ensuring completion |
| Checkout | BA and/or Approved THA. BSR and PSR as required. | CDR (Note: A SRB may be required) | Contractor Project Engineer responsible for ensuring completion |
| End State- Operational Phase | Approved O&SHA BHA. BSR and PSR , or Functional Configuration Audit Form GC-1568 as required. | CDR (Note: A SRB may be required) | Completed by Contractor System Safety Assignee Engineer with input from Design Engineering |
| Maintenance & Repair | * | * | Completed by 704 TESG |
| Military Construction Projects | SSHA | 30% Design | Completed by 704 MSG |
| | SHA | 60% Design | Completed by 704 MSG |
| | O&SHA | 90% Design | Completed by Contractor Operations Engineer with input from A&E Firm. |

* As determined by AEDC/SE and/or Contractor Safety.

**NOTE:** For low risk projects, AEDC/SE may determine the extent of analysis required.

**BA-** Barrier Analysis
**BHA-** Baseline Hazard Analysis
**CDR –** Critical Design Review
**O&SHA –** Operations and Support Hazard Analysis
**PDR –** Preliminary Design Review
**SSHA –** Subsystem Hazard Analysis
**SHA –** System Hazard Analysis
**THA –** Test Hazard Analysis

## ANNEX C

## PROBABILITY INTERVAL GUIDELINES

*For determination of life cycle phase probability intervals to which risk assessment probability levels apply, the following guidelines should be used. Probability intervals selected should be consistent with the same intervals chosen for the Project Safety Report.

| EXPOSURE | PROBABILITY INTERVAL |
|---|---|
| Rocket motor testing (cells, test articles, cell buildings, and ancillary support equipment - includes test unit downtime, environmental impact, and data compromise) | Single rocket motor test |
| Turbine engine testing (cells, test articles, cell buildings, and ancillary support equipment - includes test unit downtime, environmental impact, and data compromise) | 18 months (typical engine test entry duration) |
| Wind tunnel testing (cells, test articles, cell buildings, and ancillary support equipment - includes test unit downtime, environmental impact, and data compromise) | Single wind tunnel test |
| Facility computer systems | 10 years maximum |
| Plant and utility service equipment | Same as project/activity being supported; otherwise 30 year system life |
| Personnel | Same as project/activity being supported; otherwise 30 year working lifetime |

# ANNEX D
# RECOMMENDED FORMAT FOR SAFETY REVIEW BOARD MEETINGS

## PART 1: PROJECT SAFETY REPORTS

I. Introductions
   i. Chair, Voting Board Members, Attendees
   ii. Summary / Objective of the SRB

II. Background
   i. Job Number, Name, and/or Description
   ii. Sponsor/Customers
   iii. Program supported
   iv. Facility, Utility, Test Unit(s), Systems
   v. Responsibilities: AEDC, Sponsor, Customer, others

III. Test Article/Program/Activity/System/Facility
   i. Name
   ii. Description
   iii. System maturity (age of system,)
   iv. Normal operational and maintenance modes
   v. Objectives of activity
   vi. Predicted/Expected Results of activity
   vii. Scope (e.g. schedule, test periods, envelope, etc)
   viii. Tests/Methods
   ix. Success / Failure Criteria
   x. Significant differences from previous tests/activities/ articles
   xi. Review of mishaps and lessons learned

IV. Safety Analysis
   i. Mishap Responsibilities
      1. Investigating/Reporting
      2. Mishap Accountability
   ii. System Safety
      1. The analyses that make up the BSR/PSR (block diagram).
         The Board must concur that all systems required are included and interfaces are defined.
      2. THA review (AEDC and Customer prepared)
         a. Hazard Summary (the major risks to the program/activity before countermeasures)
         b. Critical Effects (personnel, equip, downtime, etc.) and Effects Requiring a Waiver
         c. The major risk reduction countermeasures (High Level Countermeasures)
         d. Additional important minimizing procedures and corrective actions
         e. Highest risk assessment for the THA (worst case assessment)
      3. BSR Summary
         a. Changes or exceptions to baseline due to test reconfiguration
         b. Facility hazards that can impact test or test article
         c. Critical hazards that can impact facility
         d. Hazard Summary (major risks analyzed in the BSR)
         e. Critical Effects and High Level of Protection Countermeasures
         f. Highest risk assessment for the BSR (worst case assessment)
      4. Additional minimizing procedures and corrective actions
         a. Test article restrictions
         b. Qualification and training
         c. Special considerations
      5. Highest risk assessment for the PSR-which is the THA

V. Action Item Review

VI. Approval/Disapproval

VII. Example of SRB Minutes (See Page 4 of this annex,)

VIII. SRB Approval (See Page 5 of this annex.)

**ANNEX D**
**RECOMMENDED FORMAT FOR SAFETY REVIEW BOARD MEETINGS**

**PART 2: BASELINE SAFETY REPORTS**

I. Introductions
   i. Chair, Voting Board Members, Attendees
   ii. Summary / Objective of the SRB
II Facility/ System / Utility / Test Unit(s)
   i. Name
   ii. Description
   iii. System maturity (age of system)
   iv. Purpose of facility
   v. Normal operational and maintenance modes
   vi. Interfaces to other systems/utilities
   vii. Review of mishaps and lessons learned
III. Safety Analysis
   i. Mishap Responsibilities
      1. Investigating/Reporting
      2. Mishap Accountability
   ii. System Safety
      1. The analyses that make up the BSR/PSR (block diagram).
         The Board must concur that all systems required are included and interfaces are defined.
      2. BSR Review
         a. Hazard Summary (the major risks to the program/activity before countermeasures)
         b. Facility hazards that can impact test or test article
         c. Test or test article hazards that can impact the facility
         d. Critical Effects (personnel, equip, downtime, etc.) and Effects Requiring a Waiver
         e. The major risk reduction countermeasures (High Level Countermeasures)
         f. Highest risk assessment for the THA (worst case assessment)
      3. Additional minimizing procedures and corrective actions
         a. Test article restrictions
         b. Qualification and training
         c. Special considerations
IV. Action Item Review
V. Approval/Disapproval
VI. Example of SRB Minutes (See Page 4 of this annex.)
VII. SRB Approval (See Page 5 of this annex.)

**ANNEX D**
**RECOMMENDED FORMAT FOR SAFETY REVIEW BOARD MEETINGS**

**PART 3: PROJECT SAFETY REPORTS HELD CONCURRENTLY WITH TEST READINESS REVIEWS**

I. Introductions
   i. Chair, Voting Board Members, Attendees
   ii. Summary / Objective of the SRB
II. Test Article/Program/Activity/System/Facility
   i. Objectives
   ii. Predicted/Expected Results
   iii. Scope (e.g. schedule, test periods, envelope, etc)
   iv. Tests/Methods v. Success / Failure Criteria
   v. Differences from previous tests/activities/ articles
   vi. Review of mishaps and lessons learned
III. Safety Analysis
   i. Mishap Responsibilities
      1. Investigating/Reporting
      2. Mishap Accountability
   ii. System Safety
      1. The analyses that make up the BSR/PSR (block diagram).
         The Board must concur that all systems required are included and interfaces are defined.
      2. THA review (AEDC and Customer prepared)
         a. Hazard Summary (the major risks to the program/activity before countermeasures)
         b. Critical Effects (Personnel, Equip, Downtime, Etc.) and Effects Requiring a Waiver
         c. The major risk reduction countermeasures (High Level Countermeasures)
         d. Additional important minimizing procedures and corrective actions
         e. Highest risk assessment for the THA (worst case assessment)
      3. BSR review
         a. Changes or exceptions to baseline due to test reconfiguration
         b. Facility hazards that can impact test or test article
         c. Test or test article hazards that can impact facility
         d. Hazard Summary (major risks analyzed in the BSR)
         e. Critical Effects and High Level of Protection Countermeasures
         f. Highest risk assessment for the BHA (worst case assessment)
      4. Additional minimizing procedures and corrective actions
         a. Test article restrictions
         b. Qualification and training
         c. Special considerations
      5. Highest risk assessment for the PSR-which is the THA
      6. Action Item Review
IV. Action Item Review
V. Approval/Disapproval
VI. Example of SRB Minutes (See Page 4 of this annex.)
VII. SRB Approval (See Page 5 of this annex.)

**ANNEX D**
**RECOMMENDED FORMAT FOR SAFETY REVIEW BOARD MEETINGS**

**PART 4: SAMPLE SRB MEETING SUMMARY MEMORANDUM**

***MEMORANDUM***

---

**Date: Organization Mail Stop**

**To:** File

**From:**

**Subject:** Safety Review Board (SRB) Meeting Summary For _____

---

An SRB meeting was held on _____in the _____Room to discuss safety issues and review the baseline SSHA associated with conducting _____ in the _____. Attendees at the meeting included:

The meeting began with introductions of those in attendance. A briefing was given that followed the recommended SRB meeting format outlined in Annex D in SHE Standard A4 – System Safety. Presentation slides are attached to the associated Project Safety Report (PSR) residing in eMatrix®. The briefing was given by _____, the author. _____ presented _____Program overview, a _____ facility description and the upgrades that have been made to the _____ facility. The author presented an activity overview for _____ including the objectives, expected results, and test schedule.

A summary of the Baseline Hazard Analyses was presented by _____. A Hazard Analysis Risk Summary was presented. Critical hazards and the risk mitigation activities that have been performed were discussed. High-level protection countermeasures were described, including personnel training, work instructions, personal protective equipment (PPE), uninterruptible power and emergency power supply systems, and continuous monitoring of critical systems.

The overall baseline hazard analysis assessment resulted in a RPC of ____for the_____.

A list of action items from the meeting are listed below:

Example;

1) Interface diagrams need to be included in the SSHA
2) Countermeasures need to be put in place to insure that _____
3) Etc

CC: Board Members
Attendees

**ANNEX D**
**RECOMMENDED FORMAT FOR SAFETY REVIEW BOARD MEETINGS**
**PART 5: PROJECT SAFETY REPORT/BASELINE SAFETY REPORT**

**SAFETY REVIEW BOARD (SRB) RECORD FOR:**

**Project Safety Report** ☐ **Baseline Safety Report** ☐

**Project / Activity:** _____

**Facility:** _____

**Date:** _____ **Time:** _____ **Location:** _____

The SRB has determined the status to be as follows:

☐ The following exit criteria have been met and approval for the Safety Plan presented to the SRB is granted:

1. The safety plan for the project/activity has been reviewed and the hazards were identified; eliminated, minimized or controlled to an acceptable level.
2. The overall risk level of RPC _____ was established and agreed to.
3. The SRB has followed the requirements in AEDC Safety and Health Standard A4.
4. The SRB recommends approval/disapproval of the safety plan for the project or activity.

☐ Exit criteria for the SRB have been met with the exception of the deficiencies noted in the attached Deficiency Summary List (Form GC-1565) and can progress to the _____ phase once responsibility for correction of the deficiencies have been assigned and completed.

☐ Exit criteria for the SRB have not been satisfied. Deficiencies are noted in the Deficiency Summary List.

Signatures of Review Team (Name and Organization)

_____ _____ Chair

_____ _____ Government

_____ _____ Air Force/Contractor Safety

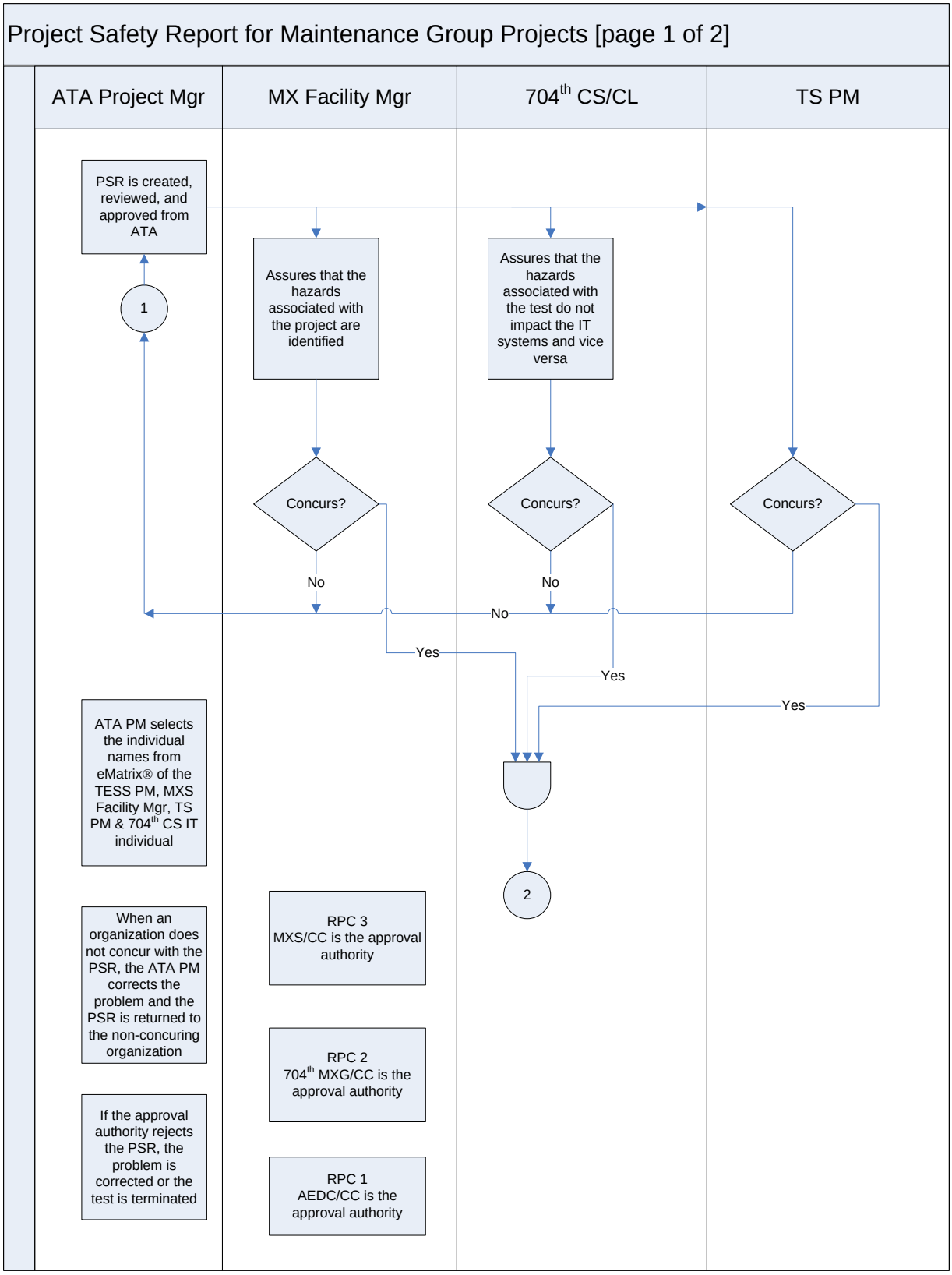
_____ _____ Other

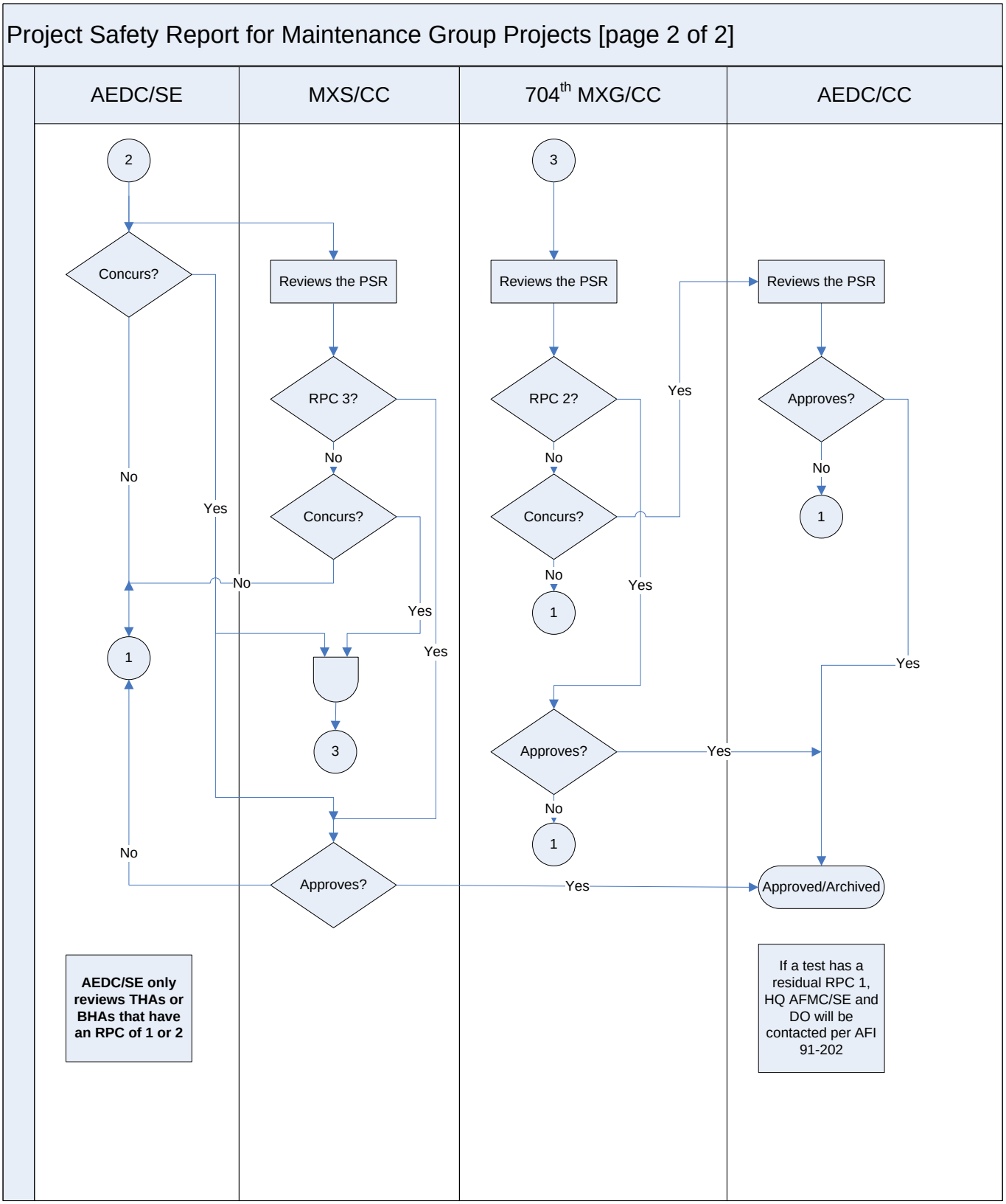
_____ _____ Other

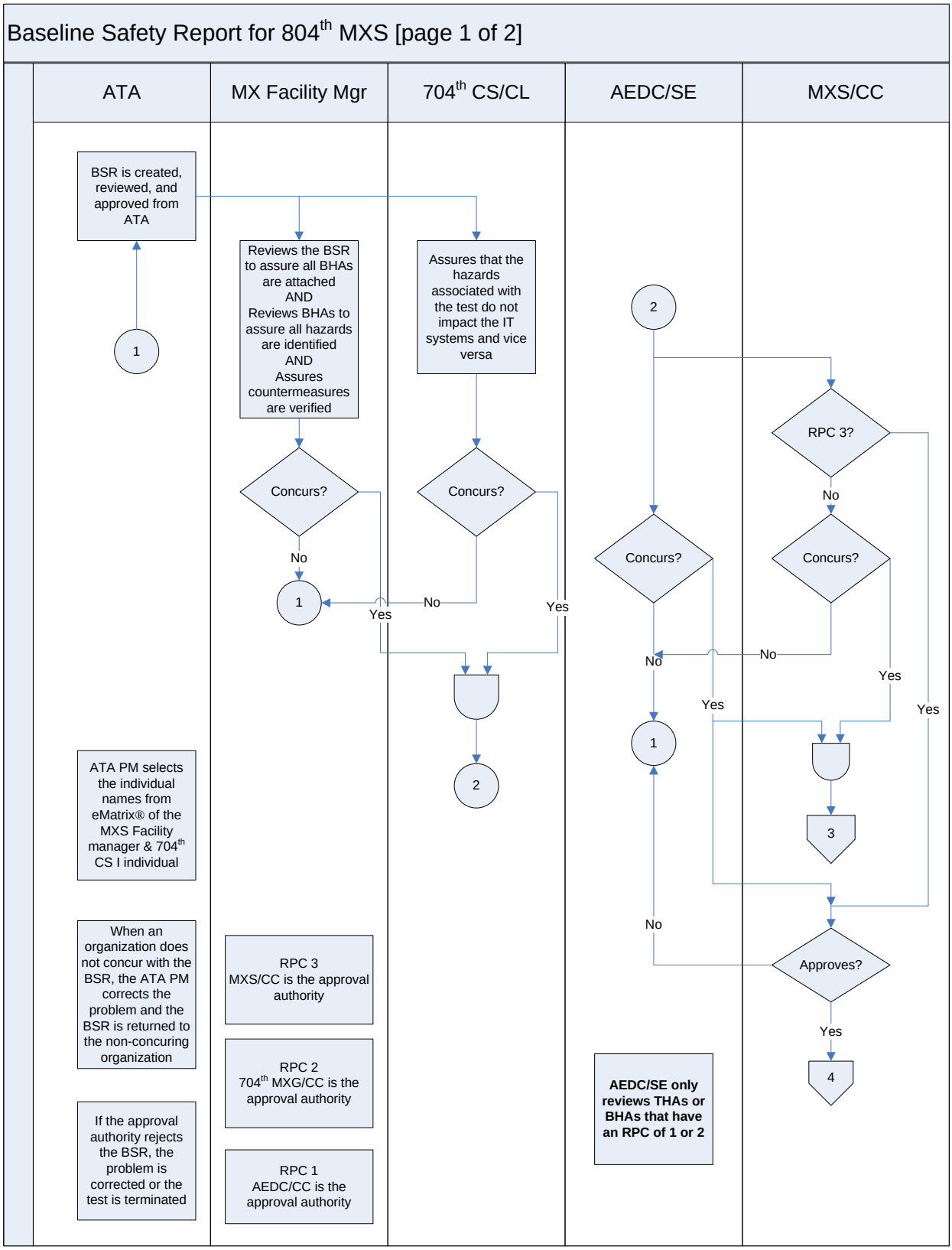
_____ _____ Other

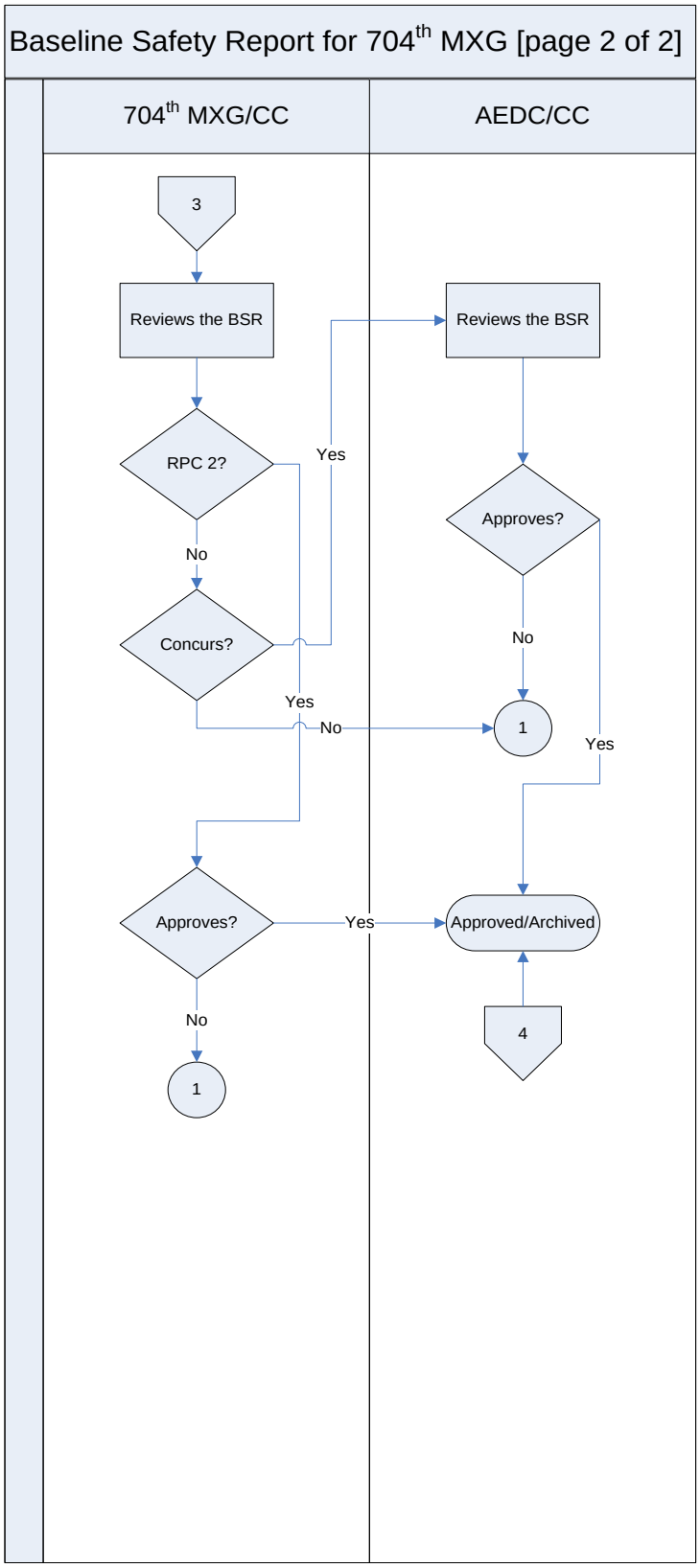
## ANNEX E

## FLOW CHARTS FOR PSR, BSR, BHA AND THA'S

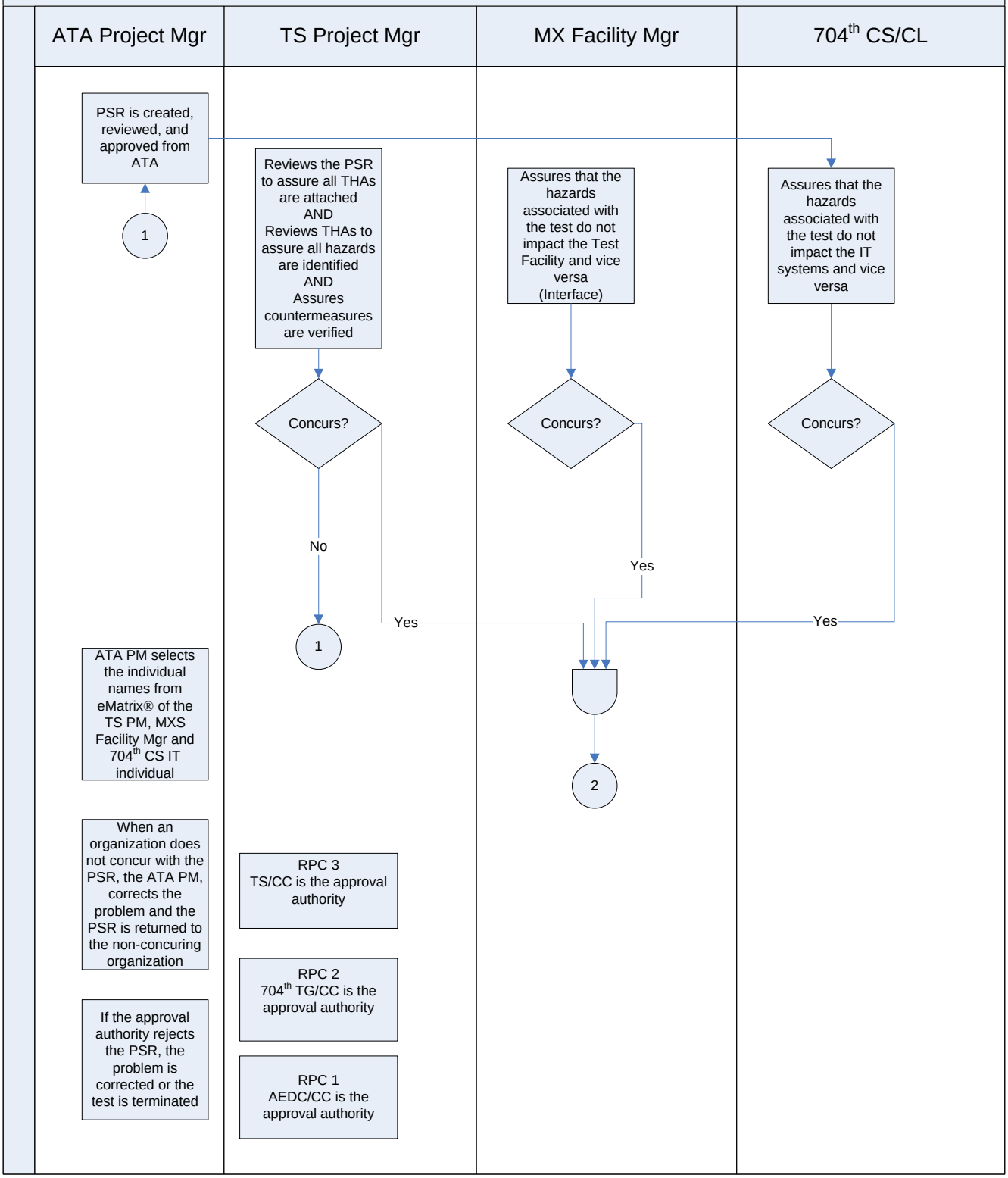


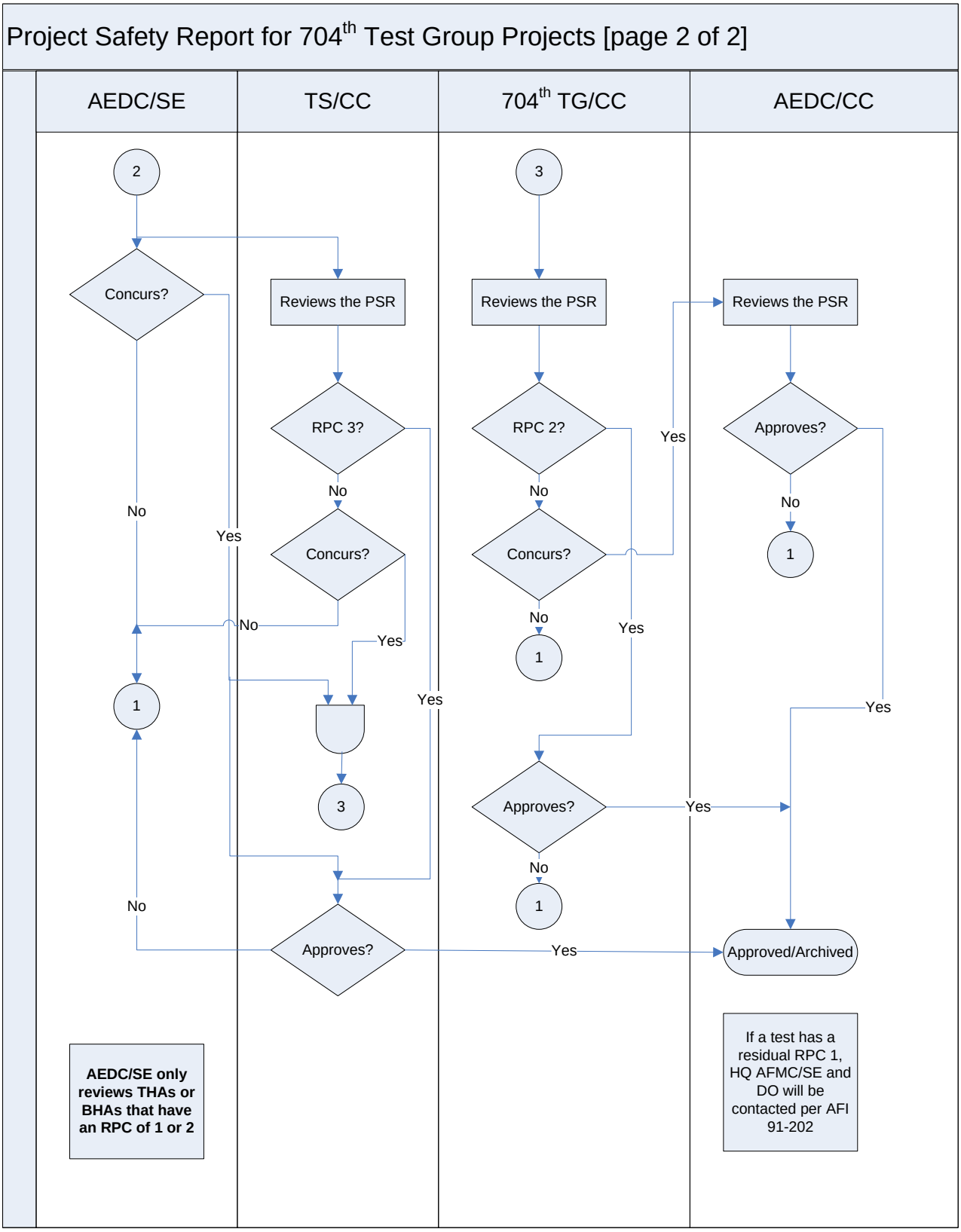

Project Safety Report for Maintenance Group Projects [page 2 of 2]
AEDC/SE
MXS/CC
704th MXG/CC
AEDC/CC
2
Concurs?
No
Yes
1
Reviews the PSR
RPC 3?
No
Concurs?
No
Yes
Yes
3
Approves?
No
Yes
3
Reviews the PSR
RPC 2?
No
Concurs?
No
Yes
1
Approves?
No
Yes
1
Reviews the PSR
Approves?
No
1
Yes
Yes
Approved/Archived
AEDC/SE only reviews THAs or BHAs that have an RPC of 1 or 2
If a test has a residual RPC 1, HQ AFMC/SE and DO will be contacted per AFI 91-202

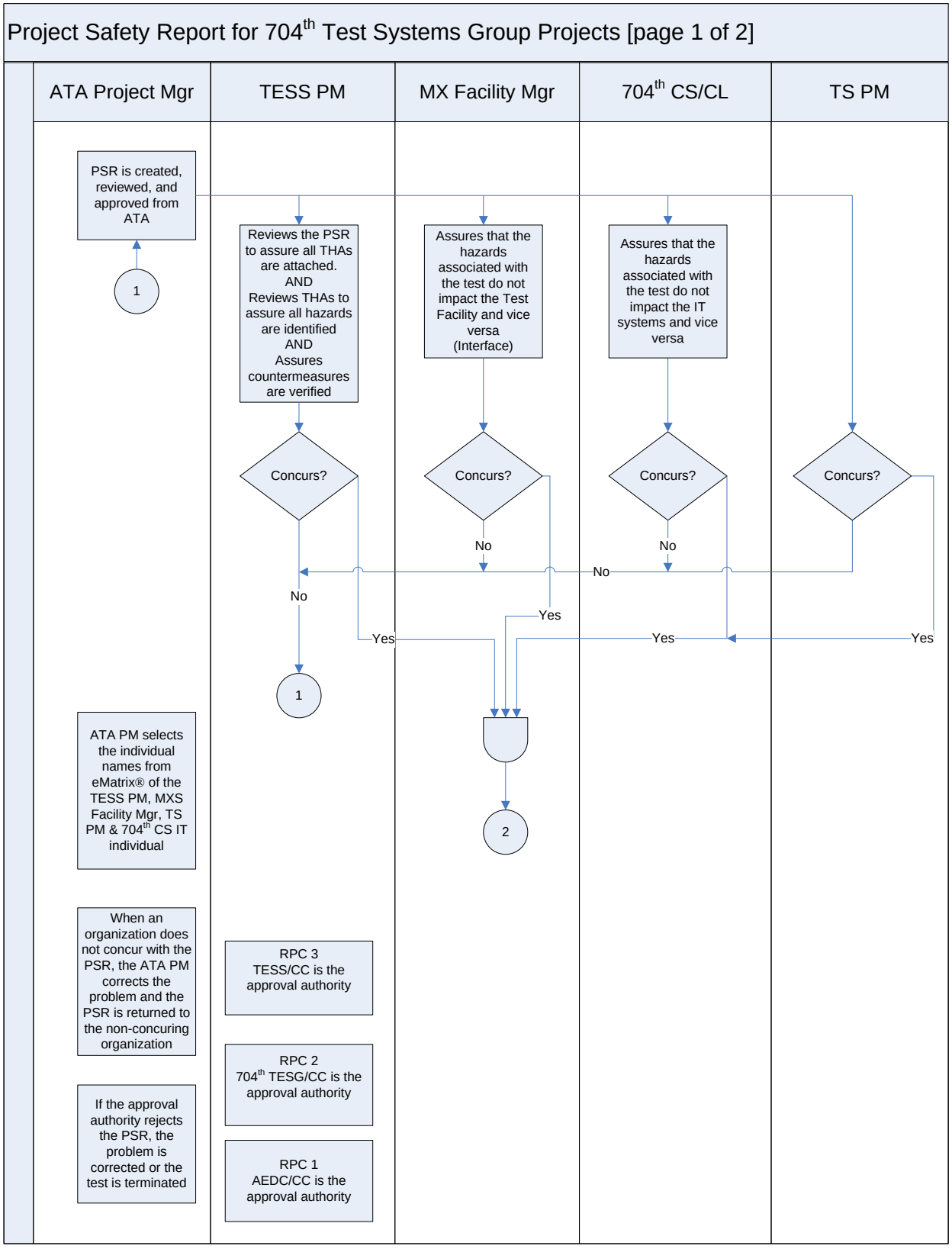

Baseline Safety Report for 804th MXS [page 1 of 2]
ATA
MX Facility Mgr
704th CS/CL
AEDC/SE
MXS/CC
BSR is created, reviewed, and approved from ATA
1
Reviews the BSR to assure all BHAs are attached AND Reviews BHAs to assure all hazards are identified AND Assures countermeasures are verified
Assures that the hazards associated with the test do not impact the IT systems and vice versa
Concurs?
Concurs?
No
1
Yes
No
Yes
2
2
RPC 3?
No
Concurs?
Concurs?
No
No
Yes
Yes
Yes
1
3
No
Approves?
Yes
4
ATA PM selects the individual names from eMatrix® of the MXS Facility manager & 704th CS I individual
When an organization does not concur with the BSR, the ATA PM corrects the problem and the BSR is returned to the non-concuring organization
If the approval authority rejects the BSR, the problem is corrected or the test is terminated
RPC 3 MXS/CC is the approval authority
RPC 2 704th MXG/CC is the approval authority
RPC 1 AEDC/CC is the approval authority
AEDC/SE only reviews THAs or BHAs that have an RPC of 1 or 2

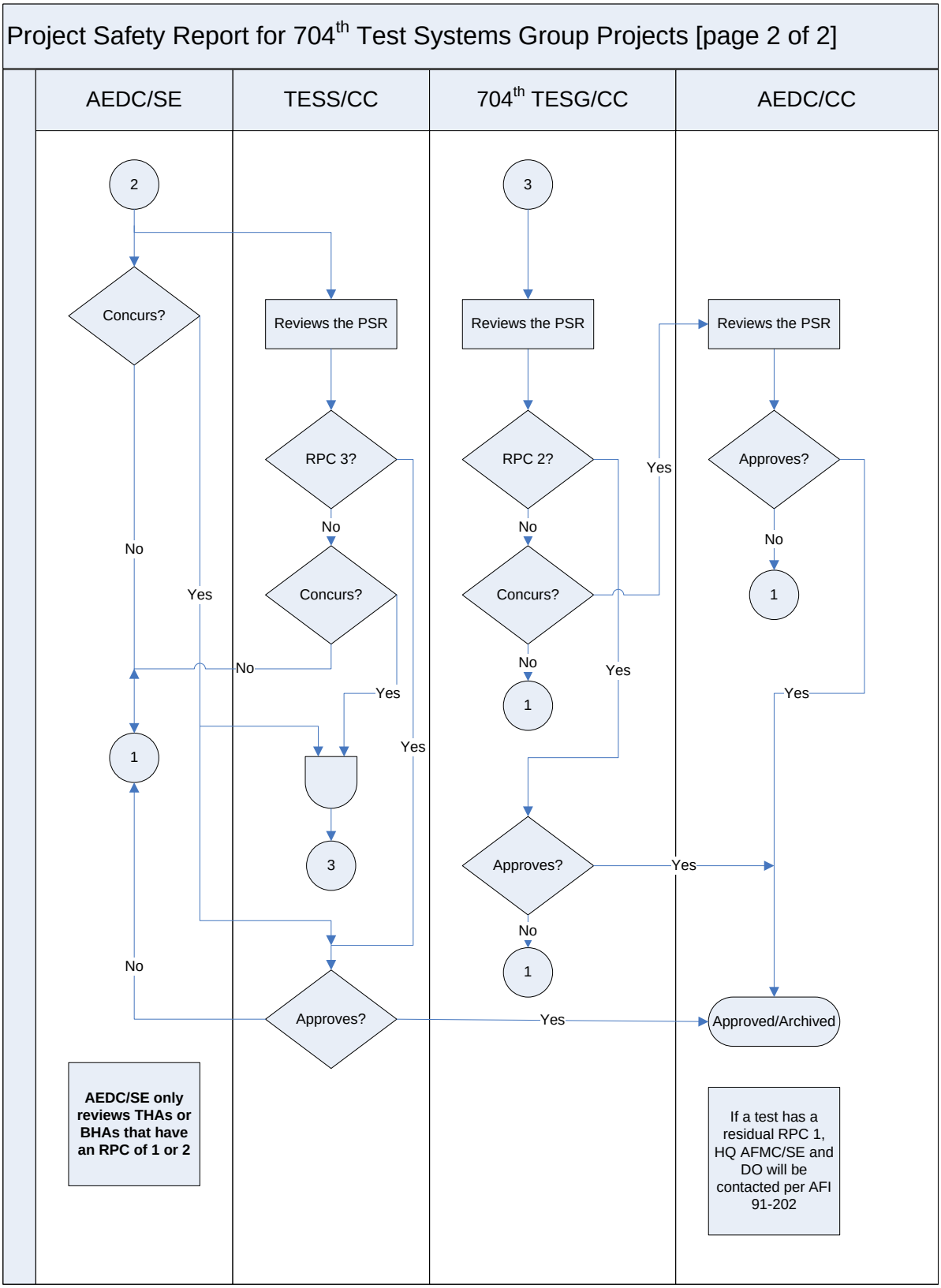

Baseline Safety Report for 704th MXG [page 2 of 2]
704th MXG/CC
AEDC/CC
3
Reviews the BSR
Reviews the BSR
RPC 2?
Yes
Approves?
No
Concurs?
No
Yes
1
Yes
Approves?
Yes
Approved/Archived
No
4
1

## Project Safety Report for 704th Test Group Projects [page 1 of 2]




Project Safety Report for 704th Test Group Projects [page 2 of 2]
AEDC/SE
TS/CC
704th TG/CC
AEDC/CC
2
Concurs?
No
Yes
1
No
Reviews the PSR
RPC 3?
No
Concurs?
No
Yes
3
Yes
Approves?
No
Yes
1
3
Reviews the PSR
RPC 2?
No
Concurs?
No
Yes
1
Yes
Approves?
No
Yes
1
Reviews the PSR
Approves?
No
1
Yes
Yes
Approved/Archived
AEDC/SE only reviews THAs or BHAs that have an RPC of 1 or 2
If a test has a residual RPC 1, HQ AFMC/SE and DO will be contacted per AFI 91-202


Project Safety Report for 704th Test Systems Group Projects [page 1 of 2]
ATA Project Mgr
TESS PM
MX Facility Mgr
704th CS/CL
TS PM
PSR is created, reviewed, and approved from ATA
1
Reviews the PSR to assure all THAs are attached. AND Reviews THAs to assure all hazards are identified AND Assures countermeasures are verified
Assures that the hazards associated with the test do not impact the Test Facility and vice versa (Interface)
Assures that the hazards associated with the test do not impact the IT systems and vice versa
Concurs?
Concurs?
Concurs?
Concurs?
No
No
No
Yes
Yes
Yes
Yes
1
2
ATA PM selects the individual names from eMatrix® of the TESS PM, MXS Facility Mgr, TS PM & 704th CS IT individual
When an organization does not concur with the PSR, the ATA PM corrects the problem and the PSR is returned to the non-concuring organization
If the approval authority rejects the PSR, the problem is corrected or the test is terminated
RPC 3 TESS/CC is the approval authority
RPC 2 704th TESG/CC is the approval authority
RPC 1 AEDC/CC is the approval authority


Project Safety Report for 704th Test Systems Group Projects [page 2 of 2]
AEDC/SE
TESS/CC
704th TESG/CC
AEDC/CC
2
Concurs?
No
Yes
1
No
Reviews the PSR
RPC 3?
No
Concurs?
No
Yes
Yes
3
Approves?
No
Yes
3
Reviews the PSR
RPC 2?
No
Concurs?
No
Yes
1
Yes
Approves?
No
Yes
1
Reviews the PSR
Approves?
No
1
Yes
Approved/Archived
AEDC/SE only reviews THAs or BHAs that have an RPC of 1 or 2
If a test has a residual RPC 1, HQ AFMC/SE and DO will be contacted per AFI 91-202

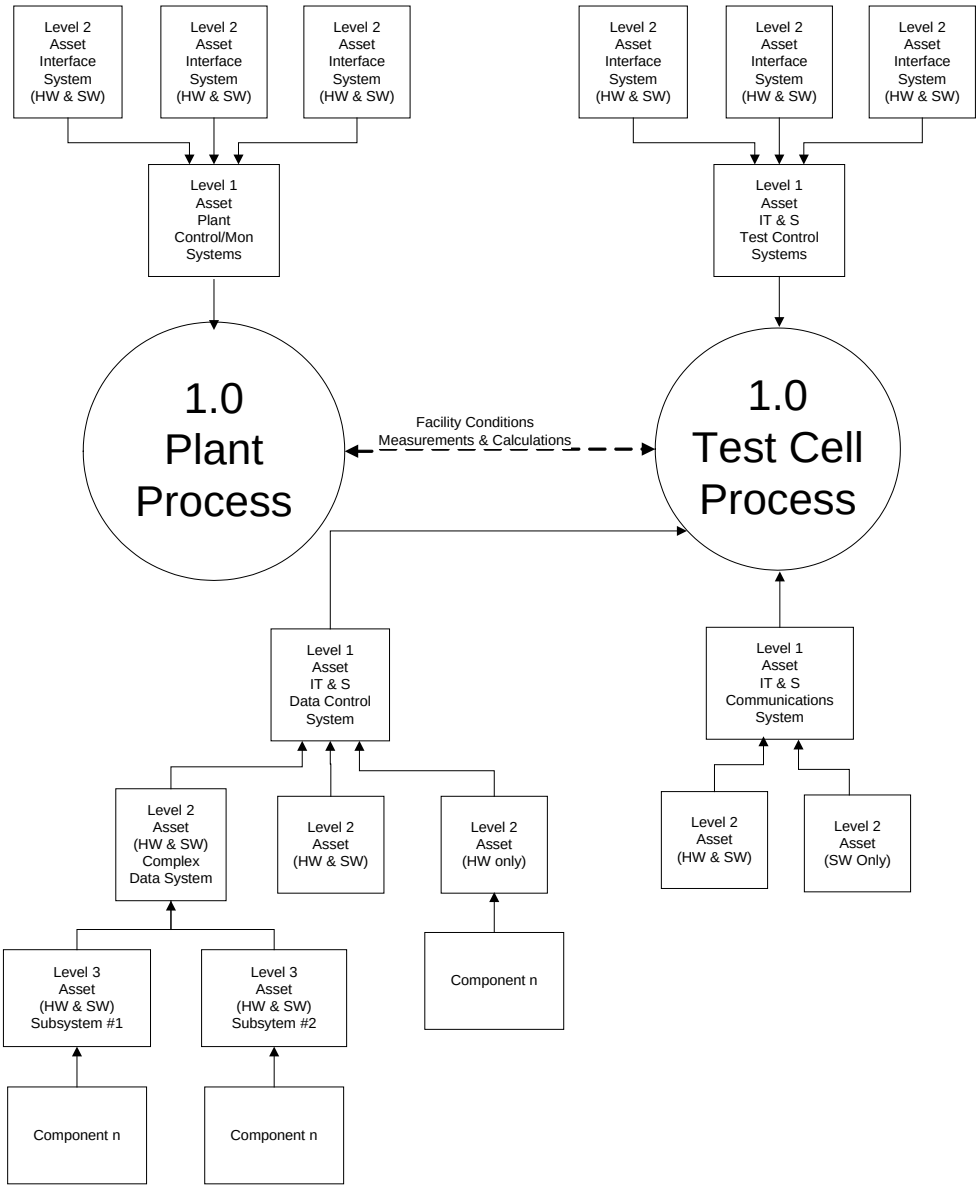
## ANNEX F

## IT&S GUIDELINES FOR BHA DEVELOPMENT

**SCOPE STATEMENT:** The BHAs developed by IT&S, whether managed by IT&S or supporting systems in other areas, will consider personnel injury/illness, equipment loss, test unit downtime, data compromise and environmental impact. The BHA will reference normal operating/maintenance procedures for RPC Levels 1 and 2 and include all appropriate mission phases with particular attention given to checkout, operations and maintenance.

**SSHA RECOMMENDATION FOR APPROVAL:** 704th Comm Sq will recommend approval for all Information Technology (IT) test support systems BHAs through eMatrix®. The 704th Comm Sq Project Manager(s) by recommending approval of the IT Test Support BHAs accepts the results of the "walk-down" of the procedure or work instruction and that it adequately addresses the countermeasures and process for any maintenance repair of the hardware, software and data required as a result of pre-test check run.

**DIAGRAM:** The following diagram shows the parent child relationship of IT&S Test Support Systems within the BHA Process. The BHA will be done for all Level 2 system assets.



# ANNEX G
# HAZARD ANALYSIS/PROJECT SAFETY REPORT REVIEW GUIDELINE

The following items are provided as a checklist of things to look for on a hazard analysis review;

## I. The Home Page

1. Check the History Page for previous comments.
   Ensure comments have been adequately addressed.
2. Check that there are appropriate block diagrams and/or pictorial sketches/schematics to review the system.
   a. Use the block diagram/pictorial representation (pictures, schematics/sketches, etc) to list mission phases and obvious hazards. This should be descriptive enough to show the interfaces and what your system consists of.
   b. The block diagram/pictorial representation has to show the interface points (where the system starts and stops) and what is coming in and going out of the system.
3. Check for mission phases, ensure there is a maintenance phase or explanation in the HA description if not.

## II. Hazard Analysis Description

Does the description explain the system/test article, interfaces, potential hazard sources, etc. well enough to understand the scope of the analysis and the potential associated hazards?

1. The description should explain the scope of the analysis, obvious things that are not in the analysis should be explained. i.e. there is no data compromise but it isn't obvious why not, Maintenance is not included as a mission phase, obvious hazards were not analyzed.
2. Use the Block Diagram/pictorial representation of the system to help in the review of the description.
3. Does the description explain the flow of the process(s) involved with the system?
4. Hazard Analysis Description Block –
   **CAPITALIZE** the following and describe in the Hazard Analysis Description:
   - SUMMARY OF REVISION
   - MAJOR SYSTEM COMPONENTS
   - ENERGY SOURCES
   - INTERFACES (System, Human)
   - LOCATION
   - PURPOSE
   - ASSUMPTIONS
   - CRITICAL WORK INSTRUCTIONS:
     List all critical work instructions that are included in the hazard analysis.
   - SUMMARY OF REVISION:
     a. Summarize changes or state that no changes were required.
     b. Either add the revision summary to the description or provide information in an HA attachment.
   - MAJOR SYSTEM COMPONENTS:
     List or describe what the major components of the system are.
   - ENERGY SOURCES:
     a. List or describe the fluids, gases, voltages, etc. that are part of or associated with the system.
     b. Ensure pressures, temperatures, voltage, or any other energy sources are specified; i.e. 4000 psi HPA, 13.8 Kv electrical, etc.
   - INTERFACES (System, Human):
     Where does the system start and where does it stop, what connects to it going in and going out.
   - LOCATION:
   - Where is the system located; building, area, etc.
   - PURPOSE:
     a. What is the purpose of the system, what is it supposed to do?
     b. What are the success criteria of the system or operation?
     c. This section can be expanded to explain the purpose of the analysis also.
   - ASSUMPTIONS:
     a. Describe or explain anything that adds value to the review and that the reviewer would not ordinarily know.

b. Examples might include explanations such that confined space hazards are covered in Hazard Analysis XXX. Or, It is assumed that the fuel farm delivers fuel at a specified pressure, flow rate and temperature.

- CRITICAL WORK INSTRUCTIONS –
  a. Any work instruction whereby serious injury, death, equipment damage exceeding $200K, or two weeks or more downtime could result if the work instruction steps are not accurately followed or not followed in sequence.
  b. Work instructions containing countermeasure steps to prevent personnel risks to known hazards for any of the following:
     1. High pressure (gas: ≥150 psig, liquid: ≥1000 psig)
     2. Fuel, oxidizers, or explosives
     3. Confined spaces or fall potential
     4. High-voltage electricity (≥600v)
     5. Toxic chemicals or extreme temperatures
  c. Other O&M work instructions containing countermeasure steps to prevent potential impact to safety, the environment, or the operation.
  f. Instructions for operation or maintenance of systems/subsystems requiring critical alignment of components (i.e. a drive train).
  g. Instructions detailing countermeasures to reduce a risk priority code 1 or 2 to a lower level 2 or 3.
  h. Any work instruction which, if not followed, could result in an environmental release in excess of the federal or state reportable quantities (RQs), a release not captured prior to compliance point without biological impact, Notice of Violation (NOV) with compliance order or NOV with fines of $10K or greater, or a remedial action of $25K or greater.
  i. Work instructions deemed by the system engineer or subject matter expert to be critical.

## III. Mission Phases

1. Are appropriate mission phases included? If not, why not. Typically Operations and Maintenance are the two phases that shall be included at a minimum. If Maintenance is not included in the analysis, the Hazard Analysis Description Section must explain why it is omitted.
   An appropriate mission phase is one that considers the hazards peculiar to that phase of the operation of the system. Some hazards may be unique to only certain mission phases. For example, hazards to personnel during 'operations' may not exist because personnel are evacuated by procedure and the area is checked clear prior to operating. However, there may be serious hazards to personnel during the pre and/or post operations phase.
   Risk may vary from phase to phase for some hazards present during several different mission phases. Risk may be low during pre-operations, nonexistent during operations, but very high during post operations.
2. Clearly define the mission phase. Describe in detail the scope of the mission phase being analyzed; do not simply repeat the mission phase title. The mission phase defines the scope of the hazard analysis at a level lower than the hazard analysis description. For example, if the mission phase is "operations," describe what is meant by "operations." When does it begin? When does it end? What does it entail? Describe specific or peculiar aspects of the mission phase that would not be apparent to the reviewer.

## IV. Hazards

What is a hazard? Does the thing, event, process, access, energy source, and/or activity result in risk of harm or damage? Does it decrease reliability, effect downtime, data compromise or the environment?
A checklist of hazards is included in Annex H of this SHE Standard A4.

1. Do the hazards for the mission phase actually belong under the mission phase? (i.e., discussing post operational hazards under a maintenance phase.)
2. Check that the hazard is truly a hazard (i.e., energy source) and is clearly defined. Refer to SHE Standard A4 for guidance.
3. Specify the noise level. Proper hearing protection depends upon the noise level. For very high noise levels, personnel exposure may have to be time-limited.
4. Is there an adequate explanation and description of the hazard?
5. Does the mission phase include all hazards obvious from a review of the block diagram/sketch/schematic included?
6. Do the hazard/cause/effect relationships make sense for this system and mission phases? Do they stand alone (not require further explanation)?

**V. Cause**

1. Does each cause have a separate block? "Or" statements usually mean the causes are lumped together.
2. Is there enough explanation of the cause to understand what could cause the hazard to happen?

**VI. Effects (targets)**

1. Does the target description adequately explain the result of the hazard? For example, if the target is data-compromised, what are the data that could be lost, corrupted, or compromised? If the target is personnel, what is the injury that could result from the mishap/hazard? Do not simply repeat the target title, i.e. equipment, as the target description. Provide specifics.
2. Are target descriptions limited to a single target? Avoid multiple target descriptions. For example, do not include both equipment and personnel in the same description.
3. Does the target really relate to the hazard/cause?
4. Does Equipment, Personnel, Environmental, Downtime, Data Compromise belong as a target?
5. For the hazard/cause, are all relevant targets included? Was one left out or analyzed without explanation?
6. Downtime:
   a. If the RPC for Downtime BEFORE implementation of countermeasures is a 1 or 2, then DT has to be fully assessed as a target.
   b. If the RPC for Downtime BEFORE implementation of countermeasures is a 3, then DT does not have to be fully assessed as a target. Instead, this statement will be put into a separate countermeasure block of the Equipment target;
   'Based on an ending probability of _____ for equipment loss/damage and an initial severity of _____ for DT, the resulting RPC for DT is assessed as a 3 and no further analysis is required'.
   c. If the analyst feels that a recommendation is necessary to mitigate downtime, then the downtime target will have to be assessed as is currently done.
   d. The beginning probability for downtime should match the ending probability for equipment.
   b. Does the description of Downtime explain what that is for the hazard/cause being evaluated?
   c. Are there ameliorators for Downtime (Spare Parts, Length of time to repair/replace, backup power supplies, etc.)
   d. CMs for Equipment do not have to be repeated for Downtime.
   For each equipment target there should be a downtime target or an explanation as explained in b. above.
7. Data Compromise
   a. Does the description of Data Compromise explain what that is for the hazard/cause being evaluated.
   b. Are the cm's for Data Compromise a repeat of those for equipment / downtime or a fair analysis of the actual target of Data Compromise.
   c. Are there ameliorators for Data Compromise? (i.e. data backup)

**VII. Beginning Severity, Probability, RPC**

Does the Severity and Probability make sense for the hazard/cause? Is it too high or too low? Remember that the beginning is analyzed without CMs in place.

**VIII. Countermeasures (CMs)**

1. What ensures the CMs are accomplished? Are the requirements specified?
2. Is the CM descriptive enough to ensure that it actually reduces risk? Each CM must stand alone based on the description, thus the description should be detailed enough to allow the reader to understand how the CM mitigates the hazard, cause, or effect.
3. Does the CM answer how the hazard / cause / effect is mitigated?
4. Does the CM relate to the mission phase?
5. For data compromise and downtime see Section VI Paragraphs 6 and 7.
6. Lockout/Tagout (LOTO) –
   a. Ensure there is a specific Work Instruction used to perform LOTO, or specify how point of protections are identified.
   b. If LOTO will be developed and issued for the specific work/job to be performed, specify the critical, specific points of protection to be locked out. The system engineer or knowledgeable craft supervisor may be designated as being the person responsible for identifying and verifying points of protection.
   c. Develop a checklist or generic work instruction that describes the points of protection and verification. The analysis should detail how we are protecting people specifically

7. Confined Space – Ensure the analysis conforms to requirements in Safety Standard B5 (Specifically, critical valves called out, retrieval device addressed, Permit or Non-Permit designation on the analysis, etc.
8. Noise - Does the CM specify hearing protection for the noise level being addressed; i.e., earplugs, double protection, time limits? Is an Industrial Hygiene noise level survey of the area needed?
9. Training - What ensures training is completed? How is it documented?
10. Alarms – What actions are required in event of an alarm; i.e., emergency procedure, work instruction, test engineer direction, operator experience and training?
11. Industrial Hygiene Issues – Are MSDSs specified, specific training for hazardous substances analyzed, and specific PPE for hazardous substances identified? Are hazardous substances clearly identified and potential exposure mitigated?
12. Personal Protective Equipment (PPE) – Is specific PPE required? What ensures the PPE will be used?
13. Work Instructions –
    a. A list of work instructions may be attached to the analysis. Specific work instructions listed in the attachment may be referred to in the CM; i.e., "Ref. 1."
    b. It is assumed that some work instructions may not be fully developed by the time the hazard analysis is reviewed, but there should be a place-holder title/number for it in the analysis.
14. Comments – Ensure comments (in red) have been adequately addressed. Retain all Safety Office comments.
    **NOTE:** Some comments can be additional information that should actually be included in the CM block.
15. Recommendations – Ensure recommendations include an ECD (Estimated Completion Date) and OPR (Office of Primary Responsibility). There should be no recommendation to incorporate a work instruction; this should already be developed or assumed to be in place prior to operation.
16. Beginning and Ending Severity, Probability and RPC – Review and verify these items. If no change is required, include an explanation in the CM as to why not. For example, if the initial RPC is a II C 3 and the ending is a II C 3, explain why there is no change.
17. High-Level CMs
    a. Required if;
        - Reduces severity by one or more levels and/or
        - Significantly reduces probability (2 or more levels)
        - If beginning RPC was a 1 or a 2 and the ending RPC is a 3
        - If the ending RPC is a 1 or a 2.
        - In addition this could be an engineering judgment that the level of protection should be High, depending on the criticality of the Hazard, Countermeasure and Effect.

        (**NOTE:** If HIGH is selected, this countermeasure is critical to reduce risk and answers to the Countermeasure Verification questions are mandatory).
    b. There must be at least one high level countermeasure if any "required if" item in 17 a above applies.
    c. Ensure any other CMs that seem to be critical are listed as high level.
18. If this is a baseline hazard analysis for a system that is in operation and mature, do not use work instructions as CMs unless the work instructions are complete and approved.

## IX. Verification

1. Verification Description – Specify how the CM is checked to ensure it is being accomplished. Verification must describe methods to ensure the CM is in place and functioning properly. Explain what ensures the verification is done.
2. Verification Interval – Specific time interval, if "As Required" is used (typically as a last resort); if used, state what "as required" means.

## X. Ending Severity, Probability, RPC

1. Does the Severity and Probability make sense for the hazard/cause? Is it too high or too low? Remember that the beginning is analyzed without CMs in place.
2. If the ending RPC is a 1 or a 2, a recommendation is required or an explanation must be provided as to why a recommendation is not appropriate.
3. Is the risk assessment consistent with the analysis? Are you convinced that risk has been reduced to the level stated?

## XI. Repeat IV through IX for Each Mission Phase

**XII. Comments**

1. Check that comments have been adequately addressed.
2. If you are in the review cycle, make appropriate comments. Be specific and clear on what the deficiency is as well as on the recommendation for correction. Follow your comment with your initials.

**XIII. Approval / Rejection**

1. Approve or reject the analysis. If the analysis is rejected, provide a brief explanation in the rejection/ approval comment block; if appropriate, reference the 215 Report for comments.
2. The reviewer may approve the analysis with comments. This is a judgment call as to the seriousness of the issues involved. If the comments are of a minor nature, i.e. verification description is weak or inadequate; the reviewer should comment that the review is approved with the understanding that the comments shall be addressed at the next review of the hazard analysis.
3. Note that a hazard analysis that has gone past it's due approval date is 'Overdue'

# PROJECT SAFETY REPORT FORMAT

(Minimum information for the PSR)

**Summary of Risk:**

## Summary of Changes:

Describe any changes from previous PSRs (if it is a revision, why the revision).

## Purpose of the PSR:

State the purpose of the PSR. The description should explain the purpose of the PSR

Description of Test/Activity: Describe the Activity. Does the description identify the scope of the test sufficiently to determine what test peculiar hazards might exist?

## Major System Components:

i.e.; Vacuum System, Tanks, Test Control Sequencer

## Hazard Summary:

1. Provide a summary of the Test Peculiar Hazards

a. Hazards that the facility may impose on the test article
b. Hazards that AEDC or User personnel may impose on the test article
c. Hazards that the test and test article may impose on the facility
d. Hazards that the test and test article may impose on AEDC or User personnel
e. Hazards that the test article and test may impose on the environment
f. Hazards that the environment may impose on the test article
g. Test peculiar hazards that may result in data compromise or loss.
h. Hazards that the test article brings to AEDC, in maintenance procedures, handling procedures associated equipment and or personnel.
i. Unique aspects of the test that are not covered in or are in conflict with the baseline hazard analysis for the facility to be used.

If the answer is documented to be no to a though i, then a Test Hazard Analysis may not be required.

2. Identify the adequacy of the BSRs. Are there exceptions to the BSRs (i.e. that a system or hazard does not apply to this test?).

3. Address the following as applicable:

All hazard analyses in the BSR have been reviewed for applicability to this test, and all are applicable.

All hazard analyses in the BSR have been reviewed for applicability to this test, and all are applicable except for the following systems that are not being used.

All hazard analyses in the BSR have been reviewed for applicability to this test, and all are applicable except for … which is addressed in a test peculiar hazard analysis

4. All countermeasures described in the Test Hazard Analysis, Baseline Hazard Analyses, and the attachments are in place and have been verified. Or; All countermeasures described in the System Safety Hazard Analyses referenced in the attached BSRs and THAs will be in place, and their operation verified before the test.

## Critical Work Instructions

Ensure the critical work instructions are listed on the attached BSR and THA (or list here).

## Block Diagram

Ensure that a block diagram for the BSRs are attached, showing the systems and interfaces.

The reason for this is to supply to the Air Force and Management a depiction of what individual hazard analyses belong with the baseline. This will clarify which systems should be part of the baseline and what hazard analyses should be expected with the BSR package.

# ANNEX H

| **Hazards Checklist** Execution phase for Project | | | | | | |
|---|---|---|---|---|---|---|
| | **Notes:** | **Energy Source / Hazard** | **Notes:** | **Energy Source / Hazard** | **Notes:** | |
| **ELECTRICAL** | | **Thermal** | | **Heavy Lifting** | | **Human Factors** |
| Electrical - Inadvertent activation | | High Temp/Over-Temperature | | **Structural Damage/Failure** | | Inadvertent Operation |
| Electrical - Loss of Power | | Cold/cryogenic | | **Vehicle Traffic** | | Operator error |
| Elect. - Exposure to energized circuits | | Loss of Heating/cooling | | **Heavy Equipment Movement** | | Failure to operate |
| Static Electricity | | | | **Excavation** | | Fatigue |
| Short Circuit | | **Chemical** | | Trench collapse | | |
| Arc Flash | | Release/Spill/Leak | | Disruption of utility -Cut | | **Operability** |
| Electrostatic Discharge | | Inadvertent Reaction | | **Weather** | | Inaccessability |
| Lightning Strike | | Process Safety Limits | | Moisture / rain / dew | | **Maintainability** |
| Overheating | | Contamination | | Heat Stress | | Inaccessability |
| Underground Contact | | Exposure - MSDS | | Cold Stress | | **Utility Outage** |
| Overhead Contact | | **Gases** | | Lightning | | Steam Loss |
| **MECHANICAL** | | Inadvertent release | | High Winds | | Ventilation loss |
| Rotating Equipment | | Unwanted buildup | | Flooding - Water | | Shop Air loss |
| Pinch Points | | **Corrosion** | | Solar Radiation | | Heat/Cool loss |
| Dropped Load | | **Vibration** | | Freezing | | Vacuum loss |
| Instability-Toppling, falling | | **Radiation** | | **Contamination of system** | | **Inadequate lighting** |
| Slips/Trips | | **Fire** | | **Biological** | | |
| Inadvertent movement | | **Explosion** | | Insects | | |
| Falling Objects | | **Power Source Failure** | | Poisonous Plants | | **Control of Energy** |
| **PNEUMATIC/HYDRAULIC** | | **Component Failure** | | Animals | | **Ergonomic** |
| Overpressure- Hydraulic, Pneumatic, Cryogenic systems | | **Excessive Noise** >85db | | **Inability to communicate - Loss of communication** | | Controls inadequate |
| Loss of pressure | | **Ameliorators for Downtime** | | **Falls - Fall Protection** | | Restricted Access |
| Implosion | | **Sys/Equip Fails to operate** | | **LEAD PAINT** | | Repetitive Motion |
| Pipe/vessel/duct Rupture | | **FOD** | | **ASBESTOS** | | |
| Backflow/Cross connection | | **Confined Space** | | **PCBs** | | |
| Pipe/Hose whip | | **Personnel Evacuation** | | **Emergency Actions** | | **Accessibility For Disabled** |
| **NOTE: Hazards checked are to be analyzed on sheet 3** | | | | | | |