Use (and Misuse) of System Safety Terms

Don Swallom

January 18, 2012

NASA SAFETY TRAINING CENTER

A CHARLATAN'S GUIDE to QUICKLY ACQUIRED QUACKERY

The TROUBLE with SYSTEM SAFETY

P. L. Clemens
September 2001

http://www.fault-tree.net/papers/clemens-master-quack.pdf

FOLLOW THE STANDARDS AND THEIR DEFINITIONS...

- **No single set of universally recognized definitions.** *(The technical societies haven't succeeded at it — not quite yet.)*
  - **Exquisite variety among contemporary authors.** *(Each source picks its very own favorites because each is unequivocally correct.)*
    - **Logic inconsistencies abound in venerated standards.** *(Flawed definitions lead to bizarre syllogisms.)*

But, the Definitions often Lack Logic!

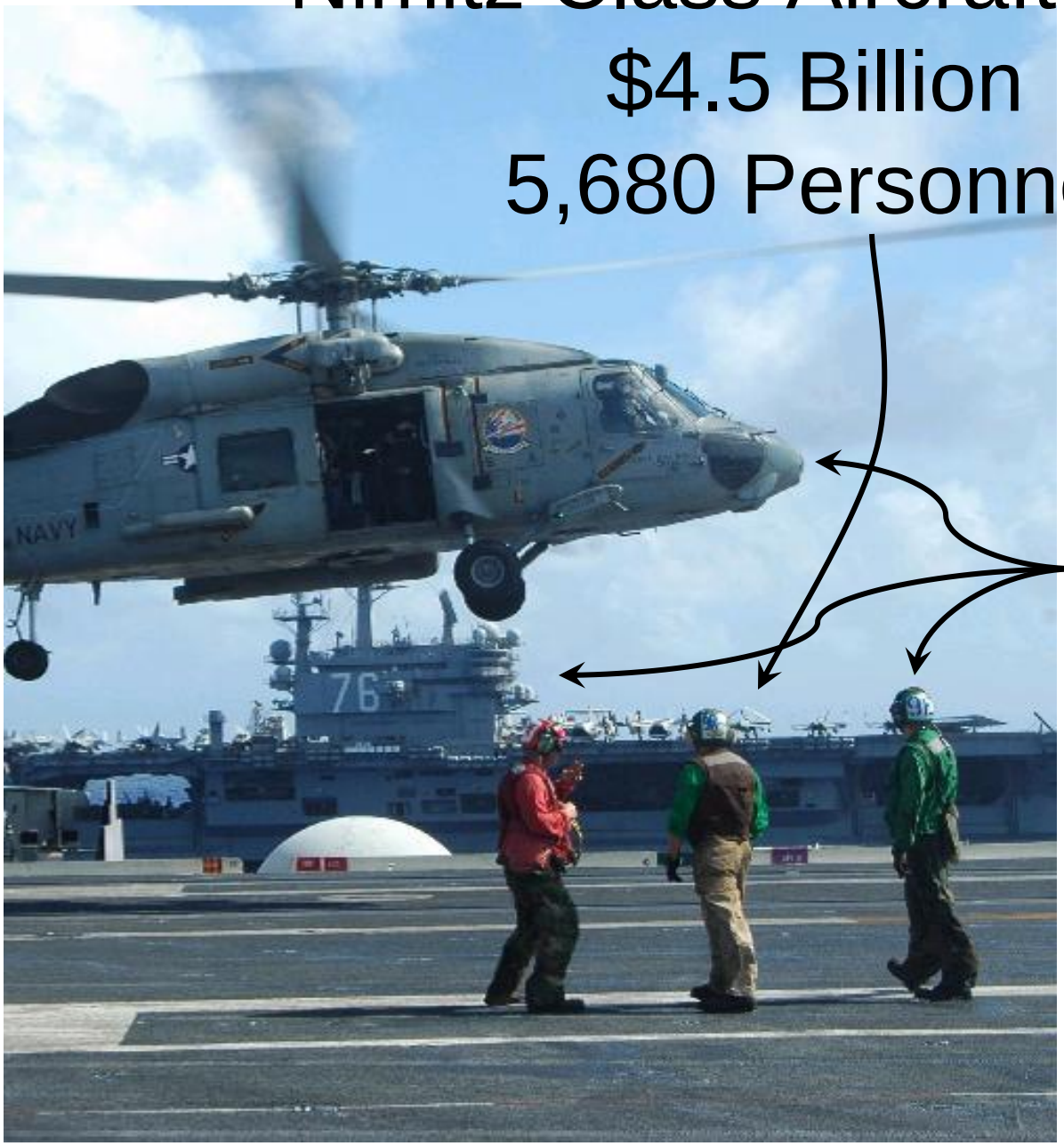
MIL-STD-882D

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	**I**	**Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation**
Critical	**II**	**Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation**
Marginal	**III**	**Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished**
Negligible	**IV**	**Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation**

Nimitz Class Aircraft Carrier

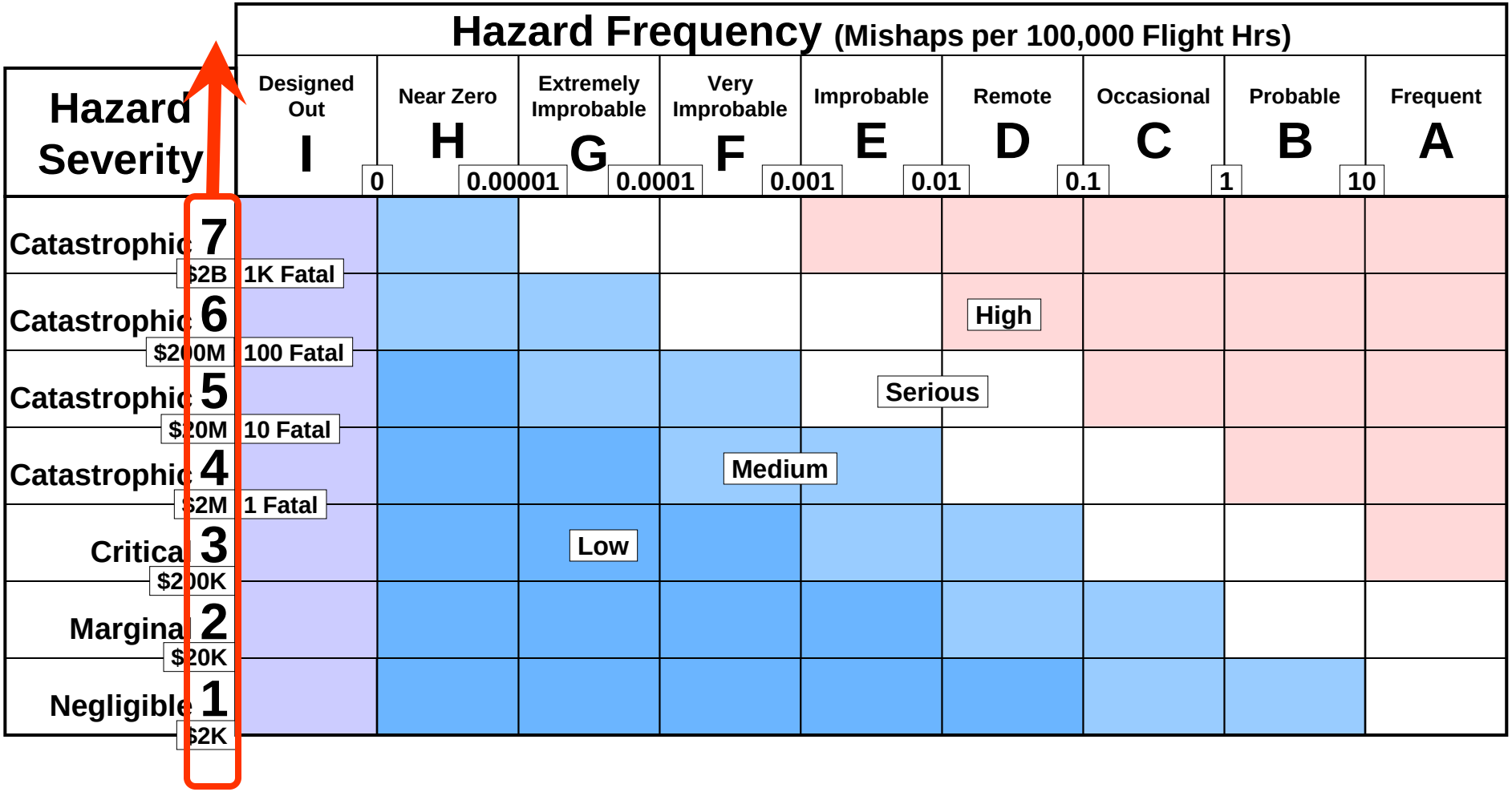
$4.5 Billion

5,680 Personnel



Class A
Severity 1
“Catastrophic”

Severity category numbered to increase with severity



Mercalli Intensity Scale

I.	Instrumental	Generally not felt by people unless in favorable conditions.
II.	Weak	Felt only by a few people at best, especially on the upper floors of buildings. Delicately suspended objects may swing.
III.	Slight	Felt quite noticeably by people indoors, especially on the upper floors of buildings. Many do not recognize it as an earthquake. Standing motor cars may rock slightly. Vibration similar to the passing of a truck. Duration estimated.
IV.	Moderate	Felt indoors by many people, outdoors by few people during the day. At night, some awaken. Dishes, windows, doors disturbed; walls make cracking sound. Sensation like heavy truck striking building. Standing motor cars rock noticeably. Dishes and windows rattle alarmingly.
V.	Rather Strong	Felt inside by most, may not be felt by some outside in non-favorable conditions. Dishes and windows may break and large bells will ring. Vibrations like large train passing close to house.
VI.	Strong	Felt by all; many frightened and run outdoors, walk unsteadily. Windows, dishes, glassware broken; books fall off shelves; some heavy furniture moved or overturned; a few instances of fallen plaster. Damage slight.
VII.	Very Strong	Difficult to stand; furniture broken; damage negligible in building of good design and construction; slight to moderate in well-built ordinary structures; considerable damage in poorly built or badly designed structures; some chimneys broken. Noticed by people driving motor cars.
VIII.	Destructive	Damage slight in specially designed structures; considerable in ordinary substantial buildings with partial collapse. Damage great in poorly built structures. Fall of chimneys, factory stacks, columns, monuments, walls. Heavy furniture moved.
IX.	Violent	General panic; damage considerable in specially designed structures, well designed frame structures thrown out of plumb. Damage great in substantial buildings, with partial collapse. Buildings shifted off foundations.
X.	Intense	Some well built wooden structures destroyed; most masonry and frame structures destroyed with foundation. Rails bent.
XI.	Extreme	Few, if any masonry structures remain standing. Bridges destroyed. Rails bent greatly.
XII.	Cataclysmic	Total destruction – Everything is destroyed. Lines of sight and level distorted. Objects thrown into the air. The ground moves in waves or ripples. Large amounts of rock move position. Landscape altered, or levelled by several meters. In some cases, even the routes of rivers are changed.

Moment Magnitude Scale

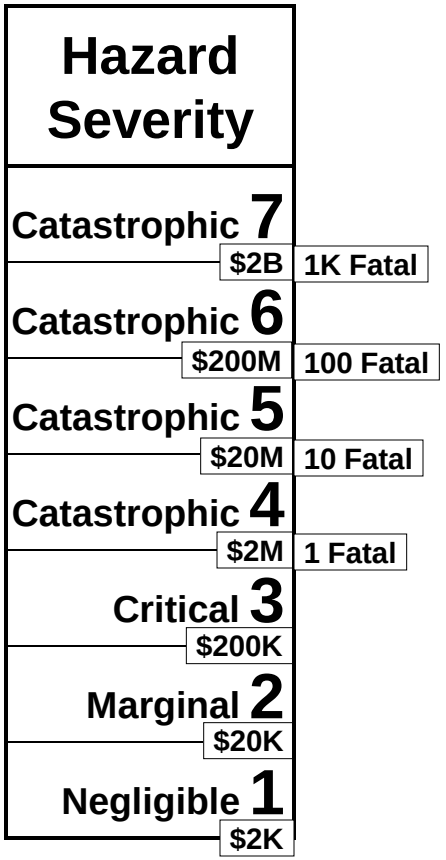
$$M_w = \frac{2}{3} \log_{10} M_0 - 10.7$$

Formerly Richter Magnitude Scale

Magnitude	Earthquake Effects	Frequency of Occurrence
Less than 2.0	Microearthquakes, not felt	About 8,000 per day
2.0-2.9	Generally not felt, but recorded	About 1,000 per day
3.0-3.9	Often felt, but rarely causes damage	49,000 per year (est.)
4.0-4.9	Noticeable shaking of indoor items, rattling noises. Significant damage unlikely	6,200 per year (est.)
5.0-5.9	Can cause major damage to poorly constructed buildings over small regions. At most slight damage to well-designed buildings	800 per year
6.0-6.9	Can be destructive in areas up to about 100 miles across in populated areas	120 per year
7.0-7.9	Can cause serious damage over larger areas	18 per year
8.0-8.9	Can cause serious damage in areas several hundred miles across	1 per year
9.0 or greater	Devastating in areas several thousand miles across	1 per 20 years

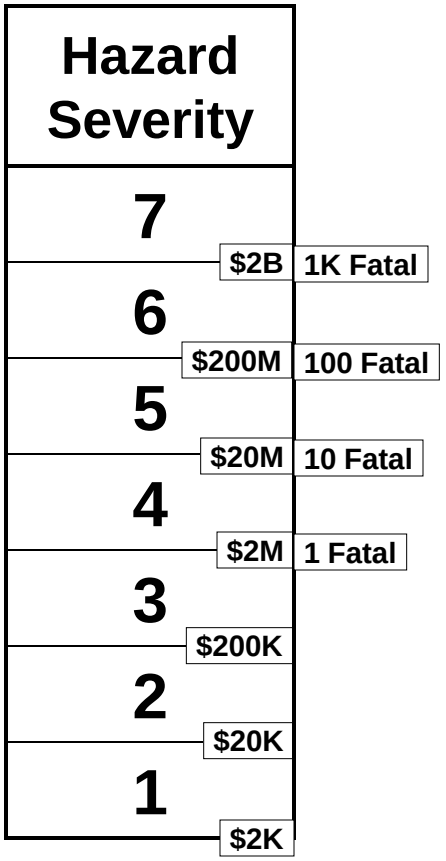
Labels

- “Catastrophic”
- “Critical”
- “Marginal”
- “Negligible”
- Needed?
- Diversity of meaning from person to person



Labels

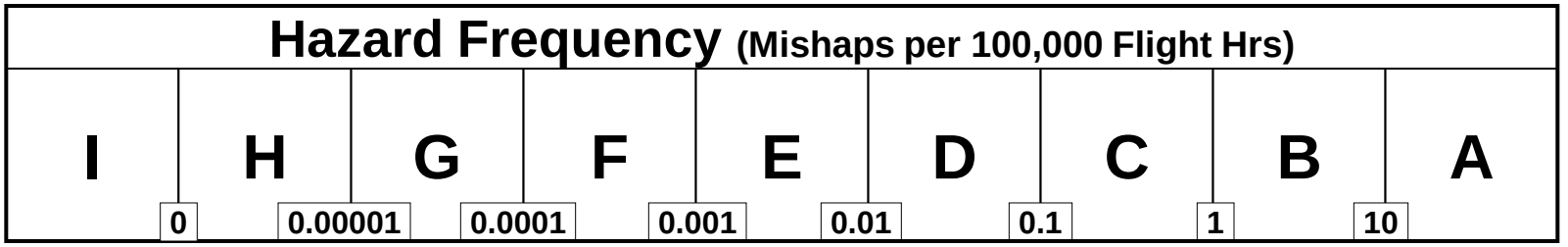
- “Severity Category 4”
- “Category 4”
- “Severity 4”
- No denotative baggage



Frequency (Probability)

Hazard Frequency (Mishaps per 100,000 Flight Hrs)								
Designed Out	Near Zero	Extremely Improbable	Very Improbable	Improbable	Remote	Occasional	Probable	Frequent
I	**H**	**G**	**F**	**E**	**D**	**C**	**B**	**A**
0	0.00001	0.0001	0.001	0.01	0.1	1	10	

Frequency (Probability)



“Hazard”

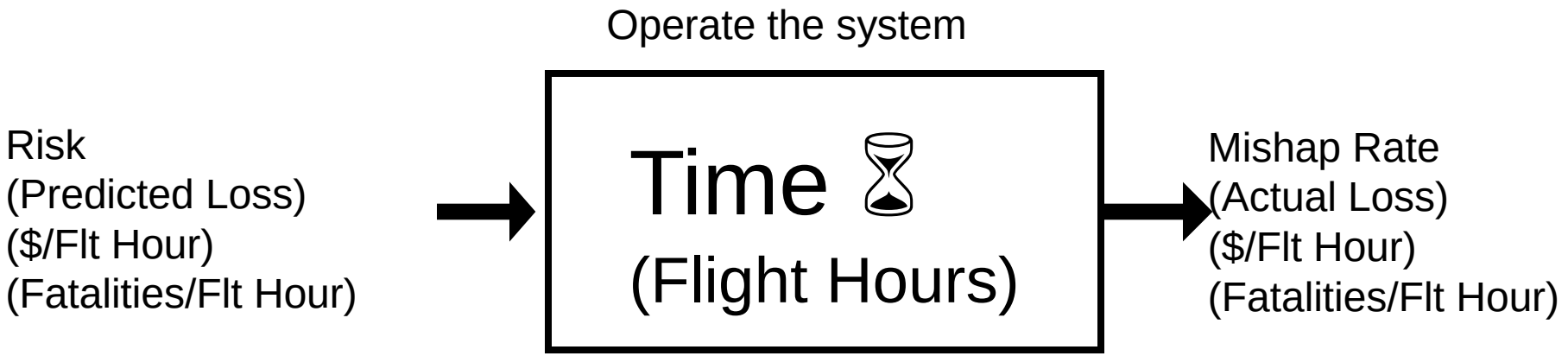
Potential for harm (the threat of harm)	ANSI/GEIA-STD-0010-2009 FAA System Safety Handbook
A condition that is prerequisite to a mishap	ANSI/GEIA-STD-0010-2009 Joint Software Systems Safety Engineering Handbook MIL-STD-882B, MIL-STD-882C NASA Reference Publication 1358 FAA System Safety Handbook
Any actual or potential condition that can cause injury, illness, or death of personnel or damage to or loss of equipment, property or mission degradation, or a condition or activity with potential to cause damage, loss, or mission degradation	MIL-STD-882D Draft MIL-STD-882E AR 385-10 DA Pam 385-16 OPNAVINST 5100.24B AOP-52 Air Force System Safety Handbook

“Risk”

Expected (or potential) Loss	ANSI/GEIA-STD-0010-2009 AR 385–10 FAA System Safety Handbook
An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence	ANSI/GEIA-STD-0010-2009 AR 385–10 FAA System Safety Handbook NASA Reference Publication 1358 Draft MIL-STD-882E IEEE Std 1228-1994 OPNAVINST 5100.24B MIL-STD-882D AOP 52 Joint Software Systems Safety Engineering Handbook Unmanned Systems Safety Guide MIL-STD-882B, MIL-STD-882C Air Force System Safety Handbook

Mishap Risk & Mishap Loss

Mishap Risk over Time results in Mishap Loss



“Causal Factor”

- **Causal Factor (Webster’s)**
  - **Causal - “Expressing a cause or reason”**
  - **Factor - “Any of the circumstances, conditions, etc. that bring about a result”**
- **Examples:**
  - **Materiel - equipment failure and damage that result from design flaws, component failures, etc.**
  - **Environmental – weather conditions, temperature, vibration, shock, or illumination that adversely affect the performance of the individual or equipment.**
  - **Human errors - inherent to human design, function and behavior. (slips, mistakes, omission, commission)**

Factor

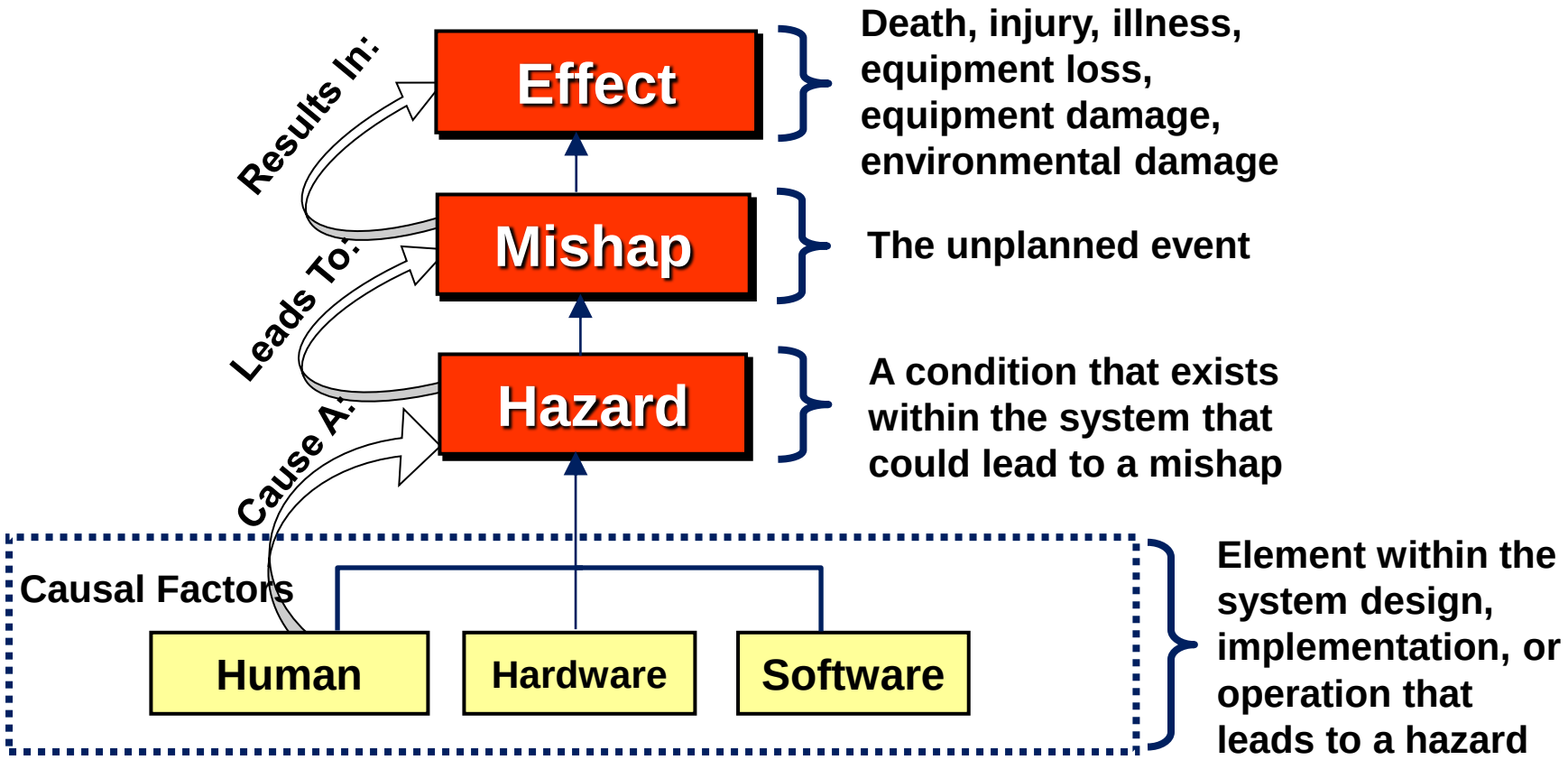
Factor. A hackneyed word; the expressions of which it forms part can usually be replaced by something more direct and idiomatic.

William Strunk, Jr. (1869–1946)
The Elements of Style, 1918.

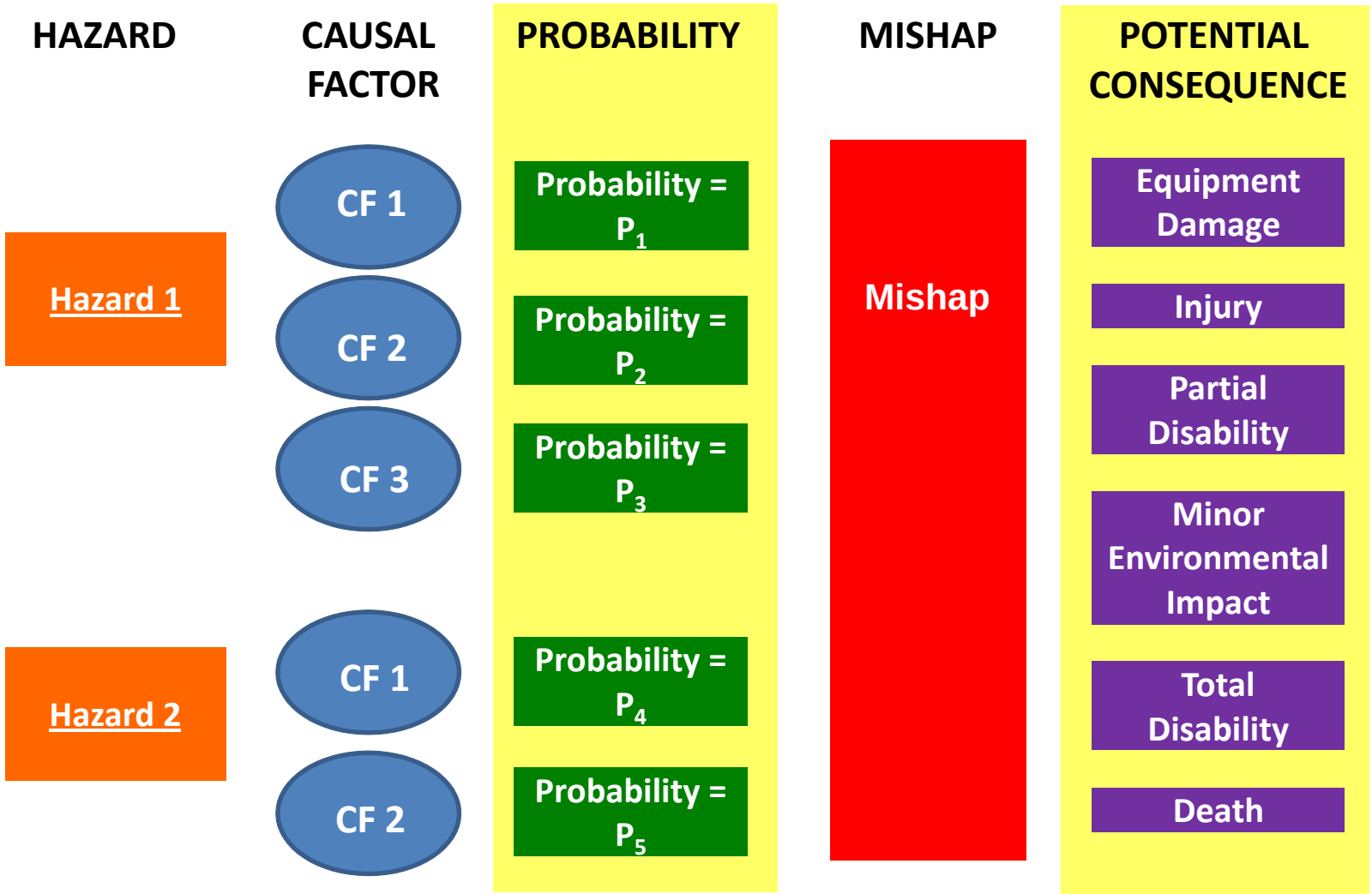
His superior training was the great factor in his winning the match.	He won the match by being better trained.
Heavy artillery is becoming an increasingly important factor in deciding battles.	Heavy artillery is playing a larger and larger part in deciding battles.

Causal factor	Cause; Hazard

Causal Factors

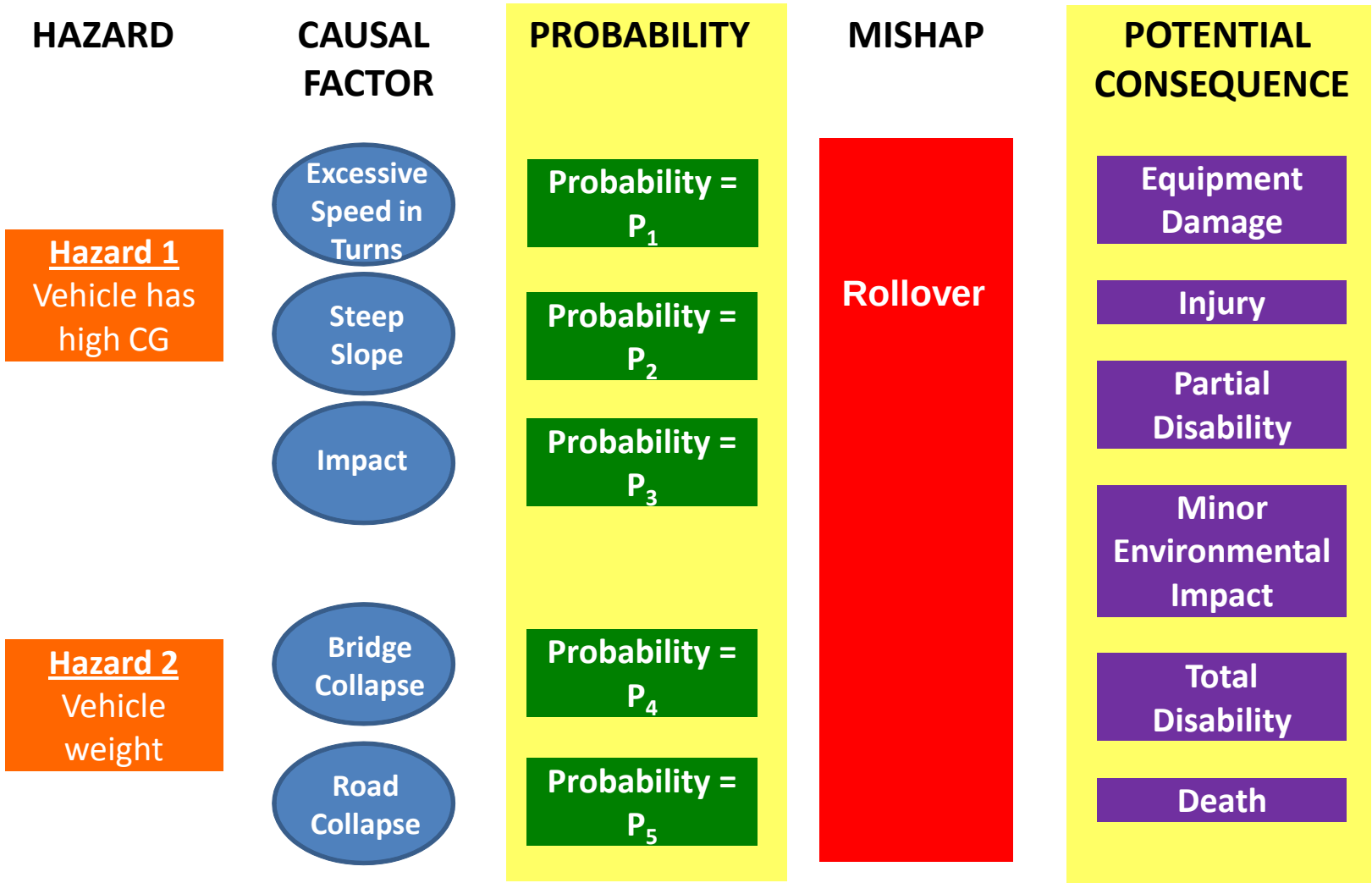


Hazard/Risk Model



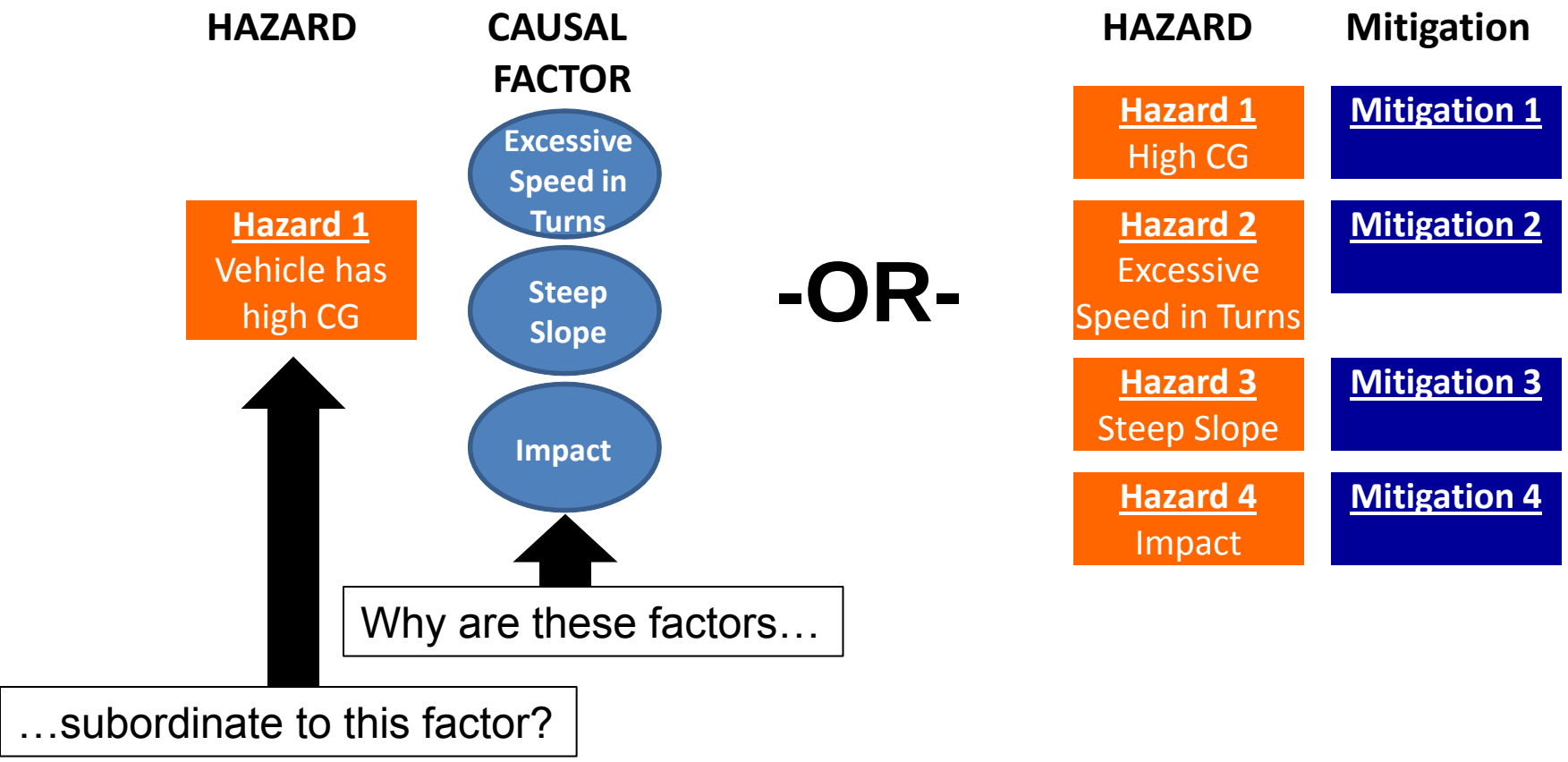
As of: 18 Aug 2010

Risk Example – MRAP Family of Vehicles

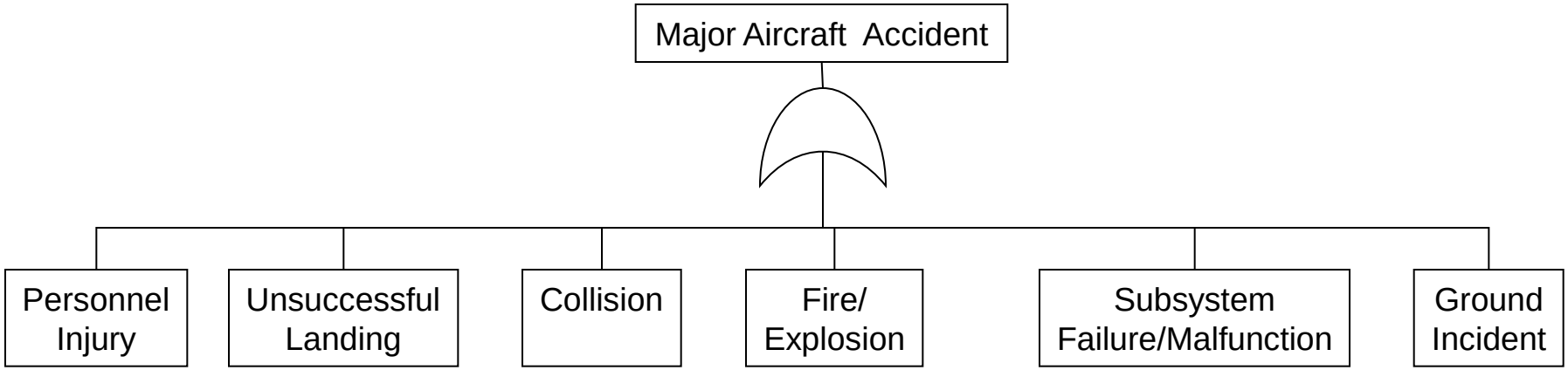


As of: 18 Aug 2010

Alternatives



Major Aircraft Accident Tree



- Electric Shock
- Toxic Fumes /Substances
- Hot Components
- Moving Parts
- High Pressure Fluids

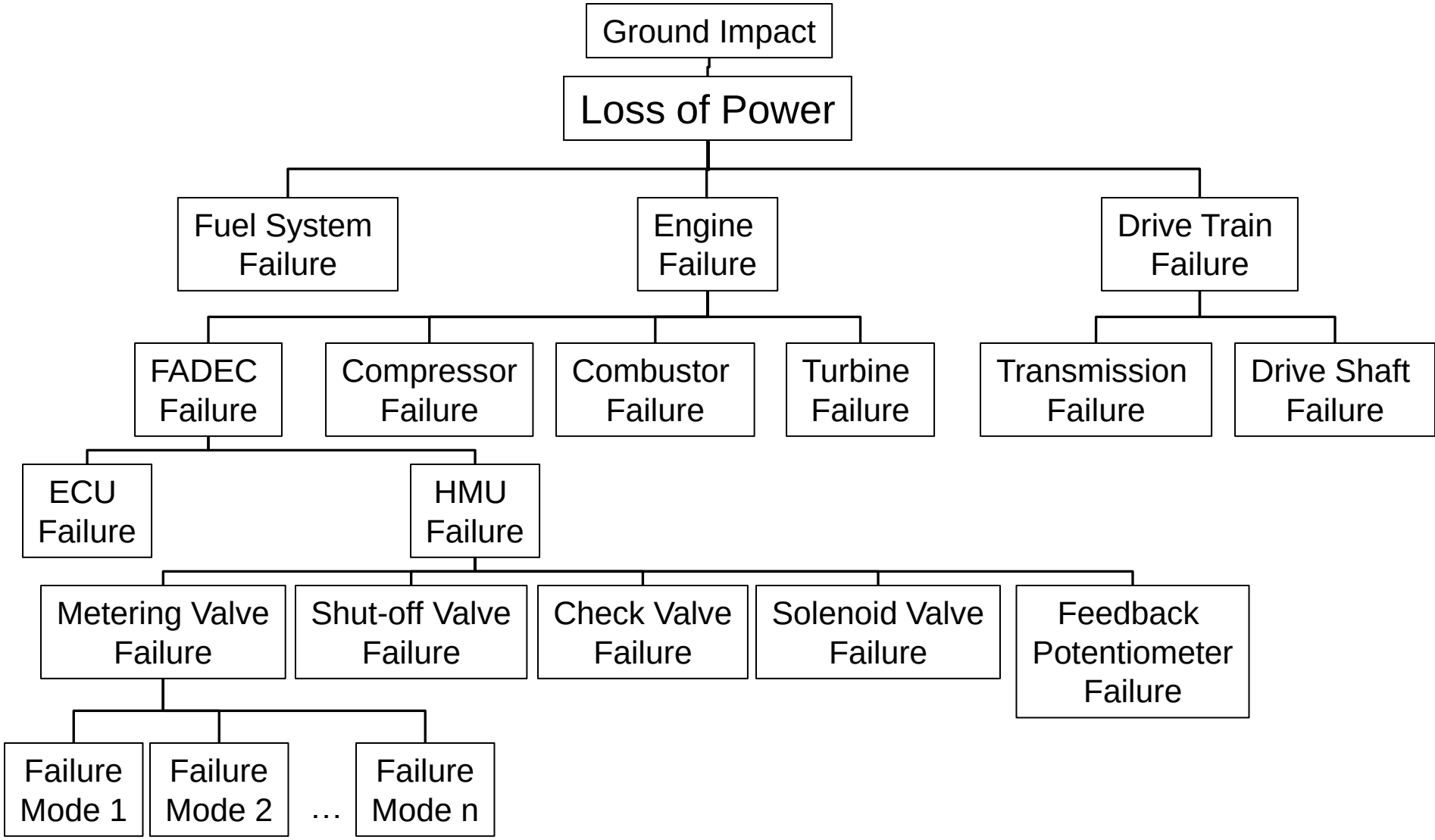
- Land on unsuitable terrain
- Tailrotor strikes ground
- Unsuccessful touchdown
- High sink rate
- Landing gear failure

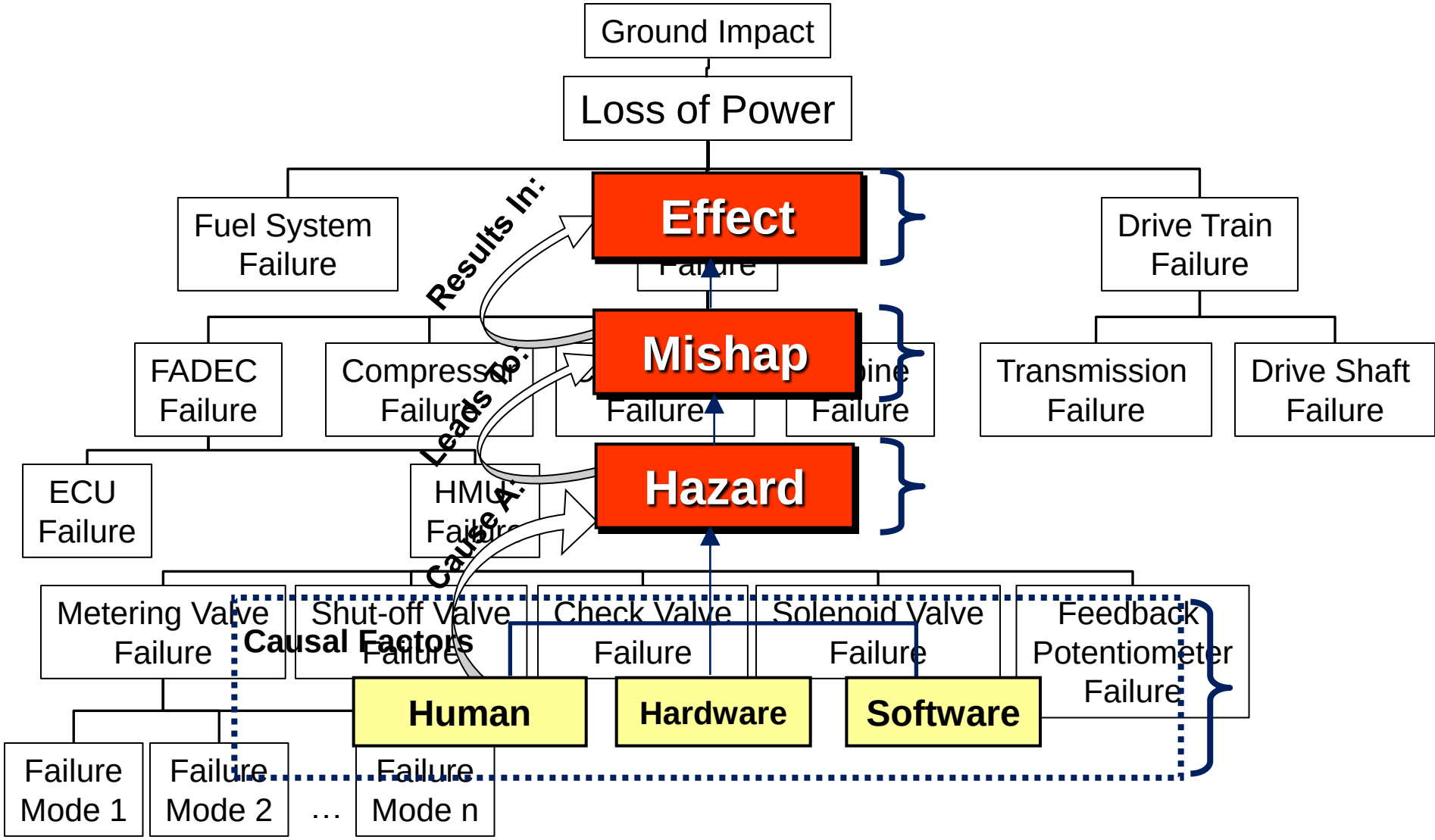
- Mid-air collision
- Hover collision
- Ground/ obstruction collision in flight
- Bird Strike

- Uncontrolled fire
- Uncontrolled explosion
- Premature armament detonation
- Premature gun actuation

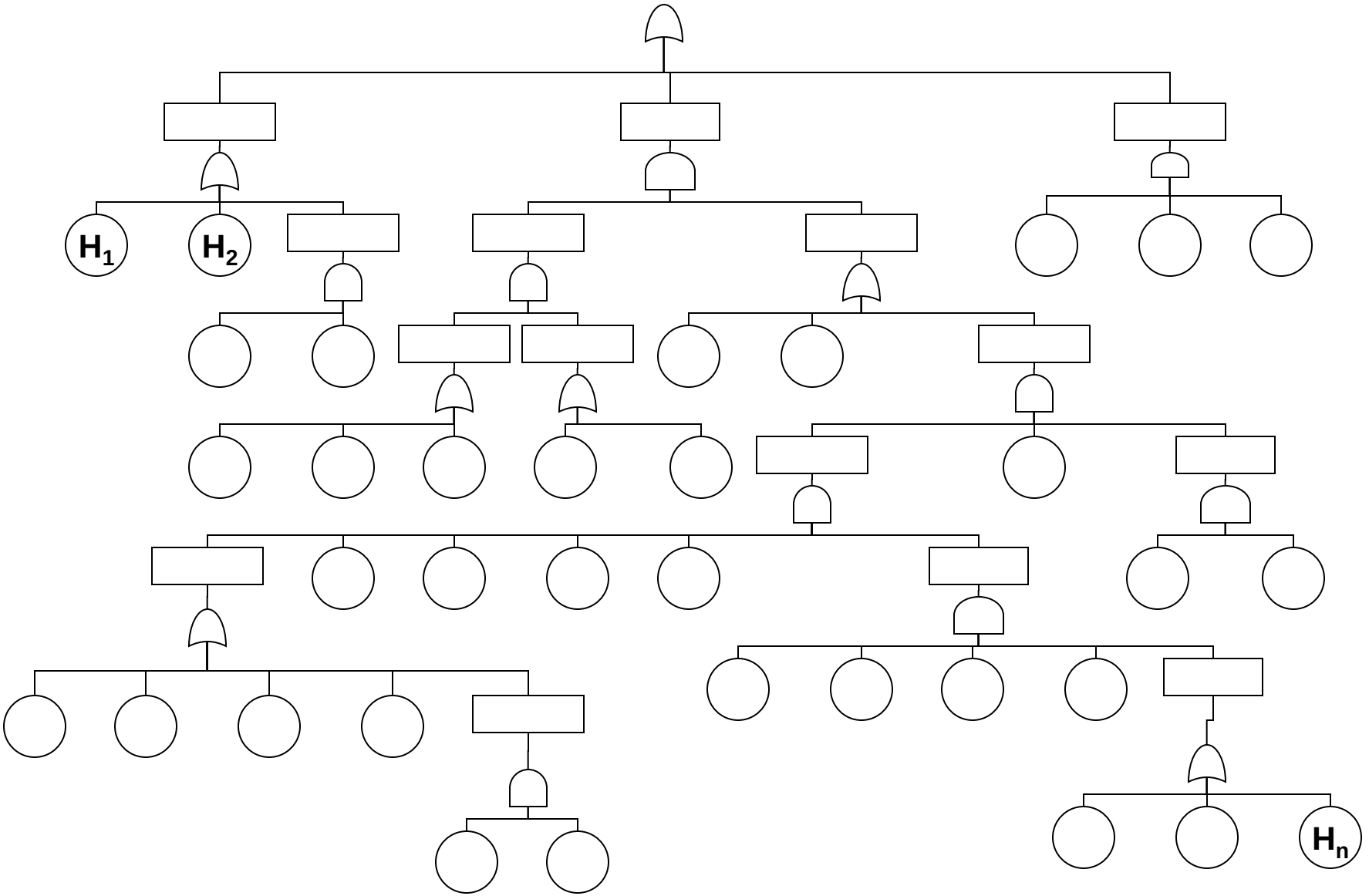
- Airframe
- Main transmission
- Main Rotor
- Tail Rotor
- Flight Control
- MEP
- Cockpit
- Hydraulic
- Electrical
- Fuel
- Powerplant

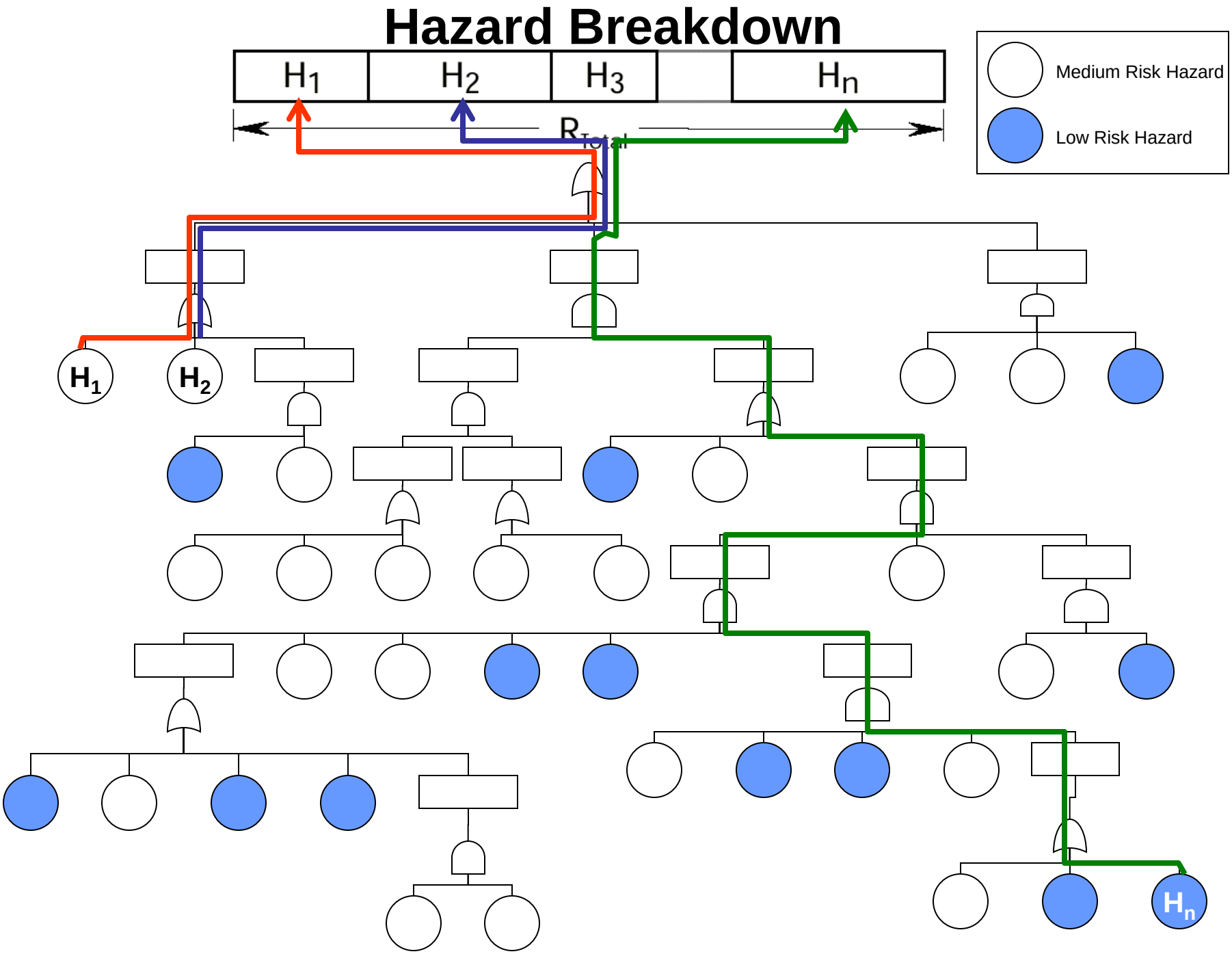
- Rotorwash
- Improper Maintenance Procedure
- Taxi Collision
- Ground Resonance
- Main rotor Strikes Tail


Ground Impact
Loss of Power
Fuel System Failure
Engine Failure
Drive Train Failure
FADEC Failure
Compressor Failure
Combustor Failure
Turbine Failure
Transmission Failure
Drive Shaft Failure
ECU Failure
HMU Failure
Metering Valve Failure
Shut-off Valve Failure
Check Valve Failure
Solenoid Valve Failure
Feedback Potentiometer Failure
Failure Mode 1
Failure Mode 2
…
Failure Mode n


Ground Impact
Loss of Power
Effect
Mishap
Hazard
Results In:
Leads to:
Caused By:
Fuel System Failure
Drive Train Failure
FADEC Failure
Transmission Failure
Drive Shaft Failure
ECU Failure
Metering Valve Failure
Shut-off Valve Failure
Check Valve Failure
Solenoid Valve Failure
Feedback Potentiometer Failure
Causal Factors
Human
Hardware
Software
Failure Mode 1
Failure Mode 2
Failure Mode n

Hazard Breakdown




Hazard Breakdown
H1
H2
H3
Hn
RTotal
Medium Risk Hazard
Low Risk Hazard
H1
H2
Hn

Rule of Thumb

Breakdown hazards to the level where you will apply mitigation.

Criticality

Criticality = Risk?

Criticality = Severity?

Criticality

Criticality: A measure of the impact of a failure mode on the mission objective. Criticality combines the potential frequency of the occurrence and the level of severity of the failure mode.

Criticality The priority rank of a failure mode, based on some assessment criteria such as operational and HSE (Health, Safety, Environment) consequences, and the likelihood of failure occurrence.

Criticality. A relative measure of the consequences of a failure mode and its frequency of occurrences. MIL-STD-1629A

Acceptable Risk

Risk that the appropriate acceptance authority (as defined in DoDI 5000.02) is willing to accept without additional mitigation. -- Draft MIL-STD-882E, System Safety, 14 Jul 2011

That part of identified risk which is allowed by the managing activity to persist without further engineering or management action. -- Air Force System Safety Handbook, July 2000

The residual (final) risk remaining after application of controls, i.e. Hazard Controls / Risk Controls, have been applied to the associated Contributory Hazards; that have been identified and communicated to management for acceptance. -- FAA System Safety Handbook, 30 December 2000

That level of residual safety risk that the managing authority is willing to assume on behalf of the agency, users, and public. -- ANSI/GEIA-STD-0010-2009, Standard Best Practices for System Safety Program Development and Execution, 12 Feb 09

Part of identified risk that is allowed to persist without further engineering or management action to mitigate or control. -- Joint Software Systems Safety Engineering Handbook, Version 1.0, August 27, 2010

Acceptable Risk

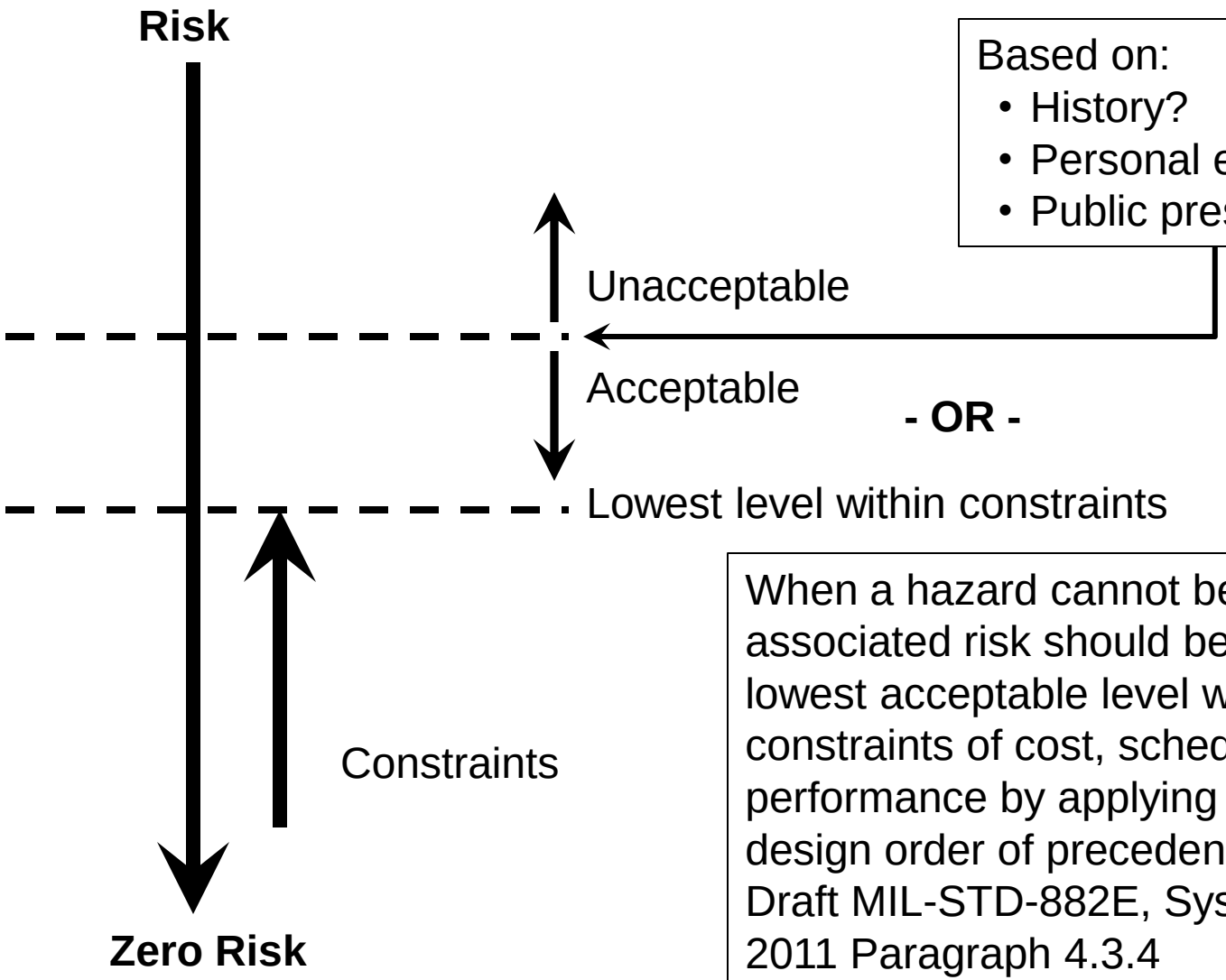
A level of risk, referred to a specific item, system or activity, that, when evaluated with consideration of its associated uncertainty, satisfies pre-established risk criteria. -- NASA General Safety Program Requirements, NPR 8715.3C, March 12, 2008 (w/Change 4, July 20, 2009)

Acceptable risk is the part of identified risk that is allowed to persist without further engineering or management action. Making this decision is a difficult yet necessary responsibility of the managing activity. This decision is made with full knowledge that it is the user who is exposed to this risk. [FAA System Safety Handbook, Dec 2000] -- Unmanned Systems Safety Guide for DOD Acquisition, 27 June 2007

Unacceptable risk. That risk which cannot be tolerated by the managing activity. It is a subset of identified risk. Unacceptable risk is either eliminated or controlled. -- Air Force System Safety Handbook, July 2000

Unacceptable risk is that risk which cannot be tolerated by the managing activity. It is a subset of identified risk that must be eliminated or controlled. [FAA System Safety Handbook, Dec 2000] -- Unmanned Systems Safety Guide for DOD Acquisition, 27 June 2007

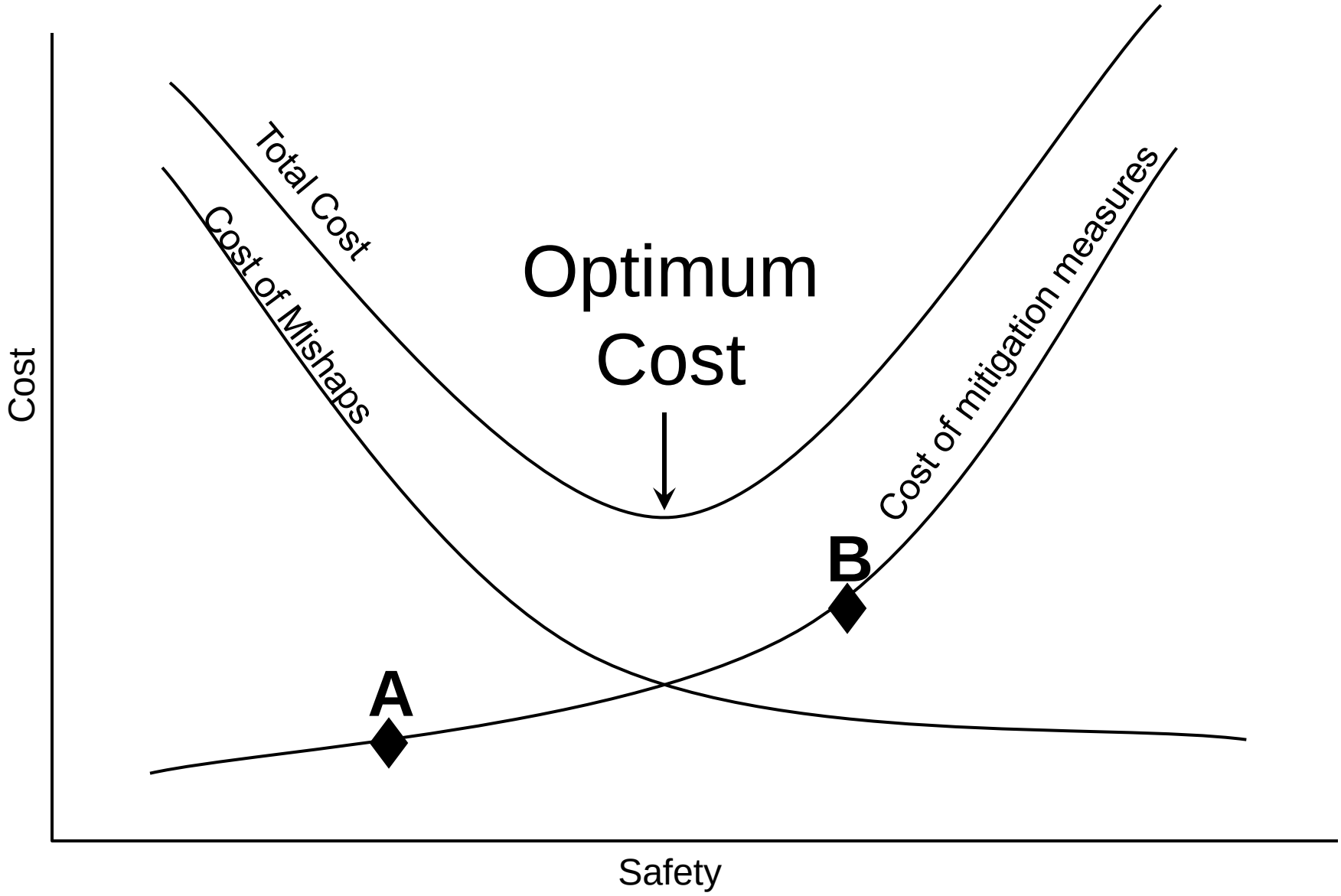
Acceptable Risk



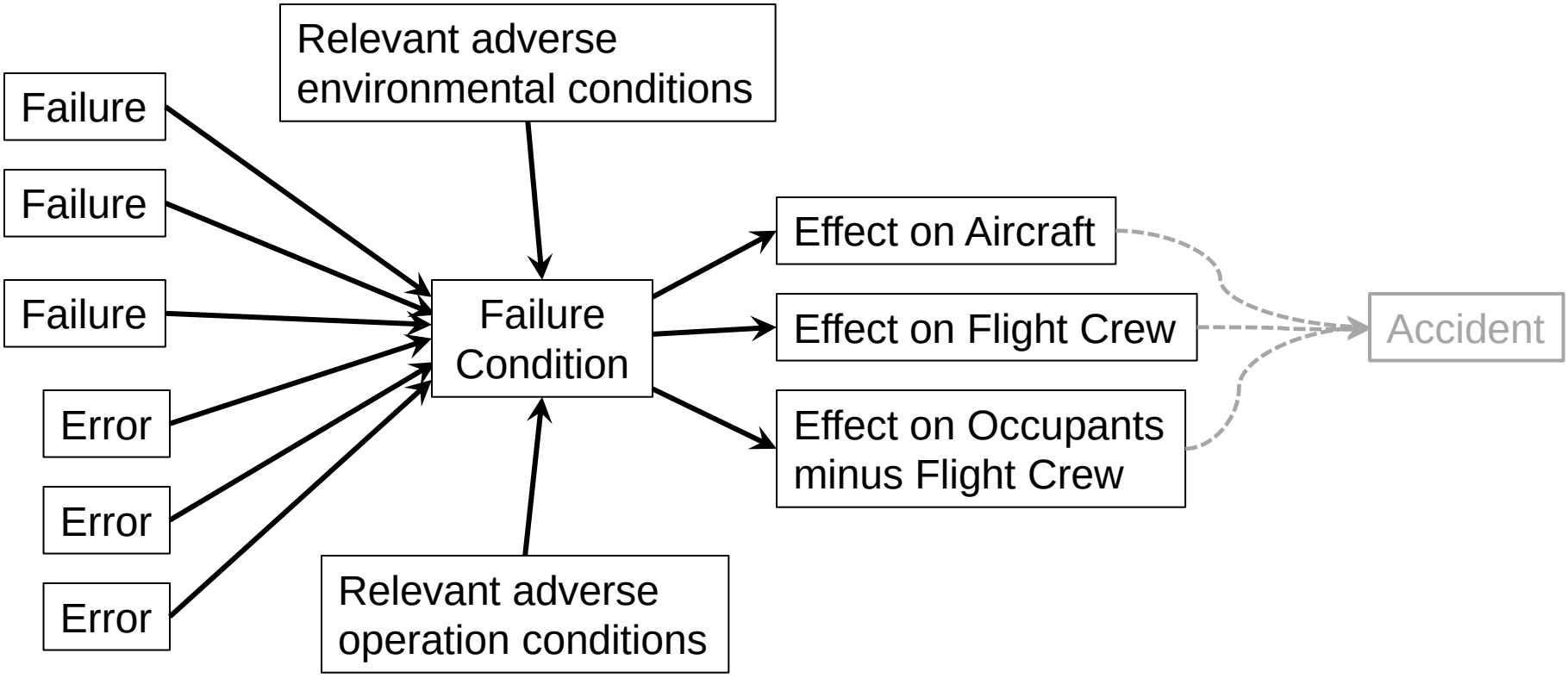
Based on:
- History?
- Personal experience?
- Public pressure?

- OR -

When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence.
Draft MIL-STD-882E, System Safety, 14 Jul 2011 Paragraph 4.3.4


Cost
Safety
Total Cost
Cost of Mishaps
Optimum
Cost
Cost of mitigation measures
A
B

Hazard vs Failure Condition



Classification of Failure Conditions	Effect on Aircraft	Effect on Flight Crew	Effect on Occupants Excluding Flight Crew	Allowable Qualitative Probability	Allowable Quantitative Probability
Catastrophic	Normally with hull loss	Fatalities or incapacitation	Multiple Fatalities.	Extremely Improbable	<1E-9
Hazardous	Large reduction in functional capabilities or safety margins	Physical distress or excessive crew workload impairs ability to perform tasks	Serious or fatal injury to a small number of passengers or cabin crew.	Extremely Remote	<1E-7
Major	Significant reduction in functional capabilities or safety margins.	Physical discomfort or significant increase in workload	Physical distress possibly including injuries	Remote	<1E-5
Minor	Slight reduction in functional capabilities or safety margins	Slight increase in workload.	Physical discomfort	Probable	<1E-3
No Safety Effect	No effect on operational capabilities or safety	No effect	Inconvenience	No probability requirement	No probability requirement

What say you?