A-P-T Research, Inc.

System Safety Engineering An Overview for Engineers and Managers

P. L. Clemens

October 2005

Topics…

- What is System Safety Engineering?
- When should System Safety be used?
- How is System Safety done?
- Who should perform System Safety analyses?
- What does System Safety Cost?
- Why do System Safety?

What's a SYSTEM?

(and a few other basics)...

- **SYSTEM**: an entity, at any level of complexity, intended to carry out a function, e.g.:
  - A doorstop
  - An aircraft carrier
  - An operating procedure
  - An implantable insulin pump
- Systems pose **HAZARDS**. Hazards threaten harm to **ASSETS**.
- **ASSETS** are RESOURCES having value to be protected, e.g.:
  - Personnel
  - The environment
  - Productivity
  - The product
  - Equipment
  - Reputation
- **RISK**, is an attribute of a hazard-asset combination — a measure of the degree of harm that is posed.

What's System Safety?

It has two chief aspects...

1

- **A DOCTRINE of Management Practice**:
  - Hazards (threats to Assets) abound and must be identified.
    - Risk is an attribute of a hazard that expresses the degree of the threat posed to an asset — risks must be assessed.
      - A non-zero Risk Tolerance Limit must be set — a management function.
      - Risks of Hazards exceeding the Tolerance Limit must be suppressed (or accepted by management).

2

- **A Battery of ANALYTICAL METHODS** to support practice of the DOCTRINE — The analytical methods are divisible into:
  - **TYPES**, addressing What / When / Where the analysis is done
  - **TECHNIQUES**, addressing How the analysis is done

The Types & Techniques of Analysis...

TECHNIQUES (How)...

- Preliminary Hazard Analysis (PHA*)[1/2/3]
- Failure Modes and Effects Analysis (FMEA)[1/3]
- Fault Tree Analysis[2/4]
- Event Tree Analysis[3/4]
- Cause-Consequence Analysis[3/4]
- Hazard & Operability Study (HAZOP)[1/3]
- Job Hazard Analysis (JHA/JSA)[1/3]
- Digraph Analysis[1/3]
- many others…

TYPES (What / When / Where)...

- Preliminary Hazard Analysis (PHA*)
- System Hazard Analysis
- Subsystem Hazard Analysis
- Operating and Support Hazard Analysis
- Occupational Health Hazard Analysis
- Software Hazard Analysis
  - many others…

The **TYPES** and **TECHNIQUES** are to…
- ***IDENTIFY HAZARDS***, and to…
- ***ASSESS THEIR RISKS***.

But, WHAT IS RISK?

[1] Hazard Inventory Tree [2] Top Down [3] Bottom Up [4] Logic

What is RISK?

RISK: An expression of the combined ***SEVERITY*** and ***PROBABILITY*** of ***HARM*** to an ***ASSET.***

SYSTEM ASSETS* may be:

- Personnel
- Equipment
- Productivity
- Product
- Environment
- …others

PROGRAMMATIC ASSETS* may be:

- Cost
- Schedule
- Mission
- Performance
- Constructability
- …others

RISK is an *attribute* of a HAZARD-ASSET combination!

THREATS to ASSETS are called *HAZARDS*.

Hazards are THREATS to ASSETS

HAZARDS
MUST BE IDENTIFIED!
…or System Safety and Risk Management cannot be practiced!

HAZARDS…

are best described as terse Loss Scenarios, each expressing

SOURCE → MECHANISM → OUTCOME

Thusly: **"Faulty control logic producing yaw overdrive and model damage."**

***NOT*: "Pranged wind tunnel model."**

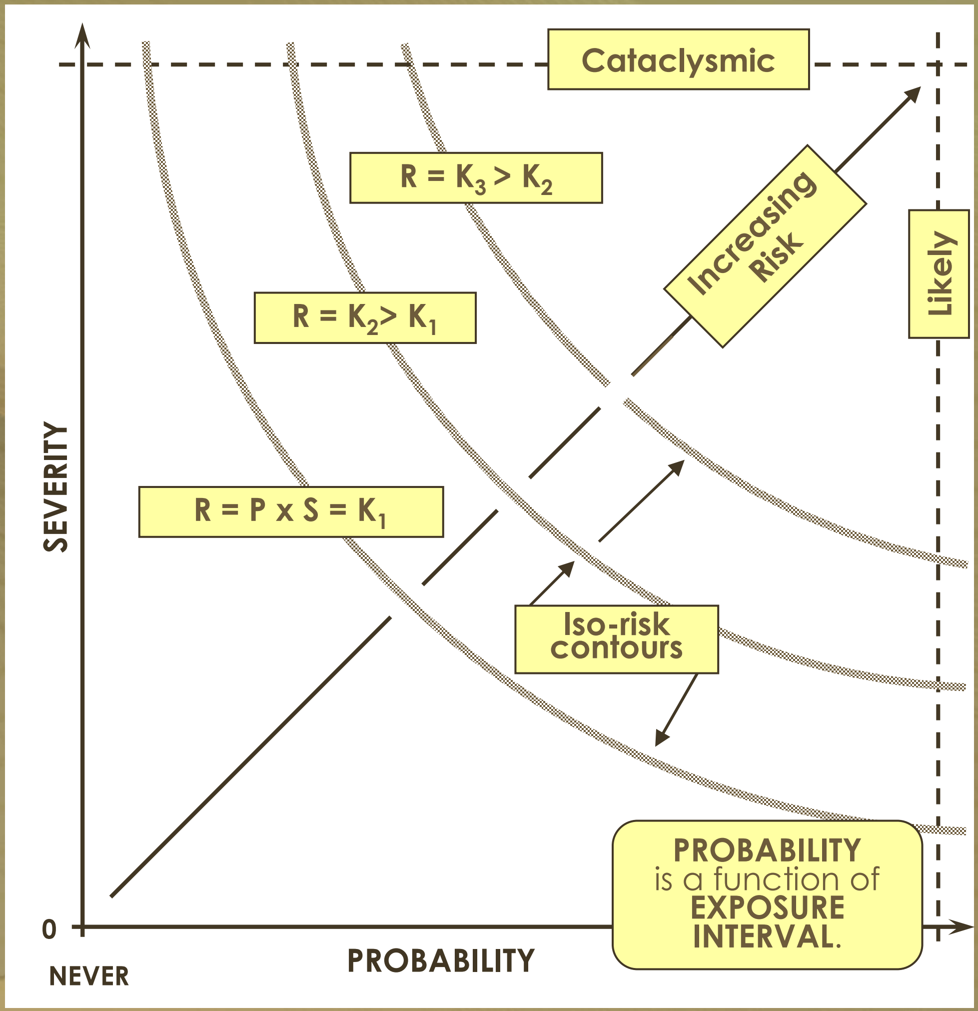
OR

"Occupancy of an unventilated confined space leading to death from asphyxia."

***NOT*: "Running out of air."**

The Risk Plane...

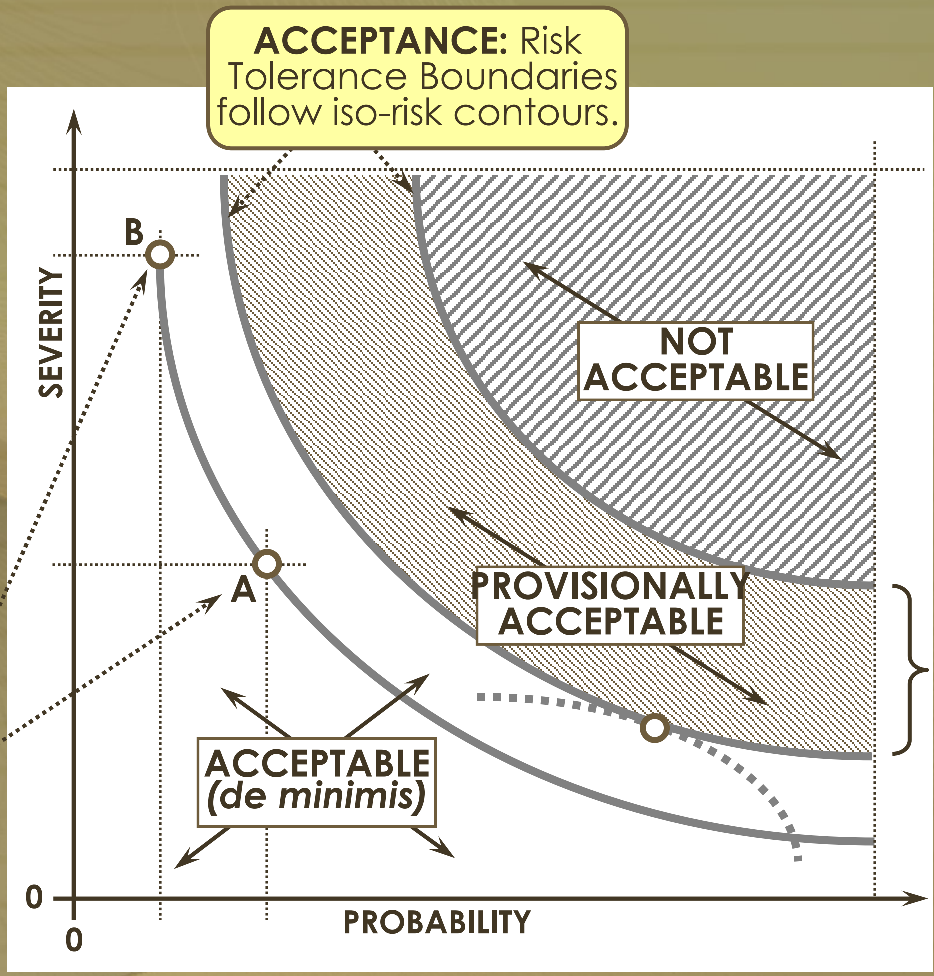
SEVERITY and **PROBABILITY**, the two variables that constitute risk, define a **RISK PLANE.**



RISK is **CONSTANT** along any **ISO-RISK CONTOUR.**

M-05-02600-8

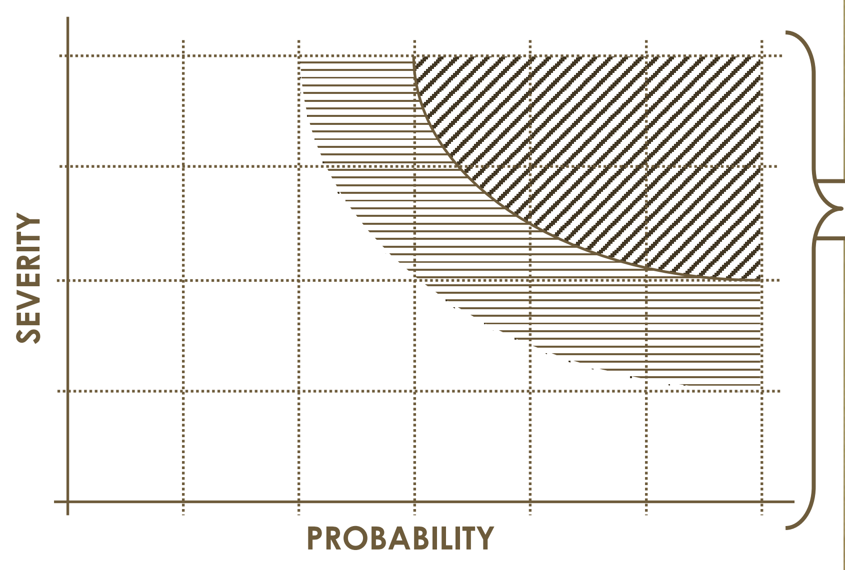
Using ISO-Risk Contours...



Further Risk Reduction Desirable.

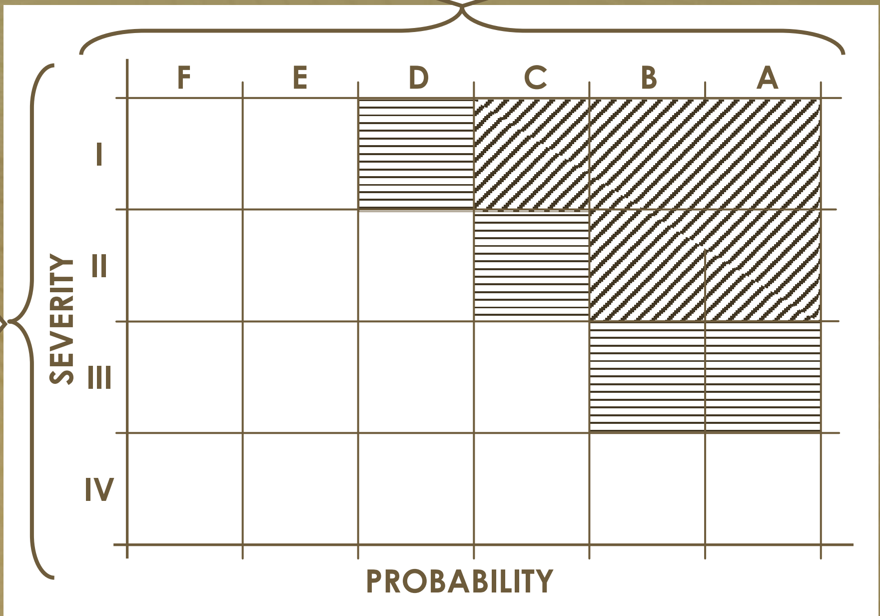
Note that risk at **A** equals risk at **B**.

The Risk Plane Becomes a Matrix...



Segmenting the Risk Plane into tractable cells produces a Matrix to enable using subjective judgment.

Matrix cell zoning approximates the continuous, iso-risk contours in the Risk Plane. Zones in the Matrix define
Risk Tolerance Boundaries.
Jeopardy



A Typical Risk Assessment Matrix*...

A guide for applying subjective judgment…

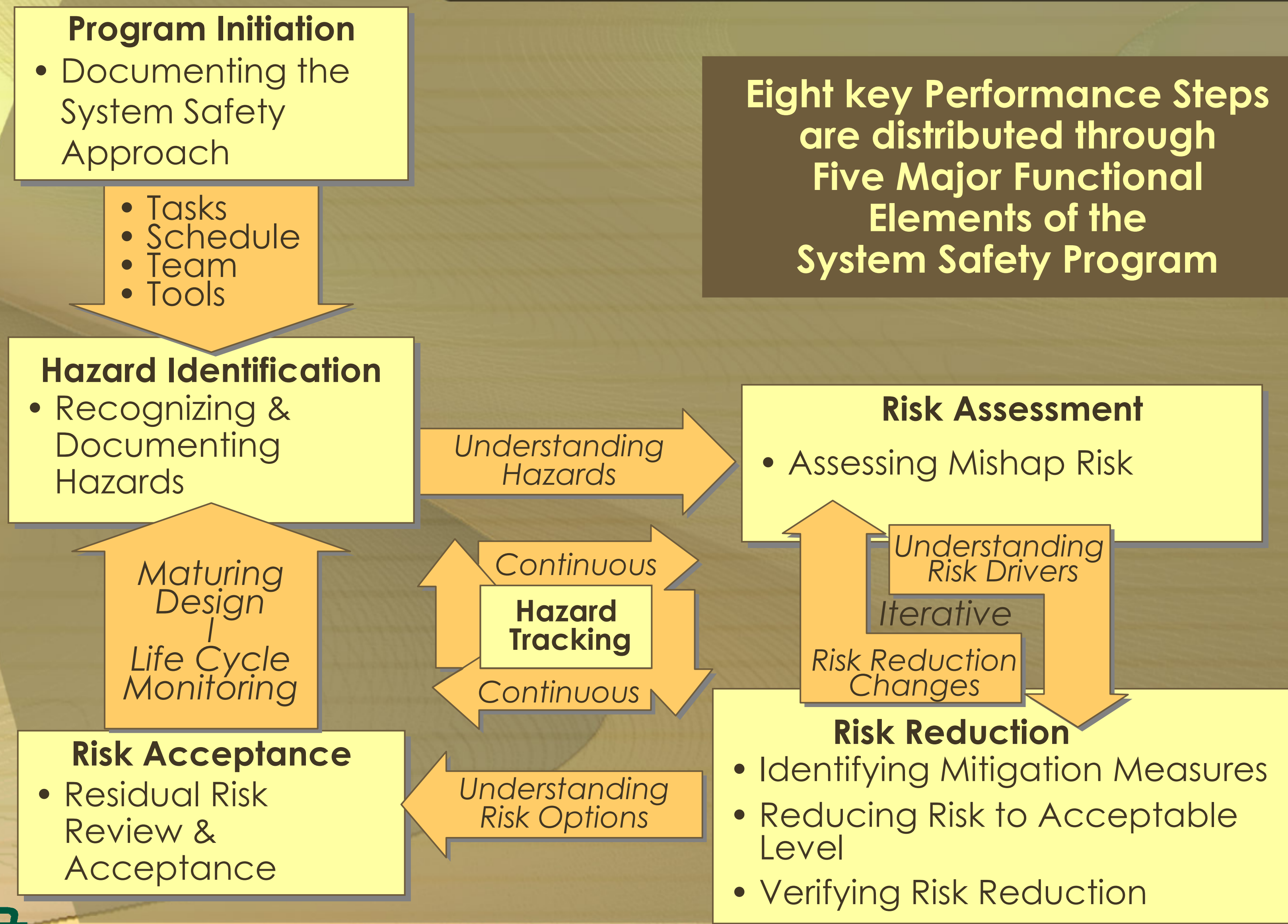
Severity of Consequences				Probability of Mishap**					
Category / Descriptive Word	Personnel Injury / Illness	Equipment Loss $	Down Time	**F** Impossible	**E** Improbable	**D** Remote	**C** Occasional	**B** Probable	**A** Frequent
I Catastrophic	Death	>1M	>4 Mo						1
II Critical	Severe Injury or Severe Illness	250K to 1M	2Wks to 4Mo				2		
III Marginal	Minor Injury or Minor Illness	1k to 250K	1 Day to 2Wks		3				
IV Negligible	No Injury or Illness	<1K	<1 Day						

*Adapted from MIL-STD-882D **Life Cycle: Personnel: 30 yrs / Others: Project Life

Risk Code/ Action			
1	Imperative to suppress risk to lower levels		
2	Operation requires written, time-limited waiver, endorsed by management		
3	Operation permissible		

The "Flow" of System Safety Practice...

Eight key Performance Steps are distributed through Five Major Functional Elements of the System Safety Program



M-05-02600-12

Major System Safety

Cross-Link Disciplines…

- Programmatic Risk Management
- The "…ilities"
  - Reliability
  - Availability
  - Maintainability
  - Survivability
- Configuration Management
- Procedures Preparation
- …others…

PROGRAMMATIC RISK MANAGEMENT treats its own special classes of hazards, posing risk to, e.g.:

- Cost
- Schedule
- Performance
- Constructability
- …others

ISN'T RELIABILITY ENGINEERING _ENOUGH_?

USUALLY NOT!

- Reliability explores the Probability of Success, _alone_.
- System Safety explores the Probability of Failure *AND* its Severity Penalty.

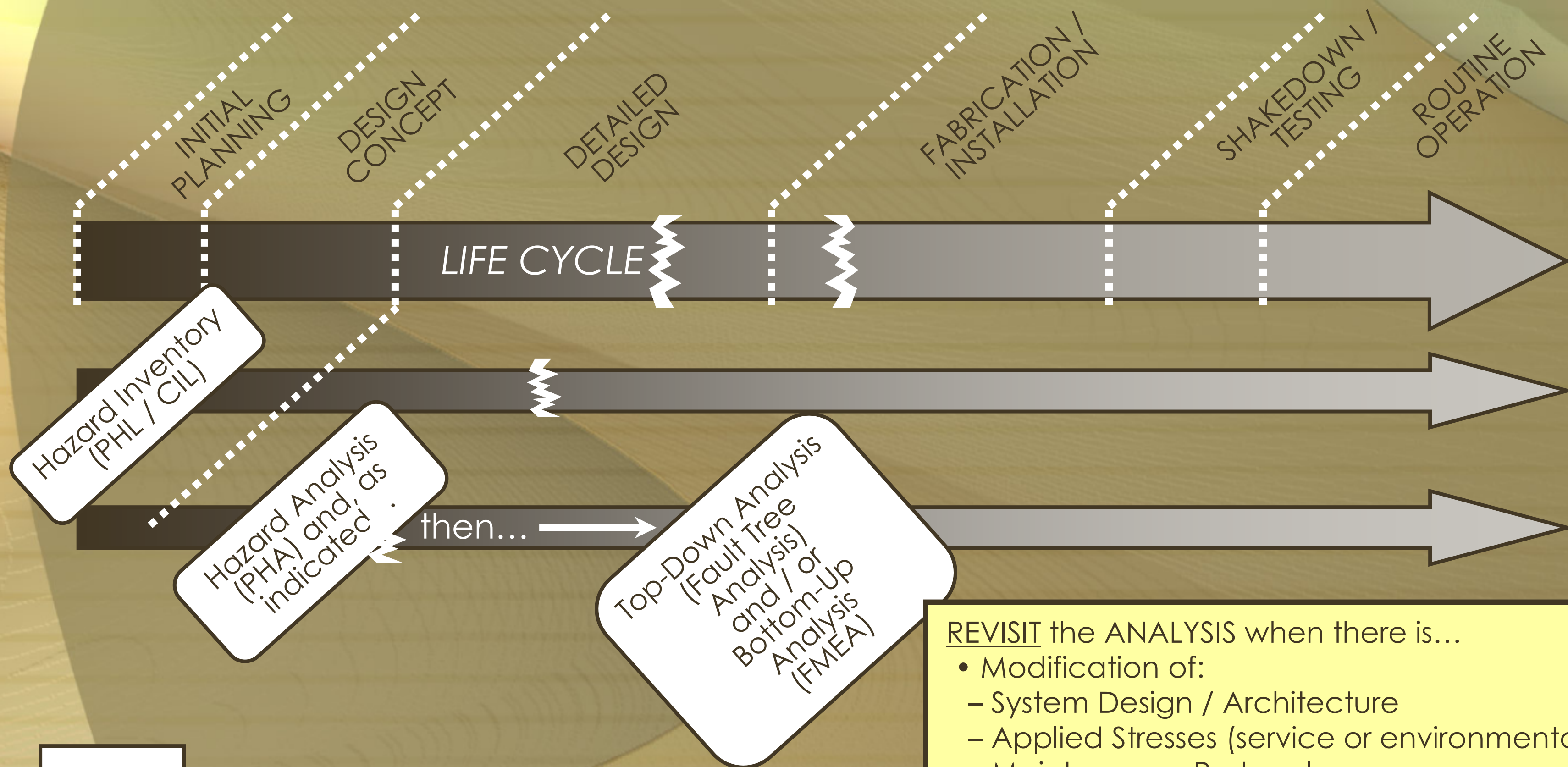
Topics...

- What is System Safety Engineering?
- **When should System Safety be used?**
- How is System Safety done?
- Who should perform System Safety analyses?
- What does System Safety Cost?
- Why do System Safety?

System* Safety Application throughout Life Cycle...

DON'T OVERLOOK:
- Operational / Mission Phases
- Maintenance
- Decommissioning
- Etc…

A typical approach:



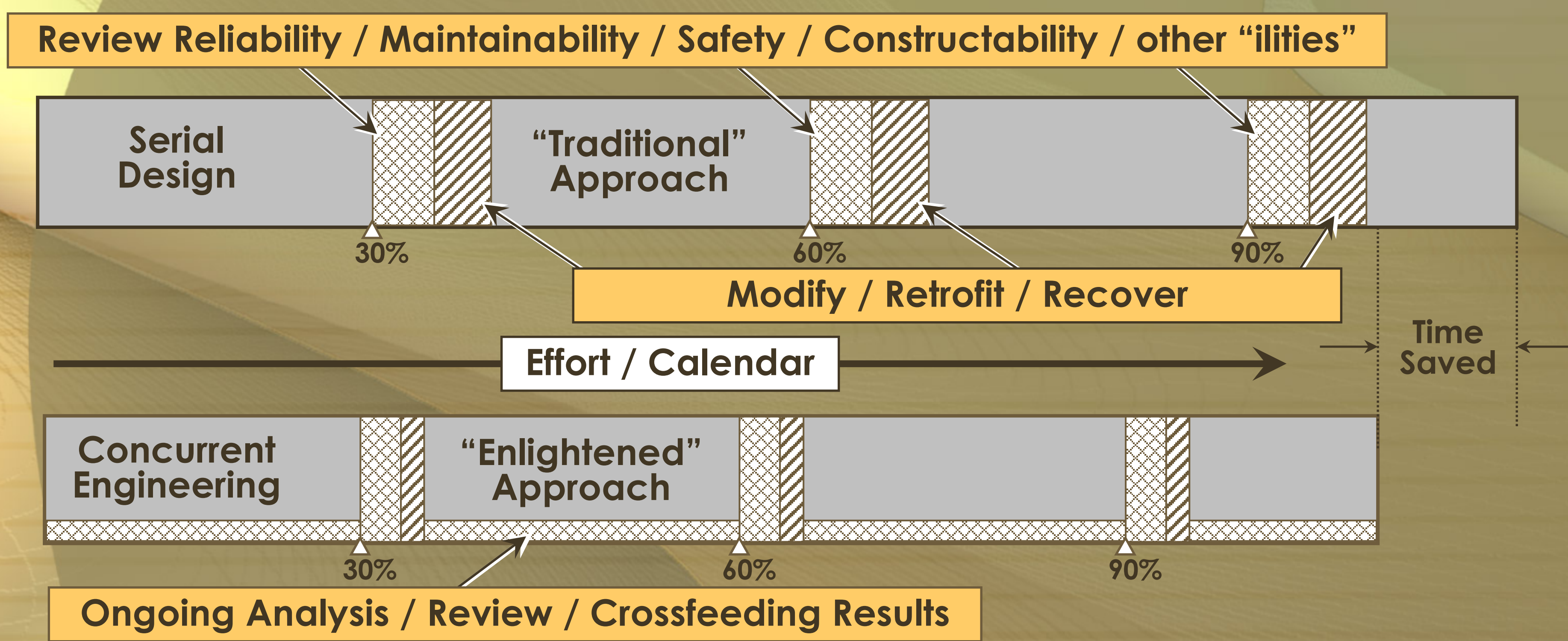
REVISIT the ANALYSIS when there is…
- Modification of:
  - System Design / Architecture
  - Applied Stresses (service or environmental)
  - Maintenance Protocol
- A "Near Miss"
- A Loss Event (to support autopsy)

*NOTE

"System" includes hardware, software, procedures, training / certification, maintenance protocol, etc. — the *GLOBAL* System.

M-05-02600-15

Comparing Two Work Models
for Design-Build Efforts*...



CONCURRENT DESIGN RESULTS:

- Continuous, iterative feedback of analysis results into design
- Earlier accommodation to findings
- Manhours and calendar time conserved
- Fewer "surprises" / performance-threatening retrofits
- Fewer awkward compromises — more coherent design

*Journal of the American Society of Safety Engineers; November, 1999

M-05-02600-16

What systems benefit *best* by System Safety application?

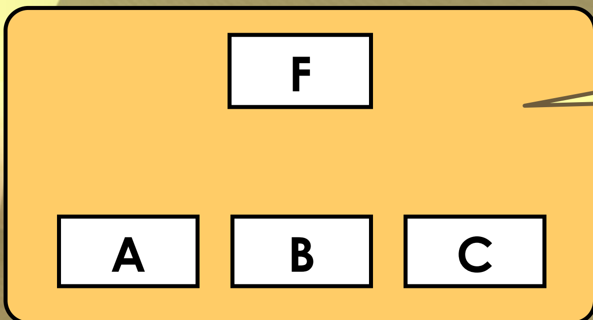
- Use System Safety if the system…
  - is complex — i.e., interrelationships among elements is not readily apparent, and/or
  - uses untried or unfamiliar technology, and/or
  - contains one or more intense energy sources — i.e., energy level and/or quantity is high, and/or
  - has reputation-threatening potential, and/or
  - falls under the purview of a mandating regulation (e.g., 29 CFR 1910.119)

Why / When use more specialized analytical techniques?

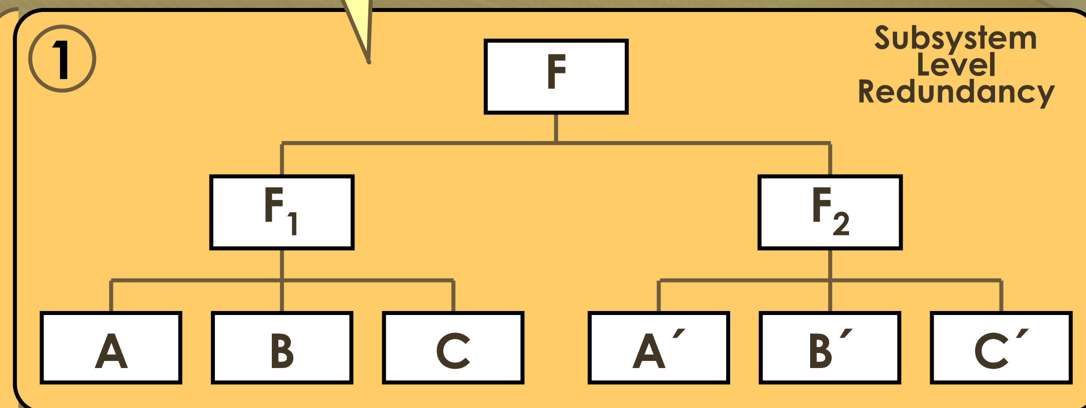
Top-down Analysis
(e.g., Fault Tree Analysis)
and / or
Bottom-up Analysis
(e.g., Failure Modes and Effects Analysis)

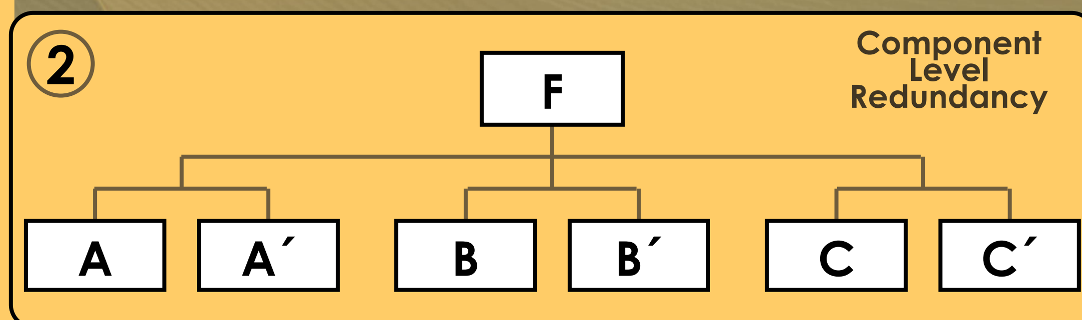
- when SYSTEM COMPLEXITY exceeds PHA capability, and/or…
- to evaluate risk more precisely in support of RISK ACCEPTANCE DECISIONS, and/or…
- to support DESIGN DECISIONS on matters of component selection/system architecture, etc.

Design Decisions — an example...



Risk too high? Then ***Go Redundant!***





But *WHERE* to redundify?

- System?
  - Subsystem?
    - Assembly?
      - Subassembly?
        - Component?
          - Piece Part?

Variations in system architecture, using the same components, can produce profound differences in system reliability and safety!

When should System Safety Analyses be *Re*-visited?

- Has there been a change in…
  - System design / architecture?
  - System use / applied stresses (i.e., service stresses / environmental stresses)?
  - Maintenance protocol?
- A "near miss?"
- A loss event?

Then,
REVIEW / REVISE
the
ANALYSIS!

Topics...

- What is System Safety Engineering?
- When should System Safety be used?
- How is System Safety done?
- Who should perform System Safety analyses?
- What does System Safety Cost?
- Why do System Safety?

An Overview of Selected Analytical Techniques...

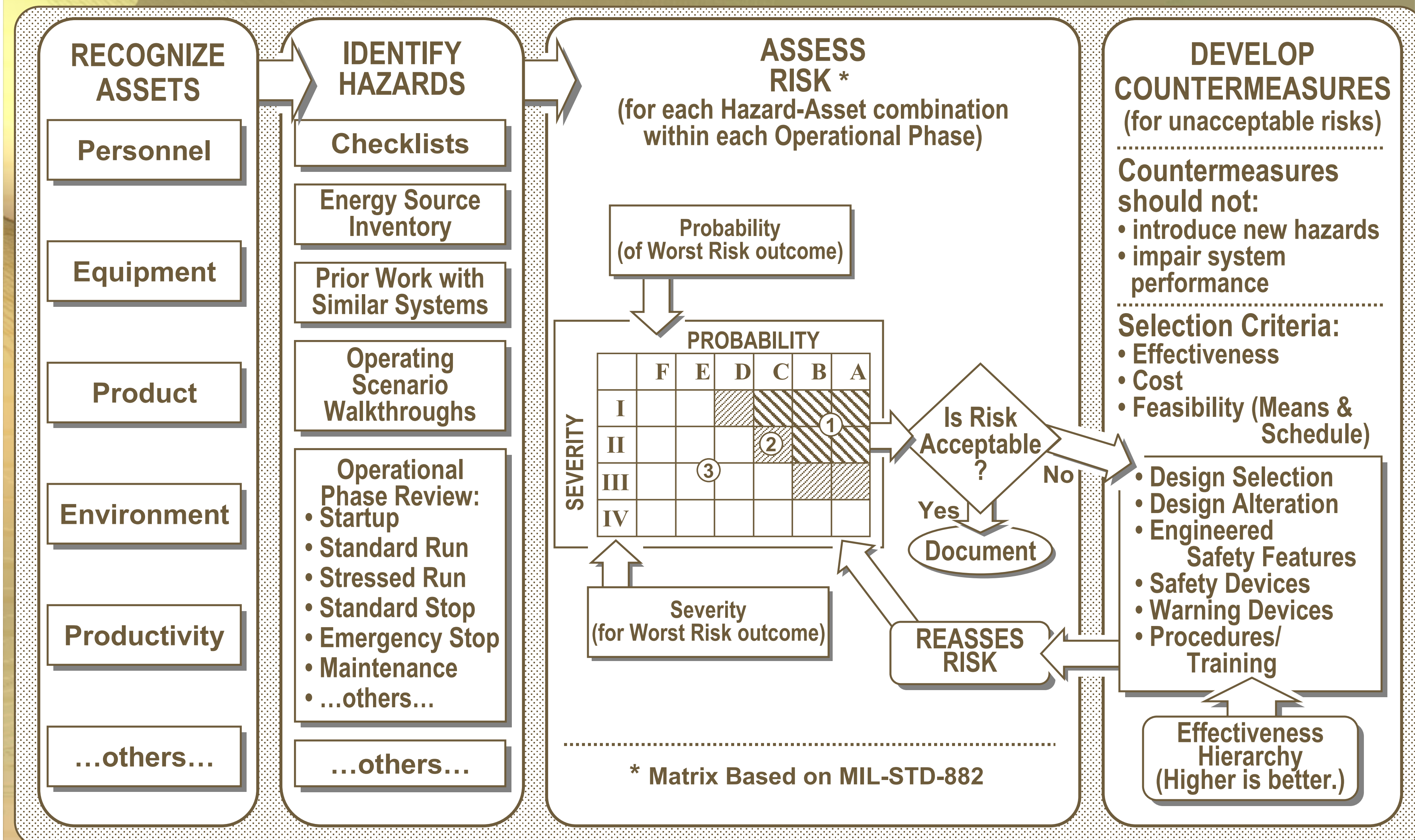
- Preliminary Hazard Analysis
  - Hazard Inventory
  - Top-Down, or Bottom-Up, or Inside-Out
- Failure Modes and Effects Analysis
  - Hazard Inventory
  - Bottom-Up
- Fault Tree Analysis
  - Logic Tree
  - Top-Down

Preliminary Hazard Analysis*…

- **WHAT**: Line-item listing of "all" system hazards, with subjective evaluations of severity/probability/risk for each.
- **HOW**: Engineering judgment; intuitive skills; checklists; operational walkthroughs; prior similar work.
- **ADVANTAGES**: Provides inventory of "all" system hazards/risks.
- **DISADVANTAGES**: Incomplete. Ignores combined hazard effects. Conceals total system risk. Non-quantitative.

* Preliminary Hazard Analysis (PHA) is an unfortunate misnomer. The method is best applied early in system life cycle but can be used at any time. It produces a running inventory of system hazards and is a convenient repository for the results of system safety analyses done by any methods that might be used.

Preliminary Hazard Analysis Flow…



A Typical PHA Worksheet...

HAZARD No. Chem/Int-001 **HAZARD TITLE:** Flange Seal A-29 Leakage ← Provide brief name for hazard. **REVISED:** 7/22/93

HAZARD DESCRIPTION

Flange Seal A-29 leakage, releasing pressurized $UnFo_3$ chemical intermediate from containment system, producing toxic vapors on contact with air and attacking nearby equipment.

Describe hazard, indicating: source, mechanism, worst-credible outcome.

EXPOSURE INTERVAL 25 years **ACTIVITY/PROCESS PHASE:** Startup/Standard Operation/Stop/Emergency Shutdown ← Identify applicable operating phases.

INITIAL RISK ASSESSMENT

Identify (X) all applicable asset(s).

(with existing of planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (worst credible)	PROBABILITY: (for exposure interval)	RISK CODE: (from Matrix)
Personnel:	X	I	D	2
Equipment:	X	II	C	2
Downtime:	X	III	C	3
Environment:	O			0
Product:	O			0

For each asset, assess severity, and probability for the worst-credible outcome. Show risk (from assessment matrix) for hazard-asset combination "as-is" – i.e., with no added countermeasures.

ADDITIONAL COUNTERMEASURES*

Surround flange with sealed annular stainless steel catchment housing, with gravity run-off conduit led to Detecto-Box™ containing detector/alarm feature and chemical neutralizer (S/W). Inspect flange at two-month intervals and re-gasket during annual plant maintenance shut-down (P). Provide personal protective equipment and training for response/cleanup crew (S/P).

Describe added countermeasures to control Probability / Severity – reduce Risk.
THESE COUNTERMEASURES MUST BE IN PLACE PRIOR TO SYSTEM OPERATION!

*Mandatory for Risk Codes 1 & 2, unless permitted by Waiver. Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (worst credible)	PROBABILITY: (for exposure interval)	RISK CODE: (from Matrix)
Personnel:	X	I	E	3
Equipment:	X	II	D	3
Downtime:	X	III	D	3
Environment:	O			0
Product:	O			0

COMMENTS

Re-evaluate before sign-off — reconsider Environment as asset.

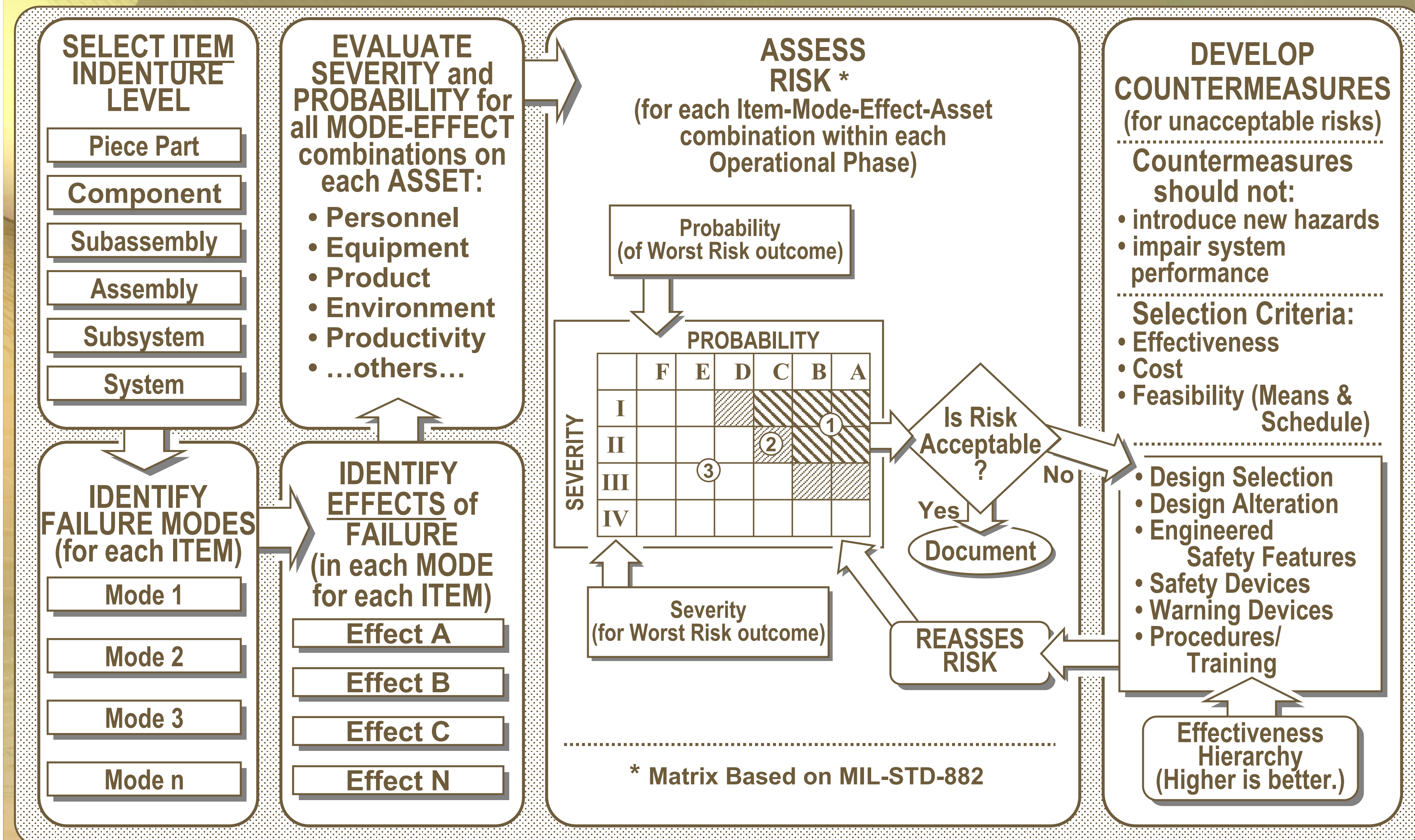
Reassesses Severity/Probability and show risk (from assessment matrix) for original hazard-asset combinations, presuming new countermeasures to be in place, if risk is not acceptable, additional countermeasures must be developed.

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

Failure Modes and Effects Analysis…

- **WHAT**: Item-by-item evaluation of consequences of individual failures within system. Evaluates severity and/or risk for each consequence. (Sometimes called Failure Modes, Effects, and Criticality Analysis, when severity and/or risk are assessed.)
- **HOW**: Develops answers to two questions:
  - (1) How can this item fail? (Modes)
  - (2) What are system consequences for each failure? (Effects)
- **ADVANTAGES**: Tightly Disciplined. Exhaustively identifies potential single-point failures.
- **DISADVANTAGES**: Ignores combined fault / failure effects. Conceals total system risk. High sensitivity to indenture level selection. Very resource hungry.

Failure Modes and Effects Analysis Flow...



M-05-02600-27

A Typical FMEA Worksheet...

FMEA No.: N/246.n Project No.: Osh-004-92 Subsystem.: Illumination System.: Headlamp Controls Probability Interval.: 20 years	**FAILURE MODES AND EFFECTS ANALYSIS**	Sheet 11 of 44 Date.: 6 Feb '92 Prep. by.: R.R. Mohr Rev. by.: S. Perleman Approved by.: G. Roper

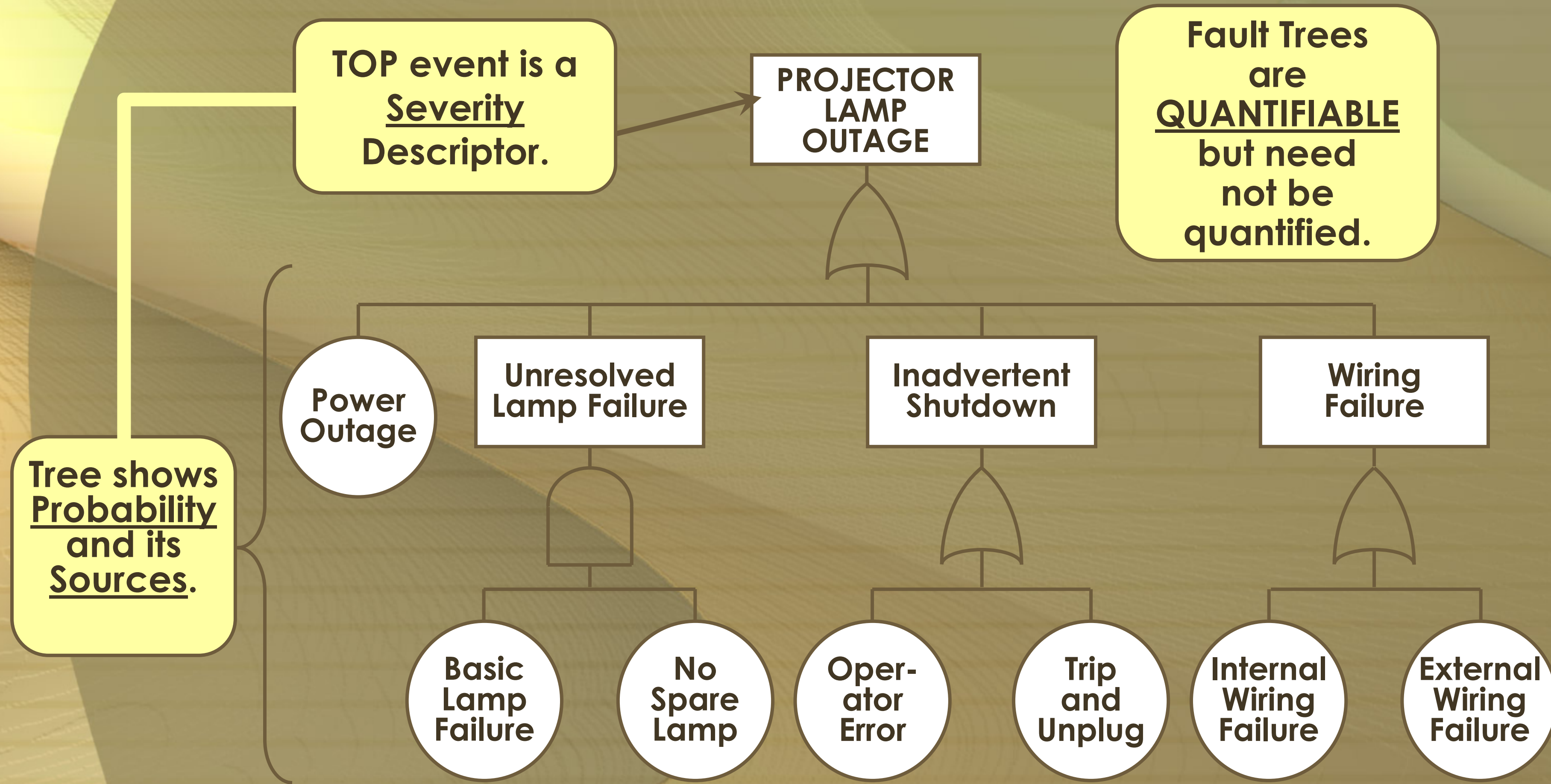
IDENT. No.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT	TARGET	RISK ASSESSMENT			ACTION REQUIRED/REMARKS
						SEV	PROB	Risk Code	
R/N.42	Relay K-28 / Contacts (normally open)	Open w / command to close	Corrosion/or mfg.defect/or basic coil failure (open)	Loss of forward illumination/ Impairment of night vision/potential collisions(s) w/unilluminated obstacles	P E T M	I III I I	D D D D	2 3 2 2	Redesign headlamp circuit to produce headlamp fail-on, w / timed off feature to protect battery, or eliminate relay / use HD Sw. at panel.

P: Personnel / **E**: Equipment / **T**: Downtime / **M**: Mission / **V**: Environment

Fault Tree Analysis…

- **WHAT**: Symbolic logic modeling of fault paths within system to result in foreseeable loss event — e.g.: sting failure; loss of primary test data; failure to ignite on command; premature ignition; ventilator failure.
- **HOW**: Apply Operations Research logic rules — trace fault / failure paths through system.
- **ADVANTAGES**: Gages system vulnerability to foreseen loss event, subjectively or quantitatively. Guides vulnerability reduction. Supports trade studies.
- **DISADVANTAGES**: Treats only foreseen events, singly. Handles sequence-sensitive scenarios poorly. Resource hungry.

A Fault Tree Example...



Fault Tree Analysis is the principal analytical tool used in Probabilistic Risk Assessment.

Topics...

- What is System Safety Engineering?
- When should System Safety be used?
- How is System Safety done?
- Who should perform System Safety analyses?
- What does System Safety Cost?
- Why do System Safety?

Who best performs the analysis?

- A Small Team, with…
  - Expertise in the appropriate disciplines, and
    - In-depth understanding of the system, and
      - Proficiency at applying the System Safety analytical techniques.

SOLO ANALYSIS is ***HAZARDOUS!***

BUT…

ONLY **MANAGEMENT** can make **RISK ACCEPTANCE** decisions!

Topics...

- What is System Safety Engineering?
- When should System Safety be used?
- How is System Safety done?
- Who should perform System Safety analyses?
- What does System Safety Cost?
- Why do System Safety?

What does System Safety COST?

AN EXAMPLE…

- NASA / ARC Unitary Plan Wind Tunnel Modernization
  - Full-System PHA
  - FMEA for all "Critical Controls"

5% to 6% of total design project cost

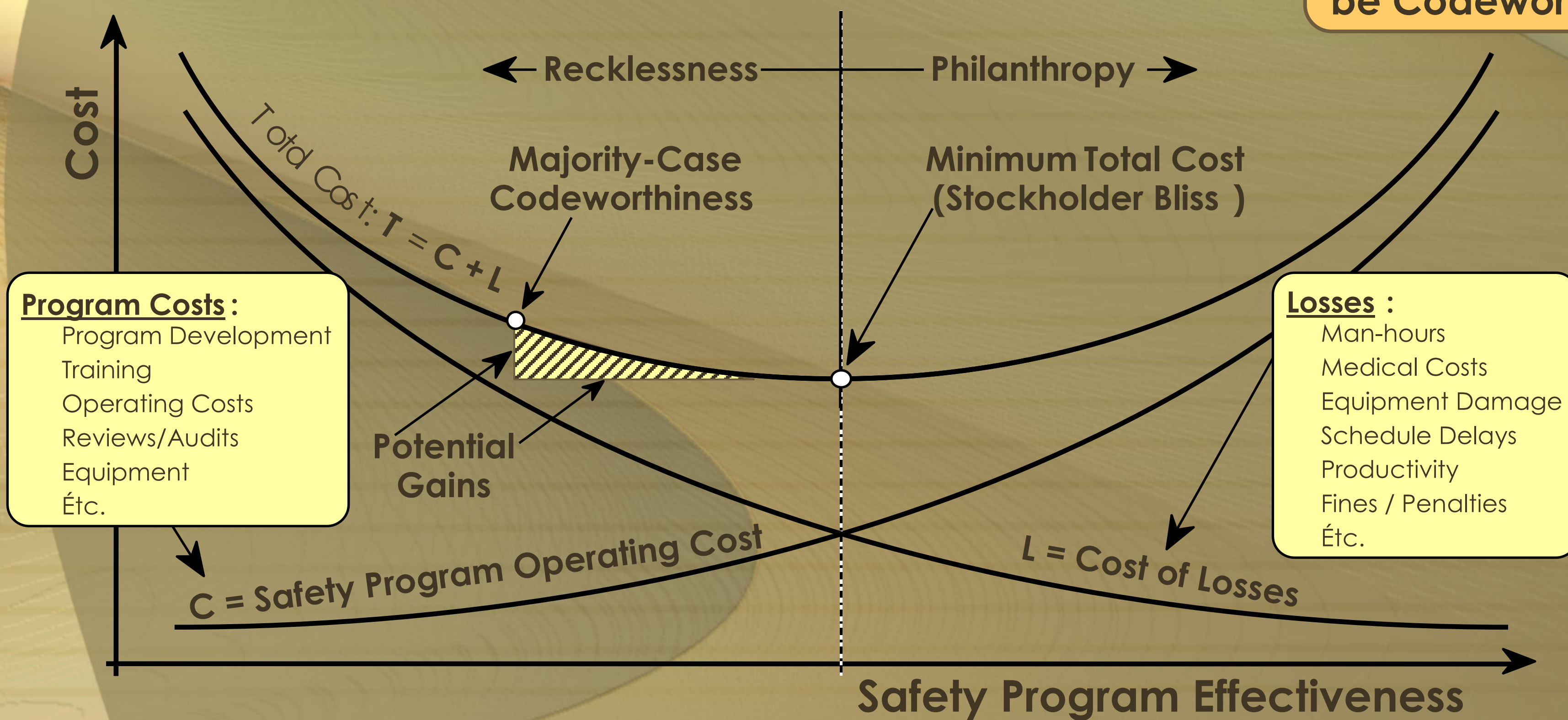
System Safety is "…simply documenting, in an orderly fashion, the thought processes of the prudent engineer."

L. T. Kije
1963

Overcoming the Codeworthiness Shortfall…

Safety effort beyond the codes has payoff*…

All Systems and Operations *MUST* be Codeworthy!



*Adapted from: Tarrants, W. E.; "The Measurement of Safety Performance" (Fig. 9.2); Garland; ISBN 0-8240-7170-0

Topics...

- What is System Safety Engineering?
- When should System Safety be used?
- How is System Safety done?
- Who should perform System Safety analyses?
- What does System Safety Cost?
- Why do System Safety?

Why do System Safety?

- to guide design decisions.
- to guide risk acceptance decisions.
- to conform to applicable codes.
- to ensure adequate safeguarding of assets.
- to demonstrate and document "due diligence."

Isn't Reliability Engineering *Enough*?...

No! ...not really:

RELIABILITY ENGINEERING

- views PROBABILITY alone — ignores SEVERITY.
- often ignores potential for CO-EXISTING faults (e.g., FMEA).
- Often ignores COMMON CAUSE threats.

"You don't need System Safety — we're doing Reliability Engineering!"
BEWARE!

RELIABILITY ENGINEERING views the *probability* that the system will operate on command, and throughout the period of need, with unimpaired performance.

SYSTEM SAFETY views the *probability* that the system will fail in a way that results in loss, AND the *severity* of loss.

A system may be very RELIABLE at it's intended function, and *equally* reliable at inducing LOSS!

A Closing Caveat...

We <u>never</u> analyze a *<u>system</u>*...
we analyze only a
conceptual model
of a system.

Make the <u>model</u>
match the <u>system</u>
as closely as possible!

To dig deeper...

- **System Engineering "Toolbox" for Design-Oriented Engineers** — B. E. Goldberg, et al. A compendium of methods dealing both with hazard recognition/risk assessment and with reliability engineering, this work describes a broad spectrum of analytical techniques. For each technique, the authors present a working level description, advice on applications, application procedure, examples, a description of advantages and limitations, and a bibliography of other resources. — 1994 — NASA Reference Publication 1358; Soft cover; large format; 303 pp

- **System Safety and Risk Management** — P. L. Clemens and R. J. Simmons. Intended as a guide for engineering college educators, this text presents the basic elements of system safety practice and risk management principles. Lesson-by-lesson chapters and demonstration problems deal with applying selected analytical techniques. Hazard inventory methods are presented, as are logic tree approaches. — 1998 — National Institute for Occupational Safety and Health, Centers for Disease Control and Prevention, Public Health Service; Soft Cover; large format; 282 pp. (NIOSH Order No. 96-37768)

- **Safeware — System Safety and Computers** — Nancy G. Leveson. An especially learned treatment of system safety viewed as a discipline to be applied in practical ways to the resolution of problems in discovering and managing risk. Fundamentals are treated in depth (e.g., the concept of causality). Analytical methods are presented, and there relative advantages and shortcomings are discussed. The importance of the role of software is emphasized, and problems in developing software risk assessments with reasonable confidence are discussed. Appendices analyze disasters and include a detailed treatment of the six Therac-25 massive overdose cases. — 1995 — Addison-Wesley; Hard cover; 680 pp. (ISBN 0-201-11972-2)

more digging...

- **Assurance Technologies** — Principles and Practices — Dev G. Raheja. Directed to design engineers at all levels of expertise, this volume devotes separate chapters to each of the product/system assurance technologies — i.e.: reliability engineering, maintainability engineering, system safety engineering, quality assurance engineering, logistics support engineering, human factors engineering, software performance assurance, and system effectiveness. (Introductory material provides background information on the influence of the assurance technologies on profits and on statistical concepts.) The treatment of each topic provides both an overview and in-depth, detailed coverage, with carefully selected illustrative examples. — 1991 — McGraw-Hill, Inc.; Hard cover; 341 pp. (ISBN 0-07-051212-4)

- **Loss Prevention in the Process Industries** — F. P. Lees. Monumentally important, tutorially prepared, and globally thorough exposition of risk assessment and reliability engineering principles and techniques, generously laced with case studies. — 1996 — Butterworths; Hard cover; Three volumes; 1316 pp. (ISBN 0-7506-1547-8)

Contact Information:

Pat Clemens

256.327.3707

A-P-T Research, Inc.

pclemens@apt-research.com