

# **Combinatorial Failure Probability Analysis Using MIL-STD 882**

P.L. Clemens

*February 2002*

5th Edition

# Origin of The Method

The combinatorial technique described here was developed for the System Effectiveness and Safety Technical Committee of the American Institute of Aeronautics and Astronautics, as a formal Committee task assignment, during the period April-September 1982. Members of the Committee reviewed the method and tested it in instances of practical application prior to giving it their approval. The method is described in complete detail in Sverdrup Handbook 6000-8 and in a similarly titled paper which appeared in Vol. 18, No. 4 of the *Journal of the System Safety Society*.

*P.L. Clemens – July 1983*

# The Need

- In system safety analysis, quantitative failure probability data are often unavailable – subjective estimates must be used (i.e., engineering judgment).
- Subjective probability scales exist to guide judgment estimates (e.g., as found in MIL-STD-882).
- Probabilities are often subjectively judged with greater confidence for contributor events and conditions than for the mishaps/failures they can cause when combined.
- The subjective scales do not guide a combinatorial process.
- Therefore, probability of the mishap/failure event itself must be judged alone with reduced confidence.

A combinatorial method is needed for subjective cases

# The Approach

- Arbitrary “Probability Values” (dimensionless numbers) have been assigned to the probability steps of MIL-STD-882.
- Subjective probabilities of contributor events/conditions are estimated as usual, using the MIL-STD-882 scale as a guide.
- “Probability Values” corresponding to the estimates are used combinatorially, as in the classical numerical methods.
- The “Probability Value” for the combined result is then re-translated into the subjective scale of MIL-STD-882.

# “Probability Values” of the Scale are

- Dimensionless numbers having no quantitative failure rate significance.
- Arbitrarily selected to afford certain properties.
  - Internally consistent decade increments separate adjacent probability values and their thresholds.
  - A two-element union (“OR”) at a given level does not escalate probability to the next level.
  - A three-element union (“OR”) at a given level does escalate probability to the next level.
  - At the highest level, a two-element intersection (“AND”) does not lower probability to the next level.
  - At the highest level, a three-element intersection (“AND”) does lower probability to the next level.

# The Probability Scale

AIAA/SESTC		MIL-STD-882	
Threshold Level	Probability Level*	Level	Descriptive Word
	$3 \times 10^{-1}$	A	Frequent
$8 \times 10^{-2}$ →			
	$3 \times 10^{-2}$	B	Probable
$8 \times 10^{-3}$ →			
	$3 \times 10^{-3}$	C	Occasional
$8 \times 10^{-4}$ →			
	$3 \times 10^{-4}$	D	Remote
$8 \times 10^{-5}$ →			
	$3 \times 10^{-5}$	E	Improbable

\* Arbitrarily selected, dimensionless numbers

# Cautions

- If actuarial data are available or can be estimated, their use is preferable to this method. Use subjective, judgmental methods only when objective data are unavailable.
- A probability period – i.e., operating duration or number of trials – must be selected and applied consistently in all combinatorial methods (e.g., six months, three tests, 25-year system life cycle).
- Use of this method is not “magic.” It cannot confer less uncertainty upon the final result than is the uncertainty of probability judgment for the ingoing contributor events/conditions.

# Example I

## Intersection of Contributors

**Problem/Background** – A confined space, equipped with a forced ventilation system, contains an inert gas distribution system. No history of system leakage is available, but there are many connections and threaded fittings. The confined space must be entered often by work crews. (Full-time occupancy becomes a reasonable assumption.) An oxygen deficiency detection and alarm system is permanently installed, has battery backup, and is maintained and tested on a regular basis. This system has been found inoperative several times over a 10-year period, but recent refurbishment is thought to have corrected its faults. Three independent factors, by co-existing, would contribute to asphyxia in the confined space. Based on engineering judgment, probability levels are to be assigned to each factor and the probability of an unannounced life-threatening atmosphere is to be determined for the coming year.



## Example I

Contributing Factor	Level/ Probability Value	Justification
Inert gas distribution system leak	A = “Frequent” $3 \times 10^{-1}$	Experience with similar systems having many threaded fittings.
Failure of ventilation system to maintain habitable atmosphere	B = “Probable” $3 \times 10^{-2}$	Power outages occur from time to time and produce system shutdown. Maintenance personnel report that filters have been found blocked in two recent instances.
Failure of Oxygen–Deficiency Detection and Alarm System	C = “Occasional” $3 \times 10^{-3}$	The system has suffered occasional unannounced outages. Refurbishment has been recent and insufficient time has elapsed to observe the effect with confidence.

## Example I

**Calculation** – For the atmosphere in the confined space to fail to support life, and for this to be undetected, the three contributing factors must co-exist. Therefore, their combined probability  $P_c$  is given by the product of the individual probabilities  $P_n$ . This is the “AND” gate case of fault tree analysis:

$$P_c = P_1 \times P_2 \times P_3$$
$$P_c = (3 \times 10^{-1}) (3 \times 10^{-2}) (3 \times 10^{-3}) = 2.7 \times 10^{-5}$$

The combined probability ( $2.7 \times 10^{-5}$ ) corresponds to level E/“Improbable.” The combined probability may now be judged to fall at that level with the same confidence that accompanied the assignment of probability levels to the contributing factors.

**Comments:** Note that installing a feature that detects and annunciates failure of the ventilation system (preferably with battery backup) could further reduce probability. A move to eliminate threaded fittings from the confined space, although probably less practical, could have the same effect.

# Example II

## Union of Contributors

**Problem/Background** – An air-breathing turbine-type aircraft engine is to be tested under simulated altitude conditions in a test cell. Intolerable damage to the engine will be a result of either the uncommanded closure of a large valve upstream to the test cell or engine ingestion of foreign objects from the cell or the air supply ducting system. The two phenomena are independent. Occurrences of both kinds have been experienced, but no trustworthy database exists. Moreover, recent preventive measures against occurrences of both kinds have been implemented, and their effectiveness is not quantitatively determinable. Probability that either might occur during the next test period must be found.

## Example II

Contributing Factor	Level/ Probability Value	Justification
Upstream Valve closure without command	<b>E = “Improbable”</b> <b>3 x 10<sup>-5</sup></b>	Uncommanded valve “slam” has been experienced several times. Not all causes have been determined with certainty, but engineered safety features thought to be effective have been imposed.
Foreign Object Damage	<b>E = “Improbable”</b> <b>3 x 10<sup>-5</sup></b>	Damages experienced in the past have been attributed to corrosion scale flakeoff and human error. A periodic cleanup routine has been imposed to control foreign objects. Neither change has been proven in practice.

## Example II

**Calculation** – Either of the two independent contributing factors will produce intolerable engine damage. Thus the sum of the individual probabilities  $P_n$  gives the combined probability  $P_c$ . (Summing the probability makes use of the “rare-event approximation,” producing a pessimistically high value for  $P_c$ . This is the “OR” gate case of fault tree analysis:

$$P_c = P_1 + P_2$$
$$P_c = (3 \times 10^{-5}) + (3 \times 10^{-5}) = 6 \times 10^{-5}$$

This combined probability corresponds to level E/“Improbable.” The combined probability may now be judged to fall at that level with the same confidence that accompanied the assignment of probability levels to the contributing factors.

**Comments:** Note that the addition of another, independent contributor to intolerable engine damage, having the same probability level (i.e., E;  $3 \times 10^{-5}$ ), would raise the combined probability  $P_c$  to the level D/“Remote.”

$$P_c = 3 \times (3 \times 10^{-5}) = 9 \times 10^{-5}$$

# Example III

## Combined Union and Intersection of Contributors

**Problem/Background** – Four critical rocket motor performance parameters are to be measured and recorded during an important one-of-a-kind test. The four parameters are wholly independent of one another. Loss of data describing any one of the parameters would void the test. The instrumentation setup is largely new and unproven. The measurement environment is hostile. To counter the threat of data loss, three completely independent sensors and measurement channels will be used to instrument each of the four critical parameters. The probability of critical data loss during the test is sought – i.e., loss of data from all three channels serving any one of the four parameters.

**Contributing Factor and Probability Value** – Based on prior experience with similar tests, a single probability level has been judged to apply to the loss of data from any one of the 12 channels.

$$P_C = B... \text{“Probable”} ... 3 \times 10^{-2}$$

## Example III

**Calculation** – Using combinatorial calculations, first find probability  $P_P$  of the total loss of a given parameter having three redundant channels, all of which must be lost to lose that parameter:

$$P_P = P_C^3 = (3 \times 10^{-2})^3 = 2.7 \times 10^{-5} \leftarrow \text{combining as with Example I}$$

Then find the probability  $P_T$  of the loss of any of the four independent critical parameters:

$$P_T = 4 \times P_P = 4(2.7 \times 10^{-5}) = 1.1 \times 10^{-4} \leftarrow \text{combining as with Example II}$$

This combined probability corresponds to level D/“Remote.”

**Comments:** The system operator can now decide whether risk at this level is tolerable, whether additional redundancy is justifiable, or whether redundancy might be relaxed without elevating probability intolerably. Note the use of two rather than three channels for each of the four critical parameters would result in  $P_T = 3.6 \times 10^{-3}$  which corresponds to level C/“Occasional.”



# Example IV

## A Three-Level Fault Tree

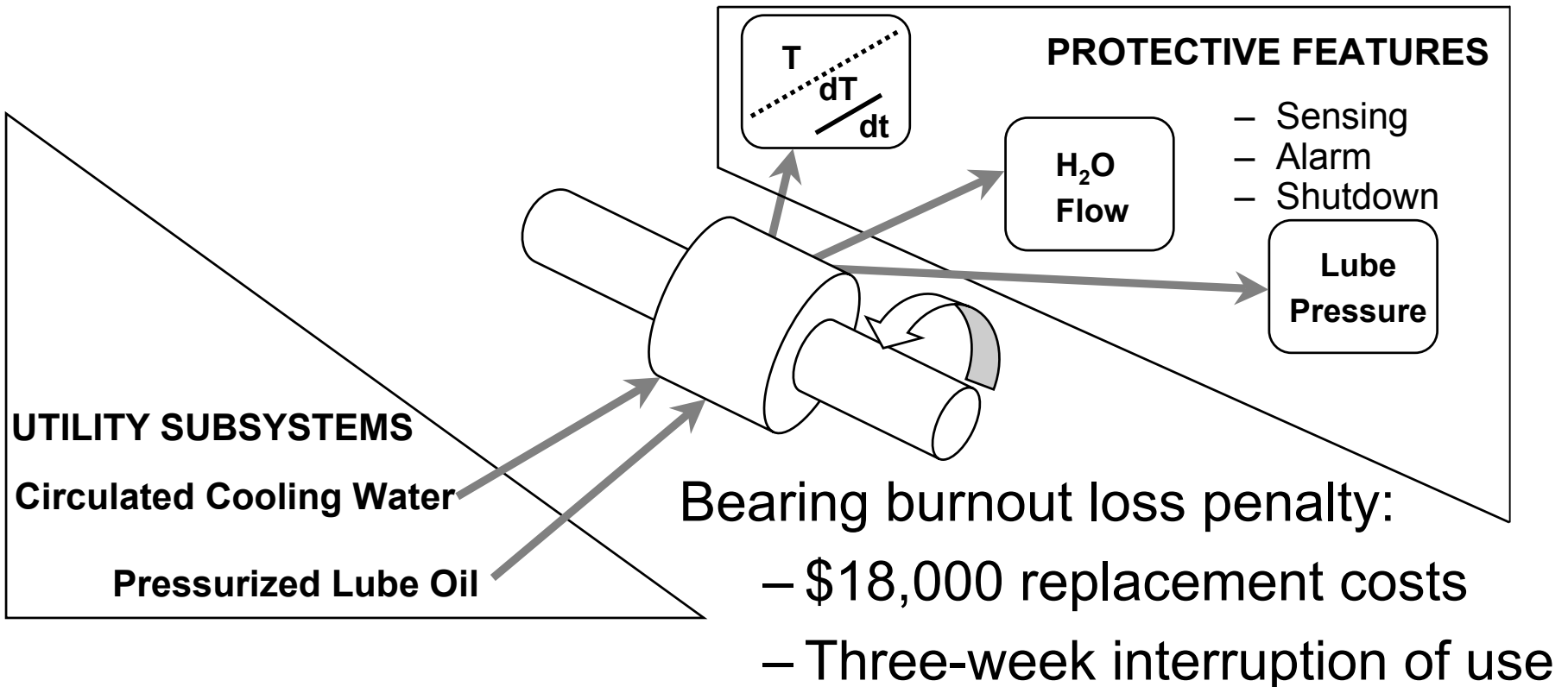
### Problem/Background

- A large rotating machine has six main-shaft bearings. Replacement of a bearing costs \$18,000 and requires three weeks of down time.
- Each bearing is served by:
  - A pressurized oil lubrication system
  - A water-cooled jacket
  - A temperature sensing/alarm/shutdown system
- In addition, there are sensing/alarm/shutdown systems for
  - Lube pressure failure
  - Cooling water loss of flow
- If they function properly, these systems will stop operation of the rotating machine early enough to prevent bearing damage. (System sensitivity makes the necessary allowance for machine “roll-out” or “coasting.”)
- Failure records for the individual system components are not available, but probabilities can be estimated using the subjective scale of MIL-STD-882.

**What is the probability that any one of the six bearings will suffer burnout during the coming decade?**

# Example IV

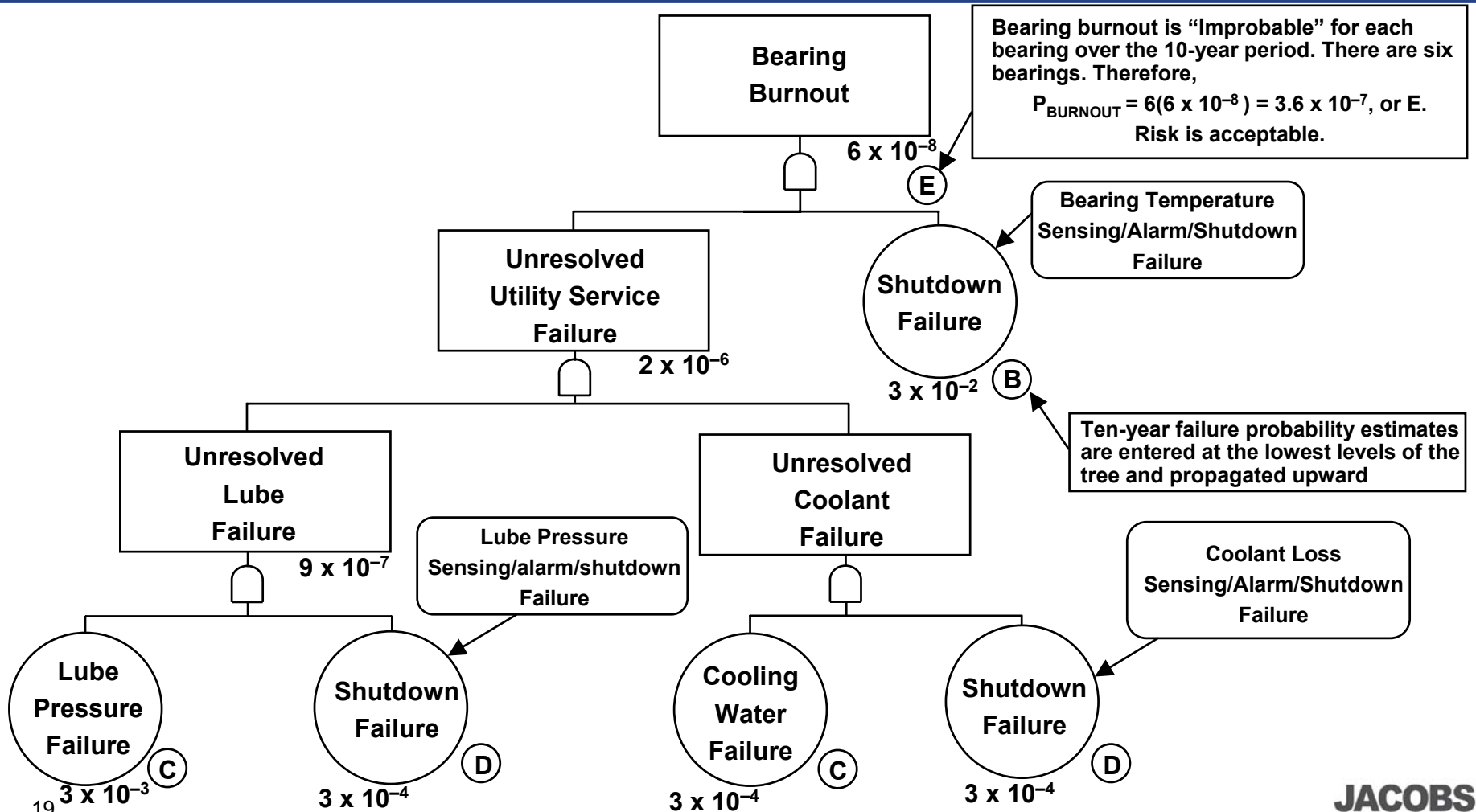
## The System



What is bearing burnout probability?

Does it represent a tolerable risk?

# A Fault Tree Models System Failure



# The Complete Scale

AIAA/SESTC		MIL-STD-882		
Threshold Level	Probability Level*	Level	Descriptive Word	Definition
$8 \times 10^{-2}$ →	$3 \times 10^{-1}$	A	Frequent	Likely to occur frequently
$8 \times 10^{-3}$ →	$3 \times 10^{-2}$	B	Probable	Will occur several times in life of an item
$8 \times 10^{-4}$ →	$3 \times 10^{-3}$	C	Occasional	Likely to occur sometime in life of an item
$8 \times 10^{-5}$ →	$3 \times 10^{-4}$	D	Remote	Unlikely but possible to occur in life of an item
	$3 \times 10^{-5}$	E	Improbable	So unlikely if can be assumed occurrence may not be experienced

\* Arbitrarily selected, dimensionless numbers