LA-UR-23-31739

Approved for public release; distribution is unlimited.

Title:	Brief Introduction to the Hazard Analysis Process
Author(s):	Kuropatwinski, James J.
Intended for:	University lecture
Issued:	2023-10-13

Los Alamos
NATIONAL LABORATORY

Los Alamos
NATIONAL LABORATORY

Brief Introduction to the Hazard Analysis Process

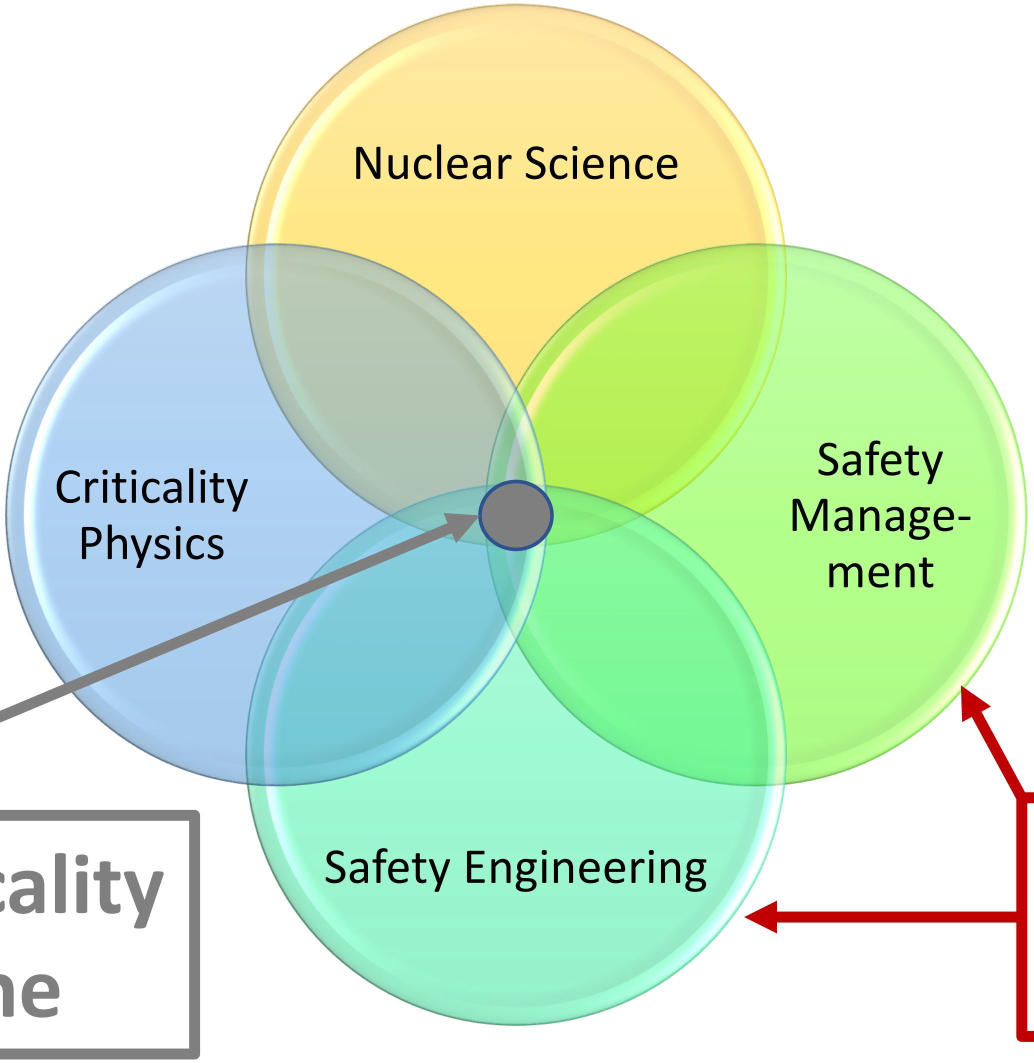
James J. Kuropatwinski, NCS

LA-UR-23-TBD

LEARNING OBJECTIVES

- Refresher of the factors that affect criticality safety
- Overview of hazard analysis concepts
- Overview of hazard analysis techniques
- Real world example

INTERSECTION OF NUCLEAR, CRITICALITY, SAFETY



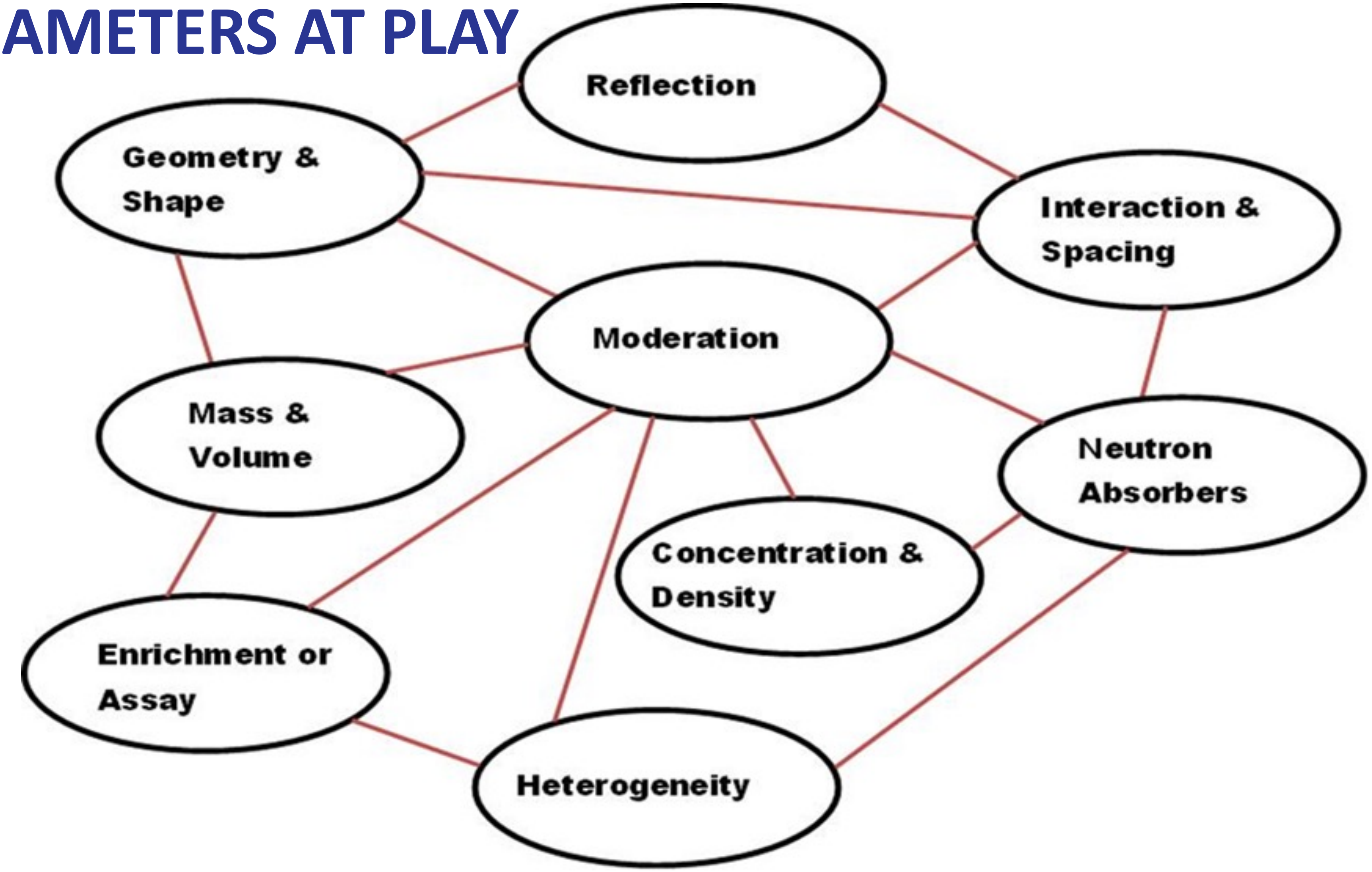
The Nuclear Criticality Safety Discipline

Process Analysis/ Hazard Analysis

K-EFF IN TERMS OF PARAMETERS

PARAMETER	n PROD	n LOSS	AFFECT ON K		
			PARAMETER ↓	OPTIMUM	PARAMETER ↑
MASS	X		↓		↑
DENSITY		X	↓		↑
ENRICHMENT/ASSAY	X	X	😃	😃	😃
ABSORPTION		X			↓
VOLUME		X			↓
GEOMETRY/SHAPE		X	↓	😃	↓
REFLECTION		X			↑
SPACING/INTERACTION		X	↑	😃	↓
MODERATION	X	X	🤬	🤬	🤬

NCS PARAMETERS AT PLAY

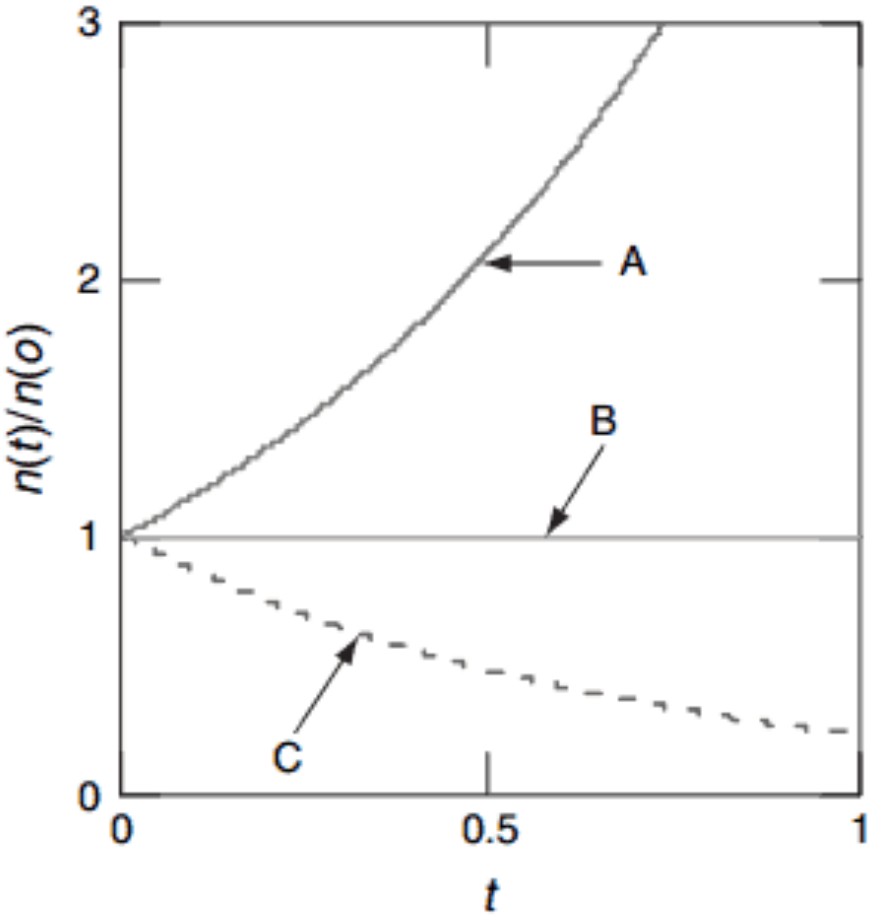


Taken from: *Nuclear Criticality Safety: Evaluations, Calculations, and Experiences*

TYING IT TOGETHER

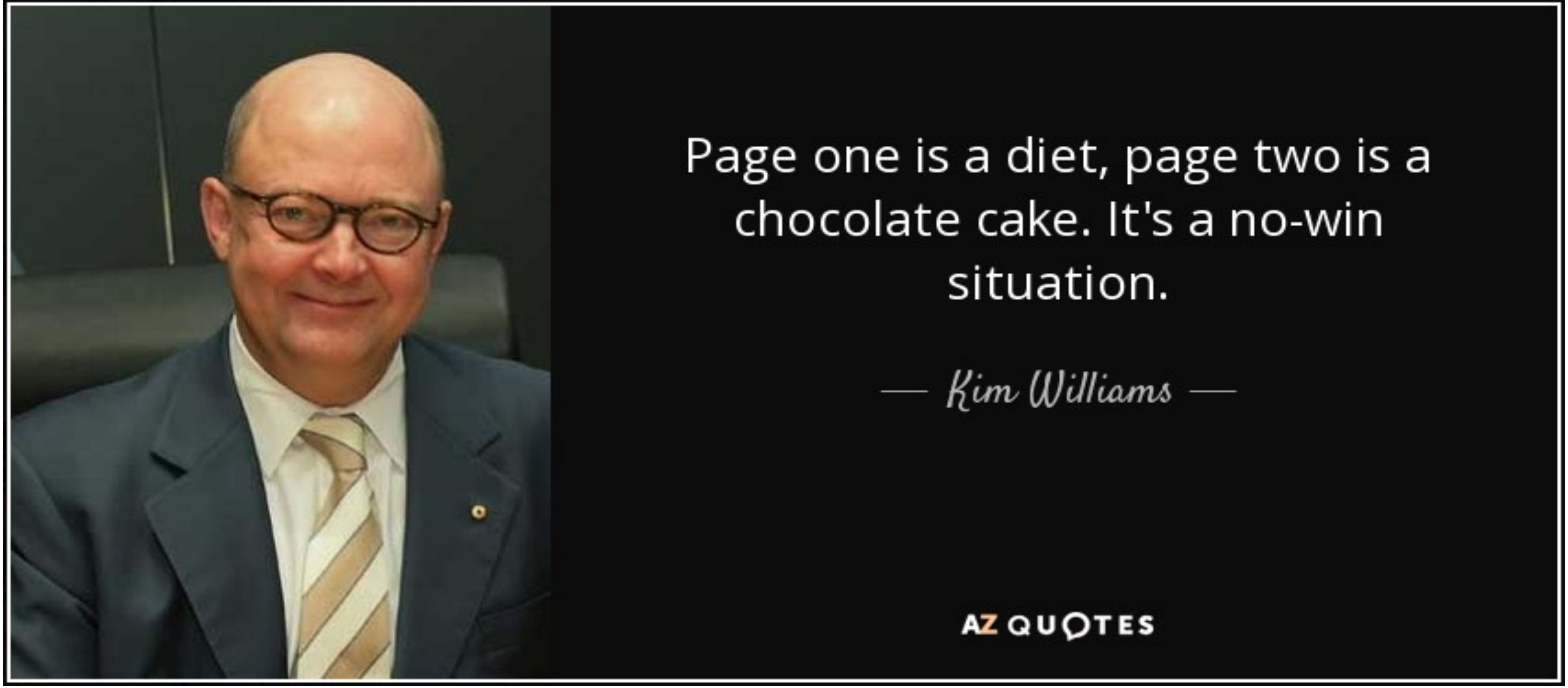
PARAMETER	n PROD	n LOSS	AFFECT ON K		
			PARAMETER ↓	OPTIMUM	PARAMETER ↑
MASS	X		↓		↑
DENSITY		X	↓		↑
ENRICHMENT/ASSAY	X	X	😃	😃	😃
ABSORPTION		X			↓
VOLUME		X			↓
GEOMETRY/SHAPE		X	↓	😃	↓
REFLECTION		X			↑
SPACING/INTERACTION		X	↑	😃	↓
MODERATION	X	X	🤬	🤬	🤬

$$Power \approx flux \approx n(t) = n_o e^{\left(\frac{\Delta k}{l}\right)t}$$



A curve is supercritical
B curve is critical
C curve is subcritical

INTRODUCTION TO THE HAZARD ANALYSIS PROCESS



Page one is a diet, page two is a chocolate cake. It's a no-win situation.

— Kim Williams —

BASIC DEFINITIONS

Hazard

- A source of danger (i.e. material, energy source, or operation) with the potential to cause illness, injury, or death to personnel or damage to an operation or to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation). (10 CFR 830)

Risk

- Combination of probability and consequence

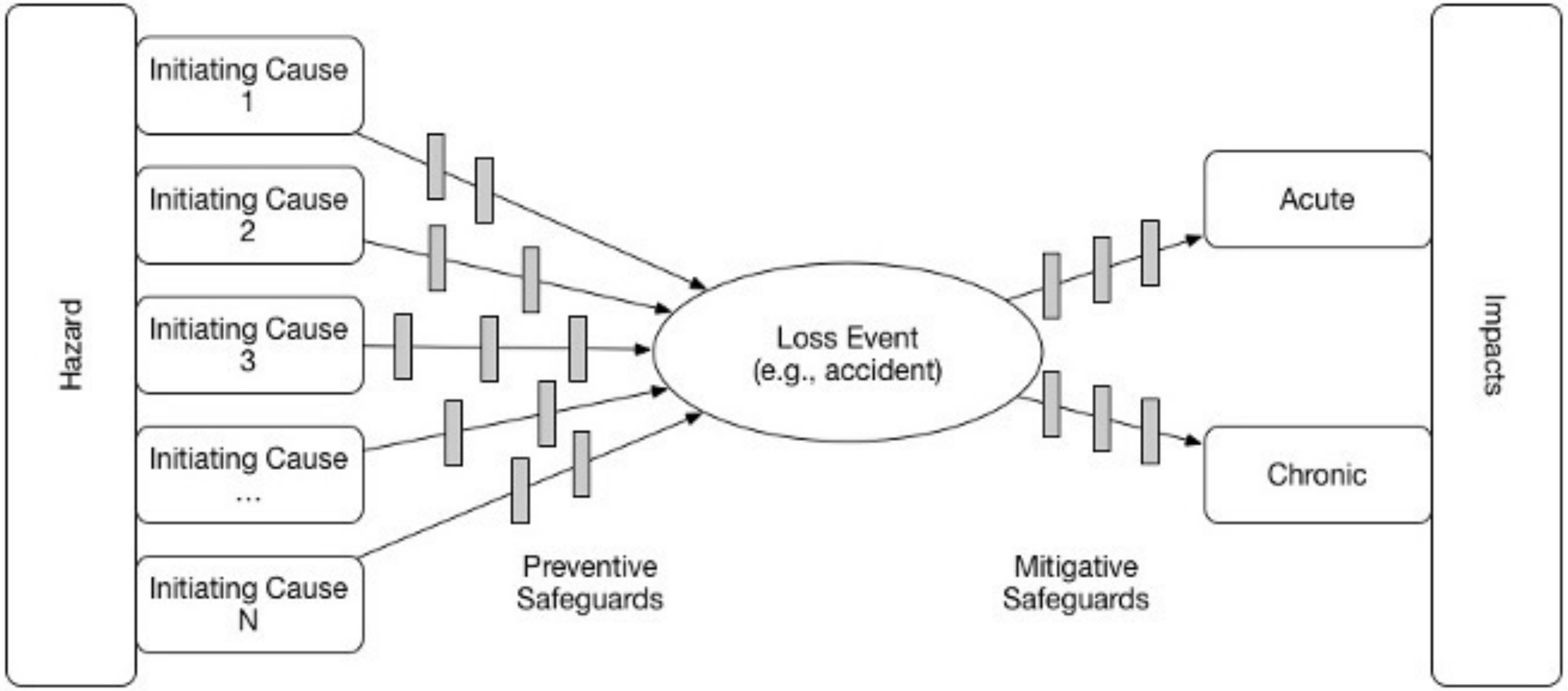
Safety

- An emergent property of a complex system to avert or not cause injury, danger, or loss.

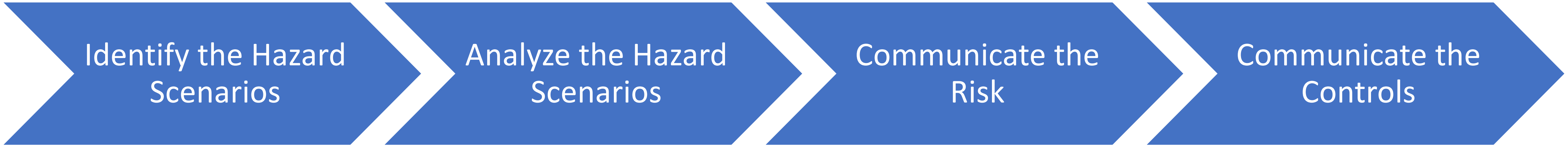
Accident sequence (a.k.a. Scenario)

- An unplanned event (or series of events) that results in a loss event and its associated impacts, including the success or failure of safeguards (i.e., controls).

VISUALIZATION OF THE PROCESS



BASICS OF THE PROCESS



- Likelihood/Frequency
- Consequence

- Risk Table

- Tables

HAZARD SCENARIO LIKELIHOOD IS ESTIMATED

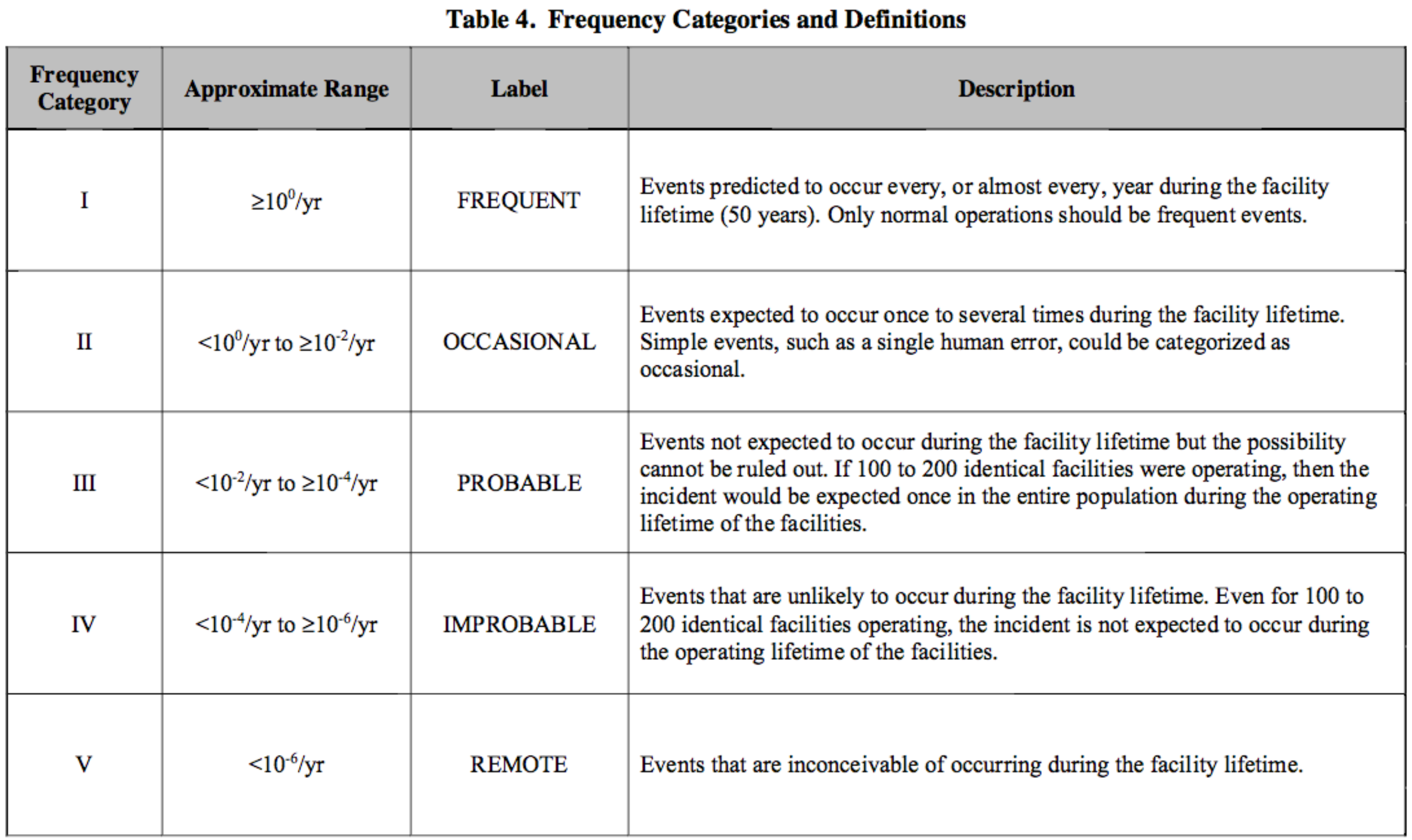
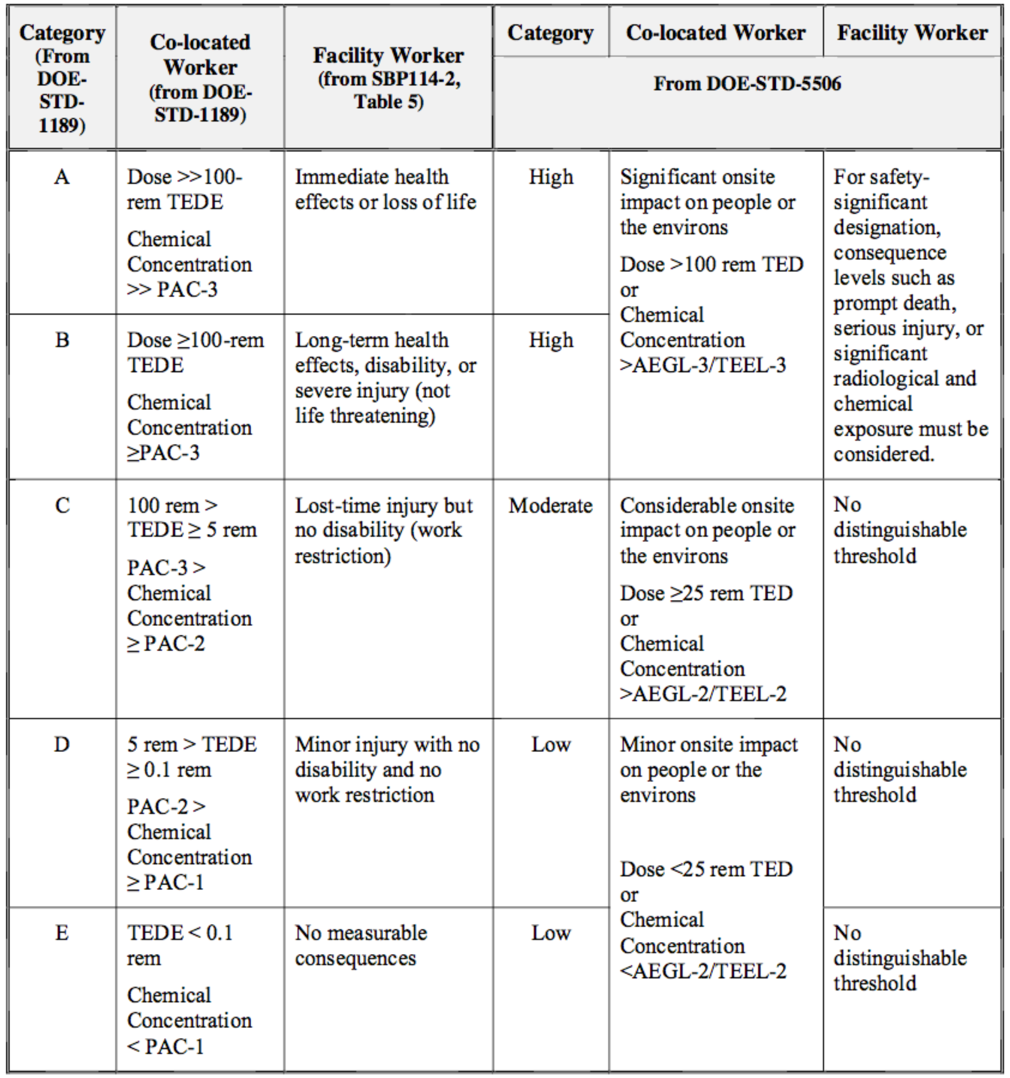


Table 4. Frequency Categories and Definitions

Frequency Category	Approximate Range	Label	Description
I	$\geq 10^{0}$/yr	FREQUENT	Events predicted to occur every, or almost every, year during the facility lifetime (50 years). Only normal operations should be frequent events.
II	$<10^{0}$/yr to $\geq 10^{-2}$/yr	OCCASIONAL	Events expected to occur once to several times during the facility lifetime. Simple events, such as a single human error, could be categorized as occasional.
III	$<10^{-2}$/yr to $\geq 10^{-4}$/yr	PROBABLE	Events not expected to occur during the facility lifetime but the possibility cannot be ruled out. If 100 to 200 identical facilities were operating, then the incident would be expected once in the entire population during the operating lifetime of the facilities.
IV	$<10^{-4}$/yr to $\geq 10^{-6}$/yr	IMPROBABLE	Events that are unlikely to occur during the facility lifetime. Even for 100 to 200 identical facilities operating, the incident is not expected to occur during the operating lifetime of the facilities.
V	$<10^{-6}$/yr	REMOTE	Events that are inconceivable of occurring during the facility lifetime.

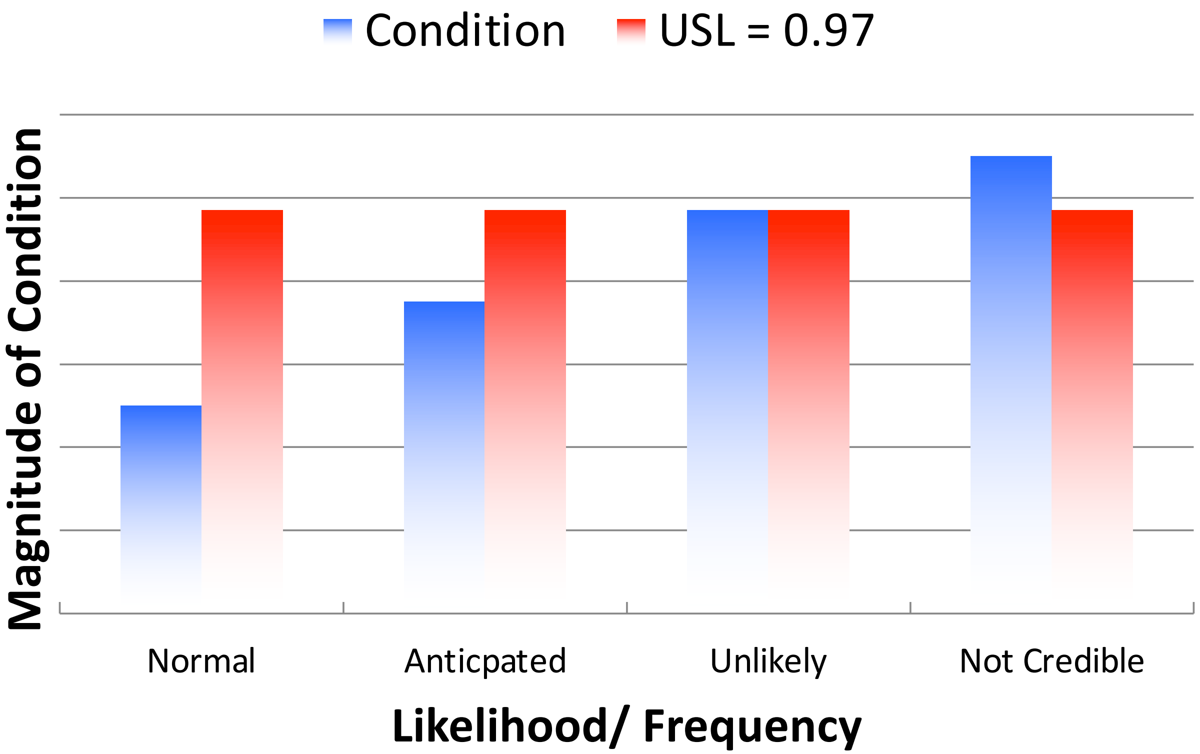
HAZARD SCENARIO CONSQUENCE IS CALCULATED

Table 6. Safety-Significant Control Criteria

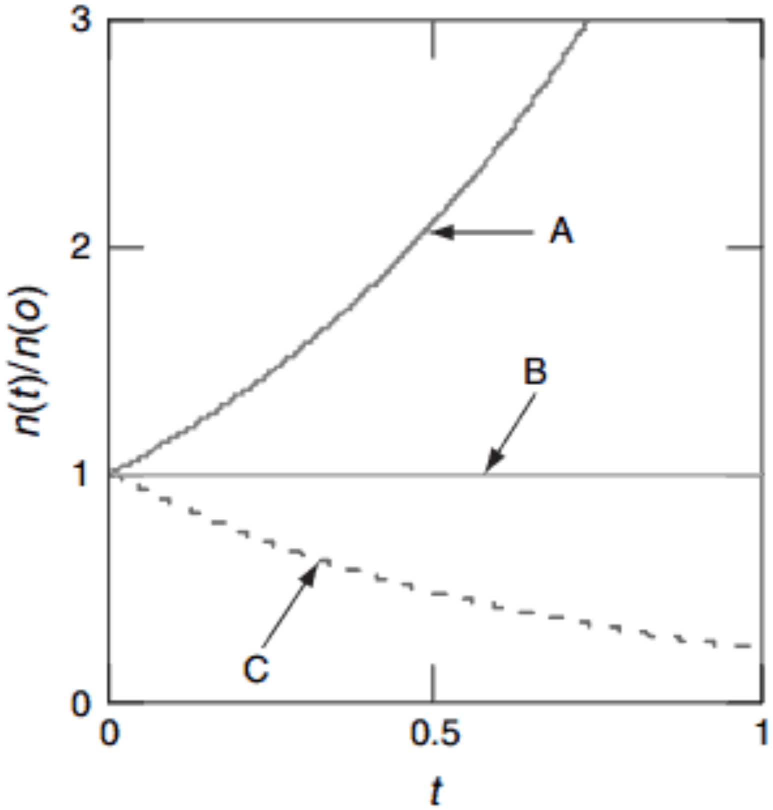


Category (From DOE-STD-1189)	Co-located Worker (from DOE-STD-1189)	Facility Worker (from SBP114-2, Table 5)	Category	Co-located Worker	Facility Worker
			From DOE-STD-5506		
A	Dose >>100-rem TEDE Chemical Concentration >> PAC-3	Immediate health effects or loss of life	High	Significant onsite impact on people or the environs Dose >100 rem TED or Chemical Concentration >AEGL-3/TEEL-3	For safety-significant designation, consequence levels such as prompt death, serious injury, or significant radiological and chemical exposure must be considered.
B	Dose ≥100-rem TEDE Chemical Concentration ≥PAC-3	Long-term health effects, disability, or severe injury (not life threatening)	High		
C	100 rem > TEDE ≥ 5 rem PAC-3 > Chemical Concentration ≥ PAC-2	Lost-time injury but no disability (work restriction)	Moderate	Considerable onsite impact on people or the environs Dose ≥25 rem TED or Chemical Concentration >AEGL-2/TEEL-2	No distinguishable threshold
D	5 rem > TEDE ≥ 0.1 rem PAC-2 > Chemical Concentration ≥ PAC-1	Minor injury with no disability and no work restriction	Low	Minor onsite impact on people or the environs Dose <25 rem TED or Chemical Concentration <AEGL-2/TEEL-2	No distinguishable threshold
E	TEDE < 0.1 rem Chemical Concentration < PAC-1	No measurable consequences	Low		No distinguishable threshold

LIKELIHOOD AND CONSEQUENCE FOR NCS PURPOSES



USL is defined as the Upper Subcritical Limit.
(It has not been defined in this class yet.)



A curve is supercritical
B curve is critical
C curve is subcritical

RISK IS COMMUNICATED

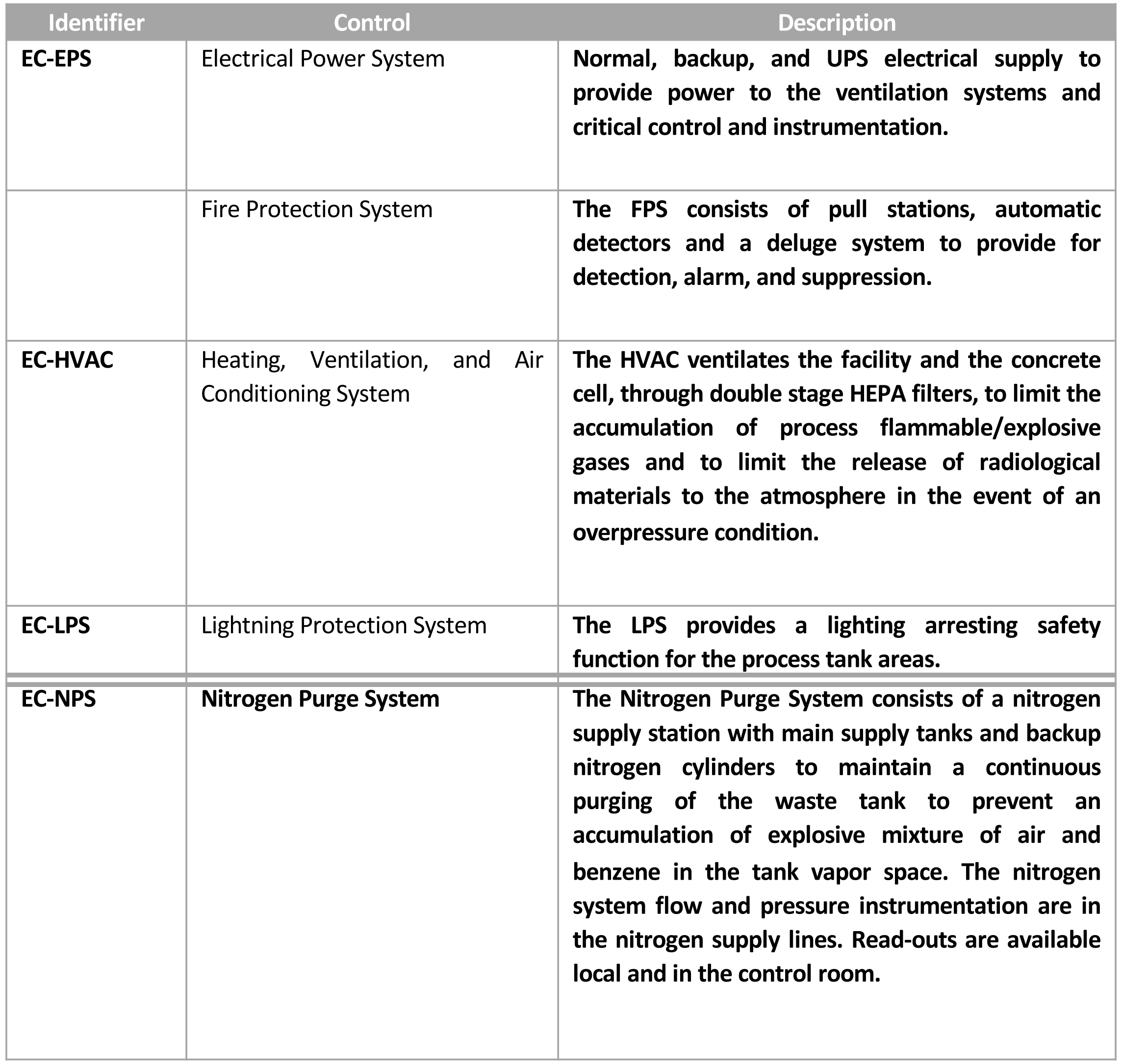
	A	B	C	D
I	🟥	🟥	🟨	🟩
II	🟥	🟥	🟨	🟩
III	🟥	🟨	🟨	🟩
IV	🟥	🟨	🟩	🟩

Red: unacceptable risk

Yellow: some additional 'safeguards' or 'controls' are necessary

Green: risk is acceptable

SAFETY CONTROLS ARE COMMUNICATED



Identifier	Control	Description
EC-EPS	Electrical Power System	**Normal, backup, and UPS electrical supply to provide power to the ventilation systems and critical control and instrumentation.**
	Fire Protection System	**The FPS consists of pull stations, automatic detectors and a deluge system to provide for detection, alarm, and suppression.**
EC-HVAC	Heating, Ventilation, and Air Conditioning System	**The HVAC ventilates the facility and the concrete cell, through double stage HEPA filters, to limit the accumulation of process flammable/explosive gases and to limit the release of radiological materials to the atmosphere in the event of an overpressure condition.**
EC-LPS	Lightning Protection System	**The LPS provides a lighting arresting safety function for the process tank areas.**
EC-NPS	**Nitrogen Purge System**	**The Nitrogen Purge System consists of a nitrogen supply station with main supply tanks and backup nitrogen cylinders to maintain a continuous purging of the waste tank to prevent an accumulation of explosive mixture of air and benzene in the tank vapor space. The nitrogen system flow and pressure instrumentation are in the nitrogen supply lines. Read-outs are available local and in the control room.**

HAZARD ANALYSIS TECHNIQUES

Disciplined approach to perform hazard evaluation

Guidelines for Hazard Evaluation Procedures is a very useful resource to select an appropriate hazard analysis technique

- What-If: dependent on expertise of individuals; very flexible
- HAZOP: guidewords selected for various design phases
- Failure Modes and Effects Analysis (FMEA): best for mechanical systems
- Fault-Tree/Event-Tree: helps define dominant accident sequences and accidents involving multiple failures (last resort)

HAZARD ANALYSIS TECHNIQUES

What If….

What-If analysis technique is a creative brainstorming approach to hazards evaluation.

- Group of experienced people familiar with the subject process ask questions or voice concerns about possible undesired events.
- Not highly structured like HAZOP analysis or FEMA.
- Leader needs to guide group to ensure thorough coverage of the required scope.
- Frequently used with good results.
- Powerful technique if team is experienced; otherwise, results are likely to be incomplete.

Very flexible and can be used for any phase of a process

Example: What If?

Hazard	What-If	Consequences	May Exceed Which Criteria	Existing Protection	Action Items

HAZARD ANALYSIS TECHNIQUES

Hazard and Operability (HAZOP)

HAZOP leader systematically guides an interdisciplinary team through the plant design using “guide words” applied to “process parameters” at “study nodes” resulting in deviations.

- Guide words: no, less, more, part of, as well as, reverse, other than.
- Process parameters: flow, time, frequency, mixing, pressure, composition, viscosity, addition, temperature, pH, voltage, separation, level, speed, information, reaction.
- Study nodes: points throughout the process.
- Examples: No + Flow = No Flow; Less + Flow = Less Flow.
- Team agrees on possible causes for the deviation, consequences, controls, and recommendations.

Very effective during or after final design

Example: HAZOP

Parameter/ Guide Word	Mass	Enrich.	Chem. Form	Phys. Form	Moderation	Geometry	Spacing	Config.	Poisons	Reflection
None…	NC	NC	NC	NC	NC	NC	Sca	NA	NC	NC
More of…	SCb	SCc	NA	NA	SCd	NA	NC	NA	NC	Sce
Less of…	NC	SCf	NA	NA	NC	NC	SCh	NA	NA	NC
Part of…	NP	NP	NP	NP	NA	NA	NA	NP	NA	NA
As well as…	NP	NP	NP	NP	NP	NP	SCbb	NP	NC	NA
Reverse…	NA	NA	NA	NC	NA	NA	NA	NA	NA	NA
Other than…	NA	NA	SCw	SCx	SCy	SCz	NC	NC	NC	NA

HAZARD ANALYSIS TECHNIQUES

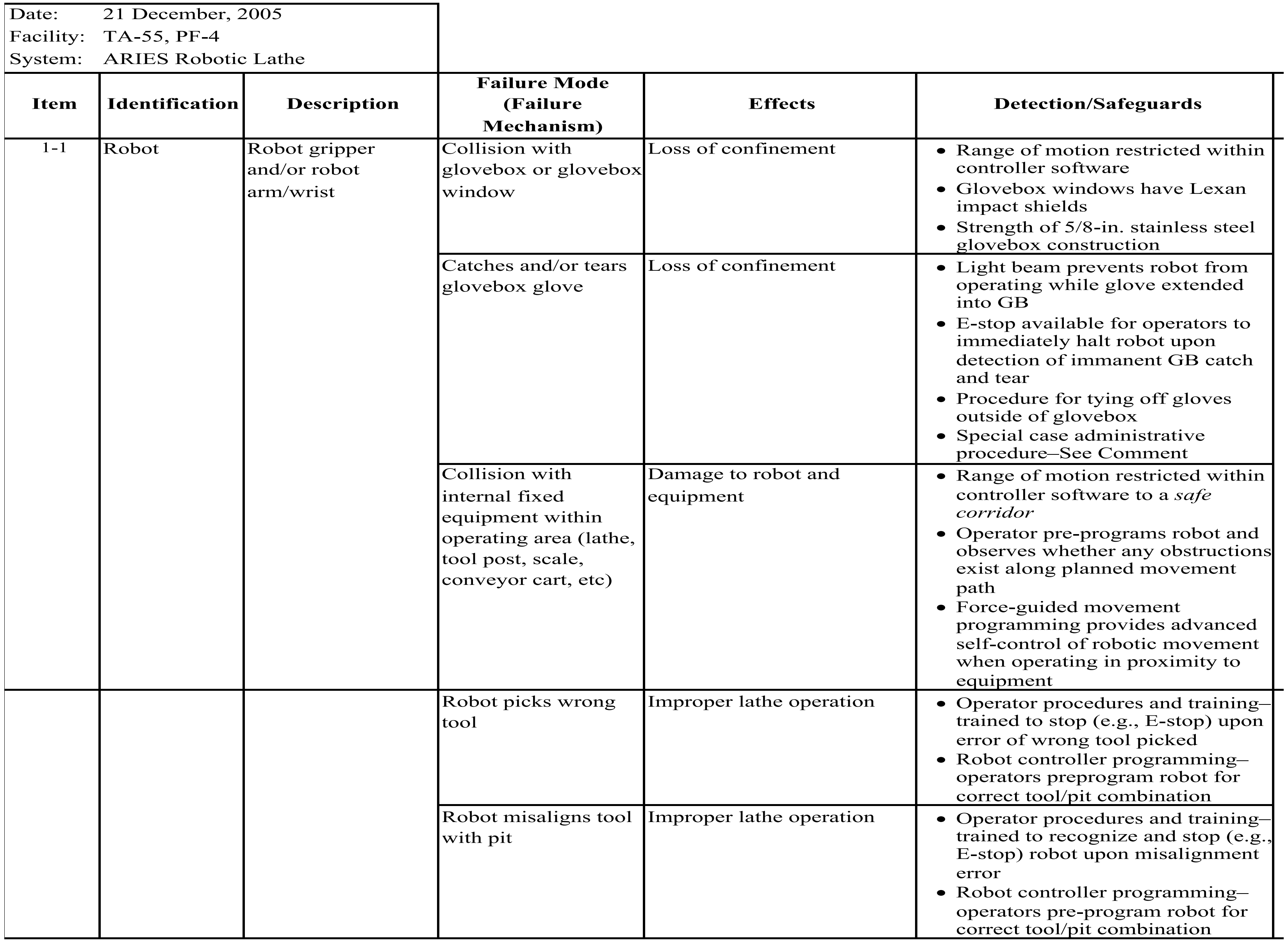
Failure Modes and Effects Analysis (FMEA)

Failure Modes and Effects Analysis tabulates failure modes of equipment (including improper operation) and their effects on a system or plant.

- Failure mode describes how the equipment fails (open, closed, on, off, leaks, ruptures, sticks, etc.).
- FMEA identifies single failure modes that directly result in or significantly contribute to an accident.
- FMEA is not efficient for identifying an exhaustive list of combinations of equipment failures that lead to accidents.

Human operator errors are usually not directly evaluated with FMEA.

Example: FEMA



Date: 21 December, 2005
Facility: TA-55, PF-4
System: ARIES Robotic Lathe

Item	Identification	Description	Failure Mode (Failure Mechanism)	Effects	Detection/Safeguards
1-1	Robot	Robot gripper and/or robot arm/wrist	Collision with glovebox or glovebox window	Loss of confinement	• Range of motion restricted within controller software • Glovebox windows have Lexan impact shields • Strength of 5/8-in. stainless steel glovebox construction
			Catches and/or tears glovebox glove	Loss of confinement	• Light beam prevents robot from operating while glove extended into GB • E-stop available for operators to immediately halt robot upon detection of immanent GB catch and tear • Procedure for tying off gloves outside of glovebox • Special case administrative procedure–See Comment
			Collision with internal fixed equipment within operating area (lathe, tool post, scale, conveyor cart, etc)	Damage to robot and equipment	• Range of motion restricted within controller software to a *safe corridor* • Operator pre-programs robot and observes whether any obstructions exist along planned movement path • Force-guided movement programming provides advanced self-control of robotic movement when operating in proximity to equipment
			Robot picks wrong tool	Improper lathe operation	• Operator procedures and training–trained to stop (e.g., E-stop) upon error of wrong tool picked • Robot controller programming–operators preprogram robot for correct tool/pit combination
			Robot misaligns tool with pit	Improper lathe operation	• Operator procedures and training–trained to recognize and stop (e.g., E-stop) robot upon misalignment error • Robot controller programming–operators pre-program robot for correct tool/pit combination

HAZARD ANALYSIS TECHNIQUES

Fault Tree

Focuses on a particular accident or main system failure (top event) and provides a method for determining its causes.

- Is a graphical model that displays various combinations of failures that can result in the main system failure of interest.
- As qualitative tool: allows the hazard analyst to focus preventive controls on the significant basic causes to reduce the likelihood of an accident.

As quantitative tool: can be used as a part of probabilistic risk analysis (with probabilities assigned to events) to determine frequency bins.

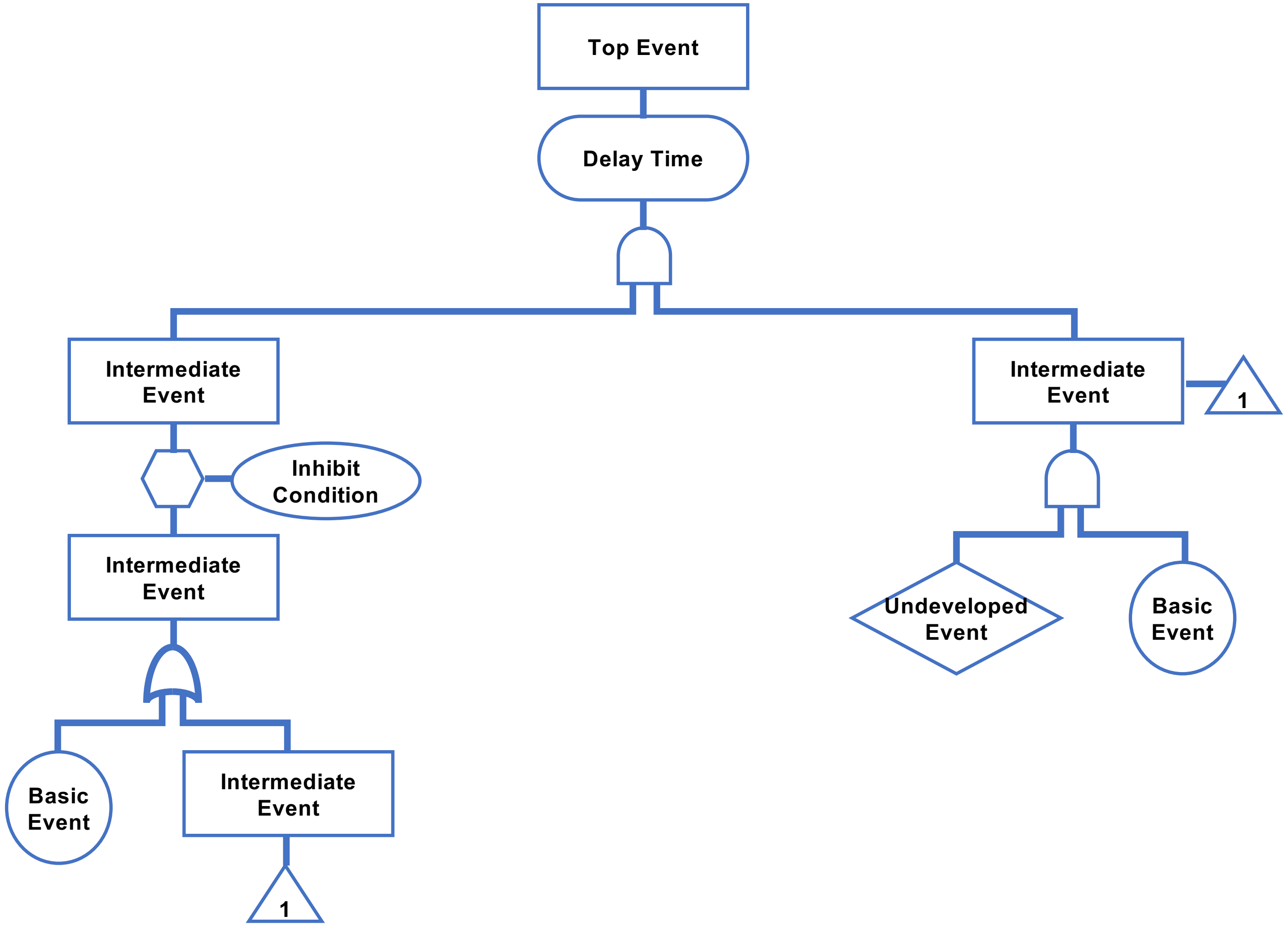
HAZARD ANALYSIS TECHNIQUES

Fault Tree

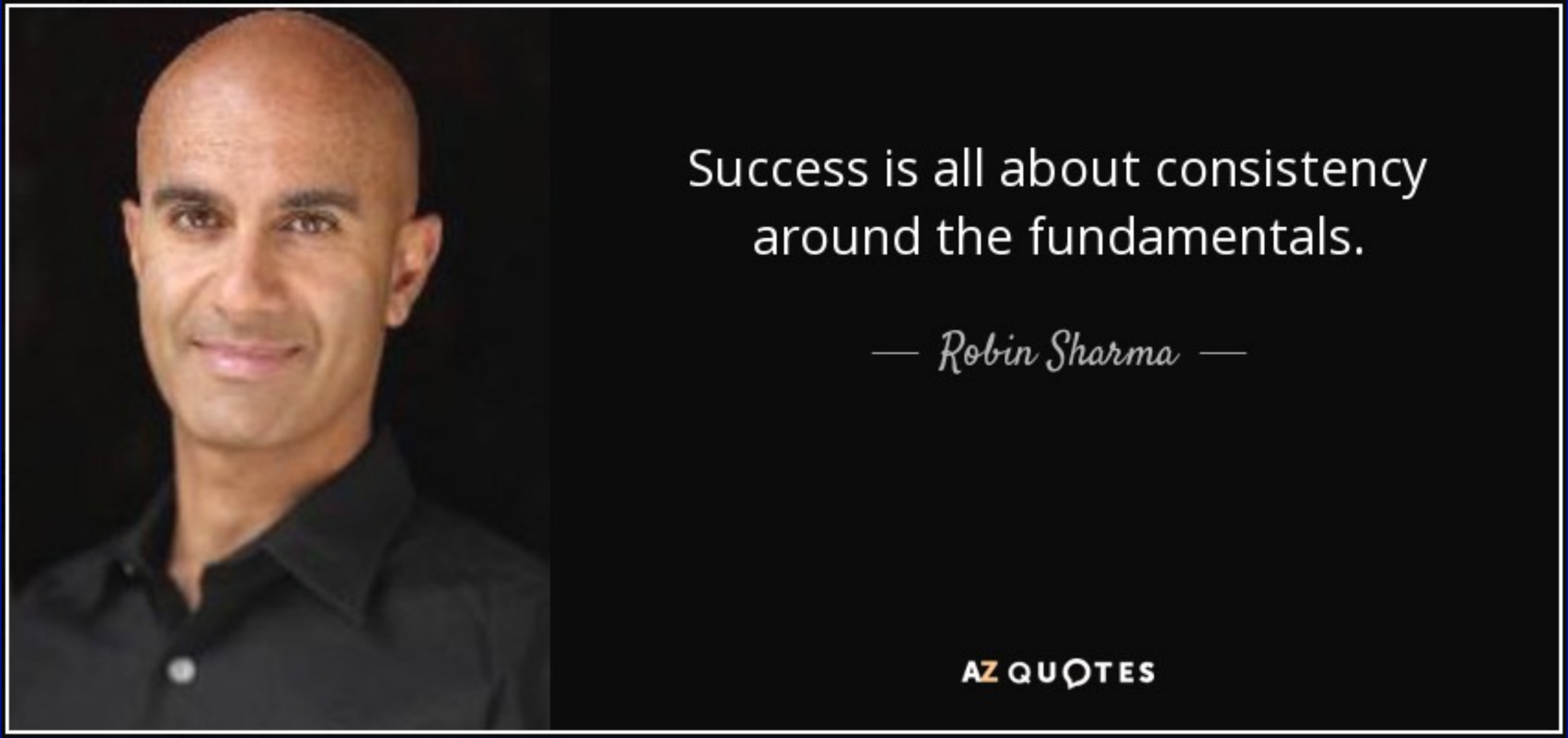
Often used when another HA technique has pinpointed an important accident of interest that requires more detailed analysis to determine causes and preventive controls.

Well suited to complex, highly redundant systems, and systems vulnerable to multiple failures.

Example: Fault Tree



CRITICALITY SAFETY EVALUATION PROCESS



Success is all about consistency around the fundamentals.

— Robin Sharma —

AZ QUOTES

ONE BASIC SAFETY CRITERION

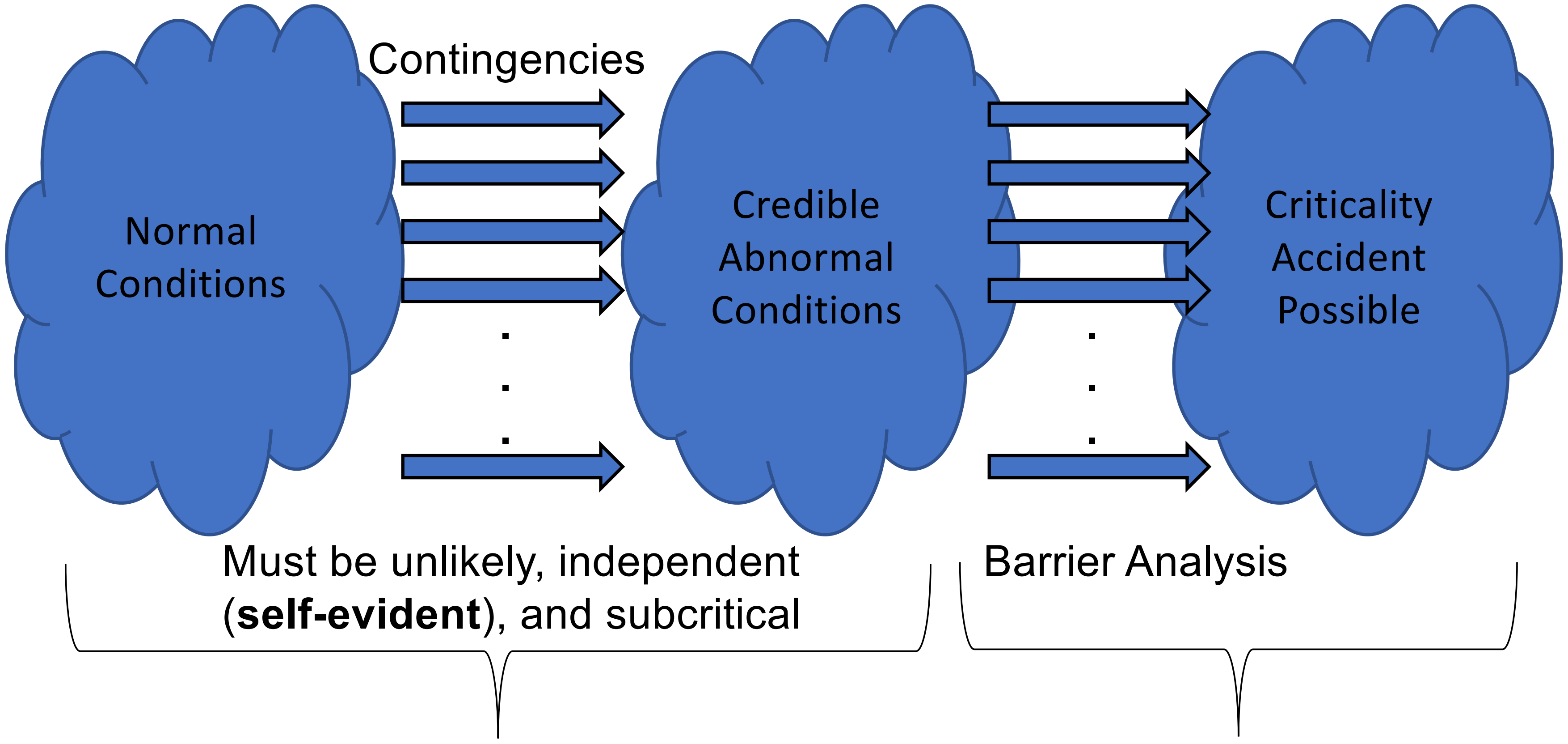
- From ANSI/ANS-8.1-2014 (§4.1.2)
  - Before a new operation with fissionable material is begun, or before an existing operation is changed, it shall be determined that the entire process will be subcritical under both normal and credible abnormal conditions.
- From ANSI/ANS-8.19 (§7.1)
  - Before a new operation with fissile material is begun, or before an existing operation is changed, it shall be determined and documented that the entire process will be subcritical for both normal and credible abnormal conditions.
- Known as the Process Analysis Requirement

ANOTHER BASIC SAFETY CRITERION

- From ANSI/ANS-8.1-2014 (§4.2.2)
  - Process designs should incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible.

- Known as the double contingency principle

CRITICALITY SAFETY EVALUATIONS – EVEN MORE SIMPLIFIED



Must be unlikely, independent (**self-evident**), and subcritical

Barrier Analysis

Typical PA

Whether or not documented, analyst must understand where criticality is possible

STANDARD FOR A CRITICALITY SAFETY EVALUATION

- From DOE-STD-3007-2017
  - Introduction
  - Description
  - Unique or Special Requirements
  - Methodology and Validation
  - Process Analysis
  - Summary of Controls and Assumptions
  - Summary and Conclusions
  - Cited References
  - Appendices

- Simplified
  - Process Description
  - Process Conditions
  - Process Analysis
  - Controls Development
  - Any additional information deemed important

NCS: IS THE RING DUNK TRADITION SAFE?

CLASSROOM EXERCISE – UP TO 30 MINUTES

- Make a bullet procedure
- Develop a scenario table

Table 1 – Process Description Based Hazard Analysis Table

Process Description	Normal Condition	Parameter/ Assumption Influenced	Conceivable Condition (What If…)	Frequency (Anticipated, Unlikely, Not Credible)	Implementing Measure(s) (Controls)	Credible Condition
State the aspect of the process description under consider-ation	*State the 'normal condition'*	*State that NCS parameters or operational assumption that would be influenced*	*State the 'What-if' that could go wrong.*	*State the agreed upon frequency*	*State the control that is relied upon that makes the frequency as determined*	*Provide the credible condition that may exist if the scenario occurs*

Table 2 – Parameter Based Hazard Analysis Table

Parameter	Normal Condition	Control Method	Conceivable Condition (What if…)	Frequency (Anticipated, Unlikely, Not Credible)	Implementing Measure(s) (Controls)	Credible Condition
State the NCS parameter	*State the 'normal condition'*	*State how control is exercised*	*State the 'What-if' that could go wrong. (Or, use HAZOP key-word.)*	*State the agreed upon frequency*	*State the control that is relied upon that makes the frequency as determined*	*Provide the credible extreme value that the parameter may take if the scenario occurs*

Table 3 – Parameter Based HAZOP Table

(Refer to HAZOP Slide)

CONCLUSION

- Refresher from factors that affect criticality safety
  - Hazard analysis/process analysis is within the safety engineering and safety management spheres of NCS
- Overview of hazard analysis concepts
  - Likelihood/frequency
  - Consequence
  - Risk and safety controls communication
- Overview of hazard analysis techniques
  - What If?, HAZOP, FMEA, Fault/Event Trees
- Real world example
  - Ring dunk results