BY ORDER OF THE COMMANDER OF ARNOLD ENGINEERING DEVELOPMENT COMPLEX

DEPARTMENT OF THE AIR FORCE INSTRUCTION 91-202

AIR FORCE MATERIEL COMMAND Supplement

ARNOLD ENGINEERING AND DEVELOPMENT COMPLEX Supplement

1 MAY 2026

Safety

THE DEPARTMENT OF THE AIR FORCE MISHAP PREVENTION PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no restrictions on the release of this publication

---

OPR: AEDC/SE

Certified by: AEDC/SE
(Mr. Ted Larson)

Pages: 38

This publication supplements Department of the Air Force Instruction (DAFI) 91-202 Air Force Materiel Command (AFMC) supplement, *The US Air Force Mishap Prevention Program*. This supplement includes additional System Safety and System Software Safety Guidance as well as additional supporting guidance in relation to system safety and risk acceptance, specifically Chapters **11** and **13**. This publication applies to all AEDC personnel. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Department of the Airforce (DAF) Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate chain of command. Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program*, and disposed of IAW the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). This

publication may not be supplemented. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the publication OPR for non-tiered compliance items. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Department of the Air Force.

11.1.1. The identification and management of hazards regarding System Safety are covered in Additional System Safety Guidance – see **paragraph 13.14**.

11.3.1. A hazard analysis as described in **paragraph 13.14** will be prepared instead of a System Safety Risk Assessment.

11.3.3. This section does not apply to AEDC.

11.3.4. High System Safety Risk in MIL-STD-882E (C1) Table III is equivalent to High Risk in the AEDC risk assessment matrix (**Figure A3.1**.). High Risk will be determined using the AEDC risk assessment matrix and will require approval by the AEDC/CC. No other coordination external to AEDC is required prior to risk acceptance. AFTC/SE and AFMC/SE will be notified within five government working days after risk acceptance. High Risk hazards will be reviewed on a yearly basis or when modifications to the system occur. Risk will be re-assessed and re-accepted per **paragraph 11.3.7**, when system modifications occur, or when there is a change to the system safety plan.

11.3.5. Serious System Safety Risk in MIL-STD-882E (C1) Table III is designated as a Medium Risk in the AEDC risk assessment matrix. Medium Risk will be determined IAW **Figure A3.1**, and Medium Risk hazards will require approval from the responsible AEDC Group or Division commander/director. No other coordination external to AEDC is required prior to risk acceptance. Medium Risk hazards will be reviewed every two years or when modifications to the system occur. Risk will be re-assessed and re-accepted per **paragraph 11.3.7**, or when system modifications occur, or when there is a change to the system safety plan.

11.3.6. Medium and Low System Safety Risk in MIL-STD-882E (C1) Table III are designated as a Low Risk in the AEDC risk assessment matrix. Low Risk will be determined IAW **Figure A3.1**, and Low Risk hazards will require approval from the responsible AEDC Squadron commander/director. Low Risk hazards will be reviewed every three years or when modifications to the system occur. Risks will be re-assessed and re-accepted when system modifications occur or when there is a change to the system safety plan.

11.13.6. **(Added)** The assessment of risk for software will be IAW the AEDC System Software Criticality Matrix (See **Table A4.1**.). Differences between AEDC software risk assessment versus MIL-STD-882E (C1) software risk assessment are as follows:

11.13.6.1. **(Added)** System Software Control categories are changed from 1 through 5 in MIL-STD-882E to A through E in the AEDC matrix.

11.13.6.2. **(Added)** Serious Risk in MIL-STD-882E (C1) is treated as High Risk in the AEDC matrix.

11.13.6.3. **(Added)** No Safety Risk in MIL-STD-882E (C1) is treated as Low Risk in the AEDC matrix.

11.13.6.3.1. **(Added)** While treated as Low Risk these Category E software will just need a statement stating that software has no safety impact.

11.13.6.4. **(Added)** Risk acceptance will follow the same acceptance authorities as laid out in paragraphs **11.3.4**, **11.3.5**, **and 11.3.6**.

11.13.6.5. **(Added) Table A4.3** and **Table A4.4** show LOR Tasks and Risk Assessment guidance for System Software Safety.

11.14. (Added) AEDC System Safety Process.

11.14.1. **(Added)** The AEDC System Safety Process consists of analyzing for risk, documenting that analysis, reviewing the analysis, verifying the risk controls are successfully validated and verified, and finally obtaining risk approval using the process shown in **Figure A6.1**.). The main elements of the process are the System Safety Plan (SSP) containing a single Baseline Hazard Analysis (BHA) or a Baseline Safety Report (BSR), and Operational Readiness Reviews (ORRs). The process begins with the planning phase, continues through all phases of the system's life cycle, and includes an in-depth analysis of subsystems, systems, operations, and maintenance.

11.14.2. **(Added)** System safety engineering techniques and principles will be applied to reduce safety risk. A few examples are Fault Tree Analysis, Failure Modes and Effects Analysis, and Fish Bone Diagrams.

11.14.3. **(Added)** Safety assessments will be technically objective and unbiased to the maximum extent possible. Assumptions will be avoided, when possible. But if deemed necessary, assumptions will be conservative, and the justification clearly identified.

11.14.4. **(Added)** System safety will be used to identify design requirements and apply the system safety order of precedence, as defined in Section 4.3.4 of MIL-STD-882E (C1).

11.14.5. **(Added)** Safety assessments and analyses will consider historical safety data to include lessons learned from other systems or facility activities.

11.14.6. **(Added)** Safety assessments will include human factors engineering to evaluate behavioral-based safety hazards and address the human role in the relevant task or activity. Personnel participating in the task or activity will be involved in the assessment of hazards and identification of appropriate controls.

11.14.7. **(Added)** System safety methods will be used to protect Information Technology resources (i.e. Servers, Computers, Network Switches, etc.).

11.14.8. **(Added)** System safety management processes (as described in AFI 63-101/20-101) will be applied throughout the System Engineering Process.

13.14. (Added) Additional System Safety Guidance.

13.14.1. **(Added)** Hazard Analysis. All hazard analyses will characterize both elements of risk (severity and probability). The analysis will address the risk of the hazard not the failure. No hazard will be excluded due to the inability to quantify the hazard. The system safety order of precedence will be applied to eliminate, mitigate, or control a hazard. First, every attempt will be made to alter the design to eliminate the hazard or reduce it to an acceptable level. If that is not practical, physical guards and barriers will be considered to isolate potential unwanted energy releases, harmful environments, or other hazards from potential targets. After physical guards and barriers have been established to the greatest extent practical, warning devices will be installed, if practical, to provide sufficient warning (visual and/or audible) to shut down the system, neutralize the potential hazard, and/or evacuate the area. Finally, after all other control measures have been considered, procedures, training, signage, and other administrative controls will be put in place to

control any unacceptable risks further. This last control is not a standalone control and will be used in conjunction with any of the other controls. The residual risks that remain after these controls are in place are then formally accepted by the Government. However, if the Government has determined that the risks have not been controlled to an acceptable level, new efforts to control the hazard must be made or the Government must make an exception. (See **Figure A9.1**.)

13.14.1.1. **(Added)** Hazard Analysis Types and Methods/Techniques. 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 will be performed, documented, reviewed, and approved per the requirements of this publication. Analyses such as preliminary, subsystem, or system hazard analyses should be considered for applicable stages of the systems engineering process. Analyses will 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 in MIL-STD-882E (C1).

13.14.1.1.1. **(Added)** Two types of hazard analyses required per this standard are BHA and System Integration Analysis.

13.14.1.1.2. **(Added)** Recommended hazard analysis techniques are the following: Fault Tree Analysis (FTA), Sneak Circuit Analysis (SCA), Energy Trace Analysis in conjunction with another technique, FMEA (Failure Modes and Effects Analysis) in conjunction with another technique, and Preliminary Hazard Analysis (PHA). When applicable the STPA (Systems Theoretic Process Analysis) should be considered for Software and Controls Systems hazard. For more information on these types of analyses contact AEDC/SES.

13.14.1.2. **(Added)** Hazard Analysis Format.

13.14.1.2.1. **(Added)** Hazard analyses will be prepared using the Government-specified electronic system of record. Preparation of hazard analyses using other methods may be approved by the AF Asset Manager for cases listed below:

13.14.1.2.1.1. **(Added)** If a hazard analysis is required in an emergency or extremely time sensitive situation.

13.14.1.2.1.2. **(Added)** If required for entry into confined spaces on an emergency or time critical basis.

13.14.1.2.1.3. **(Added)** During the design phase of a System Integration Analysis; however, the final analysis for review will be prepared using the preferred electronic system.

13.14.1.2.2. **(Added)** The hazard analysis will be written in sufficient detail such that reviewers with minimal or no knowledge of the system or process can understand the potential mishaps and risk mitigations.

13.14.1.2.3. **(Added)** All hazard analyses will include the following documentation as an attachment as applicable:

13.14.1.2.3.1. **(Added)** A system block diagram and/or some form of graphical presentation (i.e. pictures, schematics, flow charts, etc.) to assist in reviewing the systems, subsystems, and process interfaces.

13.14.1.2.3.2. **(Added)** Analyses, including Vendor and Manufacturer analyses (e.g. load analysis, structural analysis, life cycle analysis, thermal analysis, etc.), if applicable.

13.14.1.2.3.3. **(Added)** Any other documentation related to the system, process, etc. (e.g. Safety Data Sheet(s) (SDS), explosive classifications, X- rays, non-destructive testing reports, etc.).

13.14.1.2.4. **(Added)** Each hazard analysis will be developed in accordance with the following format as a minimum:

13.14.1.2.4.1. **(Added)** Title. The title should be easily searchable and will describe the system or process analyzed. The title will include the assets or process.

13.14.1.2.4.2. **(Added)** Description. The description will include the system or process being evaluated, the purpose, general physical characteristics (if applicable), major system components, energy sources (quantitative and stored), interfaces (system and human), operating location and environment. Assumptions will be clearly stated. Work instructions, procedures, checklists, drawings, and other documentation used as verification of High-Level Mitigation Measures will be listed; to include numerical descriptor and title. Revisions to an approved document will include a summary of the revision. The revision history will be retained for the life of the document.

13.14.1.2.4.3. **(Added)** Mission Phase. Mission phases will be used to break the analysis into sections such as pre-ops/post-ops, operations, maintenance, handling operations, installation, confined space, etc. that are analyzed separately because they have different potential mishaps. The Mission Phase description will include enough information to explain the activity being analyzed.

13.14.1.2.4.4. **(Added)** Probability Interval (i.e., duration of exposure). Hazard probability is without meaning unless it is attached to a specific exposure period. Probability interval will be stated in terms of hours, events, lifetime of service, or remaining service life. (See **Attachment 3** and **Table A5.1**.)

13.14.1.2.4.5. **(Added)** Hazard (source). This section will provide an adequate explanation and description of the hazard and will be applicable to the mission phase being analyzed. Hazards will not refer to individual components of a system, if possible. Hazards will not contain ambiguous or vague (e.g., unsafe, unacceptable) wording in the description. See **Attachment 10** for typical hazard categories and subcategories.

13.14.1.2.4.6. **(Added)** Cause (mechanism). A hazard may have multiple causes, and each must be identified. This section will provide an adequate explanation and description of the cause and will be applicable to the mission phase being analyzed. Each cause will be listed and analyzed separately unless the causes can be controlled or eliminated via the same mitigation measures and present the same probability level.

13.14.1.2.4.7. **(Added)** Effects and Targets (outcome). All applicable effects to the Targets related to the hazard and cause will be identified. The effect description will provide an explanation of the damage or loss in quantifiable terms. Targets to be considered are Personnel, Equipment, Downtime, and Environmental. Combined Targets will be not allowed since a mitigation measure applied to reduce risk for one Target may be ineffective for another.

13.14.1.2.4.8. **(Added)** Mitigation Measures. Mitigation measures will be applicable to the mission phase being analyzed and will be described in sufficient detail in the hazard analysis such that reviewers may evaluate the effectiveness of the mitigation measure. Each mitigation measure will be listed separately and identified with the hazard/cause/effect that it eliminates or reduces. All documentation used as mitigation measures to mitigate hazards will be identified, approved, and retained on site.

13.14.1.2.4.8.1. **(Added)** Documentation used to mitigate all hazards that could result in personnel injury/illness considered Catastrophic (mishap severity category I) or Critical (mishap severity category II) will be current and formally documented and comply with Department of the Air Force (DAF) and OSHA policies and procedures.

13.14.1.2.4.8.2. **(Added)** A mitigation that targets the cause generally reduces the probability of the event occurring.

13.14.1.2.4.8.3. **(Added)** A mitigation that targets the effect to a Target generally reduces the severity if the event occurs. A mitigation that relieves the situation after the event has already begun to occur generally lowers severity even more.

13.14.1.2.4.9. **(Added)** High-Level Mitigation Measure. Actions taken to reduce the risk of a hazard from initial risk level High or Medium to lower residual risk level as well as actions or mitigations taken that reduce mishap probability by two or more levels, and/or reduces mishap severity by one or more levels.

13.14.1.2.4.9.1. **(Added)** High Level Mitigation Measures must be verifiable, specific, measurable, achievable, and realistic and time bound as possible. They will also be validated through a formal process.

13.14.1.2.4.9.2. **(Added)** High Level Mitigation Measures may be engineered safety features that can be accompanied by a complementary procedure or instruction. This complementary document is not the Mitigation Measure in and of itself. It verifies a mitigation measure is being done.

13.14.1.2.4.9.3. **(Added)** They can be a part of the system’s design.

13.14.1.2.4.9.4. **(Added)** The complementary procedure or instruction direct that a High-Level Mitigation Measure is to be done.

13.14.1.2.4.9.5. **(Added)** High Level Mitigation Measures will not be signage, personnel training, PPE, or any combination of the three as the only risk reduction method(s).

13.14.1.2.4.9.6. **(Added)** High Level Mitigation Measures are intended for some hazards with initial risk level High or Medium. However, it can be required for other hazards as well based on engineering judgement that this level of protection is needed, depending on the criticality of the Hazard, Mitigation Measure and/or the Effect.

13.14.1.2.4.9.7. **(Added)** Statistics show that human error has a probability of 0.001 to 0.1 for safety-critical applications. Thus, if human interaction is used as a High-Level Mitigation Measure the lowest mishap probability level is C for risk assessment.

13.14.1.2.4.10. **(Added)** Mishap Severity. Severity of the potential mishap will be assessed both before and after implementation of mitigation measures. Severity level is driven by the effect to a Target.

13.14.1.2.4.10.1. **(Added)** When assessing the facility downtime (DT) as a result of equipment damage, it is assumed the equipment damage/failure has occurred, therefore only the severity of downtime can be reduced.

13.14.1.2.4.10.2. **(Added)** In most cases, no mitigation measure or combination of mitigation measures can reduce the severity of a hazard by more than one level. An explanation for the rationale behind the engineering judgement used for the multi-level reduction will be provided.

13.14.1.2.4.11. **(Added)** Mishap Probability. Probability of the potential mishap will be assessed both before and after implementation of mitigation measures. Probability level is driven by the cause and mitigation measures. The initial and end probability for the facility downtime (DT) due to equipment damage will be the same as the corresponding ending probability for the equipment loss (E). It is assumed the equipment damage/failure has occurred; therefore, the probability does not change even after applying mitigation measures.

13.14.1.2.4.12. **(Added)** Risk Level. Risk level will be assessed both before and after implementation of mitigation measures via the use of the Risk Assessment Matrix provided in **Attachment 3**.

13.14.1.2.4.12.1. **(Added)** The risk level before mitigation measures is applied is known as the Initial Risk. The risk level after mitigation measures is applied is known as the Residual Risk.

13.14.1.2.4.12.2. **(Added)** Normally risk level should not be reduced diagonally on the risk assessment matrix. The risk matrix is not logarithmically scaled for both probability and severity. Therefore, a factor of severity decrease is not proportional to the factor of probability decrease, which articulates hazard aversion. Risk, which is a product of probability and severity, would not be proportional. However, on rare occasions a combination of mitigation measures can reduce the risk diagonally. If risk reduction is diagonal, the mitigation measures will be identified as either a probability or severity reducer.

13.14.1.2.4.13. **(Added)** Recommendation. If risk level after implementation of mitigation measures remains a High or Medium, additional mitigation measures may be recommended. This should include a cost estimate. It may also include, Estimated Completion Date (ECD), Office of Primary Responsibility (OPR) if known, as well as any other relevant information. If there are no additional mitigation measures to recommend that would reduce the risk, then that fact will be stated.

13.14.1.3. **(Added)** Hazard Analysis Application.

13.14.1.3.1. **(Added)** All AEDC configuration item assets that are operational or on stand-by as laid out in local standard, AEDC-STD-CM1, will either have a hazard analysis, be contained within a hazard analysis, or have a waiver for the hazard analysis. The waiver will:

13.14.1.3.1.1. **(Added)** Be constructed by the System Safety Preparer.

13.14.1.3.1.2. **(Added)** Communicate the reason for the waiver.

13.14.1.3.1.3. **(Added)** Be submitted to the appropriate DAF Asset Manager for concurrence and then to AEDC/SE for approval.

13.14.1.3.1.4. **(Added)** Be attached to the asset in the Configuration Management System using the Government-specified electronic system of record.

13.14.1.3.2. **(Added)** Hazard analyses will be prepared for normal day-to-day activities of a system, subsystem or facility. These activities include operations, calibrations, pre-and post-operations, maintenance, software upgrades, or any other activities as outlined in the mission phases. Hazard analyses will also be prepared for operations (e.g., high-energy source checkouts, major modifications and upgrades, operations involving personnel), or those that results in a new facility/system or change to an existing facility/system including but not limited to the following:

13.14.1.3.2.1. **(Added)** Explosives and propellant handling or use.

13.14.1.3.2.2. **(Added)** Confined space entry.

13.14.1.3.2.3. **(Added)** Capital Improvement Projects, for the following phases: Design, Execution/Construction, checkout, and Baseline Operations.

13.14.1.3.2.4. **(Added)** Maintenance and Repair projects.

13.14.1.3.2.5. **(Added)** Chemicals stored or used in excess of the threshold quantities contained in 29 CFR 1910.119 and 40 CFR 68.

13.14.1.3.2.6. **(Added)** Off-site operations involving hazardous or dangerous conditions.

13.14.1.3.2.7. **(Added)** Post-maintenance checkouts.

13.14.1.3.2.8. **(Added)** System activation or reactivation.

13.14.1.3.2.9. **(Added)** Utility Facility Operations and Maintenance.

13.14.1.3.2.10. **(Added)** Pressure Testing. (See local standards AEDC-ENGR-STD-T-1 and AEDC-ENGR-STD-T-2)

13.14.1.4. **(Added)** Hazard Analysis Preparation, Review, and Approval.

13.14.1.4.1. **(Added)** Air Force Asset Managers and Project Managers will ensure Hazard Analysis and required documentation are prepared and reviewed.

13.14.1.4.2. **(Added)** Personnel involved in the operation and maintenance of equipment will be included in the preparation and review of the analysis.

13.14.1.4.3. **(Added)** Hazard analyses involving occupational health, environmental hazards, or chemicals in excess of the threshold quantities will be submitted to AEDC/SE and/or AEDC Bio-Environmental Offices for review.

13.14.1.4.4. **(Added)** Hazard analysis with a personnel effect with a residual risk level High will not be submitted for review.

13.14.1.4.5. **(Added)** Hazard analyses will need approval by the Risk Acceptance Authority (RAA), and the mitigation measures will be in place prior to the work or activity commencing. If any analyses are overdue, they are no longer approved; therefore, the system safety plan (SSP) for the activity/process described in the hazard analysis is no longer valid. The hazard analysis will be defined as “Overdue” if the hazard analysis has passed the overdue date. The expiration dates are one year, two years and three years after approval of a hazard analysis with a High, Medium and Low risk level, respectively. The DAF Asset Manager may submit a waiver requesting activities continue under the Overdue hazard analysis. The waiver will be routed to the responsible AF Squadron/Branch technical authority and AEDC/SE for concurrences then to the RAA for approval.

13.14.1.4.6. **(Added)** If hazard analyses are applied to a system or activity that affects another organization, the implementing Government organization will coordinate with the affected Government organization. The implementing organization will show the affected organization the hazard analysis. This interchange between the two parties will occur through an ORR or other organized meeting, and will be documented in the SSP.

13.14.1.4.7. **(Added)** All hazard analyses will be revised to reflect any changes or modifications to the subject of the analysis after approval. The review and approval process will be re-accomplished for the revised hazard analyses.

13.14.1.4.8. **(Added)** A guideline for requirements and review of hazard analyses is provided in **Attachment 7**. Other methods or techniques may be applied as necessary. See **Attachment 6** for review and approval process flowchart.

13.14.2. **(Added) System Safety Analyses.**

13.14.2.1. **(Added)** Baseline Hazard Analyses (BHA).

13.14.2.1.1. **(Added)** Each BHA will be assigned a residual risk level. The RAA is the final determiner of residual risk.

13.14.2.1.2. **(Added)** Systems or groups of systems identified for purposes of hazard analysis will be chosen strategically to yield an adequate assessment of hazards for each mission phase.

13.14.2.1.3. **(Added)** A BHA will cover applicable mission phases, but at a minimum will include normal operation and maintenance activities. If maintenance is not included, the BHA description will include an explanation of the reason for exclusion.

13.14.2.1.4. **(Added)** Specific areas to be analyzed in the BHA include:

13.14.2.1.4.1. **(Added)** Hazards that components impose on the system.

13.14.2.1.4.2. **(Added)** Hazards that are imposed on the system by interfacing systems.

13.14.2.1.4.3. **(Added)** Hazards that the system imposes on interfacing systems.

13.14.2.1.4.4. **(Added)** Hazards that are imposed on the system by operators or maintainers.

13.14.2.1.4.5. **(Added)** Hazards that are imposed by the system or environment that may affect operators or maintainers (health hazards).

13.14.2.1.4.6. **(Added)** Hazards that the system imposes on the environment.

13.14.2.1.4.7. **(Added)** Hazards that result in downtime.

13.14.2.1.5. **(Added)** The BHA will 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. The interface diagram will include flow process and communication interactions of the system as well as interactions with other systems/components.

13.14.2.1.6. **(Added)** If the system, process, or facility is inactive and is projected to be inactive for at least the next 12 through 36 months at the required time of review, then no review is required, and the applicable DAF Asset Manager will promote the BHA to the "Inactive" state. If the system, process, or activity is re-activated, a complete review and approval of the applicable hazard analyses will be accomplished before commencing the associated mission phase.

13.14.2.1.7. **(Added)** Baseline Hazard Analysis Deadlines

13.14.2.1.7.1. **(Added)** Reviews and revisions to the BHA should be delivered to the DAF Asset Manager a minimum of 25 government working days before either the desired BHA approval date or the Overdue date of the BHA. Concurrence from the DAF Asset Manager is required before the BHA is delivered to AEDC/SE.

13.14.2.1.7.2. **(Added)** Reviews and revisions to the BHA should be delivered to AEDC/SE a minimum of 15 government working days before either the desired BHA approval date or the Overdue date of the BHA. Concurrence from AEDC/SE is required before the BHA is delivered to the RAA. AEDC/SE requires a minimum of 10 government working days to review each Hazard Analysis. These working days reset if AEDC/SE rejects the BHA.

13.14.2.1.7.3. **(Added)** Reviews and revisions to the BHA will be delivered to the RAA a minimum of five government working days before either the desired BHA approval date or the Overdue date of the BHA. If this schedule cannot be met, AEDC/SE will be coordinated with to determine an acceptable schedule.

13.14.2.1.8. **(Added)** BHAs will be reviewed and revised if any of the following activities have the potential to change hazards, causes, effects or mitigation measures for a facility, utility, etc.:

13.14.2.1.8.1. **(Added)** Civil Engineering

13.14.2.1.8.2. **(Added)** Maintenance and Repair

13.14.2.1.8.3. **(Added)** Restoration and Modernization

13.14.2.1.8.4. **(Added)** Construction Support

13.14.2.1.9. **(Added)** BHAs will be reviewed and revised after a mishap either determined to be an AF Mishap Classification A, B or C, or when directed by AEDC/SE. A revised BHA will be reviewed and approved by the appropriate RAA prior to continuation of work or facility activities via a Delta-ORR as appropriate.

13.14.2.2. **(Added)** System Integration Analysis.

13.14.2.2.1. **(Added)** A system integration analysis will use the Preliminary Hazard Analysis (PHA) technique for all Capital Improvements, Maintenance and Repair, and Military Construction Projects during the following phases, as a minimum; Design, Execution/Construction, and Checkout. More information about the PHA can be found in MIL-STD-882E(C1), Task 202.

13.14.2.2.2. **(Added)** The PHA is a tool that can be used to support risk mitigation by identifying hazards throughout the design process. Alternatively, other risk mitigation tools may be used in place of a PHA if approved by the AF Project Manager.

13.14.2.2.3. **(Added)** A PHA will cover applicable mission phases and analyze the following:

13.14.2.2.3.1. **(Added)** Hazards that the activity/components may impose on the system.

13.14.2.2.3.2. **(Added)** Hazards that may be imposed on the system by interfacing systems.

13.14.2.2.3.3. **(Added)** Hazards that the system may impose on interfacing systems.

13.14.2.2.3.4. **(Added)** Hazards that may be imposed on the system by operators or maintainers.

13.14.2.2.3.5. **(Added)** Hazards that may be imposed by the system or environment that may affect operators or maintainers (health hazards).

13.14.2.2.3.6. **(Added)** Hazards that the system may impose on the environment.

13.14.2.2.4. **(Added)** A PHA can eventually become a Baseline Hazard Analysis (BHA). A PHA may not become a BHA if there are no mitigation measures.

13.14.2.2.4.1. **(Added)** Upon exit of a Critical Design Review (CDR) a PHA with mitigation measures will become a Preliminary Baseline Hazard Analysis (PBHA).

13.14.2.2.4.2. **(Added)** After the CDR, a PBHA is a living document that can have its mitigation measures updated until presented to the Verification Readiness Review (VRR).

13.14.2.2.4.3. **(Added)** Upon exit of a VRR the PBHA will be verified and finalized. All Mitigation Measures that are to be verified via the performance of work will be accounted for and discussed during VRR.

13.14.2.2.4.4. **(Added)** Verification and finalization of the PBHA will be accomplished via a Physical Configuration Audit (PCA). If the verification of the system was a success, then all MMs are now considered verified. and upon exit of the PCA the PBHA will be used to create a Baseline Hazard Analysis to be submitted for review.

13.14.2.3. **(Added)** Other Hazard Analyses. Situations may arise where a BHA does not seem applicable, but a hazard analysis is warranted. In such cases, a hazard analysis will still be prepared. AEDC/SE, in coordination with the RAA, will determine the appropriate review cycle for the analysis.

13.14.3. **(Added) Baseline Safety Report (BSR).**

13.14.3.1. **(Added)** The BSR is a compilation of BHAs that constitutes the hazards associated with the specific operation of a facility or utility. It includes at least one BHA for each system to be operated and/or maintained. A BSR will be assigned a residual risk level which will be that of the highest residual risk level BHA as a minimum. A formal SRB for a specific test will incorporate the BSR's for all needed facilities and utilities to help identify test risks.

13.14.3.2. **(Added)** Delivery to the AEDC/SE of the initial BSR and any revision should be a minimum of 15 government working days before the desired BSR approval date. At the time of delivery to the AEDC/SE, all associated BHAs must have concurrence from the AF Asset Manager.

13.14.3.3. **(Added)** A review of the BSR for the operation and maintenance of a facility, utility, or system will occur at least every 36 months. This review will be conducted by the appropriate AF Asset Manager. AEDC/SE will be notified of the review completion and should be at least 15 government working days prior to the three-year anniversary.

13.14.3.4. **(Added)** A revision to the BSR will be required whenever:

13.14.3.4.1. **(Added)** An attached BHA is revised and approved separately from the BSR, and the BHA residual risk level is higher than the BSR risk level.

13.14.3.4.2. **(Added)** A new BHA approved separately from the BSR is attached to the BSR and the BHA residual risk level is higher than the BSR risk level.

13.14.3.4.3. **(Added)** Directed by the DAF Asset Manager, DAF Project Manager, or AEDC/SE. This direction may be made if a revised or new BHA is attached to the BSR but doesn't meet the BSR revision requirements in this publication.

13.14.3.5. **(Added)** The Summary Description in a BSR will include as a minimum a brief description of the facility/utility covered by the BSR.

13.14.3.6. **(Added)** BSRs will include documentation of BHAs and other safety related information. Attachments will include as a minimum, a diagram showing the systems that comprise the BSR and interfaces.

13.14.3.7. **(Added)** All BHAs included in the BSR will not be Overdue for the duration of the activity unless waived per **Attachment 8**.

13.14.3.8. **(Added)** Special attention must be given to communicating newly identified hazards and mitigation measures to exposed workers. Supplemental analyses will be performed, as appropriate, for projects involving hazardous materials or operations if hazard risk was not assessed in the initial or phase-reviewed analysis.

13.14.3.9. **(Added)** If a series of related activities is going to be performed, only one BSR will be required as long as the hazards associated with those activities remain the same. If the activities are going to be performed outside the parameters for which the original BSR was prepared, a new BSR will be required if the residual risk changes to a higher level (e.g., LOW to MEDIUM). If, during the activity, anything changes from the original scope described, a new BSR is required if the residual risk level changes to a higher level.

13.14.3.10. **(Added)** A guideline for requirements and review of BSRs is found in **Attachment 8**.

13.14.4. **(Added) Baseline Safety Review Board (BSRB).**

13.14.4.1. **(Added)** A formal BSRB will be required for all facility operations or checkouts after major maintenance, improvements, modernization, restoration, and mishaps.

13.14.4.1.1. **(Added)** As part of the review process, the units will ensure that the appropriate safety plan authors, reviewers and approvers have signed the safety planning documents during the safety review process. This can be done via a locally generated form, workflow process or other electronic review.

13.14.4.1.2. **(Added)** During the Review Phase the locally developed process will include a method for capturing the BSRB members' signatures, to include the BSRB Chair, operations reviewer, technical experts and any additional reviewers as deemed by the BSRB chair. These signatures are required before the Coordination and Approval Phase is accomplished. The BSRB Chair may elect to fulfill this requirement by coordinating the final safety plan with all other BSRB members for their agreement with its content and thus the BSRB Chair's signature represents all BSRB members. As the final step in the system safety process, the approval signature from the RAA must be obtained.

13.14.4.2. **(Added)** Subsequent (delta) formal BSRBs will be held if the residual risk changes to a higher risk level (e.g. low to medium).

13.14.4.3. **(Added)** Formal BSRB attendee signatures will be captured on the AEDC Form 5001, or equivalent. It will be attached to the appropriate BSR when the risk is accepted.

13.14.4.4. **(Added)** After a formal BSRB a readiness review can be held if deemed appropriate by the RAA.

13.14.4.5. **(Added)** BSRB Members will conduct a review of the Hazard Analysis(s) and how they interact with the other systems within the BSR they are set to become a part of. AEDC/SE and board members will have a minimum of 10 working days prior to the conduct of a formal BSRB unless previously coordinated with AEDC/SE

13.14.4.6. **(Added)** BSRB Chair is the same person(s) as an SRB chair laid out in AFTCI91-202_AEDCSUP.

GRANT A. MIZELL, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

(Added) 29 CFR 1910, *Occupational Safety and Health Standards*

(Added) 40 CFR 68, *Chemical Accident Prevention Provisions*

(Added) DAFI 91-202_AFMCSUP, *The US Air Force Mishap Prevention Program*, 22 Sept 2024

Prescribed forms

None

Adopted Forms

(**Added**) AEDC Form 905, *Test / Operational Readiness Review Record*

Abbreviations and Acronyms

(Added) AEDC—Arnold Engineering and Development Complex

(Added) AFRIMS—Air Force Records Information Management System

(Added) BHA—Baseline Hazard Analysis

(Added) BSR—Baseline Safety Reports

(Added) DAF—Department of the Air Force

(Added) ECD—Estimated Completion Date

(Added) FMEA—Failure Modes and Effects Analysis

(Added) FTA—Fault Tree Analysis

(Added) ORR—Operational Readiness Reviews

(Added) PHA—Preliminary Hazard Analysis

(Added) RAA—Risk Approval Authority

(Added) RDS—Records Disposition Schedule

(Added) SCA—Sneak Circuit Analysis

(Added) SDS—Safety Data Sheet

(Added) SRB—Safety Review Board

(Added) SSP—System Safety Plan

(Added) STPA—Systems Theoretic Process Analysis

Office Symbols

(Added) AEDC/CC—AEDC Commander

(Added) AEDC/SE—AEDC Safety Branch

(Added) AEDC/SES—AEDC System Safety

Terms

(Added) Acceptable Risk—Risk that the appropriate acceptance authority is willing to accept without additional mitigation.

(Added) Active Facility—Any facility that is either operating or ready for operations in either a full or partial capacity/capability. Facilities identified as "mothballed, closed, or abandoned" are inactive. See Appendix B in AEDC-STD-CM1.

(Added) Ameliorator—Mitigation measures 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. Other ameliorators include automatic sprinklers and fire extinguishers, some PPE, emergency preparedness, availability of first-aid kits, seat belts, containment basins, etc. Ameliorators never lower the probability of risk.

(Added) Asset—Systems, subsystems, and components owned by the sponsoring facility. See AEDC-STD-CM1 for additional guidance.

(Added) Baseline Hazard Analysis (BHA)—An analysis used to document known hazards concerned with the normal day-to-day activities of a system, subsystem, or facility. These activities include operations, calibrations, pre-and post-operations, maintenance, or any other activities as outlined in the mission phases. A single BHA constitutes the System Safety Plan (SSP) for the system, subsystem, or facilities as applied in the analysis.

(Added) Baseline Safety Report (BSR)—A compilation of all baseline hazard analyses for a facility, 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. A BSR constitutes the System Safety Plan (SSP) for the facility, process, utility, etc. (Added)**Cause**— The circumstance or action (mechanism, trigger or initiator) that leads to the hazard's occurrence. It may be a failure mode, operator error, or out-of-limit condition.

(Added) Confined Space—A space large enough and configured so a worker can bodily enter and perform assigned work; has limited or restricted means for entry or exit (for example: tanks, vessels, silos, storage bins, hoppers, vaults, manholes, pits, etc.); and is not designed for continuous human occupancy. Refer to OSHA 29 CFR 1910.146 and IAW AFMAN91-203.

(Added) Critical Effect—An effect that has been reduced from a residual risk level HIGH or MEDIUM to a residual risk level MEDIUM or LOW via the application of mitigation measures.

(Added) Data Compromise—An event that results in data that are inaccurate, lost, or otherwise corrupted.

(Added) Division/Group—The division/group providing the facilities, equipment, or personnel to conduct an activity.

(Added) Division/Group Commander/Division Director—The highest-ranking individual at the division/group. This individual has responsibility for the personnel, equipment and/or facilities for accomplishing the activity, and is the individual responsible for reporting mishaps involving the facilities.

(Added) Downtime—Time that a system, piece of equipment or facility is unavailable to support its intended function.

(Added) Effect—The outcome to be avoided or consequence of hazard. It identifies whom or what resources (target) will be injured, damaged, or destroyed if the hazard occurs.

(Added) Energy Trace Analysis—An analysis technique that addresses all sources of controlled and uncontrolled energy that have the potential to cause damage. It evaluates the energy source, the adequacy of any barriers or controls within the energy path, the human factors interface and the targets of uncontrolled energy flow. This technique only complements other techniques.

(Added) Environmental Impact—An adverse change to the environment wholly or partially caused by the system or its use.

(Added) Failure Modes and Effects Analysis (FMEA)—An analysis technique utilizing an inductive (bottom-up) analytical method performed at the functional or piece-part level to identify single point failures and the corresponding effects.

(Added) Fault Tree Analysis (FTA)—An analysis technique utilizing a deductive (top-down) detailed failure investigation of the systems to determine component hazard modes, causes of the hazards and resultant effects to the system and its operation using Boolean logic to combine a series of lower-level events. It is a graphical representation of events that begins with a hazard at the top of a hierarchical tree.

(Added) Geographically Separated Unit (GSU)—Any Air Force unit that is geographically separated beyond a reasonable commuting distance from its parent base.

(Added) Hazard Analysis (HA)—An analysis performed to determine how a device, task, location, system, subsystem, interfacing system operation, and human involvement 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 mitigation measures are implemented. Hazard analyses are categorized as baseline or barrier and maybe further broken down as system, subsystem, or operational and support.

(Added) Hazard Probability—The probability, expressed in quantitative or qualitative terms, that a hazard would result in a mishap of given consequence.

(Added) 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.

(Added) 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.

(Added) High Level Mitigation Measure—Actions taken to reduce the risk of occurrence of a hazard from initial risk level HIGH or MEDIUM to residual risk level lower than initial risk level. These are often shorthanded to High Level Mitigation Measures.

(Added) Initial Risk—The first assessment of the potential risk of an identified hazard. Initial risk establishes a fixed baseline for the hazard.

(Added) Interface Hazard—A hazard posed by one system/subsystem/operation upon another or the same system/subsystem/operation.

(Added) 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, facility, or product pass during its lifetime.

(Added) Mission Phase—Activities during specific phases of the lifecycle of a system for which a hazard analysis is being performed (i.e., operations, maintenance, pre-ops, post-ops, buildup, storage, transport, startup, shutdown, emergency stop, etc.). Mission phases are used to organize a hazard analysis into the logical processes being evaluated. **Note:** The risk for individual hazards may vary between mission phases.

(Added) Mitigation Measure—Action required to eliminate the hazard or when a hazard cannot be eliminated, reduce the associated risk by lessening the severity of the resulting mishap or lowering the likelihood (probability) that a mishap will occur. (MIL-STD-882E). These are also referred to as a countermeasure or a control/safety measure. Hazards are "Controlled" through Mitigation (e.g., reducing probability) or Amelioration (e.g., reducing severity).

(Added) Operational Readiness Review (ORR)—A meeting to determine the readiness for releasing a facility/system/process for operations, including reviewing the associated system safety plan to ensure hazards are identified; then eliminated, minimized, or controlled to a risk level accepted by the RAA.

(Added) Overdue—The state a Hazard Analysis goes into when a new revision is required and has not been at the proper acceptance level.

(Added) Preliminary Hazard Analysis (PHA)—A semi-quantitative analysis technique performed to identify safety critical areas within a system, identify and roughly evaluate hazards, and begin to consider safety design criteria. A PHA is performed during the conceptual design and design phases.

(Added) Preliminary Baseline Hazard Analysis (PBHA)—A working analysis that documents all known and perceived hazards concerned with the normal day-to-day activities of a system, subsystem, or facility. These activities include operations, calibrations, pre-and post-operations, maintenance, or any other activities as outlined in the mission phases. Once the system is checked out and approved this document will become a BHA.

(Added) Probability—An expression of the likelihood of occurrence of a mishap. The probability of the occurrence is the combination of the hazardous situation occurring coupled with that situation causing harm/damage.

(Added) Probability Interval—The period for which a system is evaluated for the occurrence of potential hazards.

(Added) Process—Collection of assets that make up a designated process. Processes are typically designated test cells and process air plants; however, processes are also individual buildings.

(Added) Residual Risk—The remaining mishap risk that exists after all mitigation measures have been implemented or exhausted, in accordance with the system safety order of precedence. It is the sum of the acceptable risk and unidentified risk.

(Added) Risk—A combination of the severity of the mishap and the probability that the mishap will occur. Risk for a given hazard varies from target to target, with size of the exposed population, from mission phase to mission phase, and with exposure duration. Always assess the risk for the worst-credible severity outcome.

(Added) Risk Acceptance Authority (RAA)—The Government representative responsible for accepting the activity risk, system/process risk, ORR results, and approving the activity to proceed with any residual risk.

(Added) Risk Assessment Matrix—A tool that assigns risk level based on threshold values established for severity and probability.

(Added) Risk Level—An expression of the danger posed by a hazard in terms of the severity of outcome and the probability of occurrence. Risk level is assigned to a hazard or to a combination of hazards. As such, risk levels are assigned to both a system event and the whole system.

(Added) 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.

(Added) Safety Data Sheet (SDS)—A fact sheet provided by the manufacturer or supplier of a hazardous material. The SDS describes a material's hazards in sufficient detail to develop proper storage, use, and handling procedures.

(Added) Severity—The magnitude of potential consequences of a mishap to include death, injury, occupational illness, damage to or loss of equipment or property or damage to the environment.

(Added) Sneak Circuit Analysis (SCA)—An analysis technique used to evaluate electronic circuits and electro-mechanical systems by employing recognition of topological patterns to uncover latent circuits (sneak paths) and conditions that inhibit desired functions or cause unwanted actions, without a component having failed.

(Added) Subsystem—A grouping of items satisfying a logical group of functions within a particular system.

(Added) System—The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function within a stated environment with specified results.

(Added) System Safety Order of Precedence—Alternative mitigation approaches listed in order of decreasing effectiveness. (1) Eliminate hazards through design selection; (2) Reduce risk through design alteration; (3) Incorporate engineered features or devices; (4) Provide warning devices; (5) Incorporate signage, procedures, training, and PPE.

(Added) System Safety Plan (SSP)—Safety documentation used to provide an overall risk assessment and to inform and obtain management concurrence regarding the safety and risk of an activity. The SSP contains a single BHA or a BSR depending on the activity assessed.

(Added) 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, to reduce the associated mission risk.

(Added) System Safety Evaluator—Senior-level individual responsible for assuring adequate hazard analysis and implementation of system safety requirements in each area (turbines, aircraft, space, utilities, etc.).

(Added) 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, operations and maintenance, acquisition, use and disposal of DoD weapon systems, subsystems, equipment, and facilities.

(Added) System Safety Preparer—Person responsible for performing a hazard analysis on a system.

(Added) Systems Theoretic Process Analysis (STPA)—An analysis technique that identifies unsafe control actions (source controller, type, control action, and context) of the system, causal factors (how accident could happen) and control flaws to formulate a causal scenario and then defining the controls and mitigations for the scenarios. This technique treats safety as a control problem, rather than as a failure problem by modeling accident causation and outlined on a functional control diagram of the system.

(Added) Target—Asset affected by the mishap scenario under consideration. Targets considered at AEDC are Personnel Injury/Loss (P), Equipment Loss (E), Environmental (V), and Facility Downtime (DT).

(Added) Unidentified Risk—That risk which has not been identified but possibly identified when a mishap occurs.

(Added) Waiver—Approval from the appropriate authority to deviate from both the intent and the letter of the requirement.

Attachment 3 (Added)

AEDC RISK LEVEL MATRIX

Figure A3.1. (Added) AEDC System Safety Risk Assessment Matrix.

				SEVERITY			
				Category & Description			
				I Catastrophic	II Critical	III Marginal	IV Negligible
POTENTIAL CONSEQUENCES			Environmental	•Regulatory non-compliance and definable immediate danger to environment •Release not captured prior to compliance point with biological impact (flora or fauna) NOV with fine > $10K •Remedial actions > $500K	•Release more than CERLA/EPCRA/RCRA quantity reportable (RQ) •Release not captured prior to compliance point without biological impact, NOV with compliance order of fines up to $10K •Remedial actions $25K - $500K	•Release of non-reportable quantity, captured prior to compliance point •Administrative NOV without fines •Remedial actions $5K - < $25K	•No Federal or State permit violations •Release contained at site of release •Remedial actions < $5K
			Personnel Injury/Illness	Fatality or permanent total disability	Severe injury, permanent partial disability	Minor injury, medical treatment requiring lost workdays	Superficial injury, little/no first aid required, has restricted duties
			Equipment Loss	≥ $10M	$1M to < $10M	$100,000 to < $1M	< $100,000
			Facility Downtime	> 6 Months	> 1 Month to 6 Months	1 Week to 1 Month	< 1 Week
PROBABILITY	A		Frequent $>10^{-1}$	HIGH			
	B		Probable $\leq 10^{-1}$ but $>10^{-2}$				
	C		Occasional $\leq 10^{-2}$ but $>10^{-3}$		MED		
	D		Remote $\leq 10^{-3}$ but $>10^{-6}$			LOW	
	E		Improbable $\leq 10^{-6}$				

Table A3.1. (Added) Probability Definitions.

LEVEL	DESCRIPTION	DEFINITION	1 FAILURE IN # CYCLES
A	Frequent	Very likely to occur during the probability interval of the analysis (activity/operation).	< 10
B	Probable	Likely to occur during the probability interval of the analysis (activity/operation).	10 - 99
C	Occasional	Some likelihood to occur during the probability interval of the analysis (activity/operation) but not expected.	100 - 999
D	Remote	Unlikely to occur during the probability interval of the analysis (activity/operation).	1,000 -999,999
E	Improbable	Highly unlikely to occur during the probability interval of the analysis (activity/operation).	1M - 100M

Attachment 4 (Added)

SYSTEM SOFTWARE CRITICALITY

Table A4.1. (Added) System Software Criticality Index.

		SOFTWARE CONTROL CATEGORY				
		E (5)	D (4)	C (3)	B (2)	A (1)
SEVERITY CATEGORY	Catastrophic (1)	SwCI 5	SwCI 3	SwCI 2	SwCI 1	SwCI 1
	Critical (2)	SwCI 5	SwCI 4	SwCI 3	SwCI 2	SwCI 1
	Marginal (3)	SwCI 5	SwCI 4	SwCI 4	SwCI 3	SwCI 3
	Negligible (4)	SwCI 5	SwCI 4	SwCI 4	SwCI 4	SwCI 4

Table A4.2. (Added) Software Category Descriptions.

SOFTWARE CONTROL CATEGORY DESCRIPTIONS		
LEVEL	**NAME**	**DESCRIPTION**
A (1)	Autonomous (AT)	•Software functionality that exercises autonomous control authority over potentially safety-significant hardware systems, subsystems, or components without the possibility of predetermined safe detection and intervention by a control entity to preclude the occurrence of a mishap or hazard. *(This definition includes complex system/software functionality with multiple subsystems, interacting parallel processors, multiple interfaces, and safety-critical functions that are time critical.)*
B (2)	Semi-Autonomous (SAT)	•Software functionality that exercises control authority over potentially safety-significant hardware systems, subsystems, or components, allowing time for predetermined safe detection and intervention by independent safety mechanisms to mitigate or control the mishap or hazard. *(This definition includes the control of moderately complex system/software functionality, no parallel processing, or few interfaces, but other safety systems/mechanisms can partially mitigate. System and software fault detection and annunciation notify the control entity of the need for required safety actions.)* •Software item that displays safety-significant information requiring immediate operator entity to execute a predetermined action for mitigation or control over a mishap or hazard. Software exception, failure, fault, or delay will allow, or fail to prevent, mishap occurrence. *(This definition assumes that the safety-critical display information may be time-critical, but the time available does not exceed the time required for adequate control entity response and hazard control.)*
C (3)	Redundant Fault Tolerant (RFT)	•Software functionality that issues commands over safety-significant hardware systems, subsystems, or components requiring a control entity to complete the command function. The system detection and functional reaction includes redundant, independent fault tolerant mechanisms for each defined hazardous condition. *(This definition assumes that there is adequate fault detection, annunciation, tolerance, and system recovery to prevent the hazard occurrence if software fails, malfunctions, or degrades. There are redundant sources of safety-significant information, and mitigating functionality can respond within any time-critical period.)* •Software that generates information of a safety-critical nature used to make critical decisions. The system includes several

		redundant, independent fault tolerant mechanisms for each hazardous condition, detection, and display.
D (4)	Influential (INF)	•Software generates information of a safety-related nature used to make decisions by the operator but does not require operator action to avoid a mishap.
E (5)	No Safety Impact (NSI)	•Software functionality that does not possess command or control authority over safety-significant hardware systems, subsystems, or components and does not provide safety-significant information. Software does not provide safety-significant or time sensitive data or information that requires control entity interaction. Software does not transport or resolve communication of safety-significant or time sensitive data.
NOTE: This table is modified from the MIL-STD-882E counterpart. It changes the levels of 1 through 5 to A through E to keep in line with the rest of AEDC Standards.		

Table A4.3. (Added) Levels of Rigor (LOR) Tasks.

RISK LEVEL	LEVEL OF RIGOR TASKS
HIGH	Program will perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing. Provide documentation to AEDC/SE.
MEDIUM	Program will perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
LOW	Program will conduct safety-specific testing. Unless Software Control Category is E; then no safety specific analysis or verification is required.

Table A4.4. (Added) Software LOR Tasks and Risk Assessment/Acceptance.

RISK LEVEL	SOFTWARE LOR TASKS and RISK ASSESSMENT/ACCEPTANCE
HIGH	If High LOR tasks are unspecified or incomplete, the contributions to be documented as HIGH and provided to the PM for Decision. The PM will document the decision of whether to expend the resources required to implement LOR tasks or prepare a formal risk assessment for acceptance of a HIGH risk.
MEDIUM	If Med LOR tasks are unspecified or incomplete, the contributions to the system risk will be documented as MEDIUM and provided to the PM for decision. The PM will document the decision of whether to expend the resources required to implement Med LOR tasks or prepare a formal risk assessment for acceptance of a MEDIUM risk.
LOW	If Low LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as LOW and provided to the PM for decision. The PM will document the decision of whether to expend the resources required to implement Low LOR tasks and prepare a formal risk assessment for acceptance of a LOW risk. If SCC of E, a risk assessment for a LOW risk is still required.

Attachment 5 (Added)

PROBABILITY INTERVAL GUIDELINES

A5.1. (Added) 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 Baseline Safety Report (BSR).

A5.2. (Added) The probability component has meaning *only* if it is associated with operating duration or a specific number of operations that represent system exposure to the hazard.

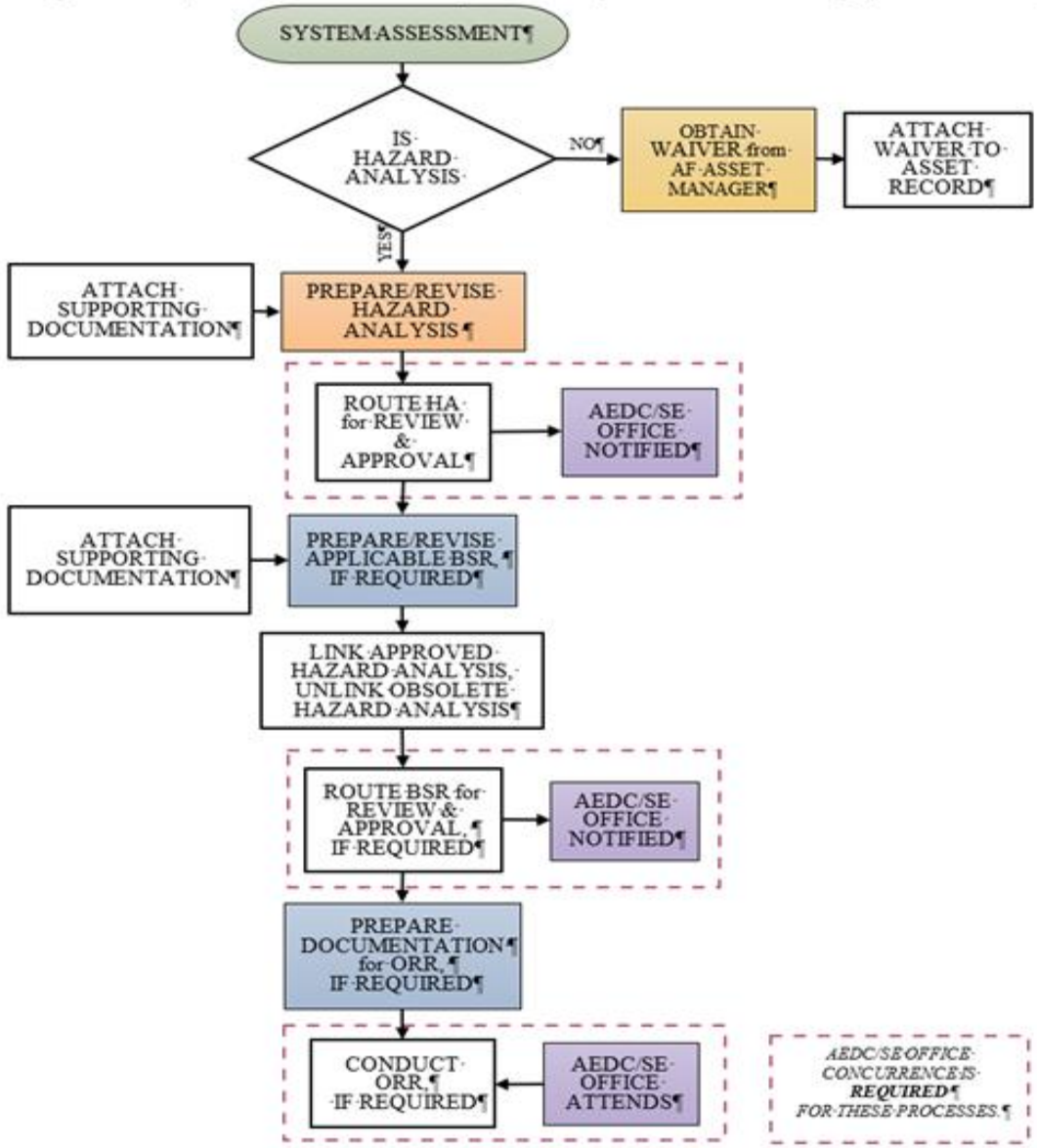
Table A5.1. (Added) Probability Intervals.

EXPOSURE	PROBABILTY INTERVAL
Facility computer systems	10 years maximum
Facility and utility service equipment	Same as activity being supported; otherwise, 30-year system life or remaining useful life of the system.
Personnel	Same as activity being supported; otherwise, 30-year system life or remaining useful life of the system. For all Confined Spaces, 30-year system life or remaining useful life of the system.

Attachment 6 (Added)

SYSTEM SAFETY RISK ASSESSMENT APPROVAL PROCESS

Figure A6.1. (Added) Flowchart for System Safety Risk Assessment Approval Process.



Attachment 7 (Added)

HAZARD ANALYSIS REVIEW GUIDELINE AND QUALITY CHECKS

A7.1. (Added) FrontPage/Details.

A7.1.1. **(Added)** Confirm the Process and Parent Asset(s), at a minimum, are connected. If other assets are addressed in the HA confirm they are connected.

A7.1.2. **(Added)** Check the History link for previous comments. Ensure comments have been adequately addressed.

A7.1.3. **(Added)** Check the Attachments link to verify appropriate block diagrams and/or pictorial sketches/schematics to review the system are attached. A thorough system analysis can't be performed without a schematic, and a thorough interface analysis can't be performed without a block diagram.

A7.1.3.1. **(Added)** Use the block diagram/pictorial representation (pictures, schematics/sketches, etc.) to list mission phases and obvious hazards. This should be descriptive enough to depict the system and the system interfaces.

A7.1.3.2. **(Added)** The block diagram/pictorial representation should show the interface points (where the system starts and stops) and the interaction in and out of the system.

A7.1.4. **(Added)** Check the Preliminary Error Check link and confirm no errors exist.

A7.1.5. **(Added)** Confirm the Description explains the system, interfaces, potential hazard sources, etc. well enough to understand the scope of the analysis and the potential associated hazards.

A7.1.5.1. **(Added)** The description should explain the scope of the analysis.

A7.1.5.2. **(Added)** Confirm the block diagram/pictorial represents the described system.

A7.1.5.3. **(Added)** Does the description explain the flow of the process(s) involved with the system?

A7.1.6. **(Added)** Verify the Summary of Revision contains adequate information describing what was updated for the revision. If no changes were made, verify a reason is provided to support the no changes required status. Verify the revision history is retained for the life of the HA.

A7.1.7. **(Added)** Confirm the major system components are listed.

A7.1.8. **(Added)** Confirm the energy sources are identified, including quantifying data for each source (i.e., 4000 psig HPA, 13.8 kV, 1000°F Air, etc.).

A7.1.9. **(Added)** Verify the system and human interfaces are stated as compared to the block diagram/pictorial representation. All interfaces should be listed, and at a minimum, the flow process directions indicated on the block diagram/pictorial representation.

A7.1.10. **(Added)** If the home details page indicates that lasers or confined spaces are included in the HA, confirm they are separated as independent mission phases. If they are not addressed in stand-alone mission phases, confirm the appropriate mission phase description identifies the assessment of laser or confined spaces is included.

A7.1.11. **(Added)** Confirm the location (building, area, etc.) of the system/systems addressed in the HA.

A7.1.12. **(Added)** Verify the purpose of the HA and the system/system(s) is adequately stated.

A7.1.13. **(Added)** Confirm all assumptions are clearly stated, e.g.:

A7.1.13.1. **(Added)** Describe or explain anything that adds value to the review and that the reviewer would not ordinarily know. 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.

A7.1.13.2. **(Added)** Obvious things that are not in the analysis should be explained, such as: down time was not analyzed because, Maintenance is not included as a mission phase due to, obvious hazards were not analyzed because..., or hazards associated with XXX are addressed in their respective HAs.

A7.1.13.3. **(Added)** Verify all reference documentation is active and approved.

A7.1.14. **(Added)** Ensure all work instructions/procedures referenced in the mitigation measures are listed in the "Work Instructions Referenced" section, to include numerical descriptor and title. And confirm the documentation is active and approved.

A7.2. (Added) Mission Phases.

A7.2.1. **(Added)** Verify all appropriate mission phase are included for the analyses. Typically, Operations and Maintenance are the two phases that will be included at a minimum.

A7.2.2. **(Added)** IF maintenance is not included in the analysis, the assumptions section must explain why it's omitted.

A7.2.3. **(Added)** Risk may vary from phase to phase for some hazards present during different mission phases. Risk may be low in pre-ops but high in post-ops.

A7.2.4. **(Added)** Confirm mission phase are clearly defined. Descriptions should be a detailed scope of the mission phase being analyzed. Not a repeat of the mission phase title.

A7.3. (Added) Hazards (sources).

A7.3.1. **(Added)** Check that the hazard is truly a hazard, with an adequate explanation/description of the hazard.

A7.3.2. **(Added)** Perform an initial evaluation of the risk scenarios of the hazard; to include, personnel harm, equipment damage, downtime, and environmental damage.

A7.3.3. **(Added)** Does the mission phase include all hazards obvious from a review of the block diagram and/or pictorial sketches/schematics?

A7.3.4. **(Added)** Do the hazards for the mission phase belong under the mission phase such, as discussing post operational hazards in the operating phase?

A7.3.5. **(Added)** Do the hazards include quantifiers when needed? Such as, proper hearing protection depends on noise level (Hazard – Excessive Noise, Exposure to > 85 dB). For very high noise levels, personnel exposure may have to be time limited.

A7.4. (Added) Causes (mechanisms).

A7.4.1. **(Added)** Verify each cause is assessed separately. Causes will not be combined unless they can be controlled/eliminated via the same mitigation measures and present the same probability level.

A7.4.2. **(Added)** Is there enough explanation of the cause to understand what could cause the hazard to happen?

A7.4.3. **(Added)** Does the cause adequately describe the risk scenario?

A7.4.4. **(Added)** Do the causes include quantifiers when needed?

A7.5. (Added) Effects and Targets (outcomes).

A7.5.1. **(Added)** Does the target description adequately explain the result of the hazard? For example, if the target is personnel, what is the injury that could result from the mishap/hazard?

A7.5.2. **(Added)** Ensure a specific description is provided. The target title will not be repeated only.

A7.5.3. **(Added)** Verify each effect/target is assessed separately. For example, do not include both equipment and personnel in the same description.

A7.5.4. **(Added)** Does the target really relate to the hazard/cause?

A7.5.5. **(Added)** Does Equipment, Personnel, Environmental, Downtime belong as a target?

A7.5.6. **(Added)** For the hazard/cause, are all relevant targets included? Was one left out or analyzed without explanation?

A7.6. (Added) Pre-Assessment Check.

A7.6.1. **(Added)** Confirm the hazard/cause/effect relationships make sense for this system and mission phases. Do they stand alone (not require further explanation)?

A7.6.2. **(Added)** Ensure Downtime (DT) is assessed as follows:

A7.6.2.1. **(Added)** If the risk level for Downtime BEFORE implementation of mitigation measures is HIGH or MEDIUM, then Downtime must be fully assessed as a target.

A7.6.2.2. **(Added)** If the risk level for Downtime BEFORE implementation of mitigation measures is LOW, then Downtime does not have to be fully assessed as a target. Instead, this statement will be added as a separate mitigation measure block of the corresponding Equipment target:

A7.6.2.2.1. **(Added)** "Based on an ending probability of ___ for equipment loss/damage and an initial severity of ___ for DT, the resulting risk level for DT is assessed as LOW and no further analysis is required."

A7.6.2.2.2. **(Added)** However, if the analyst feels that a recommendation is necessary to mitigate Downtime, then the Downtime target will be assessed.

A7.6.2.3. **(Added)** The initial probability for Downtime will match the ending probability for its Equipment companion.

A7.6.2.4. **(Added)** The probability of Downtime can't be reduced since the event has occurred, only the severity can be mitigated. Examples of mitigation measures for Downtime are spare parts, time to replace components, redundant systems, specialized training, etc.

A7.6.2.5. **(Added)** Does the description of Downtime apply to the hazard/cause being evaluated?

A7.6.2.6. **(Added)** Mitigation measures used to reduce Equipment risk will not be used again to further reduce the corresponding Downtime.

A7.6.2.7. **(Added)** For each Equipment target there should be a Downtime target or an explanation as explained in VI.2.b above.

A7.6.2.8. **(Added)** If Downtime is associated with an Equipment target assessed as HIGH then a High-Level Downtime mitigation measure does not have to be selected.

A7.7. (Added) Beginning: Severity, Probability, Risk Levels.

A7.7.1. **(Added)** Confirm the beginning severity and probability make sense for the hazard/cause/effect scenario. The beginning assessment is analyzed without mitigation measures in place. Ensure the severity and probability are consistent with the hazard/cause/effect scenario (i.e., Severity is assigned II, but effect indicates death (i.e., Severity I).

A7.7.2. **(Added)** Verify the severity reflects the worst-case credible scenario

A7.7.3. **(Added)** Verify the Probability is determined the most accurate method (fault tree, data, published information, engineering judgement, etc.)

A7.8. (Added) Mitigation Measures (MMs).

A7.8.1. **(Added)** Verify the MMs provide enough description to adequately reduce the risk. Each MM must stand alone based on the description; thus, the description should be detailed enough to allow the reader to understand how it mitigates the Cause (probability) or effect (severity).

A7.8.2. **(Added)** Ensure MM's do not induce unacceptable levels of risk when they are implemented.

A7.8.3. **(Added)** Confirm all High-level MMs are traceable to a document (procedure, code, drawing, etc.)

A7.8.4. **(Added)** Ensure personnel training, use of signage, or PPE requirements are not used as the only high-level risk reduction method for any hazards initially identified as HIGH or MEDIUM RISK. If they are identified as a high-level MM, they will not be the only method used. (doubling up these types of MM's do not count)

A7.8.5. **(Added)** Verify the MMs relate to the mission phase.

A7.8.6. **(Added)** Confirm Lockout/Tagout (LOTO) MM's meet the following requirements:

A7.8.6.1. **(Added)** Ensure there is a specific procedure or document used to perform LOTO, specify how points of protection are identified.

A7.8.6.2. **(Added)** If LOTO will be developed and issued for a specific work/job to be performed, specify the critical, specific points of protection to be locked out.

A7.8.6.3. **(Added)** The analysis should detail how we are protecting personnel.

A7.8.7. **(Added)** Ensure Confined Space MMs conform to the requirements per OSHA s29 CFR 1910.146 and IAW AFMAN91-203.

A7.8.8. **(Added)** Verify noise MM's specify hearing protection for the noise level being addressed.

A7.8.9. **(Added)** Confirm Personal Protective Equipment (PPE) MMs are specific in equipment requirements and state what procedures ensure the PPE is utilized.

A7.8.10. **(Added)** Confirm training MM's provide method for verification and documentation.

A7.8.11. **(Added)** Verify hazard material MM's contain adequate description of potential exposure, MSDS availability location, identify specific training and PPE required, as well as Industrial Hygiene requirements.

A7.8.12. **(Added)** Ensure actions required in the event of an alarm are stated.

A7.8.13. **(Added)** If using work instructions or procedures as a verification for a MM, verify they contain the step(s) used to mitigate the hazard.

A7.8.14. **(Added)** Ensure any comments have been adequately addressed. Retain all Safety Office Comments.

A7.8.15. **(Added)** When using recommendations include an Estimated Completion Date and Office of Primary Responsibility.

A7.9. (Added) Verifications.

A7.9.1. **(Added)** Confirm the verification information for all High-Level MM's is as follows:

A7.9.1.1. **(Added)** Verification Description – confirm the process for ensuring how the verification of the MM will be accomplished is specified.

A7.9.1.1.1. **(Added)** Verification will describe methods to ensure the MM is in place and functioning properly.

A7.9.1.1.2. **(Added)** Explain what ensures the verification is done.

A7.9.1.2. **(Added)** Verification Interval – Specific time interval.

A7.9.1.3. **(Added)** Date Last Inspected – Verify the MM has been inspected during this revision.

A7.10. (Added) Ending: Severity, Probability, Risk Levels.

A7.10.1. **(Added)** Confirm the ending severity and probability make sense for the hazard/cause/effect scenario based on the MM applied. If ending risk level is HIGH or MEDIUM, a recommendation is considered, or an explanation must be provided why a recommendation is not appropriate.

A7.10.2. **(Added)** Verify risk level has not been reduced diagonally on the risk assessment matrix. The risk matrix is not logarithmically scaled for both probability and severity. Therefore, a factor of severity decrease is not proportional to the factor of probability decrease, which articulates hazard aversion. There are provisions for diagonal reduction, however. These are outlined in **paragraph 13.14.1.2.2.12**.

A7.10.3. **(Added)** Verify the hazard severity has not been reduced by more than one level. If it has been reduced by more than one level, confirm MMs are justified for the reduction. Also, ensure an explanation for the rationale behind the engineering judgement used for the multi-level reduction has been provided.

A7.11. (Added) Post-Assessment Check.

A7.11.1. **(Added)** Review beginning and ending severity, probability, and risk levels. If no change in both severity and probability exists, consider adding an explanation in the MM.

A7.11.2. **(Added)** Review High Level MMs are required if:

A7.11.2.1. **(Added)** Reduction in severity by one or more levels or significantly reduces probability levels (2 or more).

A7.11.2.2. **(Added)** Beginning risk was HIGH or MEDIUM.

A7.11.2.3. **(Added)** Engineering judgement is a High-level MM, depending on the criticality of the Hazard, Effect, and MM. This High-Level MM is critical to reduce risk and answers to the Verification questions are mandatory.

A7.12. (Added) Repeat A7.3. through A7.11. for each Mission Phase.

A7.13. (Added) Comments.

A7.13.1. **(Added)** Check that comments have been adequately addressed.

A7.13.2. **(Added)** 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.

A7.13.3. **(Added)** Follow your comment with your initials.

A7.14. (Added) Approval/Rejection.

A7.14.1. **(Added)** Approve or reject the analysis. If rejected, provide a brief explanation.

A7.14.2. **(Added)** Reviewer may approve the analysis with comments. This is a judgement call as to the seriousness of the issues involved. If comments are of a minor nature, the reviewer should comment that the review is approved with the understanding that comments will be addressed at the next review of the hazard.

A7.15. (Added) A Hazard analysis that has gone past its due for approval date is "Overdue."

Attachment 8 (Added)

BASELINE SAFETY REPORT GUIDELINE AND QUALITY CHECKS

A8.1. (Added) Front Page / Details page.

A8.1.1. **(Added)** Confirm Summary Description contains description of the process/activity identifies the scope.

A8.1.2. **(Added)** Confirm summery of revisions accurately depicts revision changes.

A8.1.3. **(Added)** Confirm Test Unit/Cell/Process is stated.

A8.1.4. **(Added)** Ensure all BHA's are attached and are applicable for the activity/process as described in the scope.

A8.2. (Added) Attachments.

A8.2.1. **(Added)** Verify block diagram depicting the interfacing relationships between the system/process is attached.

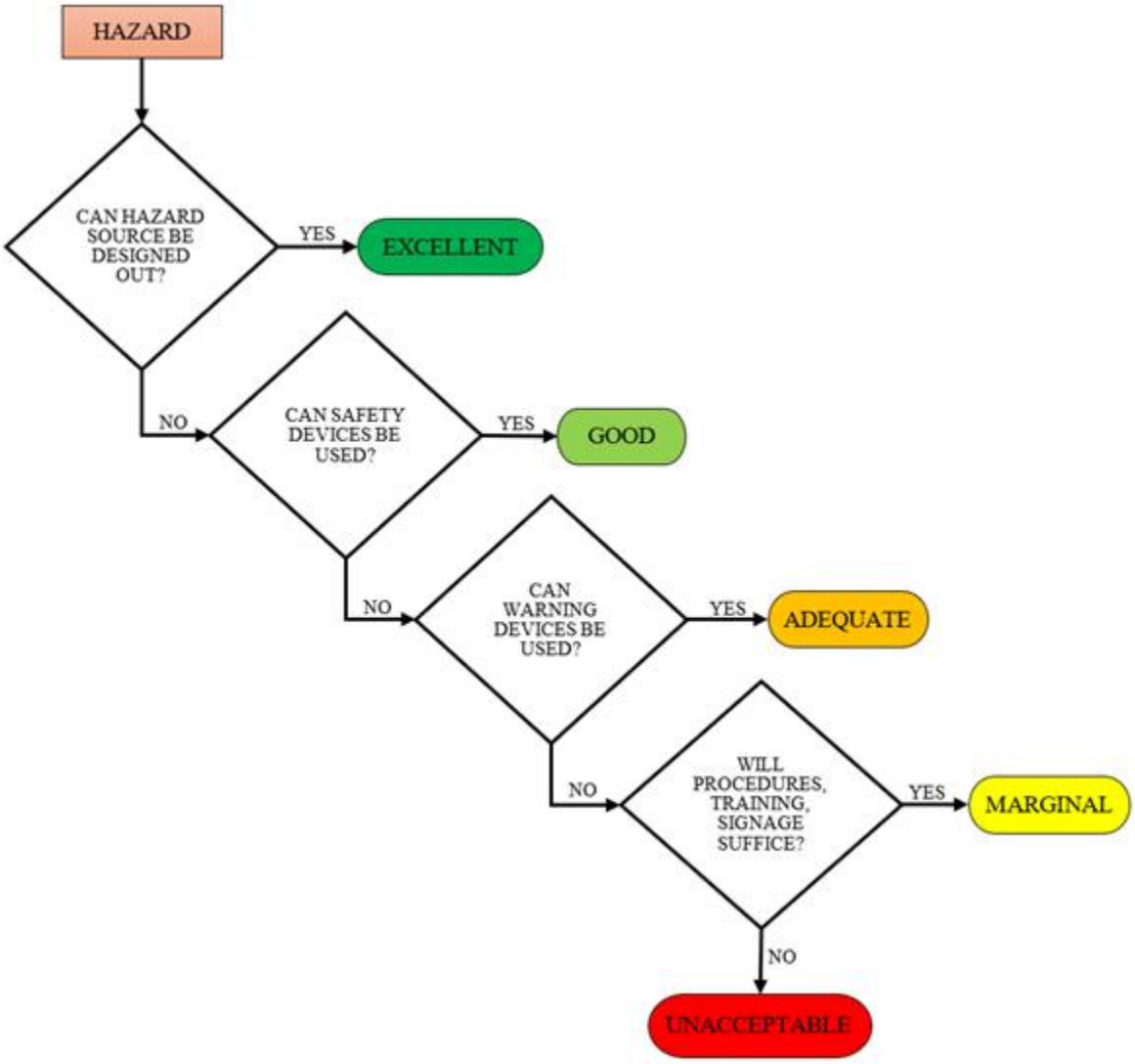
A8.2.2. **(Added)** Supporting documentation is attached.

A8.3. (Added) Baseline Safety Review(s). Confirm all hazard analyses attached to the BSR are approved.

Attachment 9 (Added)

HAZARD FLOWCHART

Figure A9.1. (Added) Hazard Flowchart.



Attachment 10 (Added)

POTENTIAL HAZARD CHECKLISTS

Table A10.1. (Added) Typical Hazard Categories and Sub-Categories.

ACCELERATION / DECELERATION				
Falling Objects	Inadvertent Motion	Slips/Trips	Falls	Fragments
ASPHYXIATES				
Insufficient O_2	Excessive N_2	Butane Or Propane		
Excessive CO_2	Other Inert Gas	Drowning		
CHEMICAL REACTION				
Fuels	Cleaning Compounds	Process Chemicals		
Explosives	Laboratory Chemicals			
CONTAMINATION				
Dirt/Dust	Pollutants	Discharge Waste	Particles	
CONTROL SYSTEM				
Sneak Circuit	Sneak Software	Power Outage		
Interference	Grounding Failure	Inadvertent Activation		
Moisture	Inadequate Controls	Facility Calibration		
CORROSION				
Bases	Oxidizers	Inorganic Acids		
ELECTRICAL				
High Voltage	Lightning Discharge	Power Outage		
Low Voltage	Electrostatic Energy	Arc Flash		
Batteries	Stored Charge	Fuel Cells		
ENVIRONMENTAL				
Flooding	Cooling	Ventilation	Egress/Ingress	
Heating	Drains	Sumps	Humidity	
EXPLOSION				
Ignition Source	Fuel System	Ordnance	High Pressure Equipment	
Reactive Materials	Compression	Propellent		
FIRE				
Fuels	Excessive O_2	Solvents Paints	Plastics	
Gases	Lubricants	Hydraulic Fluids	Wood	
HUMAN FACTORS				
Operator Error	Fatigue	Maintenance Error	Inadequate Training	
IMPACT				
Collision	Shock Wave			
MECHANICAL				
Rotating Equipment	Sharp Edges	Pinch Points	Reciprocating Equipment	
PRESSURE				
Pressurized Water	Pressurized Gas	Implosion	Vacuum	Over Pressurization
Pressurized Fluid	Pressurized Air	Hose Whip	Explosion	Trapped Pressure
RADIATION				

Ultraviolet	Infrared	Microwaves	Lasers	Ionizing
TEMPERATURE				
Hot Surfaces	Hot Fluids	Hot Exhausts	Cold Environment	
Cold Surfaces	Cold Fluids	Steam Piping		
TOXICITY				
Exhaust Fumes	Welding Fumes	SO_2		
H_2S	Solvents	Chlorine		
HCFCs	Mercury	PCBs		
Degreasers/Solvents	Corrosion Inhibitors	Methanol		
Ethylene Glycol	Asbestos	Cement		
Oil	Cadmium Compounds	Heavy Metals		
WEATHER				
Cold/Hot	Tornado	Snow/Ice		
BIOLOGICAL				
COMPONENT FAILURE				
LEAKAGE / SPILLS				
MOISTURE				
NOISE				
POWER SOURCE FAILURE				
STRUCTURAL DAMAGE				
STRUCTURAL FAILURE				
VIBRATION				