

NASA SAFETY TRAINING CENTER

**A CHARLATAN'S GUIDE
to
QUICKLY ACQUIRED
QUACKERY**

The TROUBLE with SYSTEM SAFETY

**P. L. Clemens
September 2001**

SYSTEM SAFETY: A FIELD IN WHICH QUACKERY IS READILY MASTERED!

Let's look at the

UNDERPINNINGS of SUCCESSFUL MALPRACTICE

found in:

- *traditions,*
- *folklore,*
- *revered texts,*
- *standards and regulations.*

But *first*, an *Important Concept*: 

An *Important Concept...*

“QUANTUM QUACKERY”

...widely employed, but little understood.

Its foundation is...

The QUACKON:

***“The least corpuscular
unit of quackery”***

(cf.: Photon; Electron)

TWO MAJOR QUACKON SOURCES...

- **The PRACTICES** ...with wondrous opportunities for the practicing charlatan.
- **The DEFINITIONS** ...a quagmire of madness, providing exquisite guidance.



***The
PRACTICES***

- High quality quackery is:
 - easily mastered,
 - rarely detected,
 - often required by standards.
- Basic guidelines are easy to follow.

(Not available in stores.)

QUACKERY IS A “LEGACY” PHENOMENON..

- ***The NOSTALGIA IMPERATIVE..***

- “If the errors of the past were good enough for our ancestors, they’re good enough for us!”

- “We have a four-decade history of doing it this way — therefore, it’s RIGHT!”

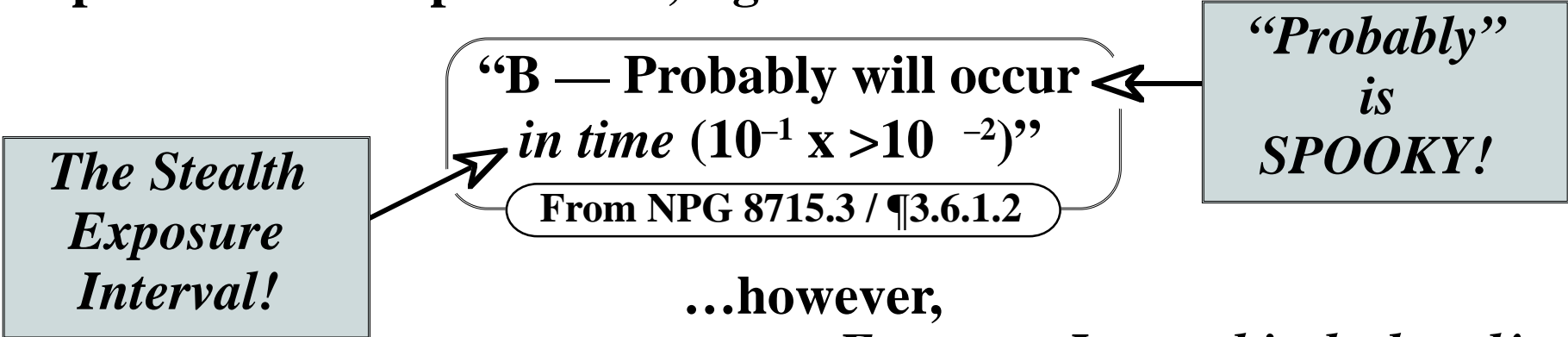
- ***DRIVEN by DREAD!***

- “Don’t ever make the wrong mistake!”
(Yogi Berra)

QUACKON 1: **Contempt for TIME** as a **Quantitative Concept...**

- **OPPORTUNITY:**

System Safety Analyses give quantitative or qualitative risk assessments, and use risk tolerance guidance based on probabilities expressed as, e.g.:



...however,
no Exposure Interval is declared!

“Time is but a dewdrop on the lotus leaf!”

QUACKON 1: (continued)

- **BUT**, fortunately, probability is Meaningless unless attached to an *Interval of Exposure* — e.g., specified hours of operation, missions flown, miles driven. Meaninglessness is the Charlatan's handmaiden!
- **SO...** exploit *meaninglessness!* Select whatever Exposure Interval produces the level of probability that suits the risk acceptance purposes at hand!

“*Improbable*”
is
COMFORTING!

“E — Improbable to
occur. (10^{-6} x)”

From NPG 8715.3 / ¶3.6.1.2

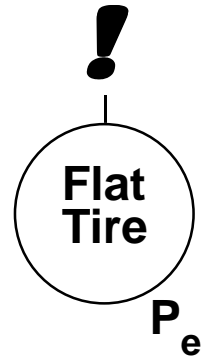
No Exposure
Interval is
declared!

If it was good
enough for
them, it's good
enough for *us!*

...*OR*, select no Exposure Interval at all!
...but be quiet about it!

“*Imprecise Precision is
conceptionally advantageous!*”

QUACKON 2: P_{TOP} too High? *Editorialize It Down...*



- **OPPORTUNITY:**

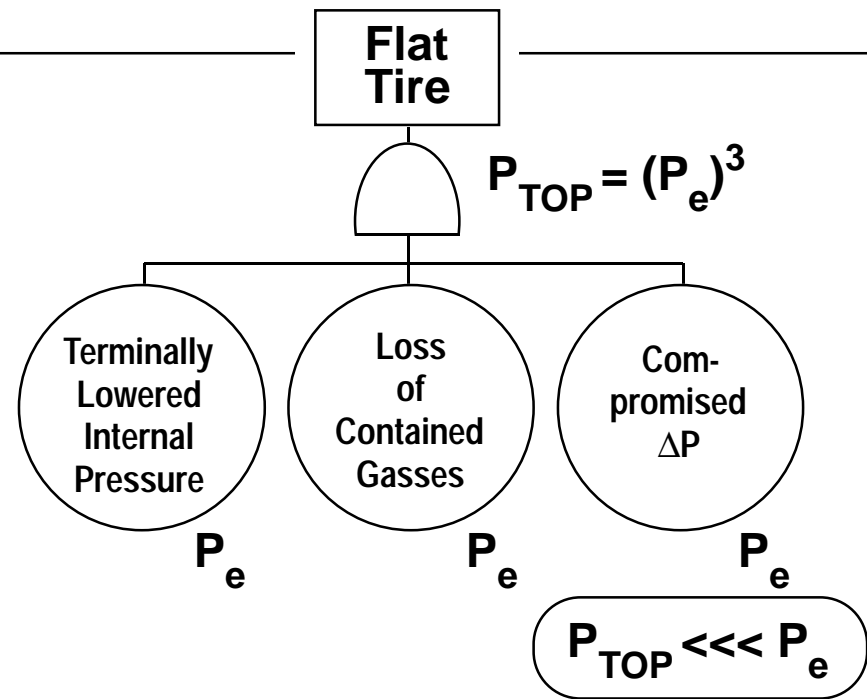
- Probability of failure for a critical system function is analyzed to be ***much too high***.
- Budget limitations preclude engineering countermeasures.
Oh, woe! (...and / or whoa!)

QUACKON 2: (continued)

BUT, the analyst can “reduce” P_{TOP} by adjusting *language* rather than *system architecture*.

SO... when *engineering* gets costly, economize with *language!*

Creative editing
is
mightier than the sword!



“Truth must never stand in the way of delivering a good product for a good price!”

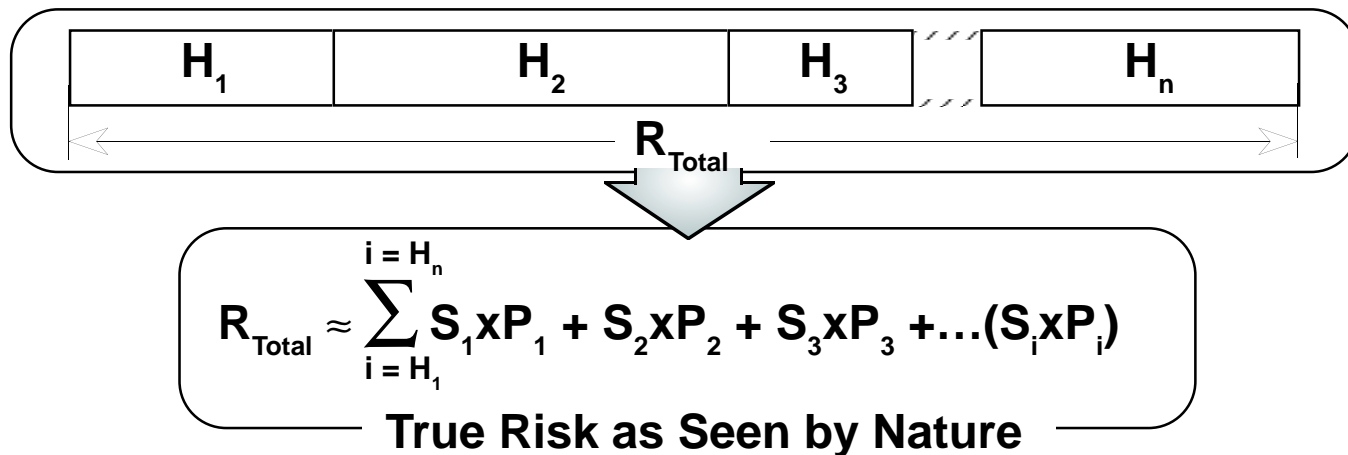
Xavier Onasis

QUACKON 3: **QUASH OUTRAGEOUS RISK...**

Summed System Risk is Spooky!

DO SOMETHING!

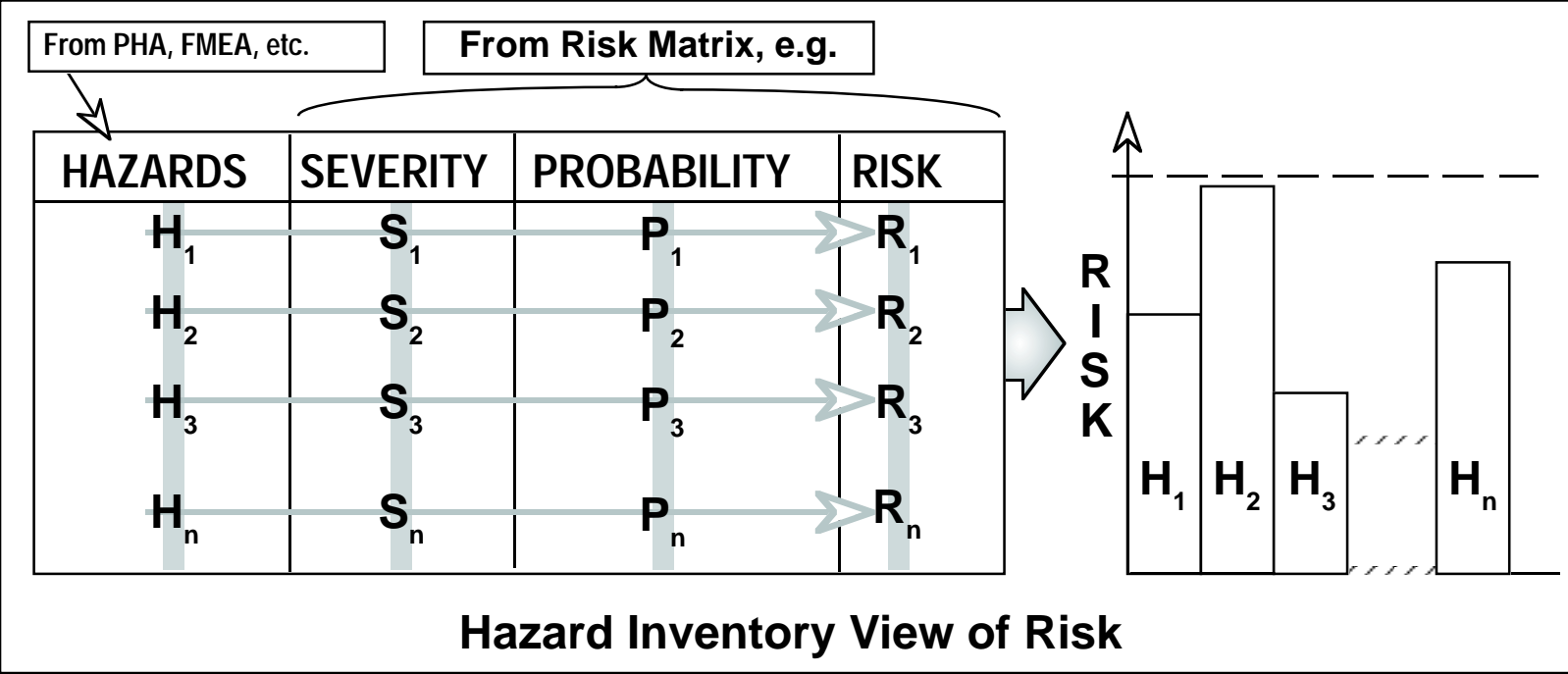
- **OPPORTUNITY:** Nature sees only *total population risk* — i.e., the *summed* risks of all individual system hazards.



This summation result is often
ALARMINGLY HIGH RISK!

QUACKON 3: (continued)

- BUT:** The hazard inventory techniques (e.g., PHA, FHA, FMEA) view risk *hazard-by-hazard*. If individual hazards pose acceptable risk, system risk is judged acceptable.



- SO...** a large inventory of individual hazards can be disguised as a “safe” system! — even though in reality it may portend a grim...

DISASTER!

“Too much analysis can make anything look perilous!”

QUACKON 4: **Ignore Operational Phasing...**

- ***OPPORTUNITY***: Most system crashes occur during performance transients:

- **Startup**
- **Shutdown**
- **E-stop**
- **Load Change**

QUACKON 4: (continued)

- **BUT**, in truth...

TRANSIENTS ARE BRIEF!

- They occupy only a small portion of total operating exposure.
 - They're also tough to analyze — things *change* during them.
- **SO...** search for hazards and analyze their risks *only for the system “full-up” and operating normally.*

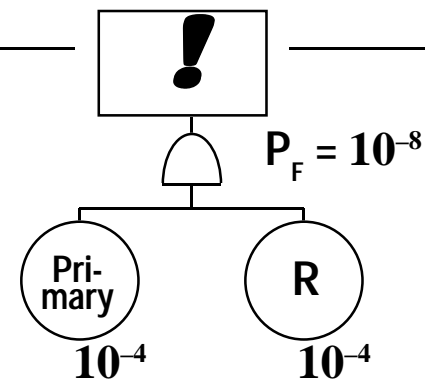
Ignore the petty stuff. Later, you'll have lots of employment opportunities ...investigating the transient mishaps!

“Transients are only a way of getting from one Steady State to another!”

QUACKON 5: To Sanctify, Redundify

...pile it on!

- **OPPORTUNITY:** Despite use of redundancy, failure probability for a critical function is reckoned at 10^{-8} , a value feared to be *much too high*.



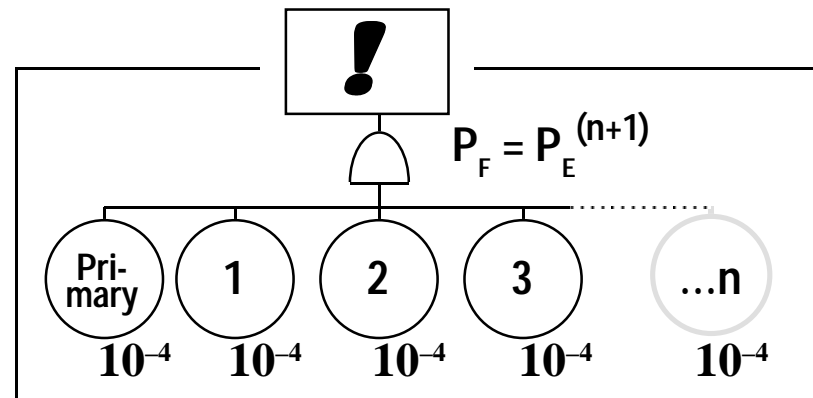
QUACKON 5: (continued)

- ***BUT***, how low is low *enough*? More redundancy'll do it!

Two levels gives 10^{-12} . Three levels gives 10^{-16} .

When they want small numbers, give 'em *small* numbers!

- ***SO...*** you don't need good engineering if you've got lots of parts! *PILE 'EM ON!*



In truth, these numbers become *preposterously low*. Probability of Earth's annihilation by collision with an extraterrestrial object is $10^{-14}/\text{hr}$. What'll *that* event do to your critical function?

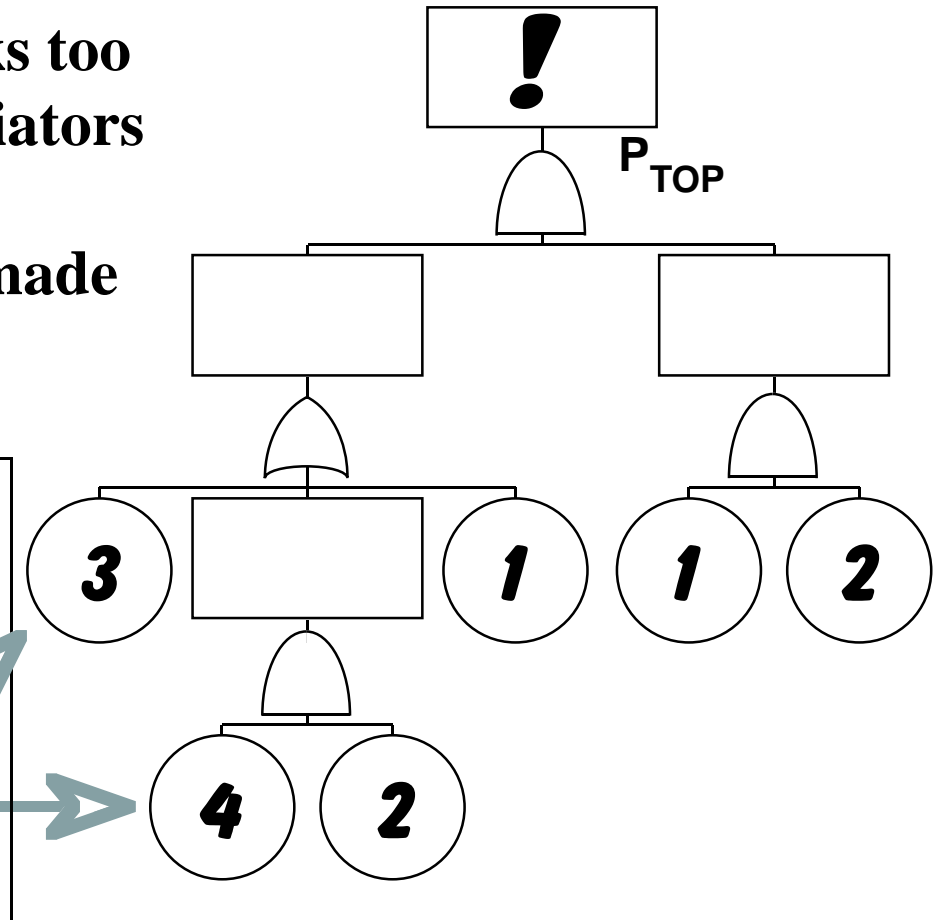
QUACKON 6: **Spend the money on the things you can fix...**

- **OPPORTUNITY:** TOP looks too vulnerable with all those initiators under it.

Initiators 3 and 4 are easily made more robust, and at low cost.

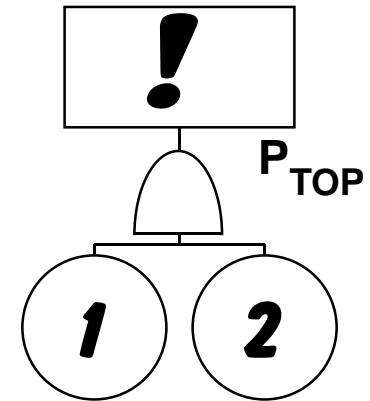
**BE A HERO!
DO IT!
SPEND THE MONEY!**

*Don't fix the SYSTEM
when it's cheaper to fix the
TREE!*



QUACKON 6: (continued)

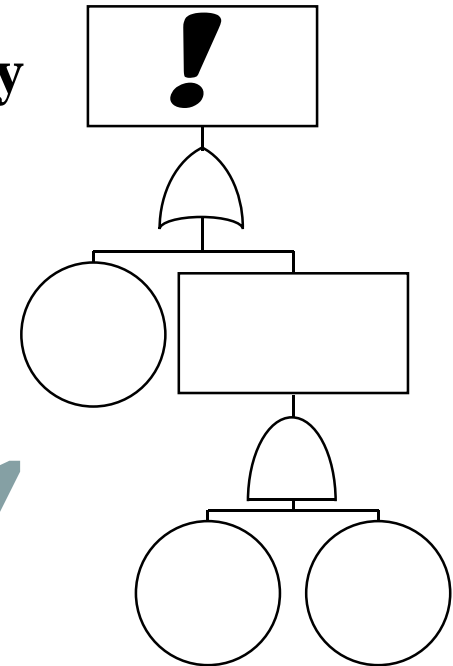
- ***BUT***, In the *pruned* logic equivalent tree, initiators 1, and 4 do not appear. They can fault in perpetuity with no effect on TOP.)



Do not show this tree to the client!
STAY A HERO!

QUACKON 7: **Metastasize your Fault Tree...**

- **OPPORTUNITY:** If probabilities for contributors to a TOP event are known with confidence at the subsystem, or assembly, or subassembly level, there's a temptation to develop the fault tree *no further down* to evaluate P_{TOP}



However, this'll give you a wimpy-looking

Fault Bush

...not very persuasive!

QUACKON 7: (continued)

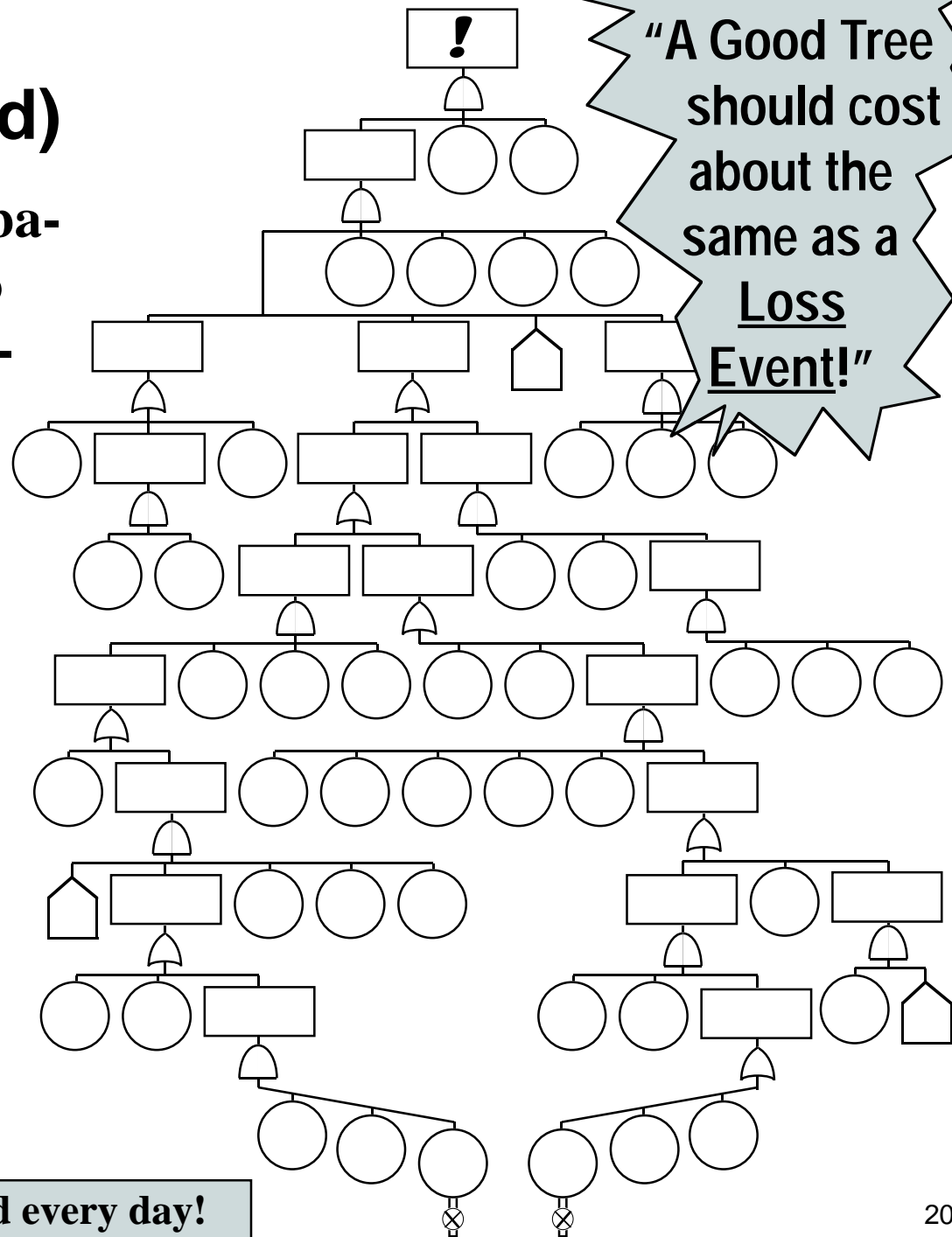
- **BUT**, you can dig out probabilities all the way down to the cotter pins — an industrial strength Mega-Manhour prospect!
- **SO...** grow that tree downward, to the individual threads on the setscrews.

Go for

FAULT KUDZU!

This'll leave the client satisfied...

and *impoverished!*



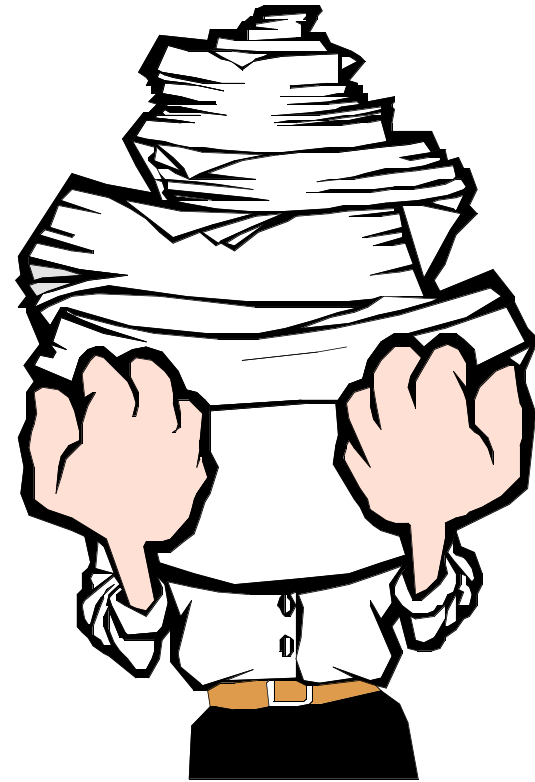
New subatomic particles are discovered every day!

QUACKON 8: **Substitute *Avoirdupois* for *Splendor*...**

- ***OPPORTUNITY***: Your analysis of a system... occupies a meager 42 pages, with figures, tables, and annexes. Brevity makes it appear to lack profundity, depth, erudition, and rigor.

QUACKON 8: (continued)

- **BUT**, inert ingredients will *add bulk at low cost* and give the appearance of excellence.
- **SO...** go for verbal kapok...*exempli gratia*:
 - a dozen pounds of FMEA, done up down at the gear-tooth level.
 - an essay on the aesthetics of shape selection for logic gates.
 - the proof for Fermat's last theorem (for mathematical elegance).
 - bafflegab...
 - *"We have carried out a multi-linear, floating indenture, fishgill analysis on all quasi-causal root threat agents."*
 - *"The peril of intersection among all unparalleled operands is under homeostatic redundancy."*



Analytical *heft* is a recognized *virtue*!
Go faux posh!

QUACKON 9: **Lumped targets lessen catastrophe...**

- ***OPPORTUNITY***: Your system contains a vile, poly-purpose hazard that threatens...

- **Severe Injury, AND**
 - **Occupational Illness, AND**
 - **Major Property Damage**

**THREE
degrees
of
EVIL!**

There's far too much **RISK** in this ominous multi-menace threat!

QUACKON 9: (continued)

- ***BUT***, the *standards* encourage lumping to bring comfort! Severity Classifications invite a mystical “blend” of exposures, e.g.:

“Class II / Critical — ...severe injury OR occupational illness, OR major property damage...”

From NPG 8715.3 / ¶3.6.1.1

A hazard that combines *multiple* threats at this severity level is no more pernicious than a hazard threatening just *one* target!

- ***SO...*** ignore combined effects — *if it's OK with the standards, it's OK with everybody!*

A Squalid System with
TOO MUCH RISK?
Try lumping the targets!



***Practice
Perfidy***

- “Real *low probability* doesn’t mean it *won’t* happen — just that it *won’t* *happen real often!*”
- “*Once* is *not often!*”
- Following any failure, *insist on changes* ...you’ll get to start a *new data base!*

PERFIDIOUS PRACTICES...

- **Be non-specific in bounding the system and scoping the analysis.**
(Mysteries excite increased reader interest!)
- **Leave the Human Operator out of it!**
(It's poor professional form and unsportsmanlike to point fingers at your fellow humans.)
- **When assessing risk, evaluate severity for one outcome and probability for another.**
(Consistency is overused, trite, and boring.)

MORE PERFIDY...

- **Make frequent shifts between “Types” and “Techniques” of analysis.**
(Clients are impressed by an SSHA done using FMECA, or an FTA under an O&SHA to support OSHA compliance. When in doubt, scowl and mumble “software” — if you can’t deliver, move into metaphysics where you can stupefy!)
- **To reduce risk, select mitigating countermeasures that’ll introduce brand new hazards.**
(Perpetuate employment opportunities and job security for others in your field!)
- **Pick countermeasures that’ll cripple the system.**
(If you can’t operate it, it won’t hurt anything!)

The DEFINITIONS



*...simply adhere to
the standards and
the textbooks.*

- If it comes out of a book, it *can't be wrong!*
- If you can't find it in a book, *it is wrong!*

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!

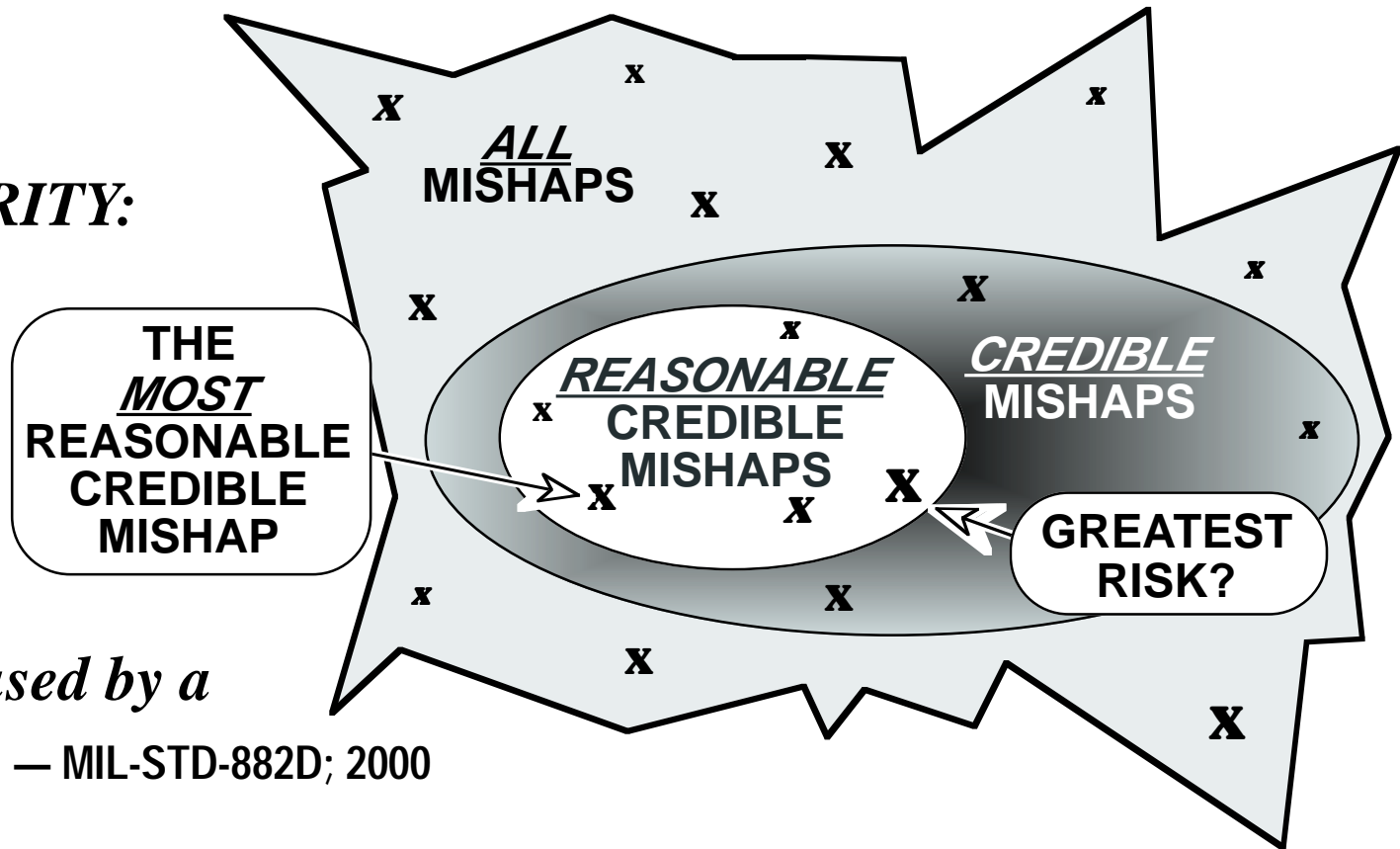


DEFINITIONS in the STANDARDS...

MISHAP SEVERITY:

“An assessment of the consequences of the most reasonable credible mishap

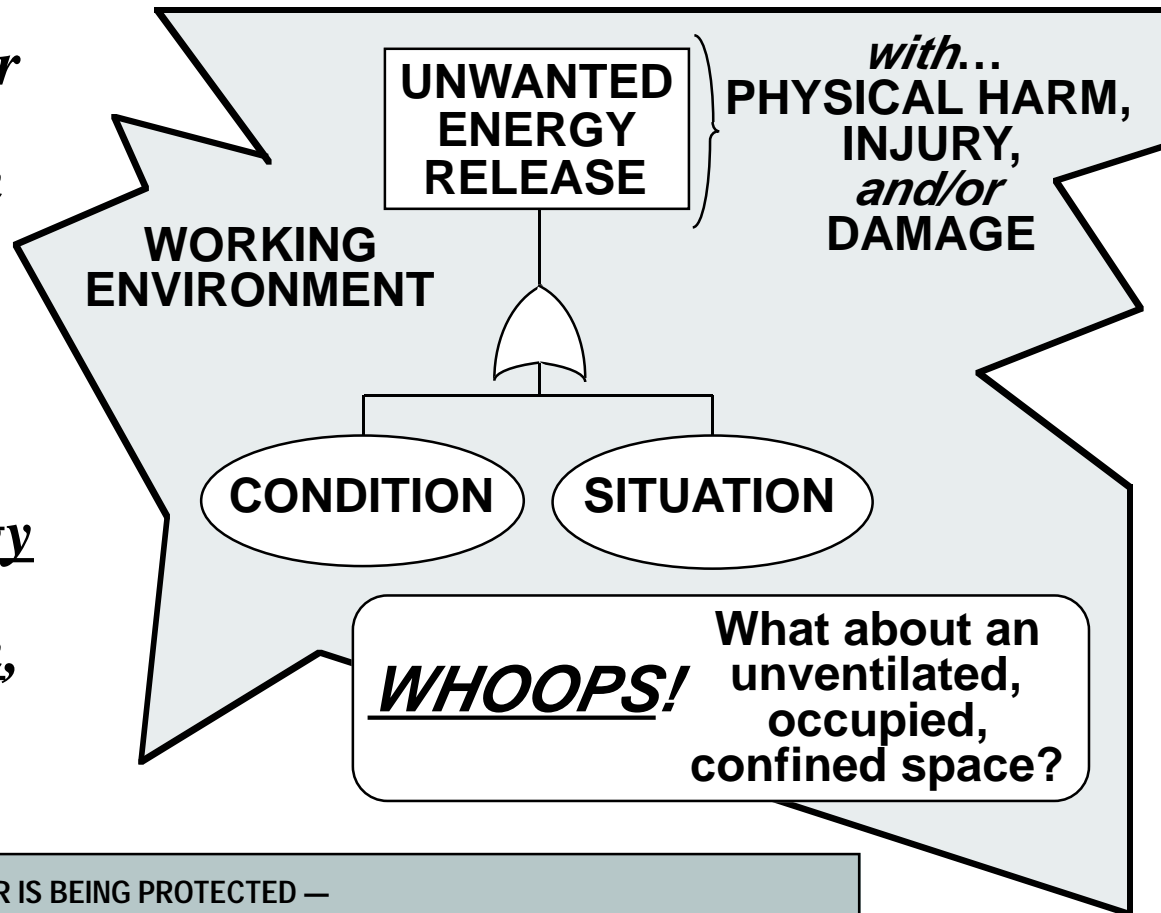
that could be caused by a specific hazard.” — MIL-STD-882D; 2000



Given our choice, should we manage ***GREATEST RISK*** ...or should we manage ***MOST REASONABLE, CREDIBLE*** threats?

DEFINITIONS in the TEXTBOOKS...

HAZARD: “A condition or situation that exists within the working environment capable of causing an unwanted release of energy resulting in physical harm, injury, and/or damage.”



THE EFFECTIVENESS HIERARCHY..

“Hazards will be mitigated according to the following stated order of precedence:

“Eliminate hazards.

“Design for minimum hazards. [*Not minimum risk.*]

“Incorporate safety devices.

“Provide caution and warning devices.

“Develop ...procedures and training.”

From NPG 8715.3 / ¶ 3.4

If it's *not* in the hierarchy, it's probably *not* a countermeasure!

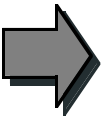
WOOPS!

How do we
classify...

- A floor drain to prevent flooding?
 - Confined space ventilation to avert asphyxia?
 - Vaccination against disease?
 - Fortified maintenance to extend MTBF?

DEFINITIONS DIFFER AMONG THE SOURCES...

- **HAZARD:** “A condition which can result in a mishap or accident under certain conditions.” — *Assurance Technologies*; Dev G. Raheja; McGraw-Hill; 1991 [13w]
- **HAZARD:** “...an inherent physical or chemical characteristic that has the potential for causing harm.” — *Guidelines for Hazard Evaluation Procedures*; AIChE Center for Chemical Process Safety; 1992 [13w]
- **HAZARD:** “Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.” — MIL-STD-882D; 2000 [29w]
- **HAZARD:** “...a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event).” — *Safeware / System Safety and Computers*; Nancy G. Leveson; Addison Wesley; 1995 [33w]



THE RESULT: Aids to Quackery...

- **Compromised communication among practitioners.**
- **Impaired program-to-program interpretability of analytical results.**
- **An opportunity for concealed linguistic malpractice. If you can't be understood, nobody can hold you responsible for what you say!**

SUCCESS CAN BE YOURS!

- **Fame & popularity**
- **Riches beyond description**
- **A reserved parking place**
- **Free junk mail subscriptions**
- **Double Frequent-Flyer miles**
- **20 x 10⁻³ CEUs**



PERSEVERE!