14863
MIL-STD-882E:
Quantitative vs. Qualitative ESOH Risk Assessments Using the 882E Risk Matrix

Robert E. Smith, CSP, Booz Allen Hamilton
NDIA Systems Engineering Conference
San Diego, CA
October 24, 2012

Purpose

- To explain two approaches to ESOH risk assessments using either qualitative or quantitative probability determinations
  - Compare probability definitions among 882C/882D/882E
  - Explore the strengths and weaknesses of each approach
  - Recommend situations where one approach may be better suited for the risk assessment than the other
  - Identify the challenges associated with use of each approach for ESOH risk assessment

Qualitative / Quantitative Definitions[1]

- Qualitative - The term used to describe those inductive analytical approaches that are oriented toward relative, non-measurable, and subjective values

- Quantitative - The term used to describe those analytical approaches that are oriented toward the use of numbers or symbols used to express a measurable quantity

Reference:
1 – System Safety Analysis Handbook – System Safety Society

MIL-STD-882E – Qualitative / Quantitative Approaches

- MIL-STD-882E methodology is to be used by all DoD Acquisition Programs (ACAT I to IV, and non-ACAT programs)
- If available and valid, quantitative data can be used to help assign probability categories with a higher level of confidence that an accurate assessment has been obtained
- Quantitative assessments are not mandatory, so quantitative probability levels are not included in the mandatory section of MIL-STD-882E

OSD sponsored a study that determined requiring DoD Quantitative Analyses would be problematic and could lead to erroneous conclusions / false sense of certainty

1993 MIL-STD-882C – Qualitative vs. Quantitative

TABLE 2. HAZARD PROBABILITY LEVELS

Description*	Level	Specific Individual Item	Fleet or Inventory**
FREQUENT	A	Likely to occur frequently	Continuously experienced
PROBABLE	B	Will occur several times in the life of an item.	Will occur frequently
OCCASIONAL	C	Likely to occur some time 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	Unlikely to occur, but possible

*Definitions of descriptive words may have to be modified based on quantity involved.
**The size of the fleet or inventory should be defined.

FIGURE 1. FIRST EXAMPLE HAZARD RISK ASSESSMENT MATRIX

HAZARD CATEGORY / FREQUENCY	(1) CATASTROPHIC	(2) CRITICAL	(3) MARGINAL	(4) NEGLIGIBLE
(A) FREQUENT ($X > 10^{-1}$)*	1A	2A	3A	4A
(B) PROBABLE ($10^{-1} > X > 10^{-2}$)*	1B	2B	3B	4B
(C) OCCASIONAL ($10^{-2} > X > 10^{-3}$)*	1C	2C	3C	4C
(D) REMOTE ($10^{-3} > X > 10^{-6}$)*	1D	2D	3D	4D
(E) IMPROBABLE ($10^{-6} > X$)*	1E	2E	3E	4E

* Example of quantitative criteria

Hazard Risk Index	Suggested Criteria
1A, 1B, 1C, 2A, 2B, 3A	Unacceptable
1D, 2C, 2D, 3B, 3C	Undesirable (MA decision required)
1E,2E,3D,3E,4A,4B	Acceptable with review by MA
4C, 4D, 4E	Acceptable without review

882C, Para 4.5.2: "Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems."

882C, Appendix A, Para 30.5.2: "Hazard categorization may also involve the determination of the likelihood of the hazardous events actually occurring. This may be reported in non-numeric (qualitative) terms; or in numeric (quantitative) terms such as one in ten thousand flights, or 1e-4/flight. Prioritization may be accomplished either subjectively by qualitative analyses resulting in a comparative hazard risk assessment or through quantification of the probability of occurrence resulting in a numeric priority factor for that hazardous condition."

2000 MIL-STD-882D – Qualitative vs. Quantitative

TABLE A-II. **Suggested mishap probability levels.**

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

*Definitions of descriptive words may have to be modified based on quantity of items involved.

**The expected size of the fleet or inventory should be defined prior to accomplishing an assessment of the system.

Section 4.3, Assessment of Mishap Risk: "The tables in Appendix A are to be used unless otherwise specified."

882D, Appendix A, A.4.4.3.2.2 – Mishap Probability: "Assigning a quantitative mishap probability to a potential design or procedural hazard is generally not possible early in the design process. At that stage, a qualitative mishap probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a mishap probability is documented in hazard analysis reports. Suggested qualitative mishap probability levels are shown in Table A-II."

2012 MIL-STD-882E – Approach Goes Back to 882C

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.

(1) When available, the use of appropriate and representative quantitative data that defines frequency or rate of occurrence for the hazard, is generally preferable to qualitative analysis. The Improbable level is generally considered to be less than one in a million. See Appendix A for an example of quantitative probability levels.

(2) In the absence of such quantitative frequency or rate data, reliance upon the qualitative text descriptions in Table II is necessary and appropriate.

Notes are included in MIL-STD-882E that specify using quantitative data is generally preferable to qualitative analysis.

Table II is in mandatory section, but does not include quantitative probability levels.

Reference Appendix A for an example of quantitative probability levels – same quantitative values that were in 882C/882D.

TABLE A-II. Example probability levels

Probability Levels				
Description	**Level**	**Individual Item**	**Fleet/Inventory***	**Quantitative**
Frequent	**A**	Likely to occur often in the life of an item	Continuously experienced.	Probability of occurrence greater than or equal to 10^{-1}.
Probable	**B**	Will occur several times in the life of an item	Will occur frequently.	Probability of occurrence less than 10^{-1} but greater than or equal to 10^{-2}.
Occasional	**C**	Likely to occur sometime in the life of an item	Will occur several times.	Probability of occurrence less than 10^{-2} but greater than or equal to 10^{-3}.
Remote	**D**	Unlikely, but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur.	Probability of occurrence less than 10^{-3} but greater than or equal to 10^{-6}.
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item	Unlikely to occur, but possible.	Probability of occurrence less than 10^{-6}.
Eliminated	**F**	Incapable of occurrence within the life of an item. This category is used when potential hazards are identified and later eliminated.		

* The size of the fleet or inventory should be defined.

Quantitative – Strengths/Weaknesses

- Strengths
  - Considered more of an engineering / scientific assessment
  - Decision makers may depend on a specific failure probability number to influence design decisions
  - Satisfy safety requirements that specify a quantitative probability threshold (e.g., inadvertent detonation is required to be less than 1E-6)
- Weaknesses
  - Validity of data could be suspect
  - Significant impact on resources, schedule, cost to perform a quantitative probability determination

Qualitative – Strengths/Weaknesses

- Strengths
  - Easy to understand
  - Less Time to develop analyses
  - Less Costly
- Weaknesses
  - “Gray” assessment
  - Open to interpretation

Appropriate Applications

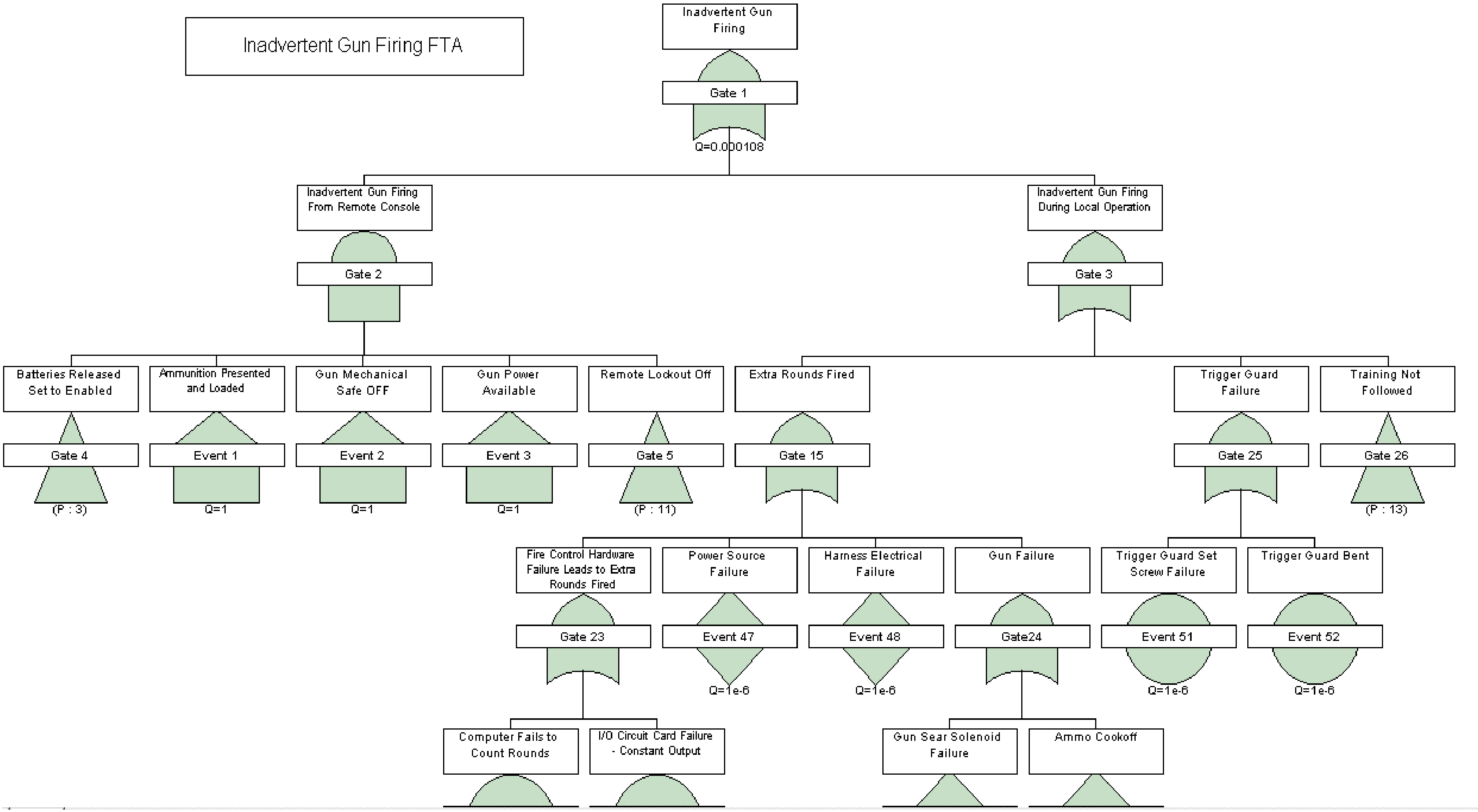
- Quantitative analyses:
  - High consequence situations/hazards
  - Specific hazards/mishaps requiring additional examination
  - Probabilistic safety requirements (e.g., fuzing, nuclear, air worthiness)
- Qualitative analyses:
  - Less complex programs
  - Rapid acquisition programs
  - Hazards associated with less significant potential mishap outcomes (marginal/negligible severities)
  - Programs with limited or no failure/reliability data

Quantitative Determination Example

- Fault Tree
- Works well to determine probability of top-level event
  - A graphic representation of the various parallel and series combinations of subsystems and component failures that can result in a specified system fault
  - When fully developed, it may be mathematically evaluated to establish the probability of the ultimate undesired event occurring as a function of the estimated probabilities of identifiable contributory events
- Based on top-level event probability calculation, one can identify the corresponding probability level in Table A-II of MIL-STD-882E

Challenges – Ensuring fault tree logic is accurate; ensuring probabilities of contributory events are accurate

Quantitative Fault Tree Example – Inadvertent Gun Firing



Challenges – Ensuring fault tree logic is accurate; ensuring probabilities of contributory events are accurate

Quantitative Fault Tree Example – Inadvertent Gun Firing Results

- Fault Tree example shows Unavailability (Q) as 1.08e-4
- From Table A-II of MIL-STD-882E, assign a probability of Remote (D) (1e-3 > X > 1e-6)
- Cut set reports can be analyzed to determine single/double points of failure and also common mode failures

Summary

Parameter:	Value
Unavailability Q:	0.000108
Failure Frequency W:	0
Mean Unavailability Qm:	0.000108
Mean Availability Am:	0.9999
CFI	0
Expected Failures:	0
Unreliability:	0
Total Down Time TDT:	18.92
Total Up Time TUT:	1.752e+5
Failure Rate:	0
MTBF:	0.0
MTTF:	0
MTTR:	0
Availability:	0.9999
Reliability:	1
No of Cut Sets:	26

FT Cut Sets Report

Date: 10/12/2012
Time: 10:47:05

Name: Inadvertent Gun Firing Q: 0.000108

Gate Name	*No*	*Cut Set*	*Set Unavailability*	*Set Failure Frequency*
Gate 1	1	Event 47	1e-6	0
Gate 1	2	Event 46	1e-6	0
Gate 1	3	Event 45	1e-6	0
Gate 1	4	Event 50	1e-6	0
Gate 1	5	Event 49	0.0001	0
Gate 1	6	Event 51	1e-6	0
Gate 1	7	Event 52	1e-6	0
Gate 1	8	Event 48	1e-6	0
Gate 1	9	Event 77 ::Event 62	1e-12	0
Gate 1	10	Event 5 ::Event 62	1e-9	0
Gate 1	11	Event 68 ::Event 62	1e-12	0
Gate 1	12	Event 19 ::Event 62	1e-12	0
Gate 1	13	Event 77 ::Event 35	1e-12	0
Gate 1	14	Event 5 ::Event 35	1e-9	0

Challenges – Ensuring fault tree logic is accurate; ensuring probabilities of contributory events are accurate

Qualitative Determination Examples

- Example 1 - System Safety Working Group (SSWG)
  - Include Users and SMEs (Designers/Engineers) on SSWG
  - Members reach consensus on probability level for a given failure
- Example 2 – Historical Failure Data
  - Typical failure data has limited fidelity
  - Use available fleet data to assign a probability level
  - MRAP Rollover occurrence data as of 20 Sept 2012:
    - 20,000 MRAPs in theater
    - 751 rollovers since Nov 2007
    - 21 rollover events have resulted in 32 US fatalities
    - Qualitative probability level of “Occasional” (will occur several times across a fleet)

Challenges – Subjective, but professional, assessment that can be subject to dispute

Conclusion

- Explained the qualitative and quantitative approaches to ESOH risk assessments
  - Strengths and weaknesses highlighted for both approaches
  - Explained the qualitative and quantitative approaches as defined in MIL-STD-882E, and differences and similarities between 882C, 882D, and 882E
- The next presentation takes you to the next step after risk assessment – risk acceptance

MIL-STD-882E provides you the option to select the safety analysis type (qualitative and quantitative) to be performed

Questions?

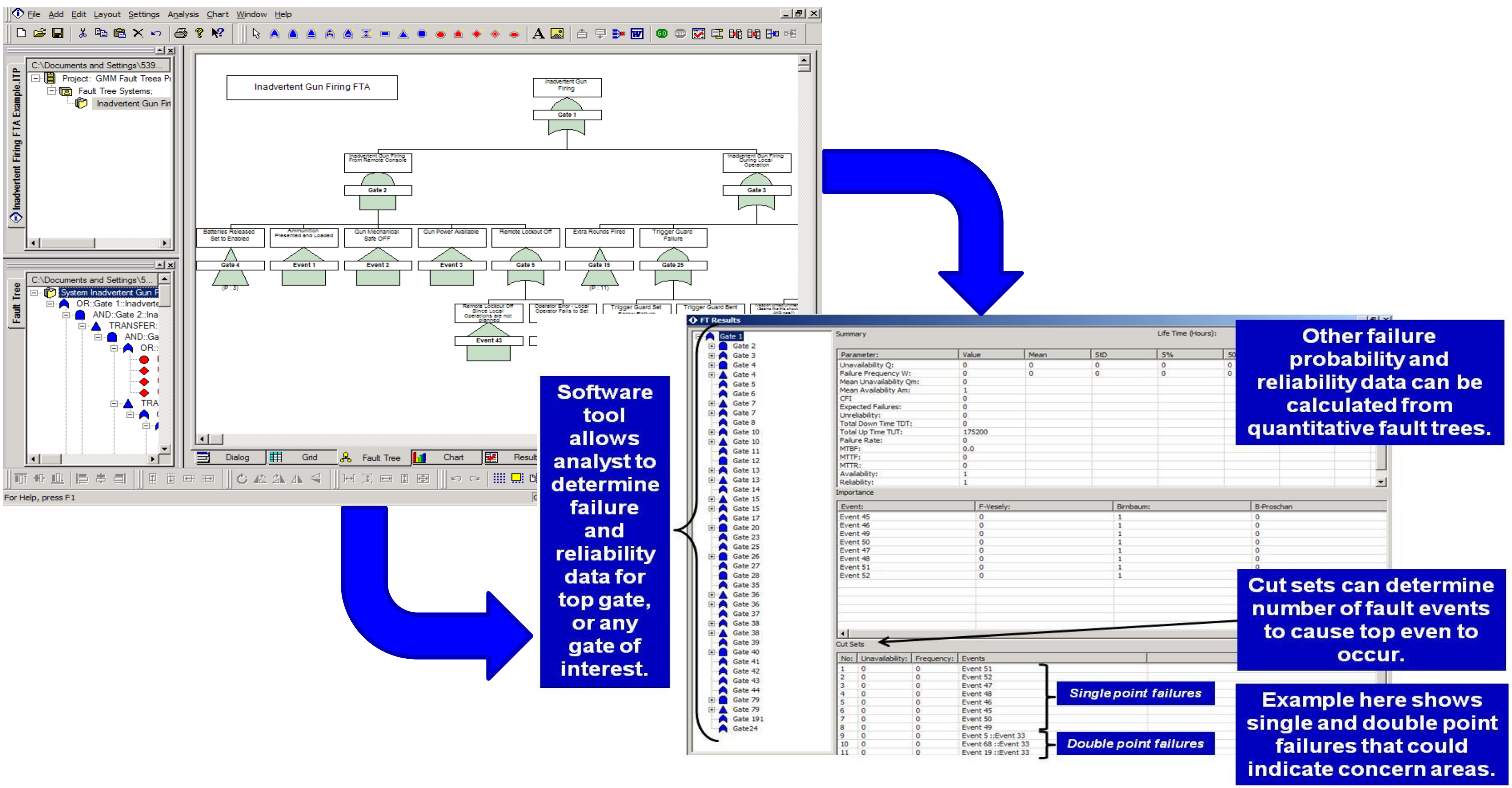
Robert E. Smith, CSP
Booz Allen Hamilton
1550 Crystal Drive, Suite 1100
Arlington, VA 22202-4158
703-412-7661
smith_bob@bah.com

Backups

Contents

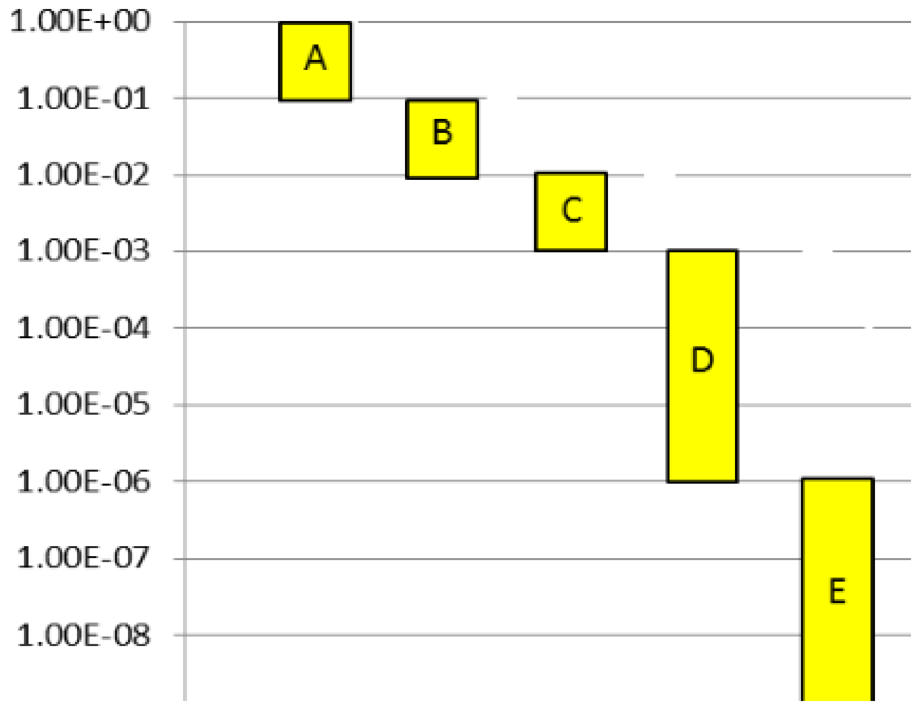
Examples of Challenges with each Assessment Approach

- Fault Tree Example



Risk Matrix Probability Bins[2]

- Figure shows differences between probability levels
- Note that D-Remote is a three orders of magnitude difference



Reference:

2 - “Quantitative vs. Qualitative Safety Assessments” Arthur D. Barondes, Ph.D.; Analytics International Corp; 2012 International System Safety Conference

Hazard Analyses - Qualitative or Quantitative[3]

Technique	Type	Identifies Hazards	Identifies Root Causes	Lifecycle Phases	Qualitative or Quantitative	Skill	Level of Detail
FTA	SSHA, SHA	P	Y	PD – DD	BOTH	SS, ENGR, M&S	MODERATE TO IN-DEPTH
ETA	SHA	P	P	PD – DD	BOTH	SS, ENGR, M&S	MODERATE TO IN-DEPTH
FMECA	SSHA	P	P	PD – DD	BOTH	SS, ENGR, M&S	IN-DEPTH
FaHA	SSHA	Y	P	PD – DD	QUALITATIVE	SS, ENGR, M&S	IN-DEPTH
FuHA	SSHA, SHA	Y	P	CD – PD - DD	QUALITATIVE	SS, ENGR, M&S	IN-DEPTH
SCA	SSHA, SHA	P	Y	DD	QUALITATIVE	SS, ENGR, M&S	MONDERATE TO IN-DEPTH
PNA	SSHA, SHA	P	N	PD – DD	BOTH	SS, ENGR, M&S	IN-DEPTH
MA	SSHA, SHA	P	N	PD – DD	BOTH	SS, ENGR, M&S	MODERATE TO IN-DEPTH
BA	SHA	Y	P	PD – DD	QUALITATIVE	SS, ENG	MODERATE TO IN-DEPTH
BPA	SSHA	Y	P	PD – DD	QUALITATIVE	SS, ENGR, M&S	IN-DEPTH
HAZOP	SSHA, SHA	Y	P	PD – DD	QUALITATIVE	SS, ENGR, M&S	MODERATE TO IN-DEPTH
CCA	SSHA	Y	P	PD – DD	BOTH	SS, ENGR, M&S	MODERATE TO IN-DEPTH
CCFA	SSHA, SHA	Y	P	PD – DD	QUALITATIVE	SS, ENGR, M&S	MODERATE TO IN-DEPTH
MORT	SSHA, SHA	Y	P	PD – DD	BOTH	SS, M&S	MODERATE TO IN-DEPTH
SWSA	SSHA, SHA	Y	P	CD – PD	QUALITATIVE	SS, ENGR, M&S	MODERATE TO IN-DEPTH

Identification of Hazards and Root Causes: *Y = Yes; N = No; P = Partial*
Lifecycle Phases: *CD = Concept Definition; PD = Preliminary Design; DD = Detailed Design; T = Testing*
Skill Required: *SS = System Safety; ENGR = Engineering (Mechanical, Software, Electrical, etc.); M&S = Math & Science*

Reference:
3 – WSESRB Interactive Safety Environment (WISE) – Attributes of Hazard Analysis Techniques

Quantitative Determination Examples

- Example 3 - Mean Time Between Failure (MTBF)
  - Failure Probability calculations work well if the system has significant test data (MTBF data)
    - MTBF = 100,000 hrs
    - Exposure Time (t) = 2,000 hrs
    - Probability of Failure over exposure time = 1.98e-2 (~2%)
    - Threshold for a Probable risk: 10-1 > X > 10-2
    - Remote (B) probability level assigned for this failure

$$P_f = 1 - R(t)$$

$$R(t) = e^{-(t/MTBF)}$$

Challenges – Ensuring MTBF data is accurate; becomes difficult to calculate for complex scenarios / multiple fault events to lead to mishap being analyzed

Quantitative Determination Examples

- Example 2 – Modeling and Reliability Data
  - Modeling data for specific failure event
    - Total number of simulation runs: 500,000
    - Total number of failure events: 125
    - Resulting probability of occurrence: 2.5e-4
  - Reliability data:
    - 577 trials with no failures
    - Probability of zero failures in 577 trials is 5.2e-3 at a 95% confidence interval
  - Multiplying modeling and reliability data (2.5e-4 * 5.2e-3),   the probability of failure is: 1.3e-6
  - From Table A-II of MIL-STD-882E, assign a probability of Remote (D) (1e-3 > X > 1e-6)

Challenges – Ensuring simulations are accurate; reaching consensus on confidence levels