Headquarters U.S. Air Force

Integrity - Service - Excellence

16985 ESOH Risk Assessment and Acceptance – The Basics

U.S. AIR FORCE

Mr. Sherman Forbes
SAF/AQRE
sherman.g.forbes.civ@mail.mil
703-254-2480

30 October 2014
Version 7

Risk Management

- A process for identifying, evaluating, and ranking potential or observed hazards associated with a system
- DoD has formalized this process for Acquisition ESOH hazards
  - Risk Assessment
  - Risk Mitigation
  - Risk Acceptance
  - Risk Tracking
- Today focus on
  - Risk Assessment
  - Risk Acceptance

Bottom Line Up Front (BLUF)

- Risk Assessment – Process fundamentally the same for both Program cost, schedule, or performance risks or ESOH risks
  - Identify the
    - Program "future event," or
    - ESOH hazard
  - Assess, qualitatively or quantitatively, the
    - Likelihood the future event could occur and cause negative consequences, or
    - Probability that the hazard could result in a mishap
  - Assess the
    - Negative consequences of the event occurring, or
    - Severity of the consequences of the mishap occurring
- Risk Acceptance
  - Program risks must be reported at Program Reviews
  - ESOH risks must be formally accepted

Program Risk vs. ESOH Risk

- Program risks: risks to program cost, schedule and performance
  - ESOH hazards can pose risks to program cost or schedule and to system performance
  - Such ESOH risks should be tracked and reported as program risks, but managed as ESOH risks
  - For non-ESOH risks, risk management for Programs should be done in accordance with the "RIsk Management Guide For DoD Acquisition," Sixth Edition, (Version 1.0), 04 August 2006
    - This guide excludes ESOH risk management, instead referring the reader to the methodology in MIL-STD-882D, Standard Practice for System Safety
    - Provides 5 by 5 matrix of likelihood versus consequence to define risk levels of High, Medium, and Low

Program Risk vs. ESOH Risk

- "RIsk Management Guide For DoD Acquisition," Sixth Edition, (Version 1.0), 04 August 2006

Likelihood 5	🟩	🟨	🟥	🟥	🟥
4	🟩	🟨	🟨	🟥	🟥
3	🟩	🟩	🟨	🟨	🟥
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩	🟩	🟩	🟨
	1	2	3	4	5

Consequence

Red = High Risks
Yellow = Medium Risks
Green = Low Risks

Program Risk vs. ESOH Risk, Cont'd

- DoDI 5000.02 Interim, 26 Nov 2013, Enclosure 3, Section 16, Environment, Safety, and Occupational Health (ESOH)
  - "…As part of risk reduction, the Program Manager will eliminate ESOH hazards where possible, and manage ESOH risks where hazards cannot be eliminated. The Program Manager will use the methodology in MIL-STD-882E, 'DoD Standard Practice for System Safety'"
  - "Prior to exposing people, equipment, or the environment to known system-related ESOH hazards, the Program Manager will document that the associated risks have been accepted by the following acceptance authorities: the Component Acquisition Executive for high risks, Program Executive Officer-level for serious risks, and the Program Manager for medium and low risks."

Program Risk vs. ESOH Risk, Cont'd

- DoDI 5000.02 Interim, 26 Nov 2013, Enclosure 3, Section 16, Environment, Safety, and Occupational Health (ESOH)
  - "The user representative, as defined in MIL-STD-882E, must be part of this process throughout the life cycle and will provide formal concurrence prior to all serious-risk and high-risk acceptance decisions."

MIL-STD-882E

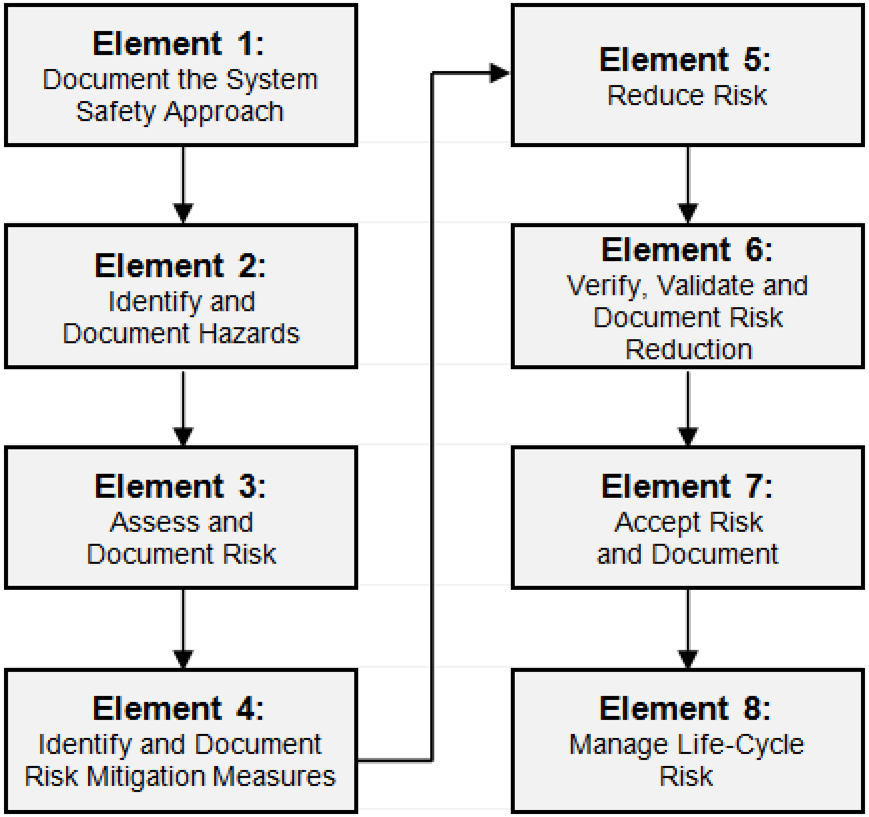


FIGURE 1. Eight elements of the system safety process

882E Identifying Hazards

- Element 1: Document the System Safety approach – for Program Offices this should occur in the Systems Engineering Plan (SEP) beginning at Milestone A
- Element 2: Identify and document hazards
  - Address system:
    - Hardware and software
    - Interfaces, to include human interfaces
    - Intended use or application
    - Operational environment

882E Identifying Hazards, Cont’d

- Element 2: Identify and document hazards, Cont’d
    - Evaluate:
        - Mishap data
        - Relevant environmental and occupational health data
        - User physical characteristics
        - User knowledge, skills, and abilities
        - Lessons learned from legacy and similar systems
        - Entire system life-cycle
        - Potential impacts to personnel, infrastructure, defense systems, the public, and the environment
    - Document identified hazards in a Hazard Tracking System (HTS)

882E Hazard Tracking System (HTS)

- Core of the MIL-STD-882E System Safety Process
- Repository for all pertinent data related to ESOH hazards, their mitigation(s), and risks
- Updated throughout life cycle as data changes or becomes known
- Mandatory HTS data include:
  - Identified hazards
  - Associated mishaps
  - Risk assessments (initial, target, event(s))
  - Identified risk mitigation measures
  - Selected mitigation measures
  - Hazard status
  - Verification of risk reductions
  - Risk acceptances

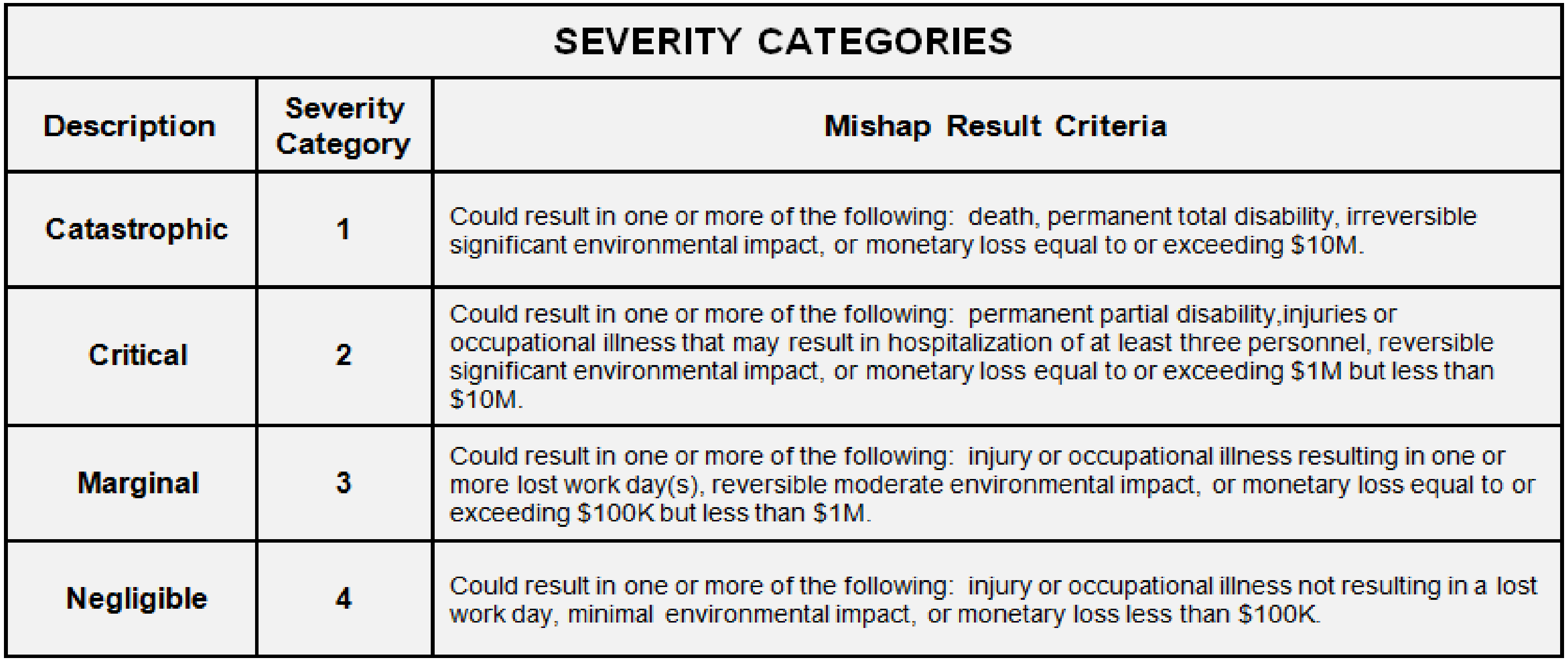
882E Hazard Tracking System (HTS), Cont'd

- Government must have "government purpose rights" to all the data recorded in a HTS
- Government publishes HTS or HTS data in the Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) document — part of the SEP beginning at Milestone B

882E Severity, Probability & Risk

4.3.3 <u>Assess and document risk.</u> The severity category and probability level of the potential mishap(s) for each hazard across all system modes are assessed using the definitions in Tables I and II.

TABLE I. Severity categories

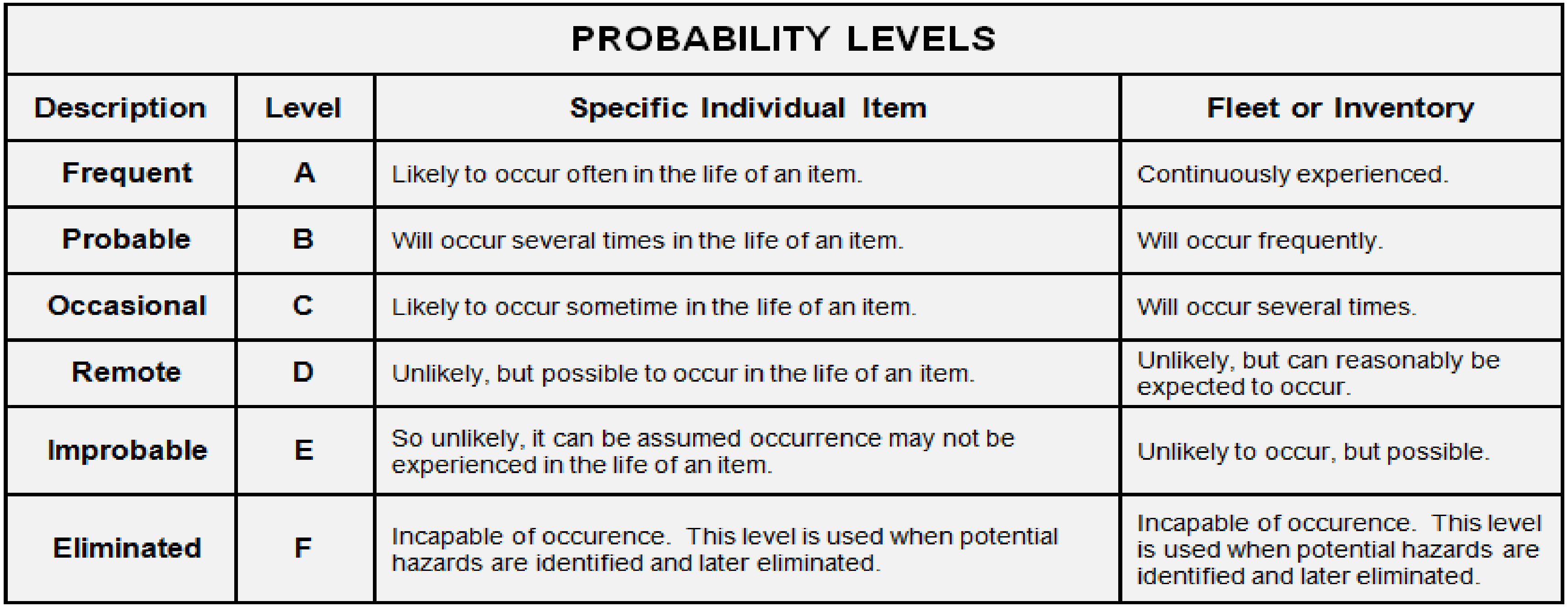


SEVERITY CATEGORIES		
Description	**Severity Category**	**Mishap Result Criteria**
Catastrophic	**1**	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
Critical	**2**	Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M.
Marginal	**3**	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	**4**	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K.

882E Severity, Probability & Risk

4.3.3 <u>Assess and document risk.</u> The severity category and probability level of the potential mishap(s) for each hazard across all system modes are assessed using the definitions in Tables I and II.

TABLE II. Probability levels

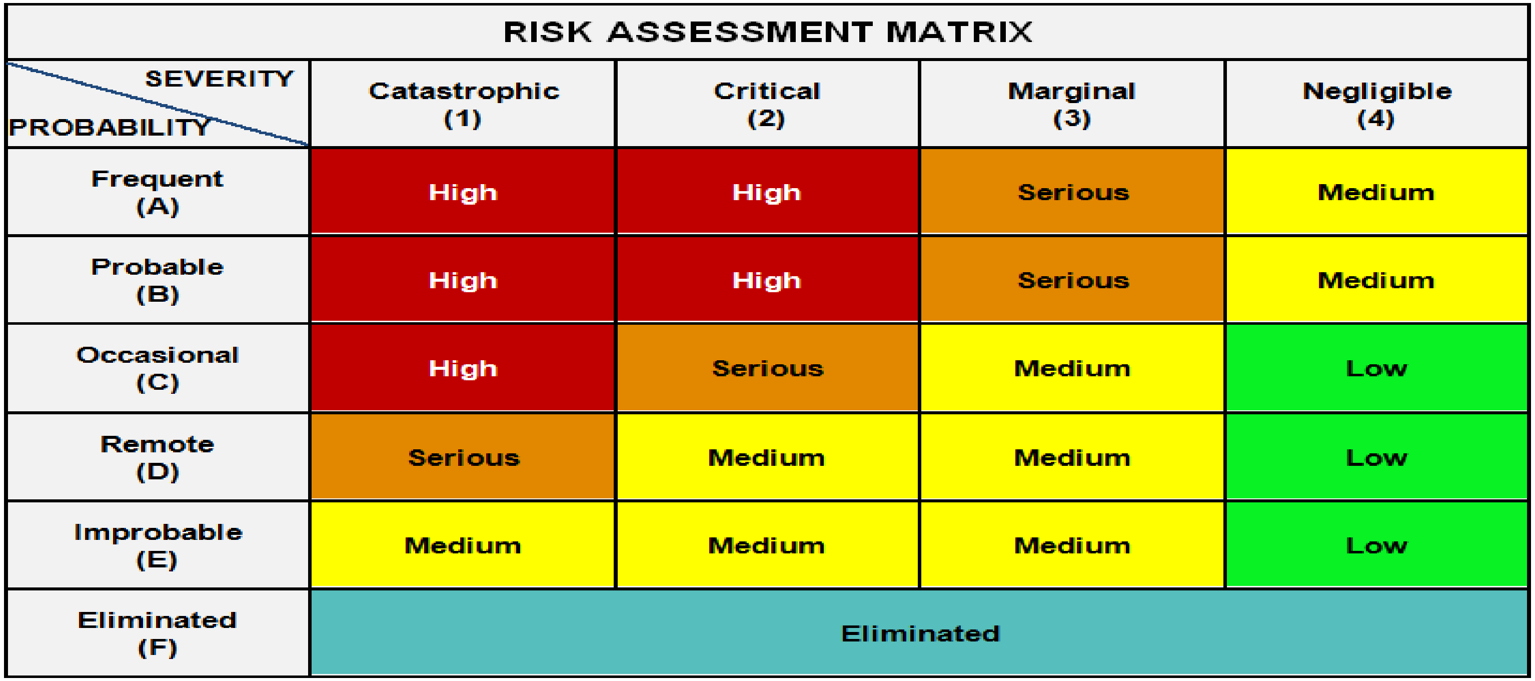


PROBABILITY LEVELS			
Description	**Level**	**Specific Individual Item**	**Fleet or Inventory**
Frequent	**A**	Likely to occur often in the life of an item.	Continuously experienced.
Probable	**B**	Will occur several times in the life of an item.	Will occur frequently.
Occasional	**C**	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	**D**	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	**F**	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.

882E Severity, Probability & Risk

4.3.3.c. Assessed risks are expressed as a Risk Assessment Code (RAC) which is a combination of one severity category and one probability level. Table III assigns a risk level of High, Serious, Medium, or Low for each RAC.

TABLE III. Risk assessment matrix



RISK ASSESSMENT MATRIX

SEVERITY PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

882E Risk Matrix Tailoring

- MIL-STD-882E, paragraph 4.3.3.d.

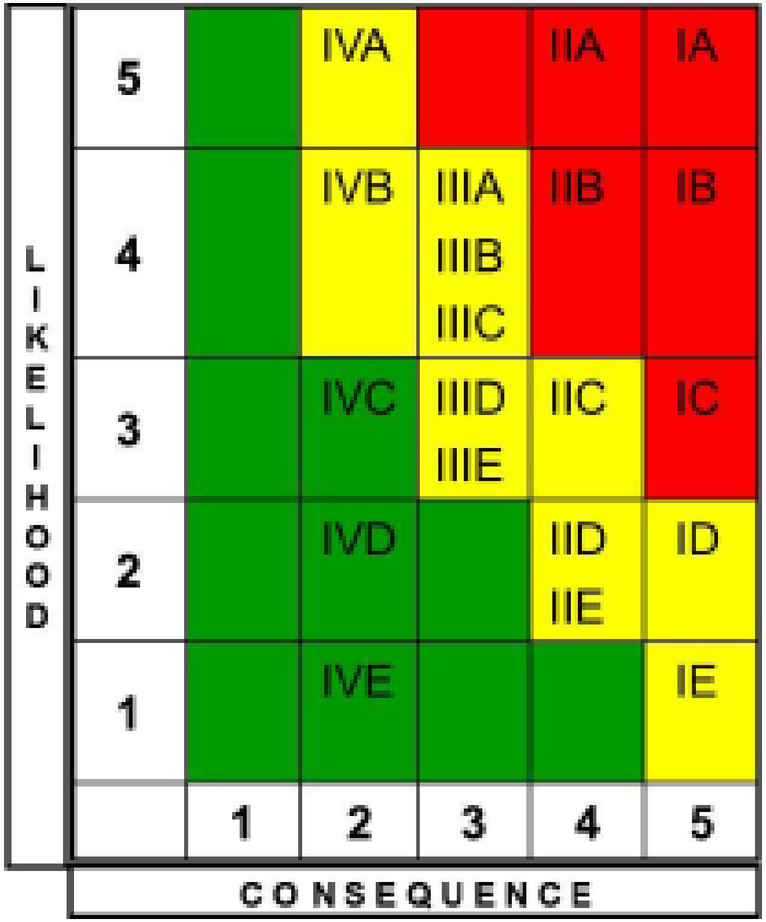
  "The definitions in Tables I and II, and the RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with DoD Component policy. Alternates shall be derived from Tables I through III."
- Air Force approach to tailoring the 882E risk matrix:
  - Program Offices may only tailor the MIL-STD-882E probability levels by adding quantitative definitions appropriate for the system and that are consistent with the existing text definitions

882E Risk Matrix Tailoring, Cont'd

- Air Force approach to tailoring the 882E risk matrix, Cont'd:
  - Program Offices may not tailor the MIL-STD-882E mishap severity category definitions
    - Required to ensure consistency of High and Serious risk levels
    - It would not be credible to ask the CAE to accept a High risk for something that did not involve loss of life, loss or damage to equipment exceeding $10M, or irreversible significant environmental damage
  - Programs must obtain Milestone Decision Authority approval for any other risk matrix tailoring
  - Program Offices are to use mandatory translation matrix to report ESOH risks assessed using the 4X5 MIL-STD-882E on the Program Risk 5X5 matrix that only uses High, Medium, and Low risk levels

882E Risk Matrix Tailoring, Cont'd

DoD Acquisition Risk Management Guide

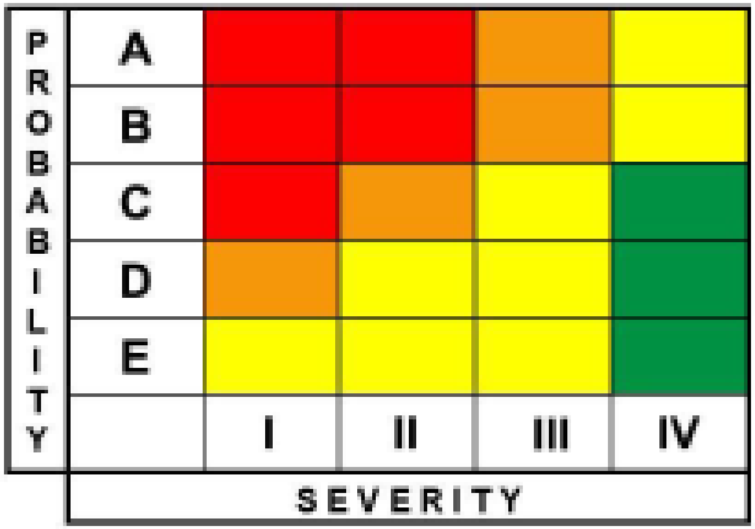


LIKELIHOOD

5	🟩	🟨 IVA	🟥	🟥 IIA	🟥 IA
4	🟩	🟨 IVB	🟨 IIIA IIIB IIIC	🟥 IIB	🟥 IB
3	🟩	🟩 IVC	🟨 IIID IIIE	🟨 IIC	🟥 IC
2	🟩	🟩 IVD	🟩	🟨 IID IIE	🟨 ID
1	🟩	🟩 IVE	🟩	🟩	🟨 IE
	1	2	3	4	5

CONSEQUENCE

MIL-STD-882



PROBABILITY

A	🟥	🟥	🟧	🟨
B	🟥	🟥	🟧	🟨
C	🟥	🟧	🟨	🟩
D	🟧	🟨	🟨	🟩
E	🟨	🟨	🟨	🟩
	I	II	III	IV

SEVERITY

MIL-STD-882E Risk Types

- **Initial risk:** The first assessment of the potential risk of an identified hazard; the initial risk assessment establishes a fixed baseline for the hazard
- **Event risk:** The risk associated with a hazard as it applies to a specified hardware/software configuration during an event (an activity that exposes people, equipment or the environment to a known system hazard); typical events include Developmental Testing/Operational Testing (DT/OT), demonstrations, fielding, post-fielding tests
- **Target risk:** The projected risk level the Program Manager (PM) plans to achieve by implementing mitigation measures consistent with the design order of precedence

Assessed risk of a given hazard may change with time as configurations change, mitigations are implemented, and as test or operational data become available

MIL-STD-882E Risk Types, Cont'd

- **Current risk:** The risk level at a given point in time for the current hardware/software configuration, to include any implemented, verified, and validated mitigation measures
- **Residual Risk:** No longer applicable

Assessed risk of a given hazard may change with time as configurations change, mitigations are implemented, and as test or operational data become available

"Residual Risk"

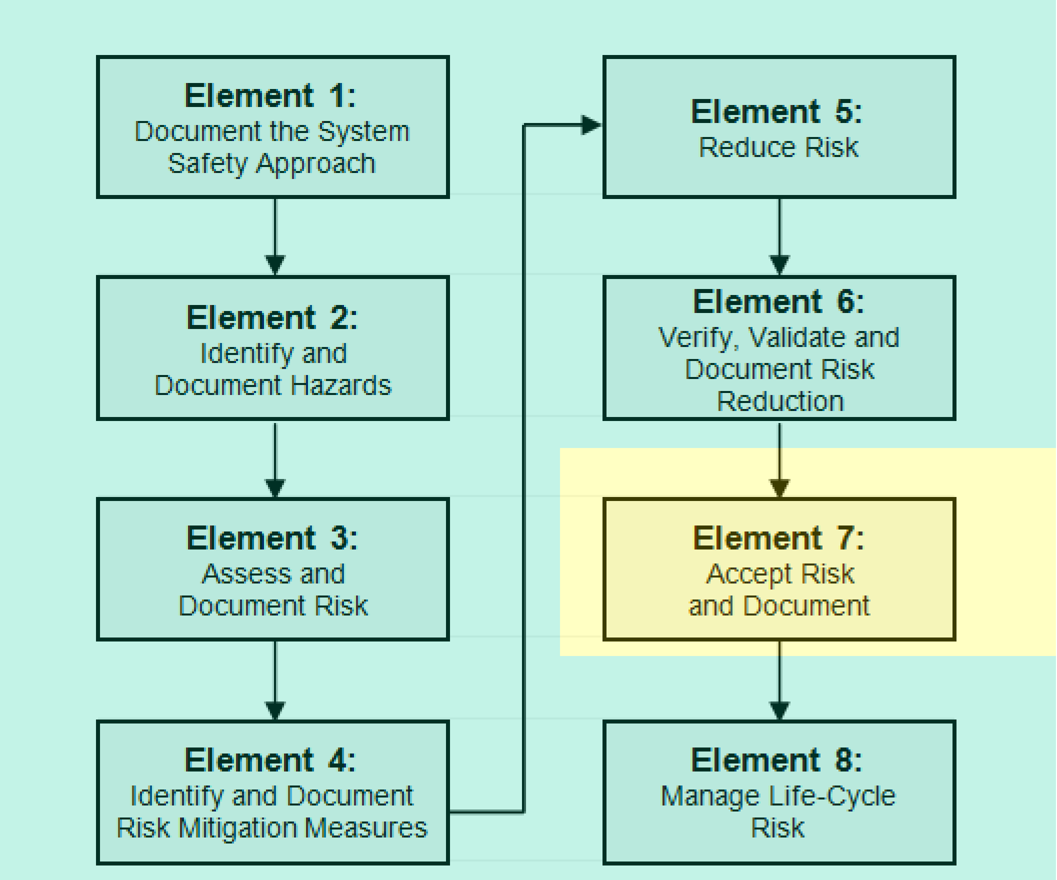
- From earlier versions of MIL-STD-882 and DoDI 5000
- No longer used because risks must be accepted at any point prior to exposing people, equipment, or the environment to known system hazards that do not have an applicable risk acceptance
- Previously, only accepted "residual risk"
  - Risk level after all selected mitigations are in place, and have been verified and validated
  - Risk acceptance typically occurred just prior to or just after fielding a system
  - Allowed exposure of people, equipment, and the environment prior to that point to hazards without management insight and approval of risks
  - Management, especially Senior management, then faced risk acceptance decisions for which there were few, if any, options available other than to accept

"Residual Risk," Cont'd

- **DoD Acquisition policy rejected this approach to ESOH risk management in 7 March 2007 USD (AT&L) Policy Memo "Defense Acquisition System Safety – Environment, Safety, and Occupational Health (ESOH) Risk Acceptance"**
  - **Since 2007 risks must be accepted prior to exposing people, equipment, or the environment to known hazards**
  - **This done in response to fatal mishaps that occurred before "residual risk" had to be reviewed and accepted (or rejected) by appropriate management levels**
    - **Aircraft undergoing Developmental Testing without all planned risk mitigations in place for the test**
    - **Tactical vehicles in use in combat but still undergoing modifications to reduce High risk of rollovers**

MIL-STD-882E

Risk Assessment



Risk Acceptance

FIGURE 1. Eight elements of the system safety process

Risk Acceptance

- **Formal acceptance of risk of a potential mishap, by an appropriate level of authority and associated user representative**
- **Must occur before exposing people, equipment, or the environment to known hazards**
- **Risk acceptance should be for a specified time period linked to**
  - **Event duration, or**
  - **Time required to implement mitigations to lower the risk, or**
  - **Remaining life of the system if no further mitigations planned**

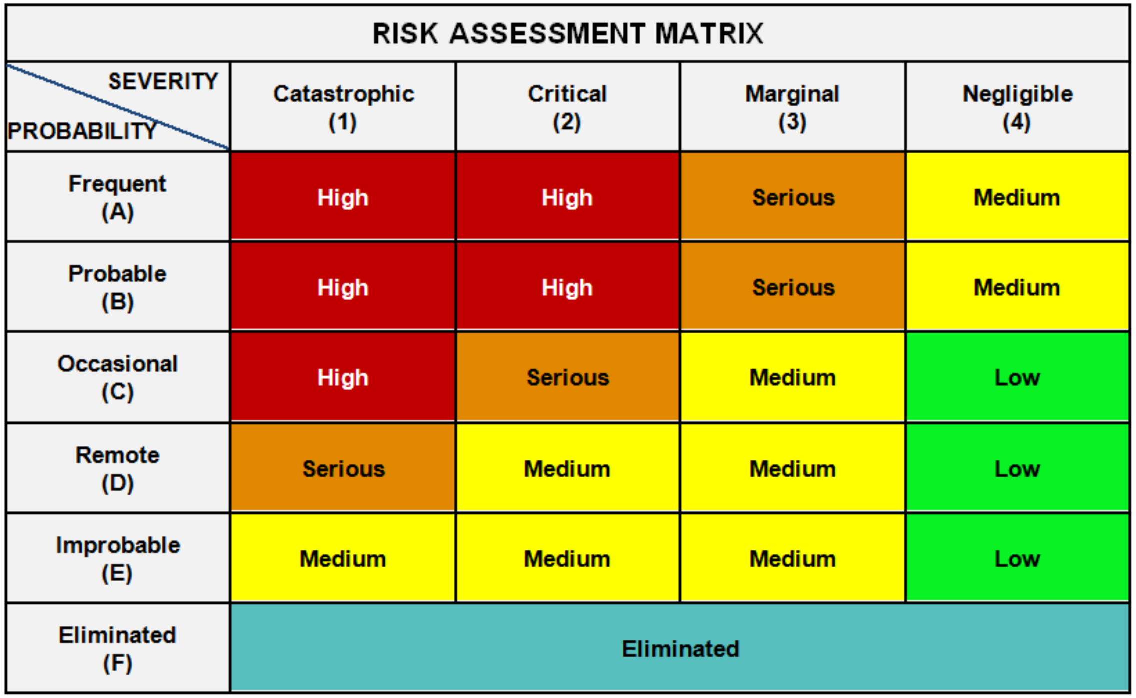
NOTE: This process only applies to system-related ESOH risks, not operational risks related to a given mission or combat activity. An operational Commander responsible for an event can always assume the operational risk for the event if it has to proceed due to mission criticality.

Risk Acceptance, Cont'd

- **If either the risk acceptance authority or user representative decides the risk is unacceptable**
  - **The event, e.g, testing or fielding, should not proceed until the risk is lowered to an acceptable level**
  - **Before proceeding with the event, further mitigations must be put into place to lower the risk and the risk then formally accepted**

NOTE: This process only applies to system-related ESOH risks, not operational risks related to a given mission or combat activity. An operational Commander responsible for an event can always assume the operational risk for the event if it has to proceed due to mission criticality.

Risk Acceptance Authorities



RISK ASSESSMENT MATRIX				
SEVERITY PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Per current DoDI 5000.02 dated 26 Nov 2013:

- **High - Component Acquisition Executive (CAE)**
- **Serious - Program Executive Officer (PEO)**
- **Medium & Low - Program Manager (PM)**

Risk Acceptance Authority and User Representative

- **Current DoDI 5000.02 dated 26 Nov 2013, Enclosure 3, Section 16, Environment, Safety, and Occupational Health (ESOH)**
  - **"For Joint Programs, the ESOH risk acceptance authorities reside within the Lead DoD Component"**
  - **"The user representative, as defined in MIL-STD-882E, must be part of this process throughout the life cycle and will provide formal concurrence prior to all serious- and high-risk acceptance decisions" by the appropriate management authority**

DoD formalized the role of the user representative in the decision whether to accept a High or Serious ESOH risk to ensure the system users (operators and maintainers) can prevent acceptance of a risk that they find unacceptable, since it is the users, not those in the Acquisition chain, that will be exposed to the risk if accepted

Risk Acceptance Authority and User Representative, Cont'd

- MIL-STD-882E definition of "User Representative":
  - For fielding events (i.e., IOC or FOC), a Command or agency that has been formally designated in the Joint Capabilities Integration and Development System (JCIDS) process to represent single or multiple users in the capabilities and acquisition process
  - For non-fielding events (i.e., Developmental Test, Operational Test, or Field User Evaluation), the user representative will be the Command or agency responsible for the personnel, equipment, and environment exposed to the risk
  - For all events, the user representative will be at a peer level equivalent to the risk acceptance authority

For Joint Programs, each participating Component should provide a user representative that would have to formally concur prior to the Lead Command accepting a High or Serious risk

Legacy (Fielded) System Risk Acceptance

- Challenge: DoDI 5000.02 requirement for formal risk acceptance prior to exposing people, equipment, or the environment to known hazard
  - Legacy or Fielded System already in use
  - If identify new, previously unknown, or changed (increased) risk, policy would require obtaining risk acceptance or suspend use ("ground") the system to avoid exposing people, equipment, or environment to this known risk
  - Real issue occurs when the risk is High and risk acceptance required by Component Acquisition Executive (CAE)

Legacy (Fielded) System Risk Acceptance, Cont'd

- Air Force approach
  - When identify High risk that does not have formal acceptance, Program Manager must notify the CAE and User Representative within 24 hours of recognition
  - Notification establishes Interim Risk Acceptance for a period of time specified by the Program Manager, typically on the order of several days
    - Unless either the CAE or User Representative objects
    - Interim Risk Acceptance period to allow Program Manager to notify field units using the system and to submit more detailed description of risk assessment and identify any short term mitigations (procedural changes) that may be possible to lower the risk (but not below High)

Legacy (Fielded) System Risk Acceptance, Cont'd

- Air Force approach, Cont'd
  - Before end of Interim Risk Acceptance period, Program Manager must submit a more detailed request to User Representative and CAE for formal risk acceptance for another, longer, specified period of time
    - Allows Program Office to determine if there are any material changes that could lower the risk to Serious or Medium, identify funding requirements, and establish an implementation schedule for the mitigations
    - If User Representative and CAE do not agree to accept the risk, then the Air Force would have to ground the system until the risk could be lowered
  - Program Manager would return to CAE and User Representative prior to end of this second risk acceptance period for extension of acceptance as necessary

Summary

- Risk Assessment
  - What: Assessment of risk of identified ESOH hazard could result in a specific mishap
  - Who: Program Office ESOH personnel
  - When: Whenever pertinent data available (experience, analyses, test results, field data, etc.); reviewed at all Technical Reviews
  - How: Assess Severity and Probability to determine risk level and document in the Program Office HTS

Summary, Cont’d

- Risk Acceptance
  - What: Formal recognition and acceptance of risk of potential mishap or non-acceptance mandating further mitigation
  - Who: Risk level dependent; requires user concurrence
  - When: Before exposing people, equipment, or the environment to known hazards
  - How: Formal acceptance by designated acceptance official and documented in the Program Office's HTS