Overview of “BSEE-2016-XXX Probabilistic Risk Assessment Procedures Guide for Offshore Applications (Partial Draft)”

Presentation to PHMSA RMWG

Bob Youngblood

March 9, 2017

BSEE: Bureau of Safety and Environmental Enforcement

www.inl.gov

Idaho National Laboratory

Disclaimer

Views expressed by the presenter are not necessarily those of the Idaho National Laboratory or Johnson Space Center.

Summary

- NASA's Johnson Space Center (JSC) is developing a PRA Procedures Guide for BSEE, initially scoped to deal with offshore drilling
- INL is helping JSC do that
- By agreement between JSC and BSEE, the starting point for the development was NASA's PRA Procedures Guide
  - Development of the NASA guide was initiated after Challenger
  - The NASA guide was heavily influenced by nuclear industry PRA guidance
    - Initially (2002), mostly logic modeling, which is good at functional dependency, redundancy, etc., but rather approximate in some ways
    - Later (2011), the guide paid some attention to simulation, which is better at timing, variations in event phenomenology, …
  - We are trying to be responsive to oil-industry risk modeling needs, not blindly assume nuclear/ NASA PRA techniques are optimal
- The Draft BSEE Guide addresses [or *will* address, when complete]
  - Standard high-end logic-model tools
  - More qualitative risk assessment tools
  - Simulation-enhanced PRA [placeholder for now]
  - Improved discussion of data analysis
  - Better understanding of uncertainty
  - Improved discussion of the USE of risk model results

*In The Late 60’s / Early 70’s, Some Were Beginning to Advocate Modern Risk Analysis**

Siting Criteria – A New [1967] Approach F .R . Farmer

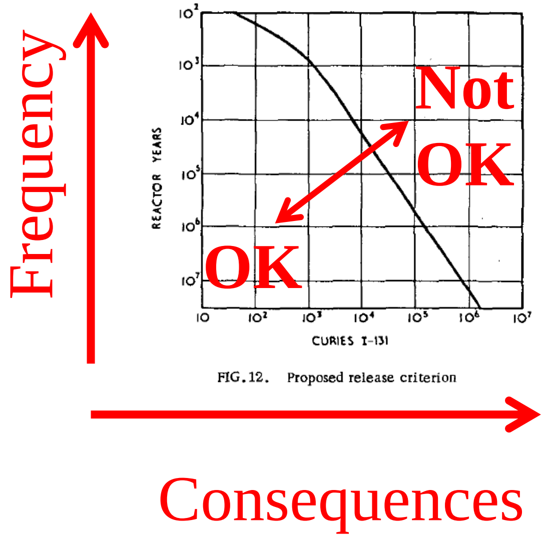


FIG.12. Proposed release criterion

Principles of Unified Systems Safety Analysis [USSA] B. John Garrick, 1970

… USSA has been evolved to both assess and monitor the level of safety while revealing necessary adjustments either in design, procedure, or both to sustain a prescribed level. … put the more analytical activities of safety analysis in context with the more routing activities of operations to assure to the extent possible their proper interactions. …

****That is, the use of logic models (event trees, fault trees) to construct and quantify a notionally complete scenario set***

Two things going on:

- **How safe is this facility?**
- **How do we best manage risk?**

Why do we do risk analysis?

- To support decisions…
- … in situations characterized by
  - High stakes
  - Complexity
  - Significant uncertainty
  - Diversity of stakeholders
- One definition of risk:
  - {scenarios, scenario frequencies, scenario consequences} (Kaplan and Garrick, 1981)
    - With treatment of uncertainty…
  - A point of this definition is that just giving the decision-maker a single number (like “expected consequences”) may help, but doesn’t indicate what more would be helpful to know, or what would be helpful to fix

OVERVIEW OF HIGH-END SCENARIO-BASED PRA

Not understood in the US at the time of WASH-1400

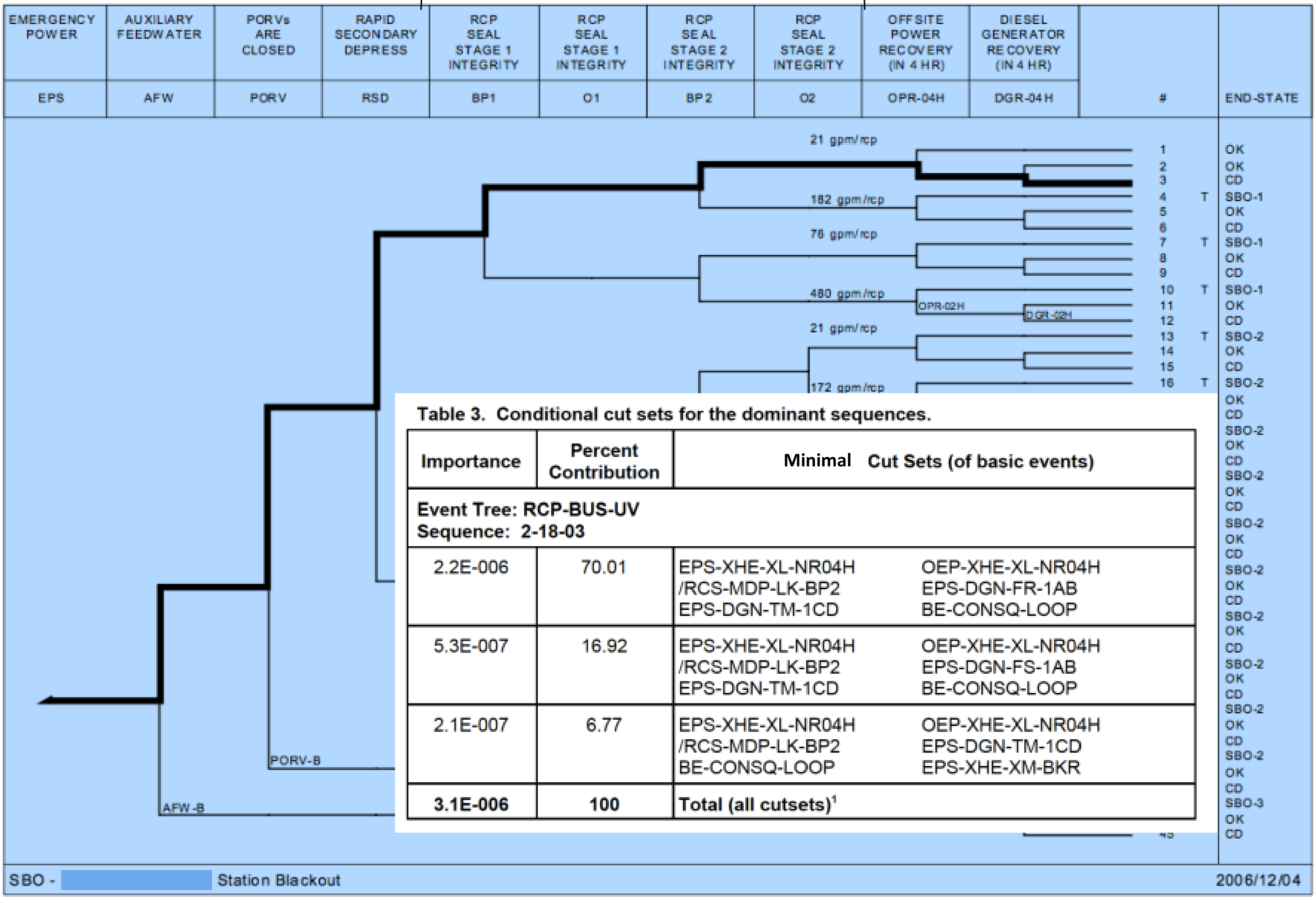


Table 3. Conditional cut sets for the dominant sequences.

Importance	Percent Contribution	Minimal Cut Sets (of basic events)	
Event Tree: RCP-BUS-UV **Sequence: 2-18-03**			
2.2E-006	70.01	EPS-XHE-XL-NR04H /RCS-MDP-LK-BP2 EPS-DGN-TM-1CD	OEP-XHE-XL-NR04H EPS-DGN-FR-1AB BE-CONSQ-LOOP
5.3E-007	16.92	EPS-XHE-XL-NR04H /RCS-MDP-LK-BP2 EPS-DGN-TM-1CD	OEP-XHE-XL-NR04H EPS-DGN-FS-1AB BE-CONSQ-LOOP
2.1E-007	6.77	EPS-XHE-XL-NR04H /RCS-MDP-LK-BP2 BE-CONSQ-LOOP	OEP-XHE-XL-NR04H EPS-DGN-TM-1CD EPS-XHE-XM-BKR
3.1E-006	**100**	**Total (all cutsets)[1]**	

Figure 4. Event tree for station blackout.

Next Generation Nuclear Plant Licensing Basis Event Selection White Paper (INL/EXT-10-19521)

Farmer

(Holbrook)

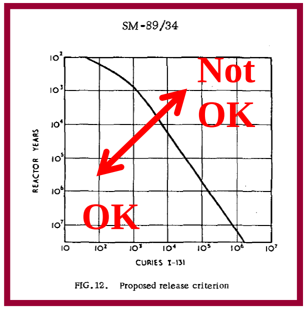
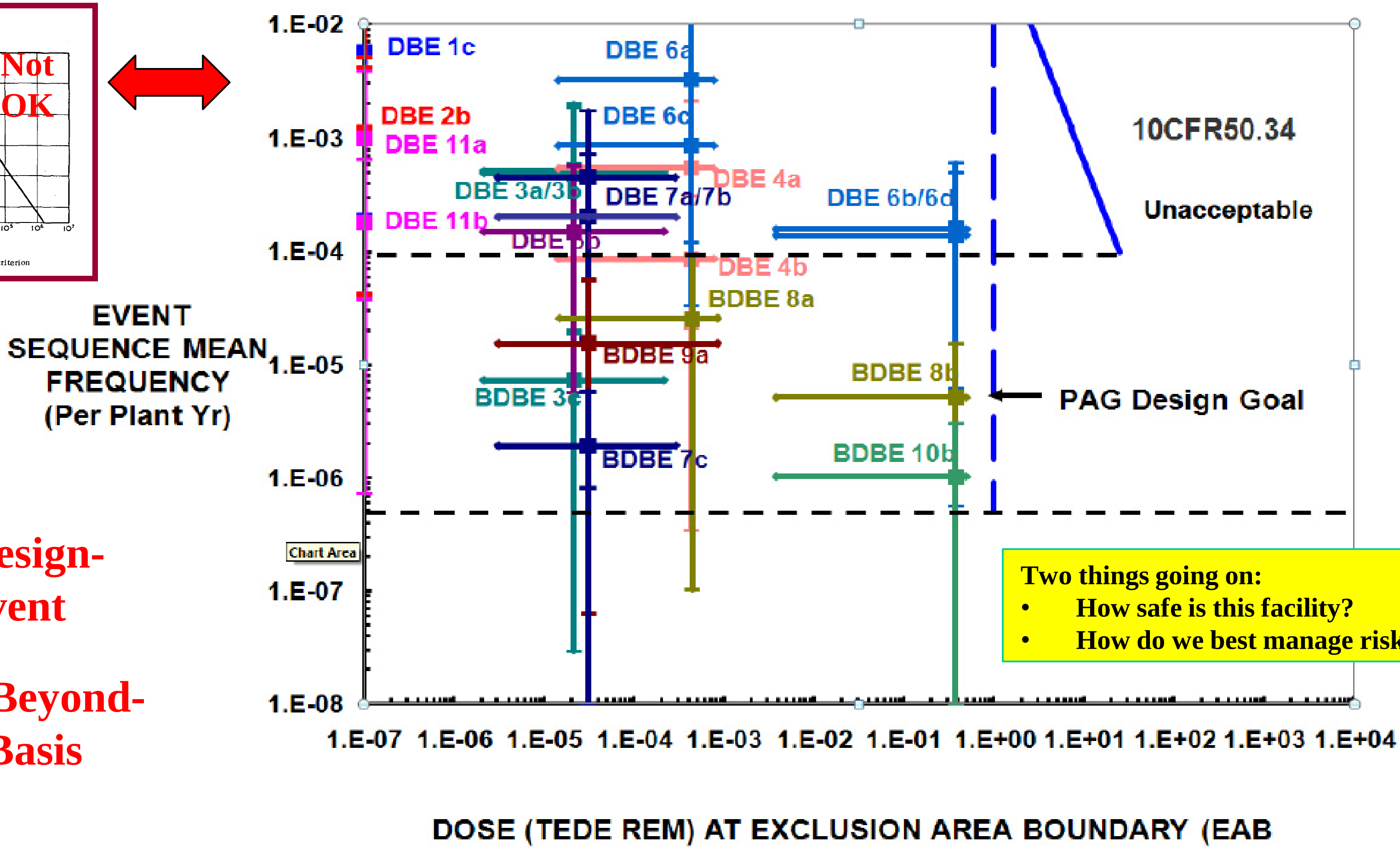


FIG. 12. Proposed release criterion



Two things going on:

- How safe is this facility?
- How do we best manage risk?

DBE: Design-Basis Event

BDBE: Beyond-Design-Basis Event

Figure 8. Use of PRA to select BDBEs.

EVOLUTION OF "PRA PROCEDURES GUIDES"

Selected “Procedures Guides”

PRA Procedures Guide, NUREG/CR-2300 (~1983)

Interim Reliability Evaluation Program Procedures Guide, NUREG/CR-2728 (1983)

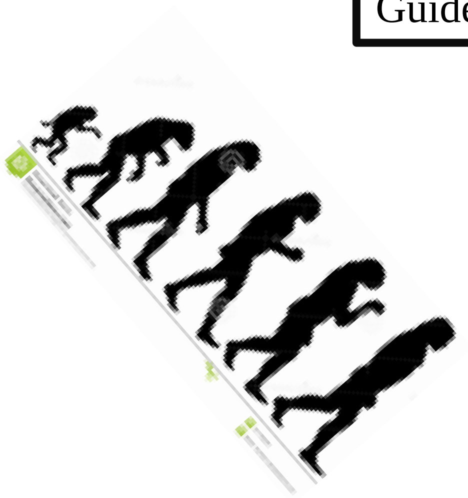
Probabilistic Safety Analysis Procedures Guide," NUREG/CR-2815, Rev. 1 (August 1985).

Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners (**2002**)

Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA/SP-**2011**-3421

BSEE: Probabilistic Risk Assessment Procedures Guide for Offshore Applications (Partial Draft) (2016)

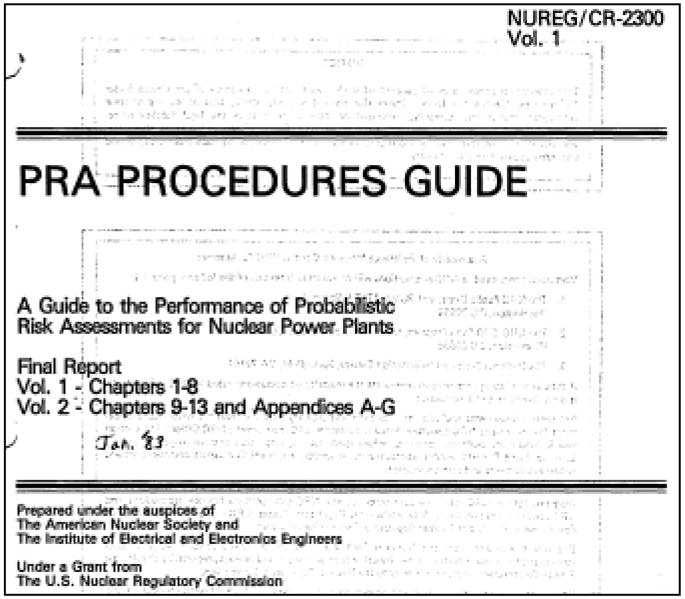
PHMSA



Consensus Standards, "PRA Quality" concerns, Other Regulatory Guidance

- PRA standards have also been under development by the American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS):
  - ASME and ANS jointly issued an at-power Level 1 and limited Level 2 PRA standard for internal and external hazards (requirements for low power shutdown conditions to be added) (Ref. 14).2
  - ASME is developing PRA standards for new LWRs applying for design certification (DC) and COLs, and for future advanced non-LWRs. ANS is developing a Level 1 and limited Level 2 PRA standard for low-power shutdown operating mode (to be incorporated into the ASME/ANS joint standard), and is also developing Level 2 and Level 3 PRA standards.
- NRC Regulatory Guide 1.200
  - When used in support of an application, this regulatory guide will obviate the need for an in-depth review of the base PRA by NRC reviewers, allowing them to focus their review on key assumptions and areas identified by peer reviewers as being of concern and relevant to the application. Consequently, this guide will provide for a more focused and consistent review process. In this regulatory guide, the quality of a PRA analysis used to support an application is measured in terms of its appropriateness with respect to scope, level of detail, and technical acceptability.

Evolution of PRA Procedures Guides



NUREG/CR-2300
Vol. 1

PRA PROCEDURES GUIDE

A Guide to the Performance of Probabilistic
Risk Assessments for Nuclear Power Plants

Final Report
Vol. 1 - Chapters 1-8
Vol. 2 - Chapters 9-13 and Appendices A-G

Jan. '83

Prepared under the auspices of
The American Nuclear Society and
The Institute of Electrical and Electronics Engineers

Under a Grant from
The U.S. Nuclear Regulatory Commission

State of the art as of ~ 1980; authored by almost the entire community of practice that existed as of 1979; focused on nuclear power plants

Not prescriptive: rather, descriptive of a buffet of techniques

Context: Post-Three-Mile-Island; General perception of the hazard (the range of potential consequences); Recognition of the need for regulators to get beyond purely prescriptive thinking; Recognition of the need for a structured approach to risk assessment

Comment on "getting beyond purely prescriptive thinking"

- Before the 1979 accident at Three Mile Island, the Reactor Safety Study (1975) had already illustrated some of what's wrong with prescriptive approaches to safety analysis
- In general, prescriptive approaches…
  - … leave undone some of what ought to be done (they miss significant risk contributors)
  - … do things that ought not to be done (expend resources preventing things that are unlikely *a priori*, or unlikely to cause real problems even if they do occur
- Risk analysis isn't perfect; you have to work hard to try to assure completeness and reasonableness of modeling, especially in areas where the community of practice has not reached consensus
- But it's better than nothing, and over the years, has come to play a very important role in NRC decision-making

Evolution of PRA Procedures Guides (continued)

NASA/SP-2011-3421

Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

NASA Project Managers:
Michael Stamatelatos, Ph.D., and
Homayoon Dezfuli, Ph.D.

NASA Headquarters
Washington, DC
Second Edition
December 2011

State of practice of fault tree / event-tree methods as of 2002-2011; authored by PRA practitioners who were also mostly conversant with NASA technologies

Context: Post-Challenger; General perception of the hazard (the range of potential consequences); Recognition of the need for a structured approach to risk assessment

BSEE PRA Guide

- Context: Post-Macondo

- Purpose
  - This Guide is intended to assist in the development of probabilistic risk assessment (PRA) of offshore drilling facilities, in order to support decision-making by Bureau of Safety and Environmental Enforcement (BSEE) and by the industry.

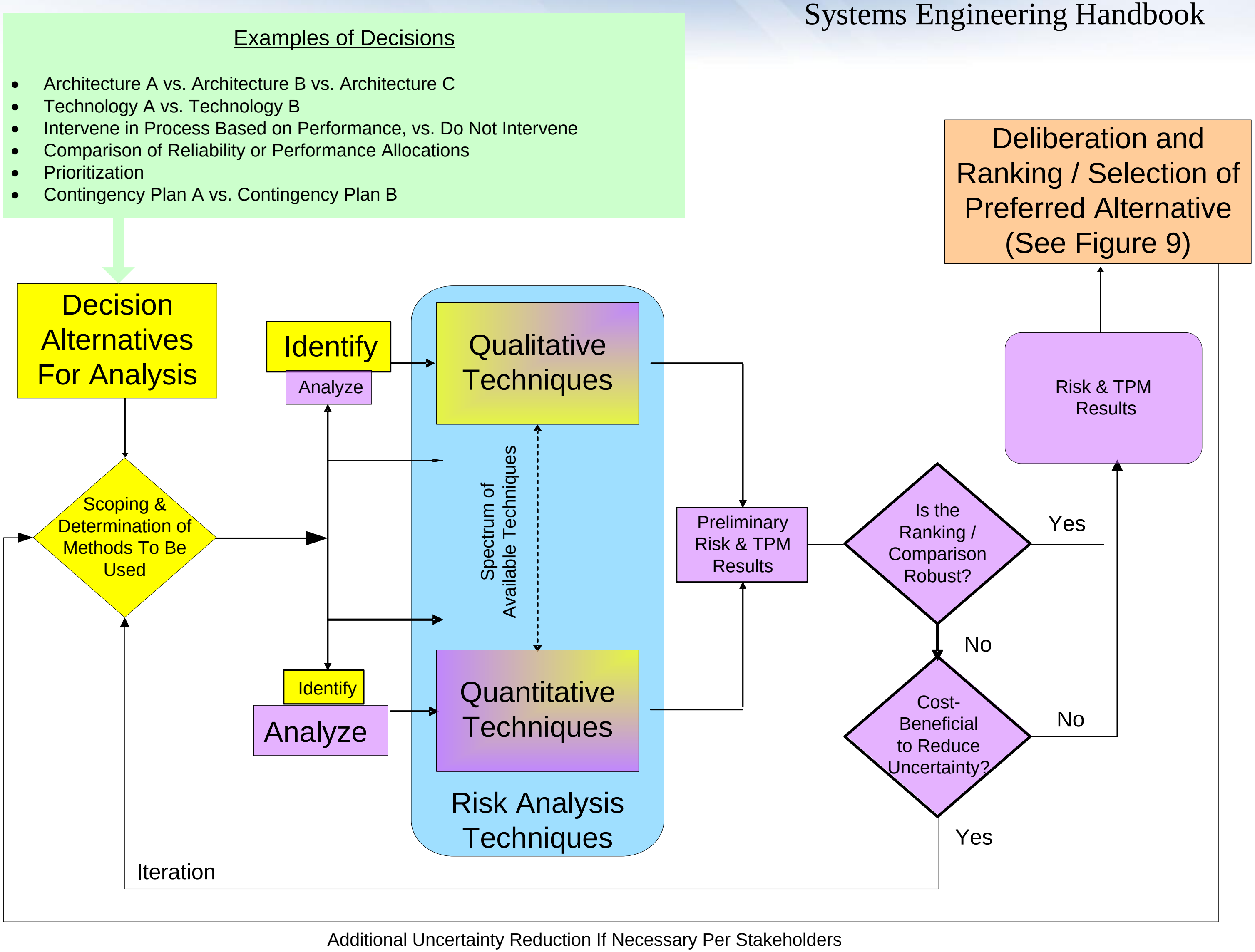
- Scope
  - This Guide is not a policy document, nor does it establish regulatory requirements; it discusses particular modeling techniques that have been found to be useful in a range of applications to decision-making about complex and high-hazard facilities.

Graded approach, keyed to decision support needs

DEVELOPMENT PHILOSOPHY

Graded Approach to System Safety Analysis

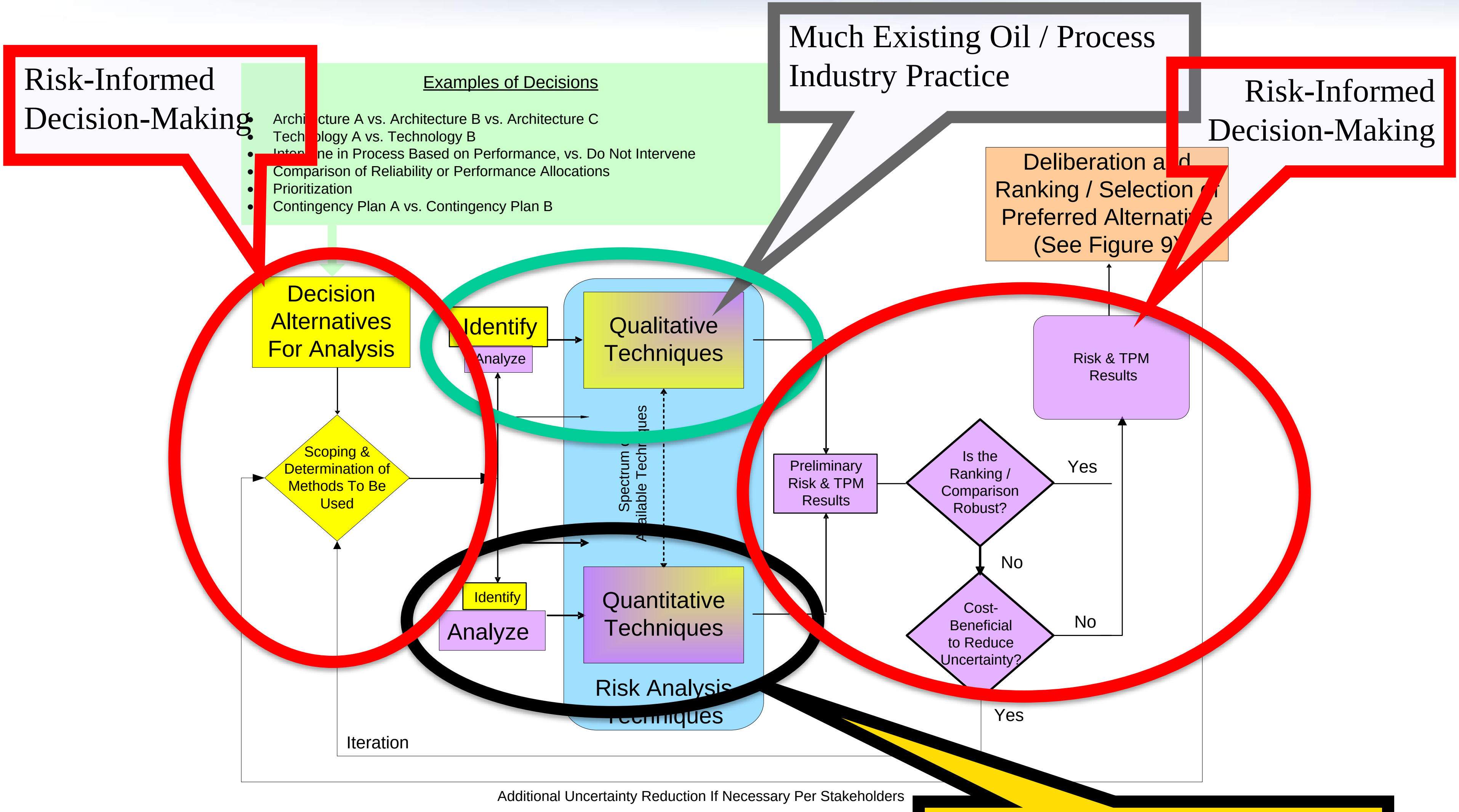
First public version of this figure was in NASA Systems Engineering Handbook


Examples of Decisions
Architecture A vs. Architecture B vs. Architecture C
Technology A vs. Technology B
Intervene in Process Based on Performance, vs. Do Not Intervene
Comparison of Reliability or Performance Allocations
Prioritization
Contingency Plan A vs. Contingency Plan B
Decision Alternatives For Analysis
Scoping & Determination of Methods To Be Used
Identify
Analyze
Qualitative Techniques
Spectrum of Available Techniques
Identify
Analyze
Quantitative Techniques
Risk Analysis Techniques
Preliminary Risk & TPM Results
Is the Ranking / Comparison Robust?
Yes
No
Cost-Beneficial to Reduce Uncertainty?
No
Yes
Risk & TPM Results
Deliberation and Ranking / Selection of Preferred Alternative (See Figure 9)
Iteration
Additional Uncertainty Reduction If Necessary Per Stakeholders

** NPR 8715.3C requires PRA in certain situations, e.g., human space flight*

Graded Approach to System Safety Analysis

Idaho National Laboratory



Risk-Informed Decision-Making

Much Existing Oil / Process Industry Practice

Risk-Informed Decision-Making

Examples of Decisions

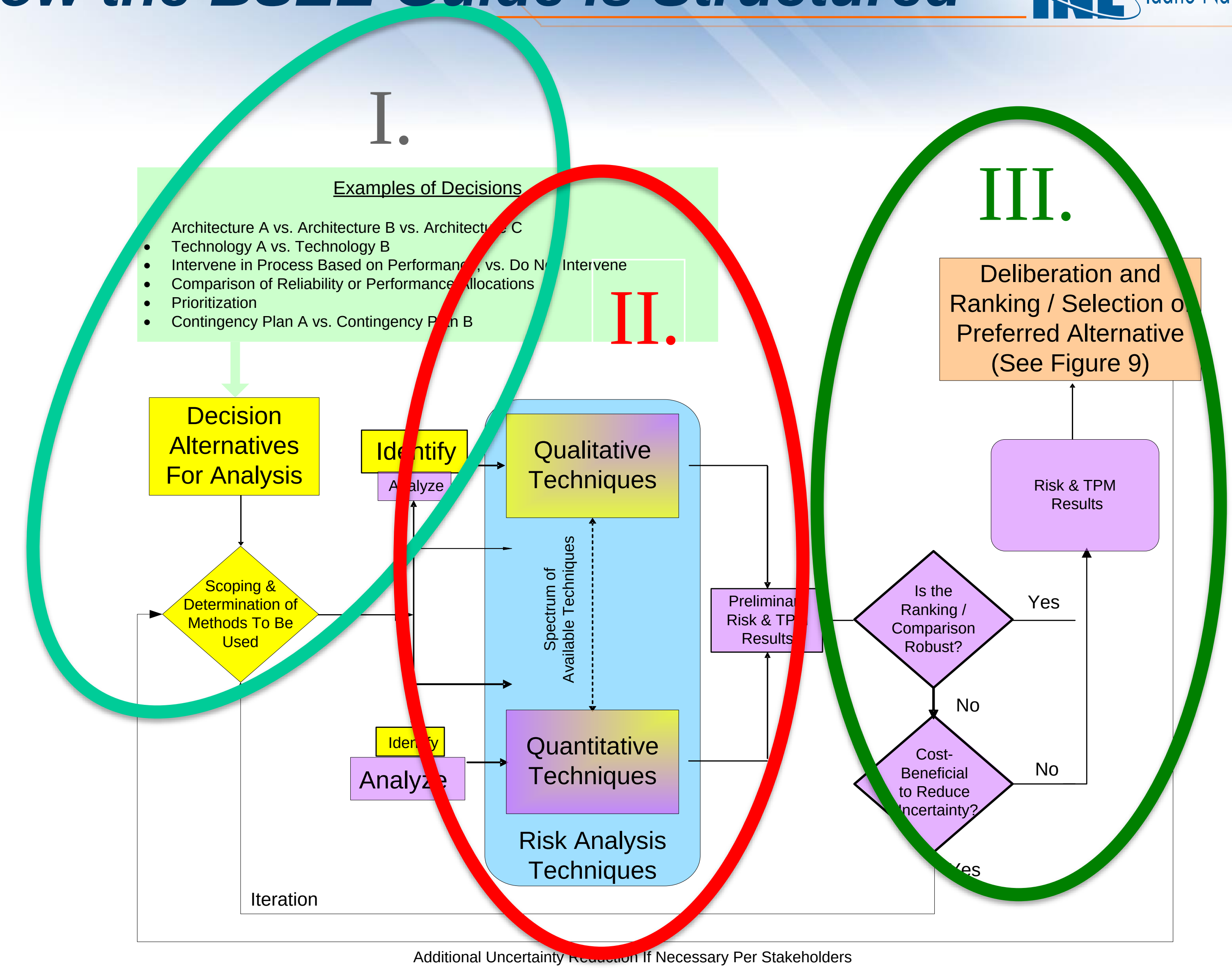
- Architecture A vs. Architecture B vs. Architecture C
- Technology A vs. Technology B
- Intervene in Process Based on Performance, vs. Do Not Intervene
- Comparison of Reliability or Performance Allocations
- Prioritization
- Contingency Plan A vs. Contingency Plan B

Decision Alternatives For Analysis
Scoping & Determination of Methods To Be Used
Identify
Analyze
Qualitative Techniques
Spectrum of Available Techniques
Identify
Analyze
Quantitative Techniques
Risk Analysis Techniques
Preliminary Risk & TPM Results
Is the Ranking / Comparison Robust?
Yes
No
Cost-Beneficial to Reduce Uncertainty?
No
Yes
Risk & TPM Results
Deliberation and Ranking / Selection of Preferred Alternative (See Figure 9)
Iteration
Additional Uncertainty Reduction If Necessary Per Stakeholders

Emphasis of both NRC and NASA PRA Procedures Guides

** NPR 8715.3C requires PRA in certain situations, e.g., human space flight*

How the BSEE Guide is Structured


I.
Examples of Decisions
Architecture A vs. Architecture B vs. Architecture C
Technology A vs. Technology B
Intervene in Process Based on Performance vs. Do Not Intervene
Comparison of Reliability or Performance Allocations
Prioritization
Contingency Plan A vs. Contingency Plan B
II.
III.
Deliberation and Ranking / Selection of Preferred Alternative (See Figure 9)
Decision Alternatives For Analysis
Identify
Analyze
Qualitative Techniques
Spectrum of Available Techniques
Quantitative Techniques
Risk Analysis Techniques
Identify
Analyze
Scoping & Determination of Methods To Be Used
Preliminary Risk & TPM Results
Risk & TPM Results
Is the Ranking / Comparison Robust?
Yes
No
Cost-Beneficial to Reduce Uncertainty?
No
Yes
Iteration
Additional Uncertainty Reduction If Necessary Per Stakeholders

** NPR 8715.3C requires PRA in certain situations, e.g., human space flight*

TABLE OF CONTENTS

BSEE PRA Guide: Table of Contents

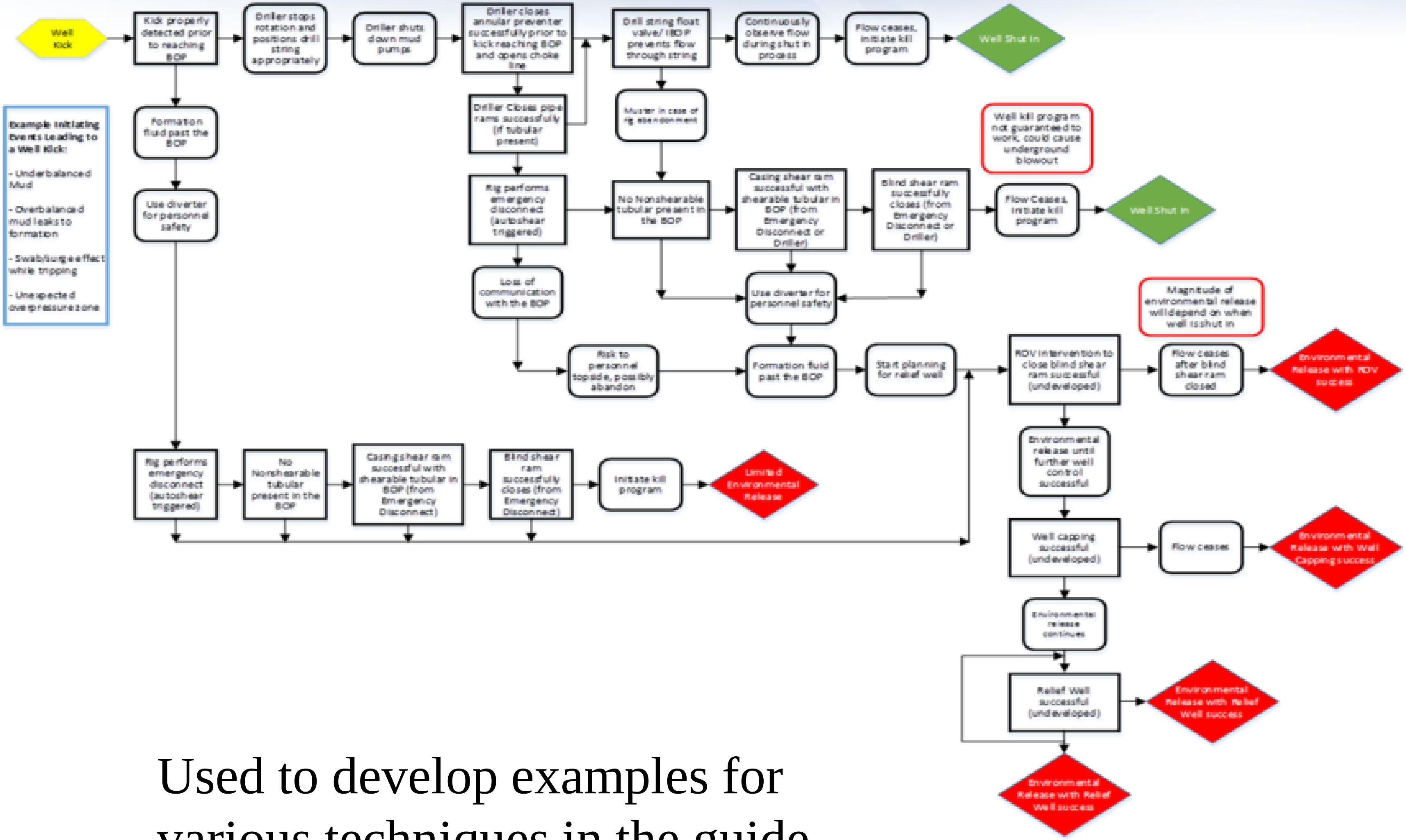
- Section 1 – Introduction
- Section 2 – Risk Analysis Techniques
- Section 3 – Results Presentation and Interpretation

- Appendix A – Example Basic Event Naming Conventions for Fault Trees
- Appendix B – Fault Tree Gate Logic and Quantification
- Appendix C – Calculating Frequency, Reliability, and Availability Metrics
- Appendix D – Common Cause (TBD)
- Appendix E – Sources of Failure Rate and Event Data

BSEE PRA Guide – Table of Contents (cont'd)

- Appendix F – Further Discussion of Bayesian Updating
- Appendix G – Population Variability Modeling (TBD)
- Appendix H – Expert Elicitation
- Appendix I – Failure Space Based Importance Measures
- Appendix J – Prevention Worth
- Appendix K – Top Event Prevention Analysis
- Appendix L – Human Reliability

Running Example in Guide



Well Kick

Kick properly detected prior to reaching BOP

Driller stops rotation and positions drill string appropriately

Driller shuts down mud pumps

Driller closes annular preventer successfully prior to kick reaching BOP and opens choke line

Drill string float valve/ IBOP prevents flow through string

Continuously observe flow during shut in process

Flow ceases, initiate kill program

Well Shut In

Example Initiating Events Leading to a Well Kick:

- Underbalanced Mud
- Overbalanced mud leaks to formation
- Swab/surge effect while tripping
- Unexpected overpressure zone

Formation fluid past the BOP

Use diverter for personnel safety

Driller Closes pipe rams successfully (if tubular present)

Muster in case of rig abandonment

Well kill program not guaranteed to work, could cause underground blowout

Rig performs emergency disconnect (autoshear triggered)

No Nonshearable tubular present in the BOP

Casing shear ram successful with shearable tubular in BOP (from Emergency Disconnect or Driller)

Blind shear ram successfully closes (from Emergency Disconnect or Driller)

Flow Ceases, Initiate kill program

Well Shut In

Loss of communication with the BOP

Use diverter for personnel safety

Magnitude of environmental release will depend on when well is shut in

Risk to personnel topside, possibly abandon

Formation fluid past the BOP

Start planning for relief well

ROV Intervention to close blind shear ram successful (undeveloped)

Flow ceases after blind shear ram closed

Environmental Release with ROV success

Environmental release until further well control successful

Rig performs emergency disconnect (autoshear triggered)

No Nonshearable tubular present in the BOP

Casing shear ram successful with shearable tubular in BOP (from Emergency Disconnect)

Blind shear ram successfully closes (from Emergency Disconnect)

Initiate kill program

Limited Environmental Release

Well capping successful (undeveloped)

Flow ceases

Environmental Release with Well Capping success

Environmental release continues

Relief Well successful (undeveloped)

Environmental Release with Relief Well success

Environmental Release with Relief Well success

Used to develop examples for various techniques in the guide

FIGURES AND TABLES FROM THE GUIDE

Following slides are taken from the guide itself

They are shown here as representative of the style and content of the guide’s coverage

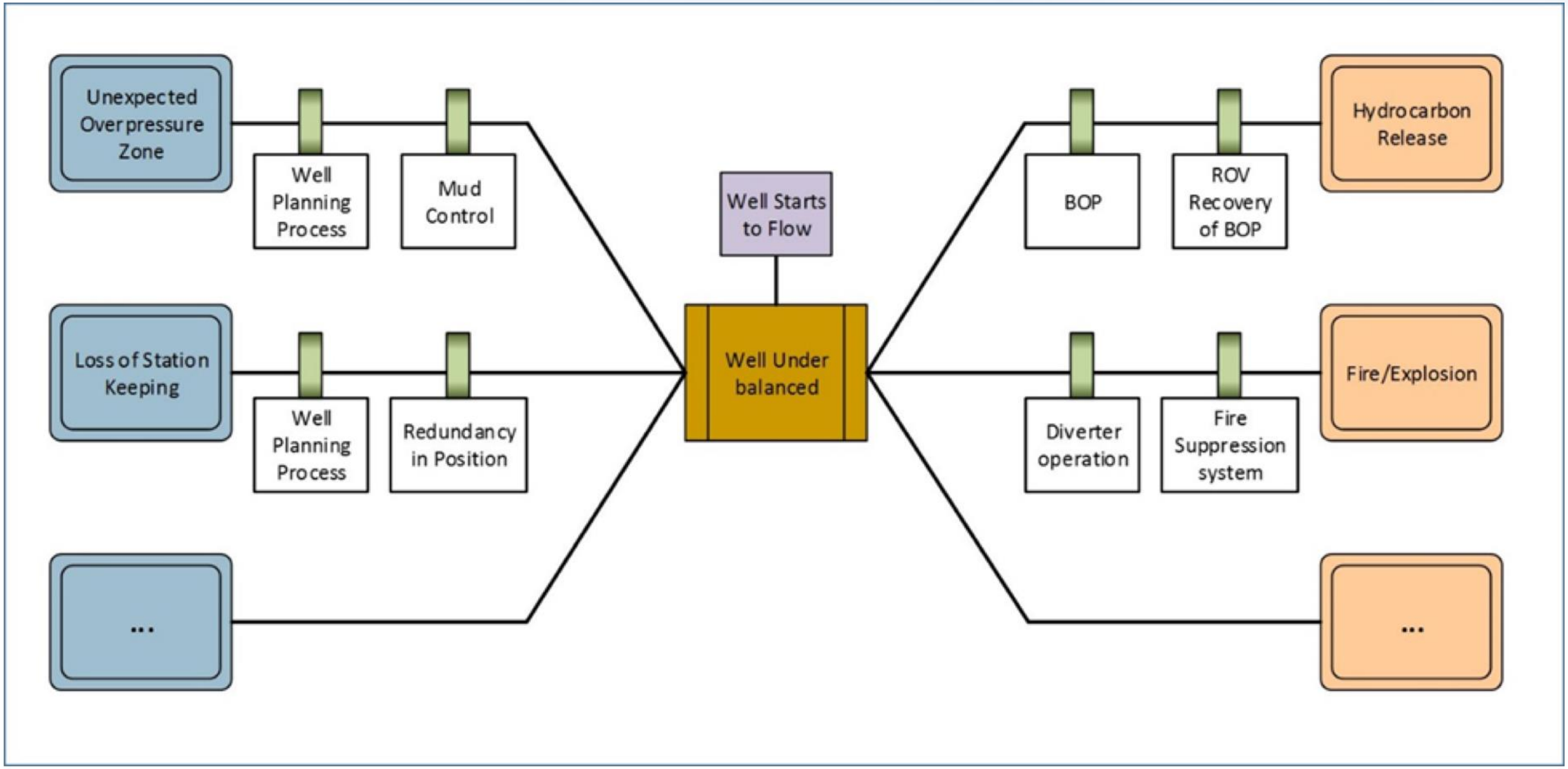
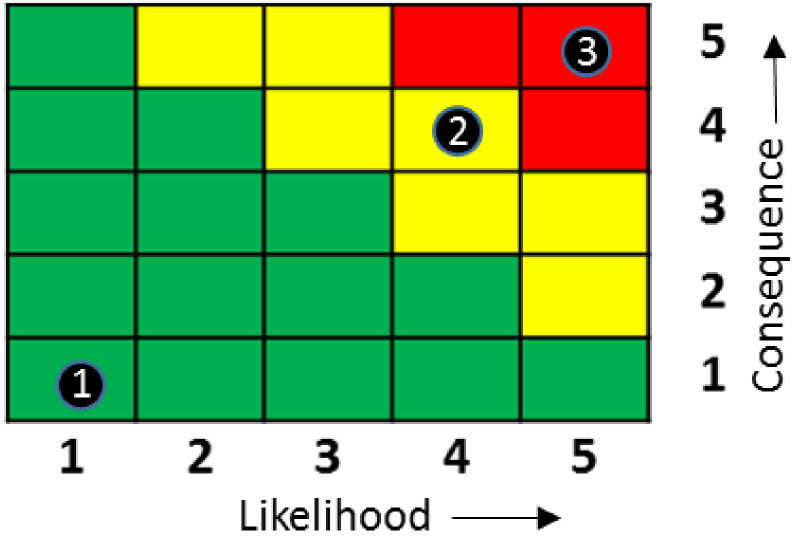
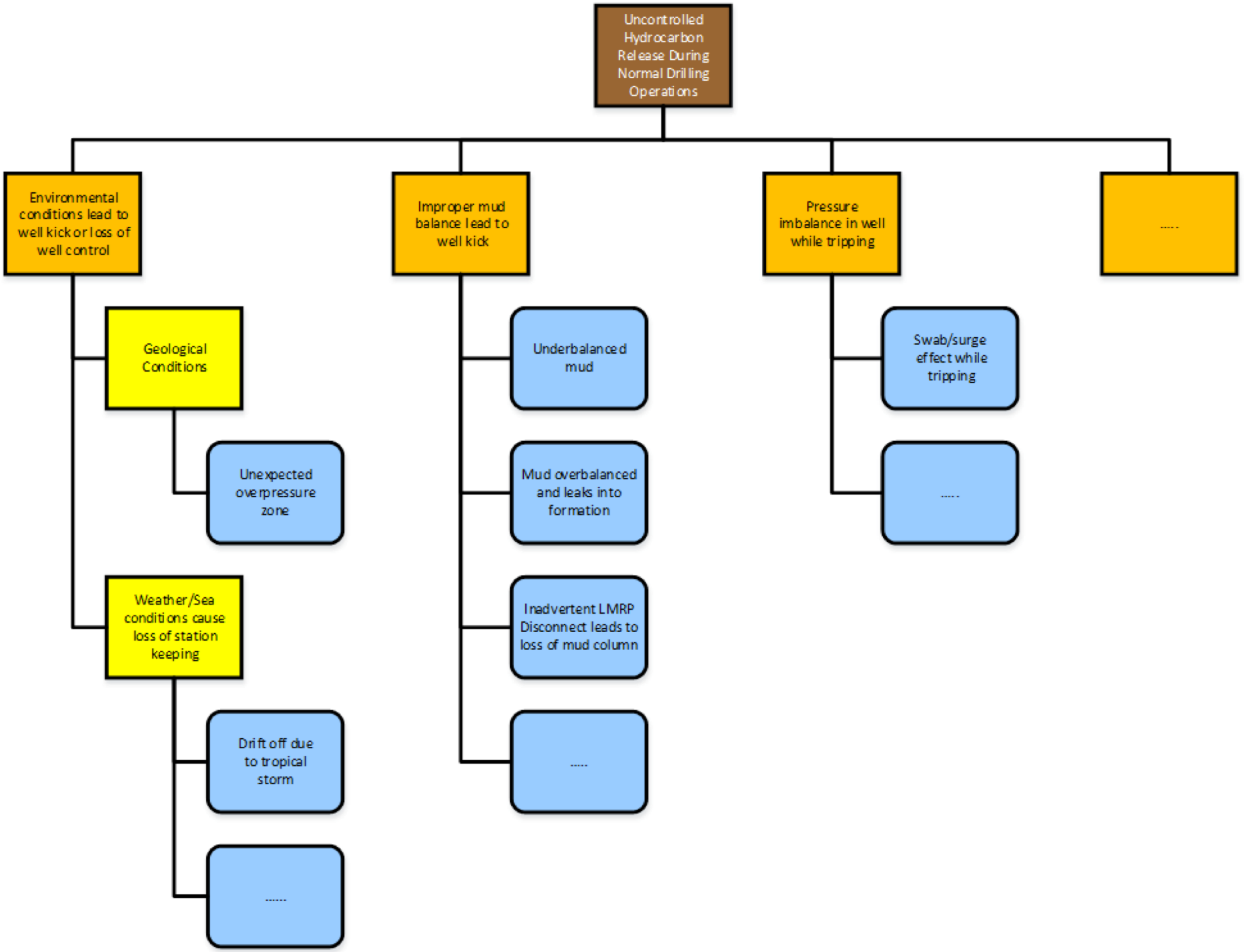


Figure 2- 1. Example of Bowtie Analysis Diagram



Consequence	1	2	3	4	5
5	🟩	🟨	🟨	🟥	🟥 ③
4	🟩	🟩	🟨	🟨 ②	🟥
3	🟩	🟩	🟩	🟨	🟨
2	🟩	🟩	🟩	🟩	🟨
1	🟩 ①	🟩	🟩	🟩	🟩

Figure 2-1. Typical Qualitative Risk Matrix



Uncontrolled Hydrocarbon Release During Normal Drilling Operations

Environmental conditions lead to well kick or loss of well control

Geological Conditions

Unexpected overpressure zone

Weather/Sea conditions cause loss of station keeping

Drift off due to tropical storm

......

Improper mud balance lead to well kick

Underbalanced mud

Mud overbalanced and leaks into formation

Inadvertent LMRP Disconnect leads to loss of mud column

.....

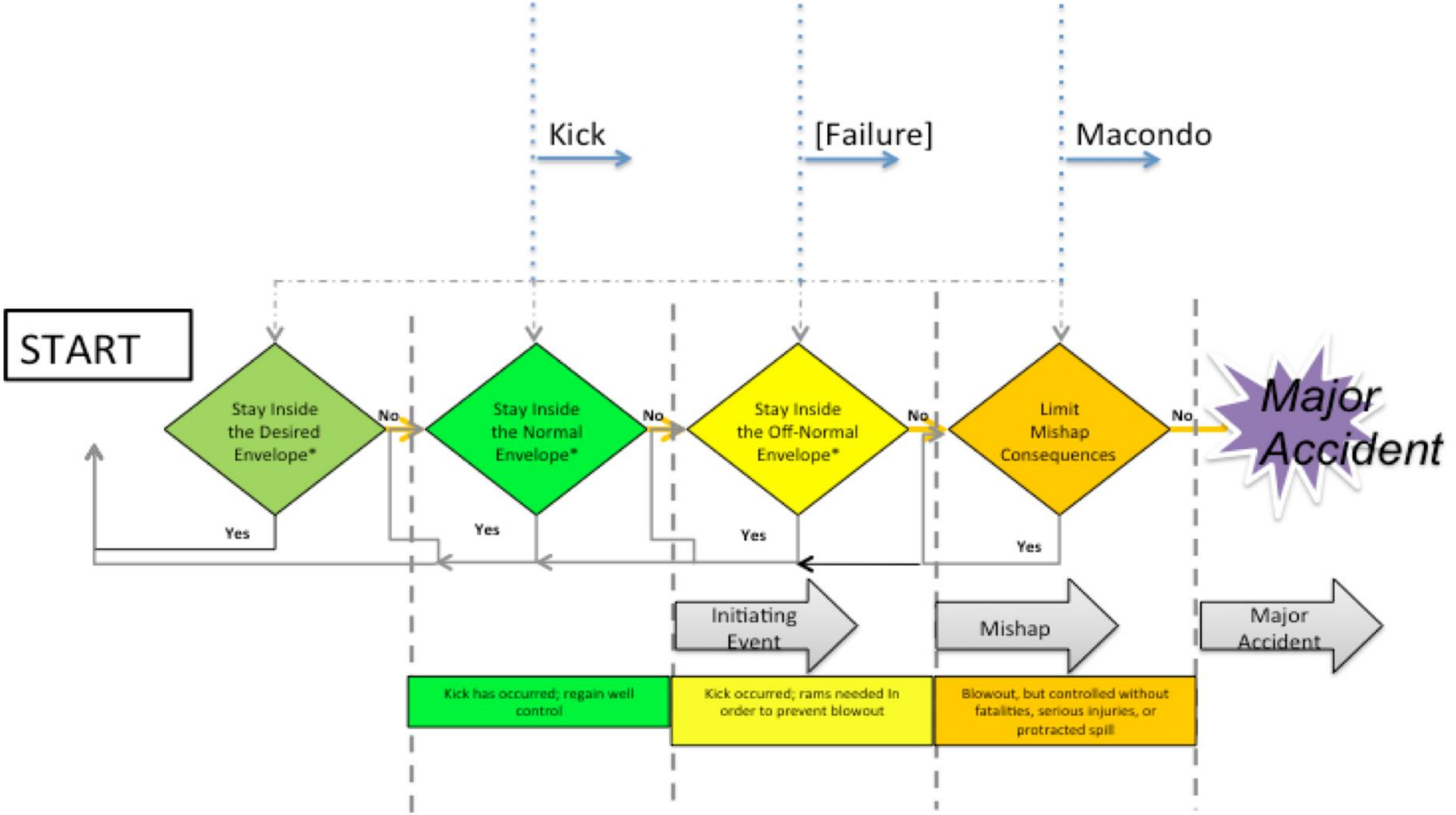
Pressure imbalance in well while tripping

Swab/surge effect while tripping

.....

.....

Figure 2-1. Notional Master Logic Diagram Related to Candidate Initiating Events

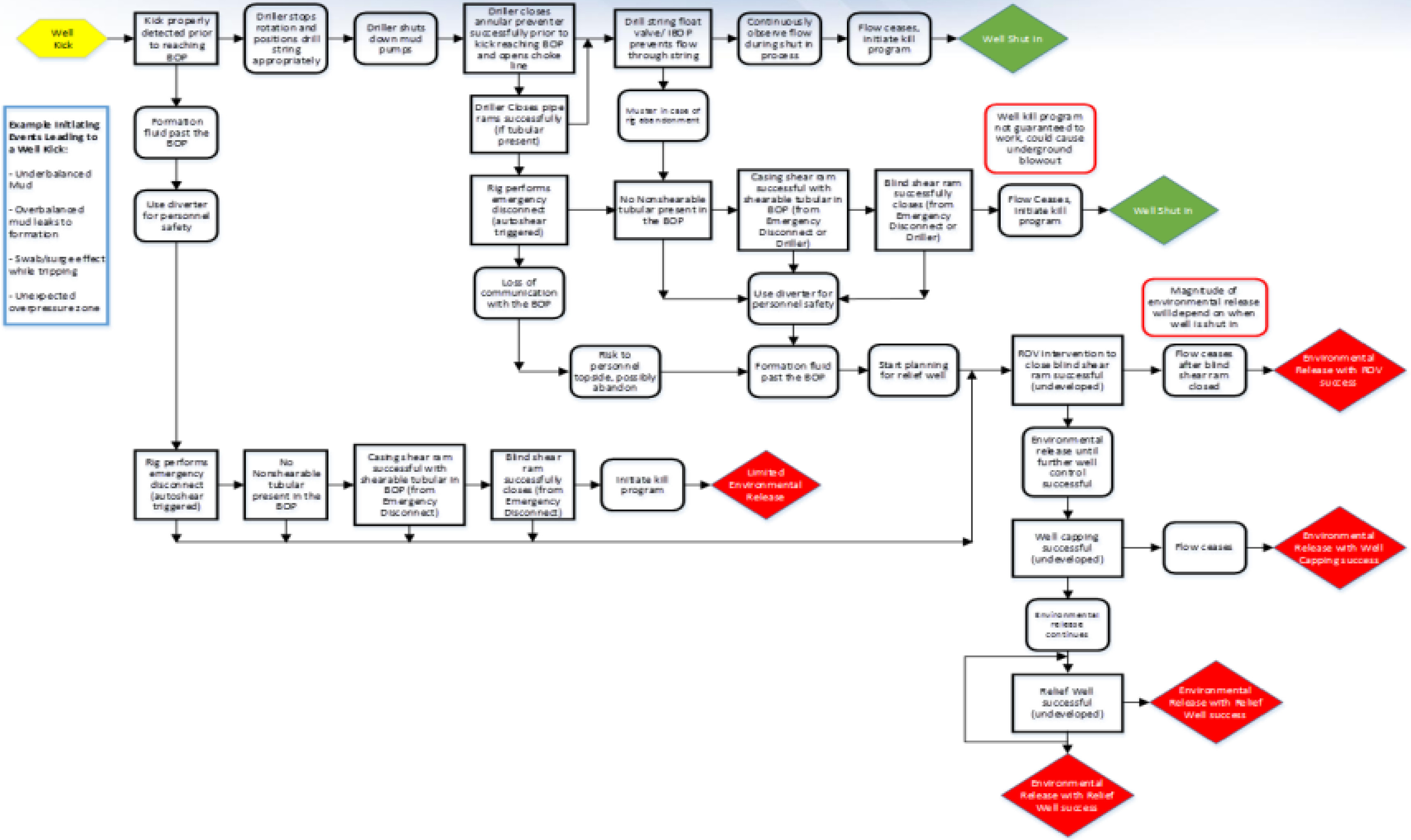

Kick
[Failure]
Macondo
START
Stay Inside the Desired Envelope*
No
Yes
Stay Inside the Normal Envelope*
No
Yes
Stay Inside the Off-Normal Envelope*
No
Yes
Limit Mishap Consequences
No
Yes
Major Accident
Initiating Event
Mishap
Major Accident

Kick has occurred; regain well control

Kick occurred; rams needed in order to prevent blowout

Blowout, but controlled without fatalities, serious injuries, or protracted spill

Figure 2-1. The Elements of an Accident Scenario



Well Kick

Kick properly detected prior to reaching BOP

Driller stops rotation and positions drill string appropriately

Driller shuts down mud pumps

Driller closes annular preventer successfully prior to kick reaching BOP and opens choke line

Drill string float valve/ IBOP prevents flow through string

Continuously observe flow during shut in process

Flow ceases, initiate kill program

Well Shut In

Example Initiating Events Leading to a Well Kick:

- Underbalanced Mud

- Overbalanced mud leaks to formation

- Swab/surge effect while tripping

- Unexpected overpressure zone

Formation fluid past the BOP

Use diverter for personnel safety

Driller Closes pipe rams successfully (if tubular present)

Muster in case of rig abandonment

Well kill program not guaranteed to work, could cause underground blowout

Rig performs emergency disconnect (autoshear triggered)

No Nonshearable tubular present in the BOP

Casing shear ram successful with shearable tubular in BOP (from Emergency Disconnect or Driller)

Blind shear ram successfully closes (from Emergency Disconnect or Driller)

Flow Ceases, initiate kill program

Well Shut In

Loss of communication with the BOP

Use diverter for personnel safety

Magnitude of environmental release will depend on when well is shut in

Risk to personnel topside, possibly abandon

Formation fluid past the BOP

Start planning for relief well

ROV intervention to close blind shear ram successful (undeveloped)

Flow ceases after blind shear ram closed

Environmental Release with ROV success

Environmental release until further well control successful

Rig performs emergency disconnect (autoshear triggered)

No Nonshearable tubular present in the BOP

Casing shear ram successful with shearable tubular in BOP (from Emergency Disconnect)

Blind shear ram successfully closes (from Emergency Disconnect)

Initiate kill program

Limited Environmental Release

Well capping successful (undeveloped)

Flow ceases

Environmental Release with Well Capping success

Environmental release continues

Relief Well successful (undeveloped)

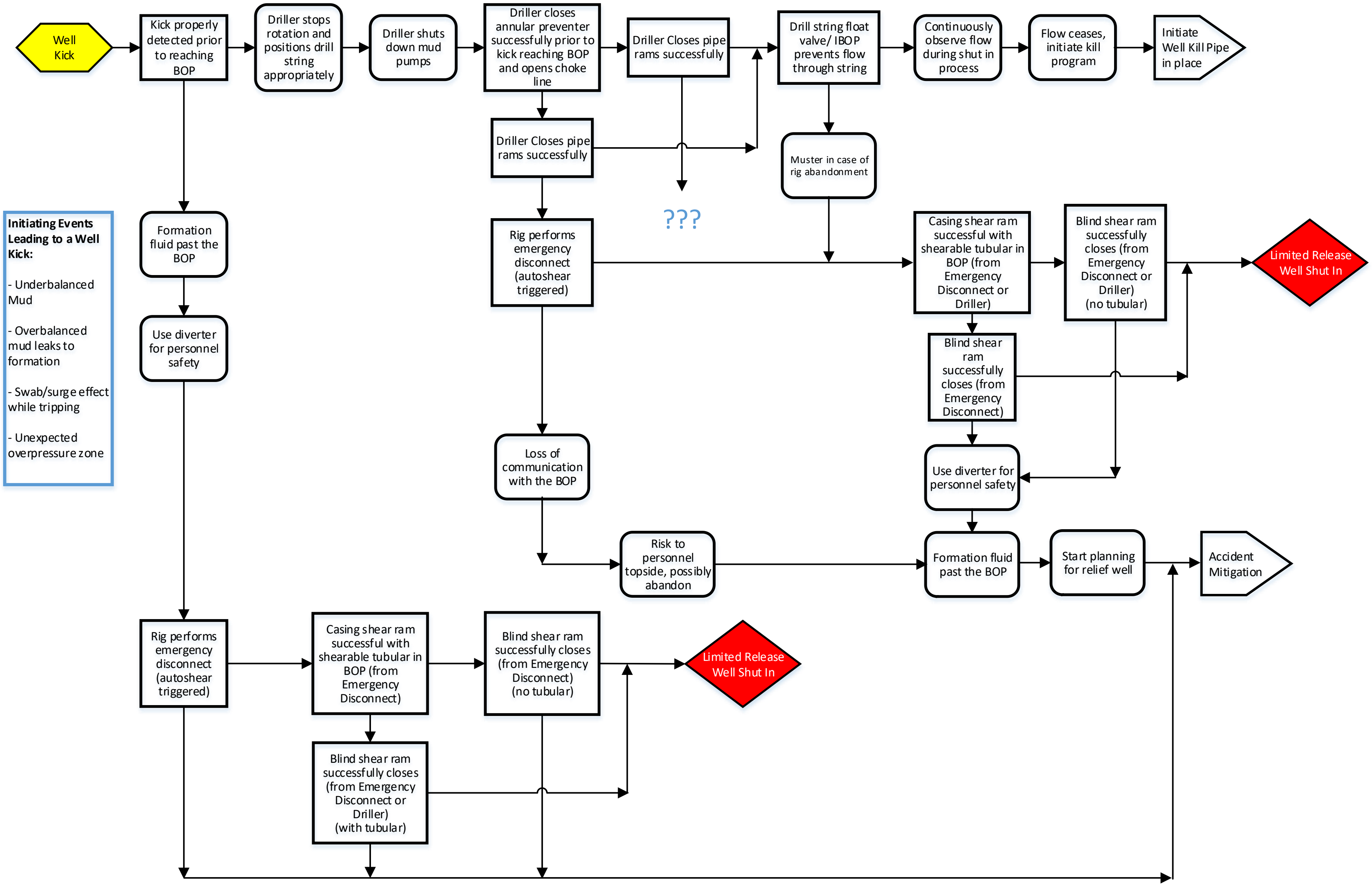
Environmental Release with Relief Well success

Environmental Release with Relief Well success

Figure 2- 6. Event Sequence Diagram for a Well Kick from an Unexpected Overpressure Zone

VISIO_Jan_30
Page 1

Event sequence diagram for environmental release in response to a kick – Dynamically Positioned Floater, Drilling HPHT Well, Drilling



Well Kick

Kick properly detected prior to reaching BOP

Driller stops rotation and positions drill string appropriately

Driller shuts down mud pumps

Driller closes annular preventer successfully prior to kick reaching BOP and opens choke line

Driller Closes pipe rams successfully

Drill string float valve/ IBOP prevents flow through string

Continuously observe flow during shut in process

Flow ceases, initiate kill program

Initiate Well Kill Pipe in place

Driller Closes pipe rams successfully

???

Muster in case of rig abandonment

Initiating Events Leading to a Well Kick:

- Underbalanced Mud

- Overbalanced mud leaks to formation

- Swab/surge effect while tripping

- Unexpected overpressure zone

Formation fluid past the BOP

Use diverter for personnel safety

Rig performs emergency disconnect (autoshear triggered)

Casing shear ram successful with shearable tubular in BOP (from Emergency Disconnect or Driller)

Blind shear ram successfully closes (from Emergency Disconnect or Driller) (no tubular)

Limited Release Well Shut In

Blind shear ram successfully closes (from Emergency Disconnect)

Use diverter for personnel safety

Loss of communication with the BOP

Risk to personnel topside, possibly abandon

Formation fluid past the BOP

Start planning for relief well

Accident Mitigation

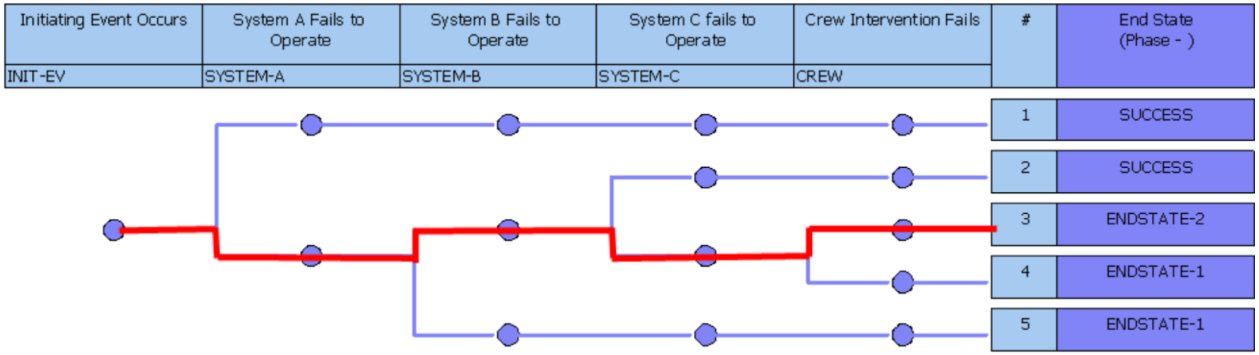
Rig performs emergency disconnect (autoshear triggered)

Casing shear ram successful with shearable tubular in BOP (from Emergency Disconnect)

Blind shear ram successfully closes (from Emergency Disconnect) (no tubular)

Limited Release Well Shut In

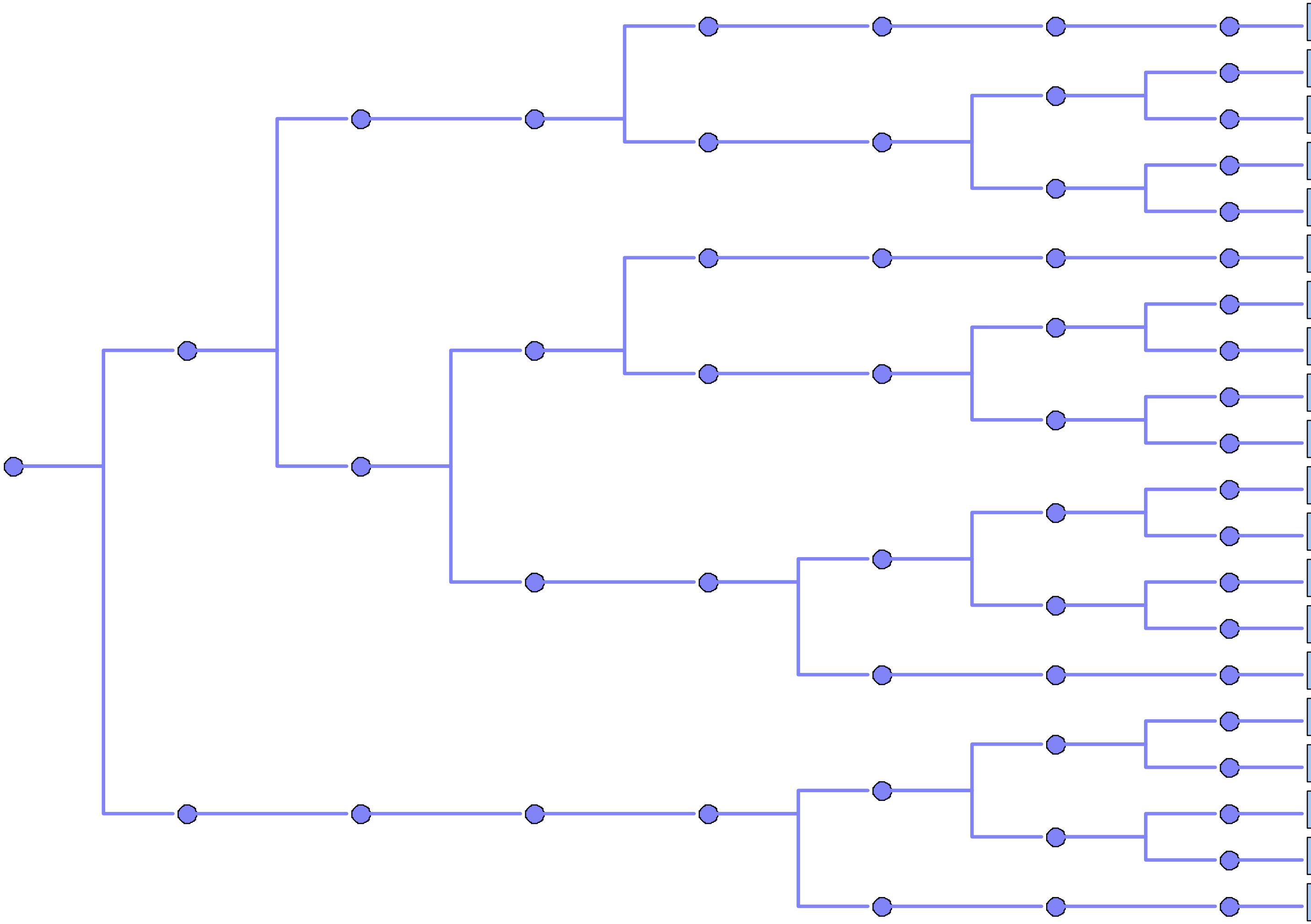
Blind shear ram successfully closes (from Emergency Disconnect or Driller) (with tubular)



Initiating Event Occurs	System A Fails to Operate	System B Fails to Operate	System C fails to Operate	Crew Intervention Fails	#	End State (Phase -)
INIT-EV	SYSTEM-A	SYSTEM-B	SYSTEM-C	CREW		

#	End State (Phase -)
1	SUCCESS
2	SUCCESS
3	ENDSTATE-2
4	ENDSTATE-1
5	ENDSTATE-1

Figure 2- 1. Example Event Tree Sequence



Well Kick While Drilling	Kick not properly detected prior to reaching BOP	Annular preventer fails to close prior to the kick reaching the BOP or pressure beyond design of annular	Driller fails to close pipe rams successfully	Drill string float valve / IBOP fails to prevent flow through string	Rig fails to perform Emergency Disconnect	Casing shear ram does not successfully operate	Blind shear ram does not successfully close	#	End State (Phase -)
DRILLINGKICK	KICKDETECT	ANNULAR	PIPERAM	IBOPFLTVLV	EMERGDISCONN	CASINGSHEAR2	BLINDSHEAR		
								1	WELLSHUTIN
								2	WELLSHUTIN
								3	WELLINTERVENTION
								4	WELLSHUTIN
								5	WELLINTERVENTION
								6	WELLSHUTIN
								7	WELLSHUTIN
								8	WELLINTERVENTION
								9	WELLSHUTIN
								10	WELLINTERVENTION
								11	WELLSHUTIN
								12	WELLINTERVENTION
								13	WELLSHUTIN
								14	WELLINTERVENTION
								15	WELLINTERVENTION
								16	LIMITEDRELEASE
								17	WELLINTERVENTION
								18	LIMITEDRELEASE
								19	WELLINTERVENTION
								20	WELLINTERVENTION

Figure 2-13. Event Tree Structure for Well Kick from an Unexpected Overpressure Zone

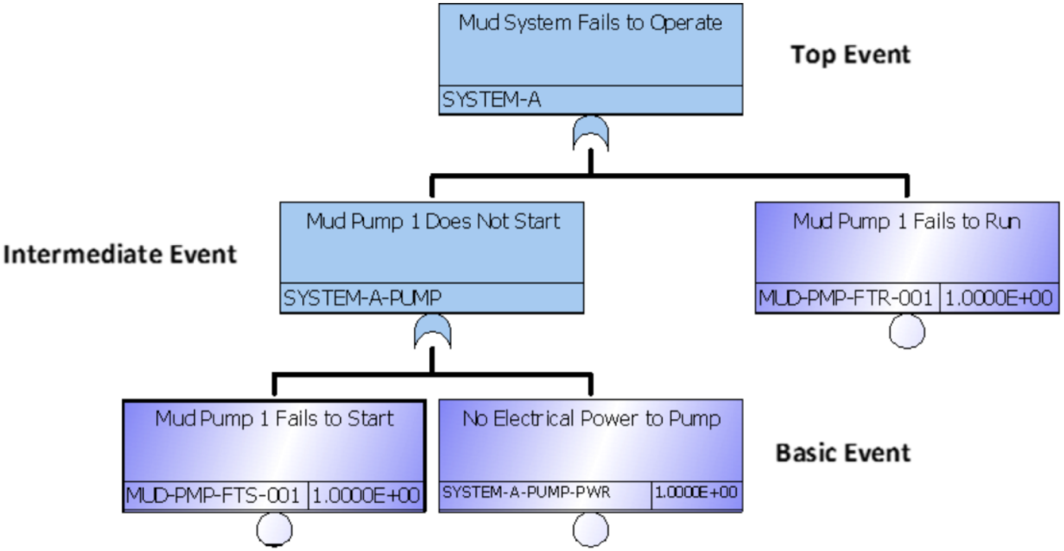


Figure 2- 1. Typical Fault Tree Structure and Symbols

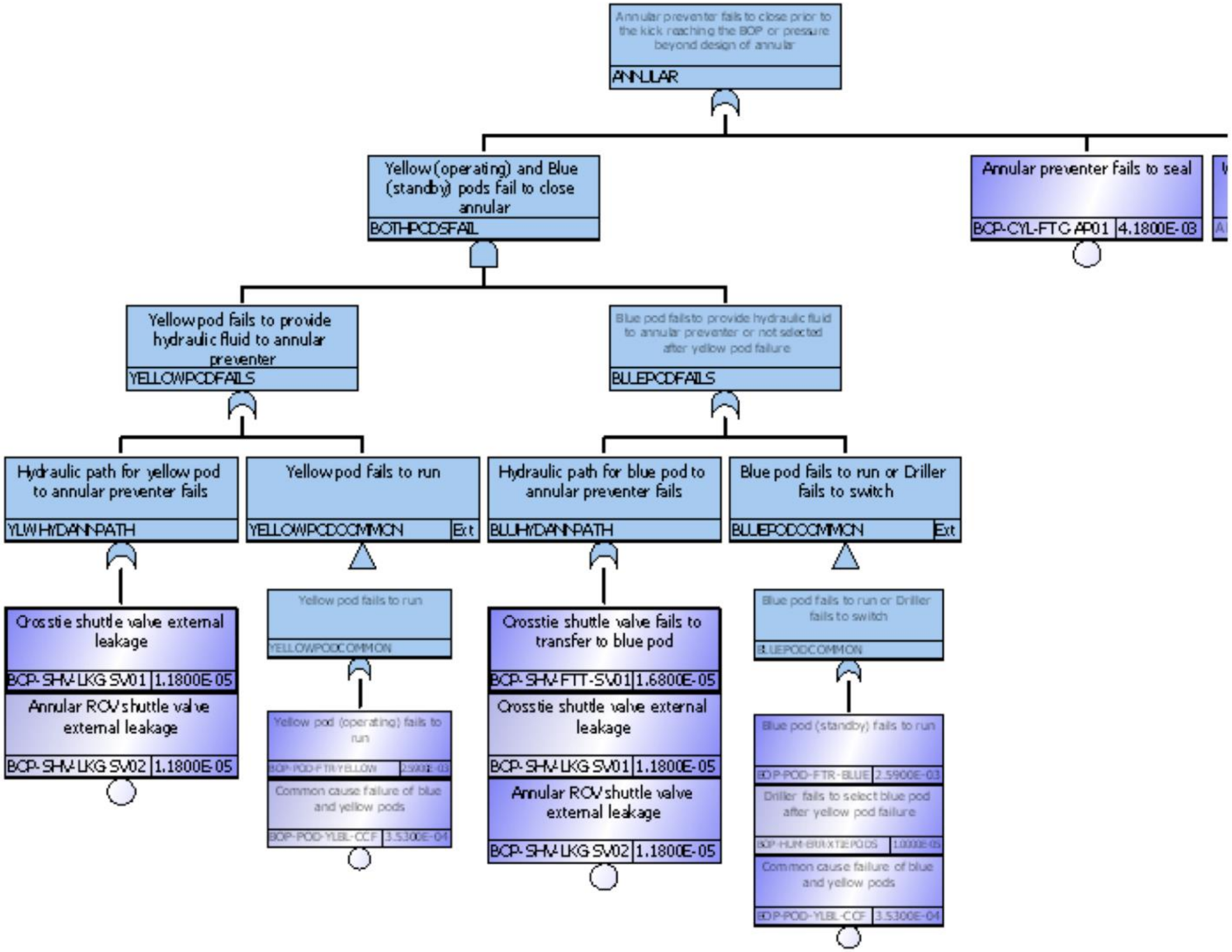
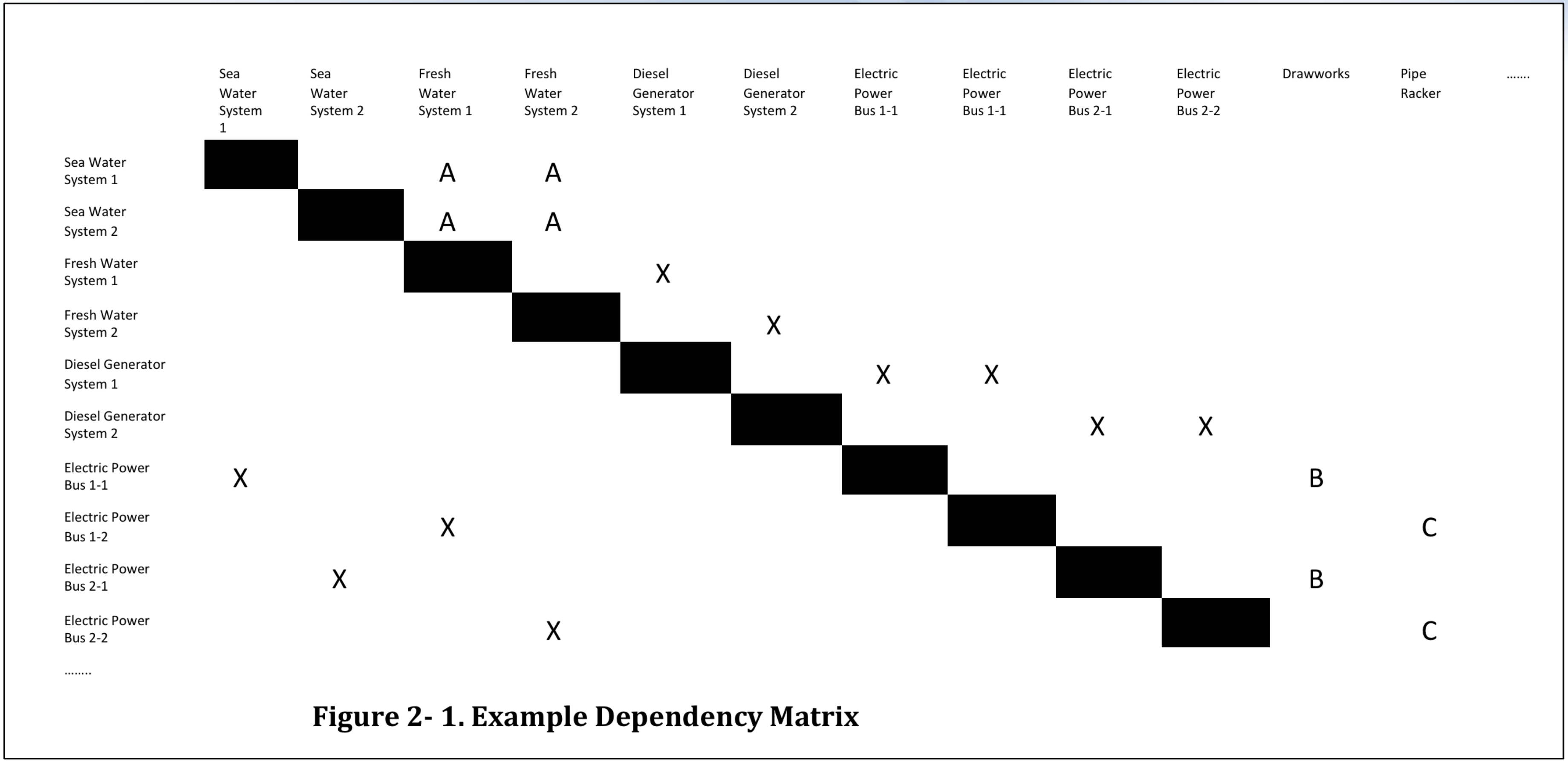

Annular preventer fails to close prior to the kick reaching the BOP or pressure beyond design of annular
ANNULAR
Yellow (operating) and Blue (standby) pods fail to close annular
BOTHPODSFAIL
Annular preventer fails to seal
BOP-CYL-FTC-AP01
4.1800E-03
Yellow pod fails to provide hydraulic fluid to annular preventer
YELLOWPODFAILS
Blue pod fails to provide hydraulic fluid to annular preventer or not selected after yellow pod failure
BLUEPODFAILS
Hydraulic path for yellow pod to annular preventer fails
YLWHYDANNPATH
Yellow pod fails to run
YELLOWPODCOMMON
Ext
Hydraulic path for blue pod to annular preventer fails
BLUHYDANNPATH
Blue pod fails to run or Driller fails to switch
BLUEPODCOMMON
Ext
Crosstie shuttle valve external leakage
BOP-SHV-LKG-SV01
1.1800E-05
Annular ROV shuttle valve external leakage
BOP-SHV-LKG-SV02
1.1800E-05
Yellow pod fails to run
YELLOWPODCOMMON
Yellow pod (operating) fails to run
BOP-POD-FTR-YELLOW
2.5900E-03
Common cause failure of blue and yellow pods
BOP-POD-YLBL-CCF
3.5300E-04
Crosstie shuttle valve fails to transfer to blue pod
BOP-SHV-FTT-SV01
1.6800E-05
Crosstie shuttle valve external leakage
BOP-SHV-LKG-SV01
1.1800E-05
Annular ROV shuttle valve external leakage
BOP-SHV-LKG-SV02
1.1800E-05
Blue pod fails to run or Driller fails to switch
BLUEPODCOMMON
Blue pod (standby) fails to run
BOP-POD-FTR-BLUE
2.5900E-03
Driller fails to select blue pod after yellow pod failure
BOP-HUM-BLUXTIEPODS
1.0000E-05
Common cause failure of blue and yellow pods
BOP-POD-YLBL-CCF
3.5300E-04

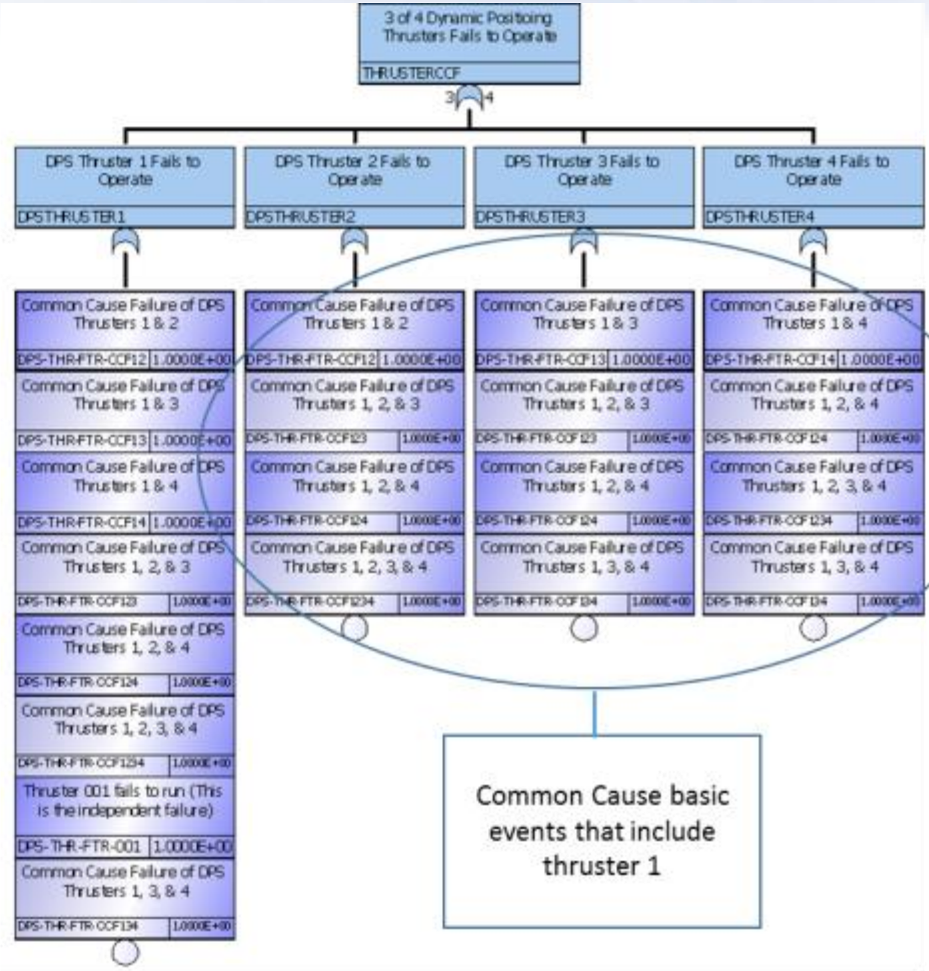
Figure 2- 1. Basic Fault Tree



	Sea Water System 1	Sea Water System 2	Fresh Water System 1	Fresh Water System 2	Diesel Generator System 1	Diesel Generator System 2	Electric Power Bus 1-1	Electric Power Bus 1-1	Electric Power Bus 2-1	Electric Power Bus 2-2	Drawworks	Pipe Racker	....
Sea Water System 1	■		A	A									
Sea Water System 2		■	A	A									
Fresh Water System 1			■		X								
Fresh Water System 2				■		X							
Diesel Generator System 1					■		X	X					
Diesel Generator System 2						■			X	X			
Electric Power Bus 1-1	X						■				B		
Electric Power Bus 1-2			X					■				C	
Electric Power Bus 2-1		X							■		B		
Electric Power Bus 2-2				X						■		C	
....													

Figure 2- 1. Example Dependency Matrix

Frequently, you can understand a lot of what a logic model is saying from a diagram like this


3 of 4 Dynamic Positioning Thrusters Fails to Operate
THRUSTERCCF
3
4
DPS Thruster 1 Fails to Operate
DPSTHRUSTER1
DPS Thruster 2 Fails to Operate
DPSTHRUSTER2
DPS Thruster 3 Fails to Operate
DPSTHRUSTER3
DPS Thruster 4 Fails to Operate
DPSTHRUSTER4
Common Cause Failure of DPS Thrusters 1 & 2
DPS-THR-FTR-CCF12
1.0000E+00
Common Cause Failure of DPS Thrusters 1 & 3
DPS-THR-FTR-CCF13
1.0000E+00
Common Cause Failure of DPS Thrusters 1 & 4
DPS-THR-FTR-CCF14
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 2, & 3
DPS-THR-FTR-CCF123
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 2, & 4
DPS-THR-FTR-CCF124
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 2, 3, & 4
DPS-THR-FTR-CCF1234
1.0000E+00
Thruster 001 fails to run (This is the independent failure)
DPS-THR-FTR-001
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 3, & 4
DPS-THR-FTR-CCF134
1.0000E+00
Common Cause Failure of DPS Thrusters 1 & 2
DPS-THR-FTR-CCF12
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 2, & 3
DPS-THR-FTR-CCF123
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 2, & 4
DPS-THR-FTR-CCF124
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 2, 3, & 4
DPS-THR-FTR-CCF1234
1.0000E+00
Common Cause Failure of DPS Thrusters 1 & 3
DPS-THR-FTR-CCF13
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 2, & 3
DPS-THR-FTR-CCF123
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 2, & 4
DPS-THR-FTR-CCF124
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 3, & 4
DPS-THR-FTR-CCF134
1.0000E+00
Common Cause Failure of DPS Thrusters 1 & 4
DPS-THR-FTR-CCF14
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 2, & 4
DPS-THR-FTR-CCF124
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 2, 3, & 4
DPS-THR-FTR-CCF1234
1.0000E+00
Common Cause Failure of DPS Thrusters 1, 3, & 4
DPS-THR-FTR-CCF134
1.0000E+00

Common Cause basic events that include thruster 1

Figure 2- 27. Common Cause Modeling for a 3 of 4 System

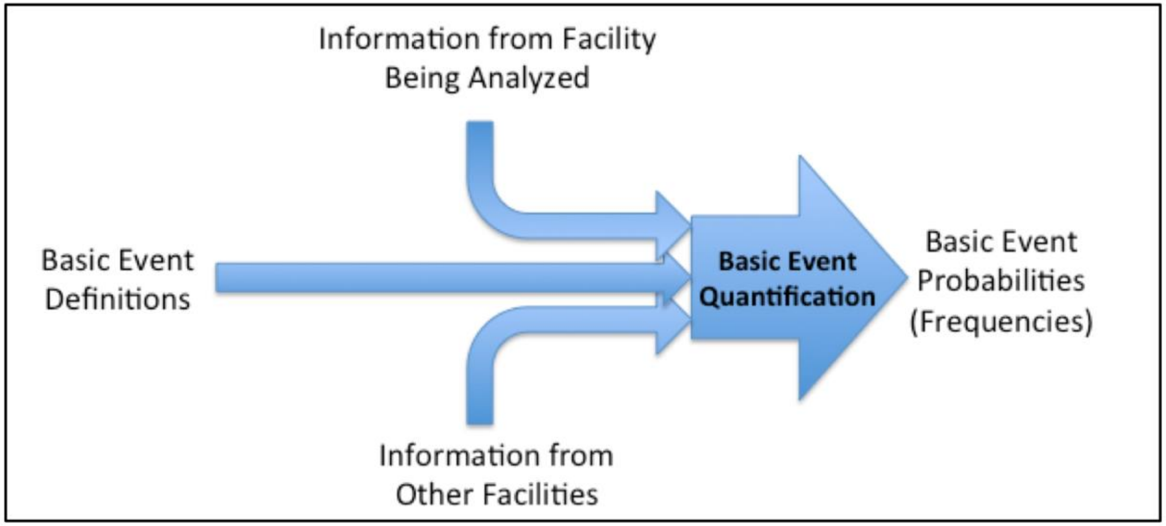


Figure 2- 1. Sources of Information for Quantification of Basic Event Likelihood

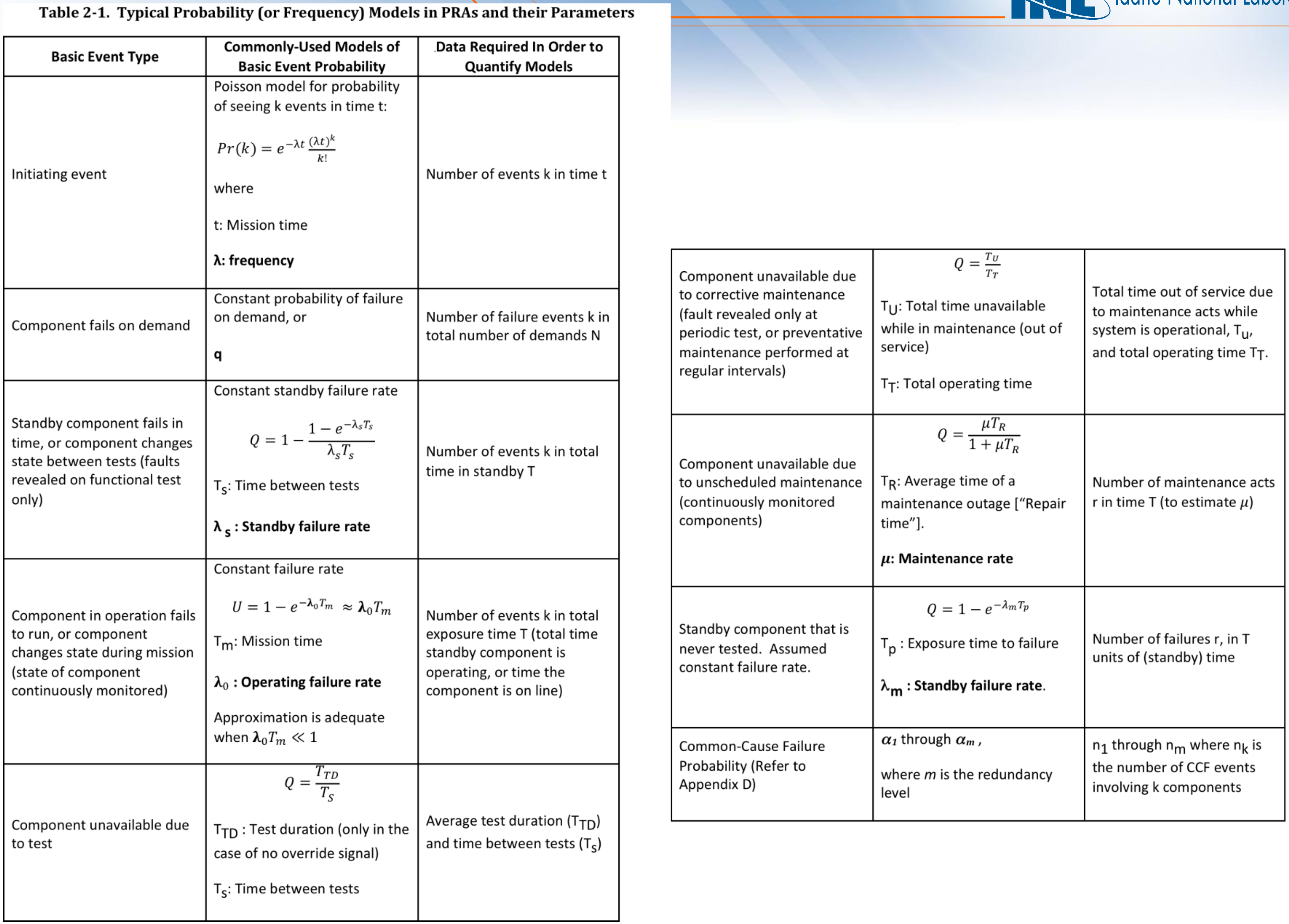


Table 2-1. Typical Probability (or Frequency) Models in PRAs and their Parameters

Basic Event Type	Commonly-Used Models of Basic Event Probability	Data Required In Order to Quantify Models
Initiating event	Poisson model for probability of seeing k events in time t: $Pr(k) = e^{-\lambda t}\frac{(\lambda t)^k}{k!}$ where t: Mission time **λ: frequency**	Number of events k in time t
Component fails on demand	Constant probability of failure on demand, or **q**	Number of failure events k in total number of demands N
Standby component fails in time, or component changes state between tests (faults revealed on functional test only)	Constant standby failure rate $Q = 1 - \frac{1 - e^{-\lambda_s T_s}}{\lambda_s T_s}$ T_S: Time between tests **λ_s : Standby failure rate**	Number of events k in total time in standby T
Component in operation fails to run, or component changes state during mission (state of component continuously monitored)	Constant failure rate $U = 1 - e^{-\boldsymbol{\lambda}_0 T_m} \approx \boldsymbol{\lambda}_0 T_m$ T_m: Mission time **λ_0 : Operating failure rate** Approximation is adequate when $\boldsymbol{\lambda}_0 T_m \ll 1$	Number of events k in total exposure time T (total time standby component is operating, or time the component is on line)
Component unavailable due to test	$Q = \frac{T_{TD}}{T_s}$ T_{TD} : Test duration (only in the case of no override signal) T_S: Time between tests	Average test duration (T_{TD}) and time between tests (T_s)
Component unavailable due to corrective maintenance (fault revealed only at periodic test, or preventative maintenance performed at regular intervals)	$Q = \frac{T_U}{T_T}$ T_U: Total time unavailable while in maintenance (out of service) T_T: Total operating time	Total time out of service due to maintenance acts while system is operational, T_u, and total operating time T_T.
Component unavailable due to unscheduled maintenance (continuously monitored components)	$Q = \frac{\mu T_R}{1 + \mu T_R}$ T_R: Average time of a maintenance outage ["Repair time"]. **μ: Maintenance rate**	Number of maintenance acts r in time T (to estimate μ)
Standby component that is never tested. Assumed constant failure rate.	$Q = 1 - e^{-\lambda_m T_p}$ T_p : Exposure time to failure **λ_m : Standby failure rate.**	Number of failures r, in T units of (standby) time
Common-Cause Failure Probability (Refer to Appendix D)	α_1 through α_m , where *m* is the redundancy level	n_1 through n_m where n_k is the number of CCF events involving k components

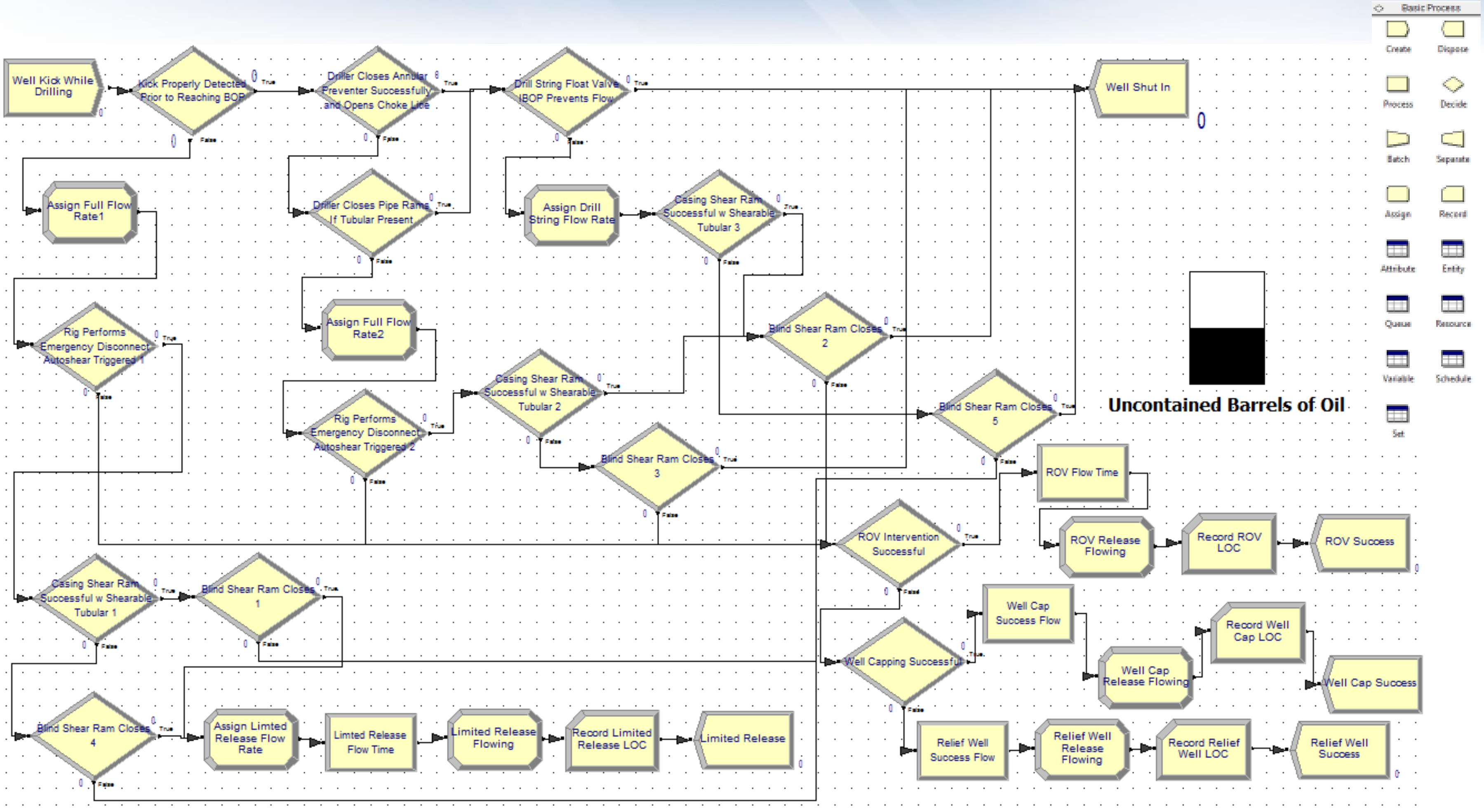
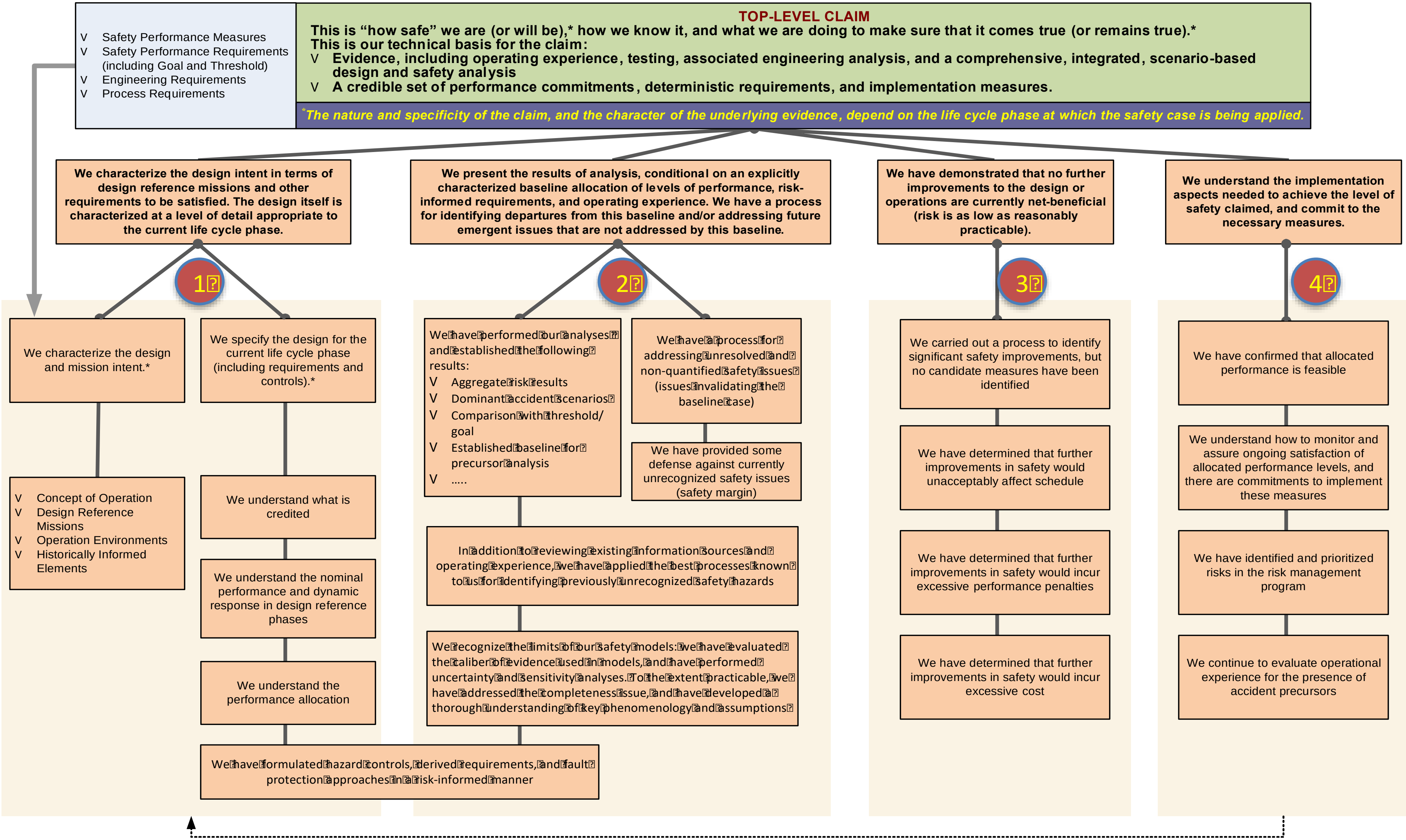

Well Kick While Drilling
Kick Properly Detected Prior to Reaching BOP
Driller Closes Annular Preventer Successfully and Opens Choke Line
Drill String Float Valve IBOP Prevents Flow
Well Shut In
0
Assign Full Flow Rate1
Driller Closes Pipe Rams If Tubular Present
Assign Drill String Flow Rate
Casing Shear Ram Successful w Shearable Tubular 3
Assign Full Flow Rate2
Blind Shear Ram Closes 2
Rig Performs Emergency Disconnect Autoshear Triggered 1
Casing Shear Ram Successful w Shearable Tubular 2
Rig Performs Emergency Disconnect Autoshear Triggered 2
Blind Shear Ram Closes 5
Uncontained Barrels of Oil
Blind Shear Ram Closes 3
ROV Flow Time
ROV Intervention Successful
ROV Release Flowing
Record ROV LOC
ROV Success
Casing Shear Ram Successful w Shearable Tubular 1
Blind Shear Ram Closes 1
Well Cap Success Flow
Record Well Cap LOC
Well Capping Successful
Well Cap Release Flowing
Well Cap Success
Blind Shear Ram Closes 4
Assign Limted Release Flow Rate
Limted Release Flow Time
Limited Release Flowing
Record Limited Release LOC
Limited Release
Relief Well Success Flow
Relief Well Release Flowing
Record Relief Well LOC
Relief Well Success
True
False
Basic Process
Create
Dispose
Process
Decide
Batch
Separate
Assign
Record
Attribute
Entity
Queue
Resource
Variable
Schedule
Set

Figure 2- 37. Example Discrete Event Simulation Model



V Safety Performance Measures
V Safety Performance Requirements (including Goal and Threshold)
V Engineering Requirements
V Process Requirements

TOP-LEVEL CLAIM

This is "how safe" we are (or will be),* how we know it, and what we are doing to make sure that it comes true (or remains true).*
This is our technical basis for the claim:
V Evidence, including operating experience, testing, associated engineering analysis, and a comprehensive, integrated, scenario-based design and safety analysis
V A credible set of performance commitments, deterministic requirements, and implementation measures.

**The nature and specificity of the claim, and the character of the underlying evidence, depend on the life cycle phase at which the safety case is being applied.*

We characterize the design intent in terms of design reference missions and other requirements to be satisfied. The design itself is characterized at a level of detail appropriate to the current life cycle phase.

We present the results of analysis, conditional on an explicitly characterized baseline allocation of levels of performance, risk-informed requirements, and operating experience. We have a process for identifying departures from this baseline and/or addressing future emergent issues that are not addressed by this baseline.

We have demonstrated that no further improvements to the design or operations are currently net-beneficial (risk is as low as reasonably practicable).

We understand the implementation aspects needed to achieve the level of safety claimed, and commit to the necessary measures.

1

We characterize the design and mission intent.*

V Concept of Operation
V Design Reference Missions
V Operation Environments
V Historically Informed Elements

We specify the design for the current life cycle phase (including requirements and controls).*

We understand what is credited

We understand the nominal performance and dynamic response in design reference phases

We understand the performance allocation

2

We have performed our analyses and established the following results:
V Aggregate risk results
V Dominant accident scenarios
V Comparison with threshold/ goal
V Established baseline for precursor analysis
V .....

We have a process for addressing unresolved and non-quantified safety issues (issues invalidating the baseline case)

We have provided some defense against currently unrecognized safety issues (safety margin)

In addition to reviewing existing information sources and operating experience, we have applied the best processes known to us for identifying previously unrecognized safety hazards

We recognize the limits of our safety models: we have evaluated the caliber of evidence used in models, and have performed uncertainty and sensitivity analyses. To the extent practicable, we have addressed the completeness issue, and have developed a thorough understanding of key phenomenology and assumptions

We have formulated hazard controls, derived requirements, and fault protection approaches in a risk-informed manner

3

We carried out a process to identify significant safety improvements, but no candidate measures have been identified

We have determined that further improvements in safety would unacceptably affect schedule

We have determined that further improvements in safety would incur excessive performance penalties

We have determined that further improvements in safety would incur excessive cost

4

We have confirmed that allocated performance is feasible

We understand how to monitor and assure ongoing satisfaction of allocated performance levels, and there are commitments to implement these measures

We have identified and prioritized risks in the risk management program

We continue to evaluate operational experience for the presence of accident precursors

Figure 3-1. "Claims Tree"

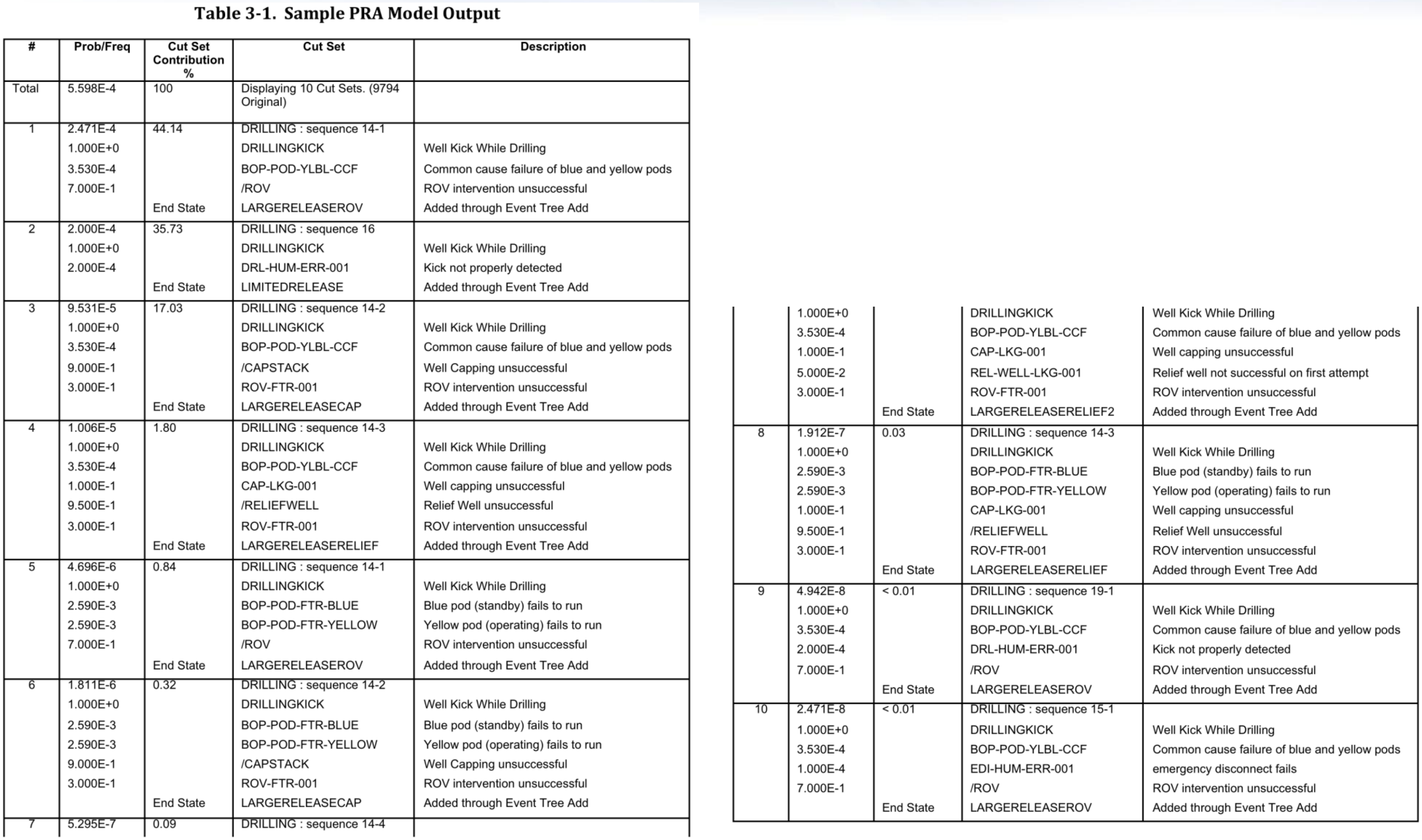


Table 3-1. Sample PRA Model Output

#	Prob/Freq	Cut Set Contribution %	Cut Set	Description
Total	5.598E-4	100	Displaying 10 Cut Sets. (9794 Original)	
1	2.471E-4	44.14	DRILLING : sequence 14-1	
	1.000E+0		DRILLINGKICK	Well Kick While Drilling
	3.530E-4		BOP-POD-YLBL-CCF	Common cause failure of blue and yellow pods
	7.000E-1		/ROV	ROV intervention unsuccessful
		End State	LARGERELEASEROV	Added through Event Tree Add
2	2.000E-4	35.73	DRILLING : sequence 16	
	1.000E+0		DRILLINGKICK	Well Kick While Drilling
	2.000E-4		DRL-HUM-ERR-001	Kick not properly detected
		End State	LIMITEDRELEASE	Added through Event Tree Add
3	9.531E-5	17.03	DRILLING : sequence 14-2	
	1.000E+0		DRILLINGKICK	Well Kick While Drilling
	3.530E-4		BOP-POD-YLBL-CCF	Common cause failure of blue and yellow pods
	9.000E-1		/CAPSTACK	Well Capping unsuccessful
	3.000E-1		ROV-FTR-001	ROV intervention unsuccessful
		End State	LARGERELEASECAP	Added through Event Tree Add
4	1.006E-5	1.80	DRILLING : sequence 14-3	
	1.000E+0		DRILLINGKICK	Well Kick While Drilling
	3.530E-4		BOP-POD-YLBL-CCF	Common cause failure of blue and yellow pods
	1.000E-1		CAP-LKG-001	Well capping unsuccessful
	9.500E-1		/RELIEFWELL	Relief Well unsuccessful
	3.000E-1		ROV-FTR-001	ROV intervention unsuccessful
		End State	LARGERELEASERELIEF	Added through Event Tree Add
5	4.696E-6	0.84	DRILLING : sequence 14-1	
	1.000E+0		DRILLINGKICK	Well Kick While Drilling
	2.590E-3		BOP-POD-FTR-BLUE	Blue pod (standby) fails to run
	2.590E-3		BOP-POD-FTR-YELLOW	Yellow pod (operating) fails to run
	7.000E-1		/ROV	ROV intervention unsuccessful
		End State	LARGERELEASEROV	Added through Event Tree Add
6	1.811E-6	0.32	DRILLING : sequence 14-2	
	1.000E+0		DRILLINGKICK	Well Kick While Drilling
	2.590E-3		BOP-POD-FTR-BLUE	Blue pod (standby) fails to run
	2.590E-3		BOP-POD-FTR-YELLOW	Yellow pod (operating) fails to run
	9.000E-1		/CAPSTACK	Well Capping unsuccessful
	3.000E-1		ROV-FTR-001	ROV intervention unsuccessful
		End State	LARGERELEASECAP	Added through Event Tree Add
7	5.295E-7	0.09	DRILLING : sequence 14-4	
	1.000E+0		DRILLINGKICK	Well Kick While Drilling
	3.530E-4		BOP-POD-YLBL-CCF	Common cause failure of blue and yellow pods
	1.000E-1		CAP-LKG-001	Well capping unsuccessful
	5.000E-2		REL-WELL-LKG-001	Relief well not successful on first attempt
	3.000E-1		ROV-FTR-001	ROV intervention unsuccessful
		End State	LARGERELEASERELIEF2	Added through Event Tree Add
8	1.912E-7	0.03	DRILLING : sequence 14-3	
	1.000E+0		DRILLINGKICK	Well Kick While Drilling
	2.590E-3		BOP-POD-FTR-BLUE	Blue pod (standby) fails to run
	2.590E-3		BOP-POD-FTR-YELLOW	Yellow pod (operating) fails to run
	1.000E-1		CAP-LKG-001	Well capping unsuccessful
	9.500E-1		/RELIEFWELL	Relief Well unsuccessful
	3.000E-1		ROV-FTR-001	ROV intervention unsuccessful
		End State	LARGERELEASERELIEF	Added through Event Tree Add
9	4.942E-8	< 0.01	DRILLING : sequence 19-1	
	1.000E+0		DRILLINGKICK	Well Kick While Drilling
	3.530E-4		BOP-POD-YLBL-CCF	Common cause failure of blue and yellow pods
	2.000E-4		DRL-HUM-ERR-001	Kick not properly detected
	7.000E-1		/ROV	ROV intervention unsuccessful
		End State	LARGERELEASEROV	Added through Event Tree Add
10	2.471E-8	< 0.01	DRILLING : sequence 15-1	
	1.000E+0		DRILLINGKICK	Well Kick While Drilling
	3.530E-4		BOP-POD-YLBL-CCF	Common cause failure of blue and yellow pods
	1.000E-4		EDI-HUM-ERR-001	emergency disconnect fails
	7.000E-1		/ROV	ROV intervention unsuccessful
		End State	LARGERELEASEROV	Added through Event Tree Add

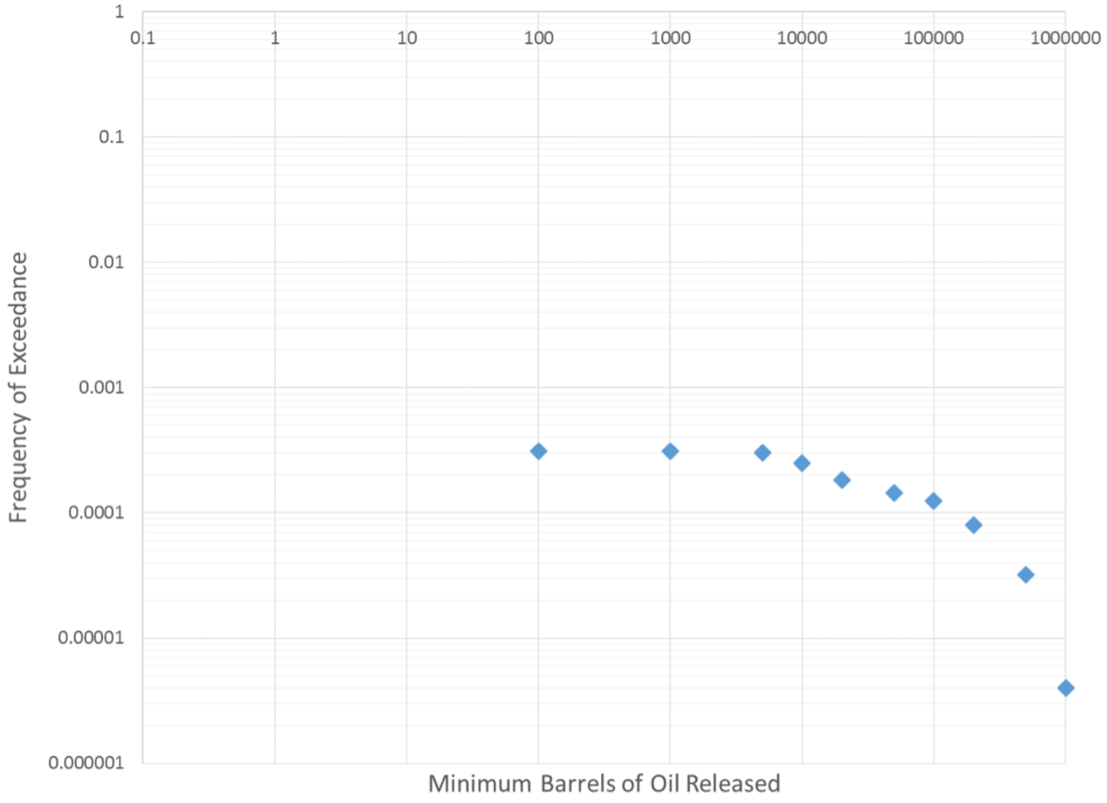
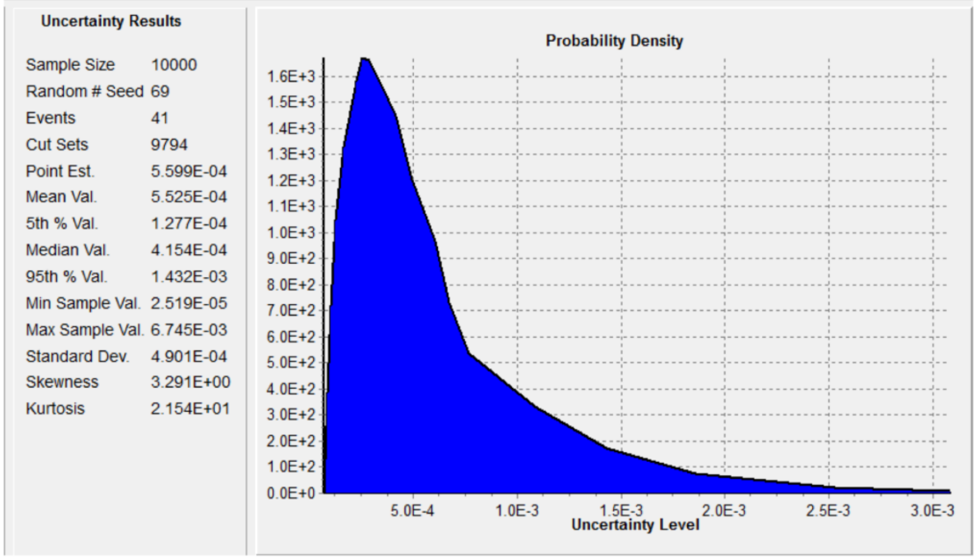


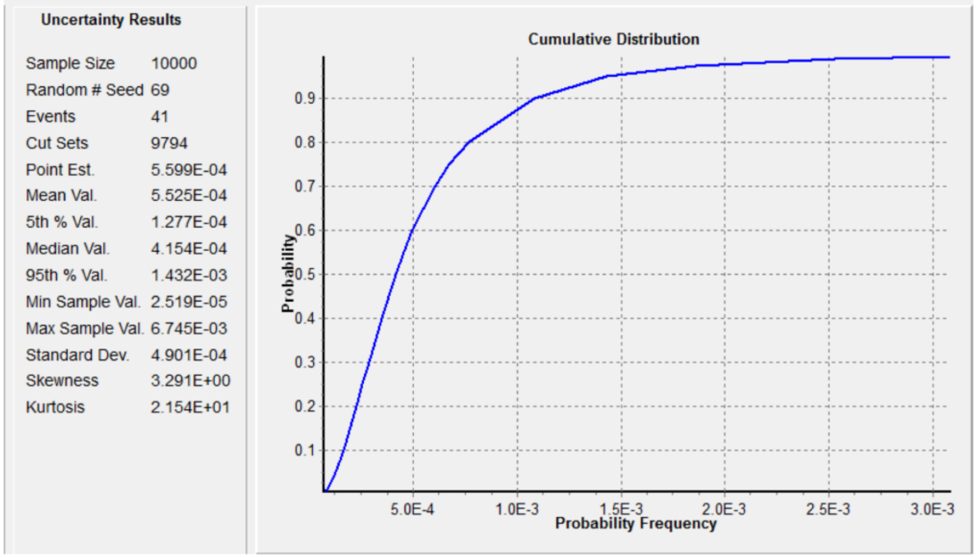
Figure 3- 1. Example Frequency of Exceedance Curve



Uncertainty Results

Sample Size	10000
Random # Seed	69
Events	41
Cut Sets	9794
Point Est.	5.599E-04
Mean Val.	5.525E-04
5th % Val.	1.277E-04
Median Val.	4.154E-04
95th % Val.	1.432E-03
Min Sample Val.	2.519E-05
Max Sample Val.	6.745E-03
Standard Dev.	4.901E-04
Skewness	3.291E+00
Kurtosis	2.154E+01

Figure 3- 1. Example Probability Density Function



Uncertainty Results

Sample Size	10000
Random # Seed	69
Events	41
Cut Sets	9794
Point Est.	5.599E-04
Mean Val.	5.525E-04
5th % Val.	1.277E-04
Median Val.	4.154E-04
95th % Val.	1.432E-03
Min Sample Val.	2.519E-05
Max Sample Val.	6.745E-03
Standard Dev.	4.901E-04
Skewness	3.291E+00
Kurtosis	2.154E+01

Figure 3- 2. Example Cumulative Probability Distribution

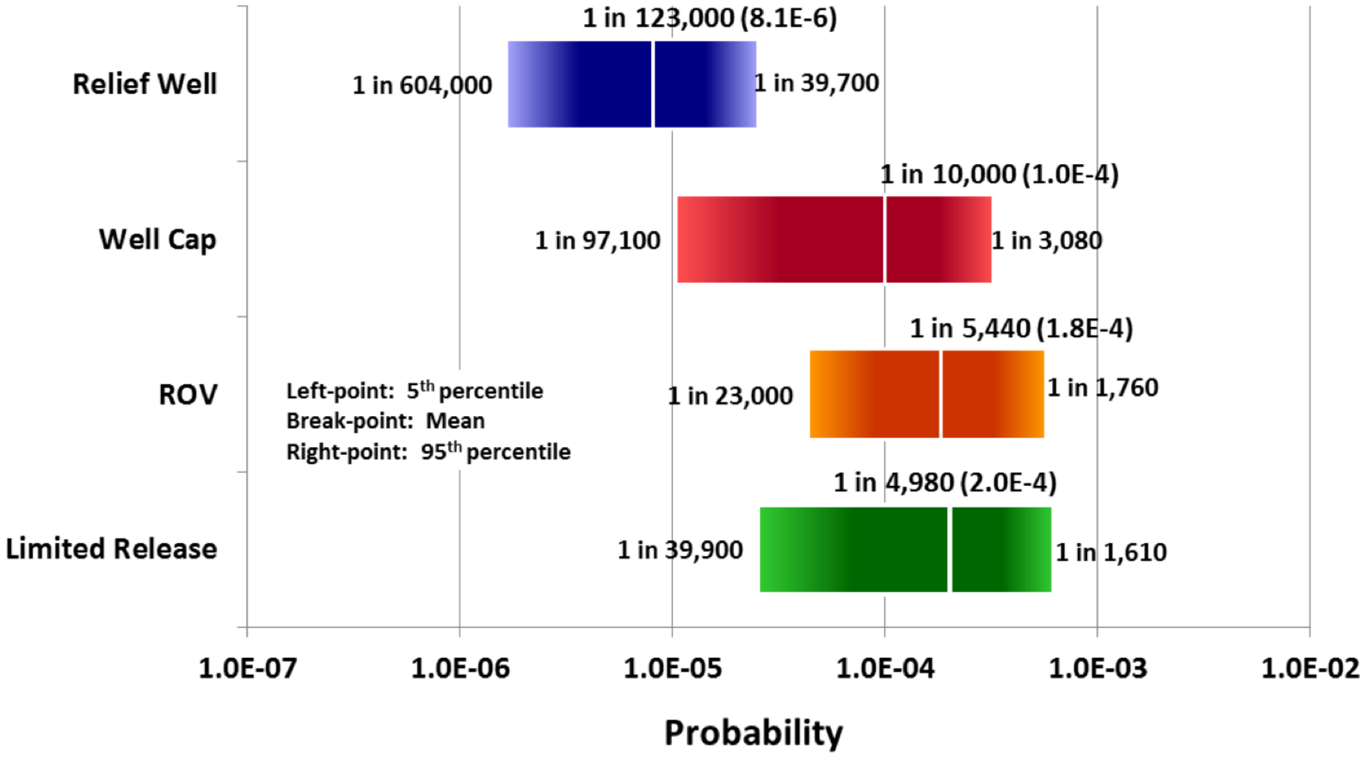
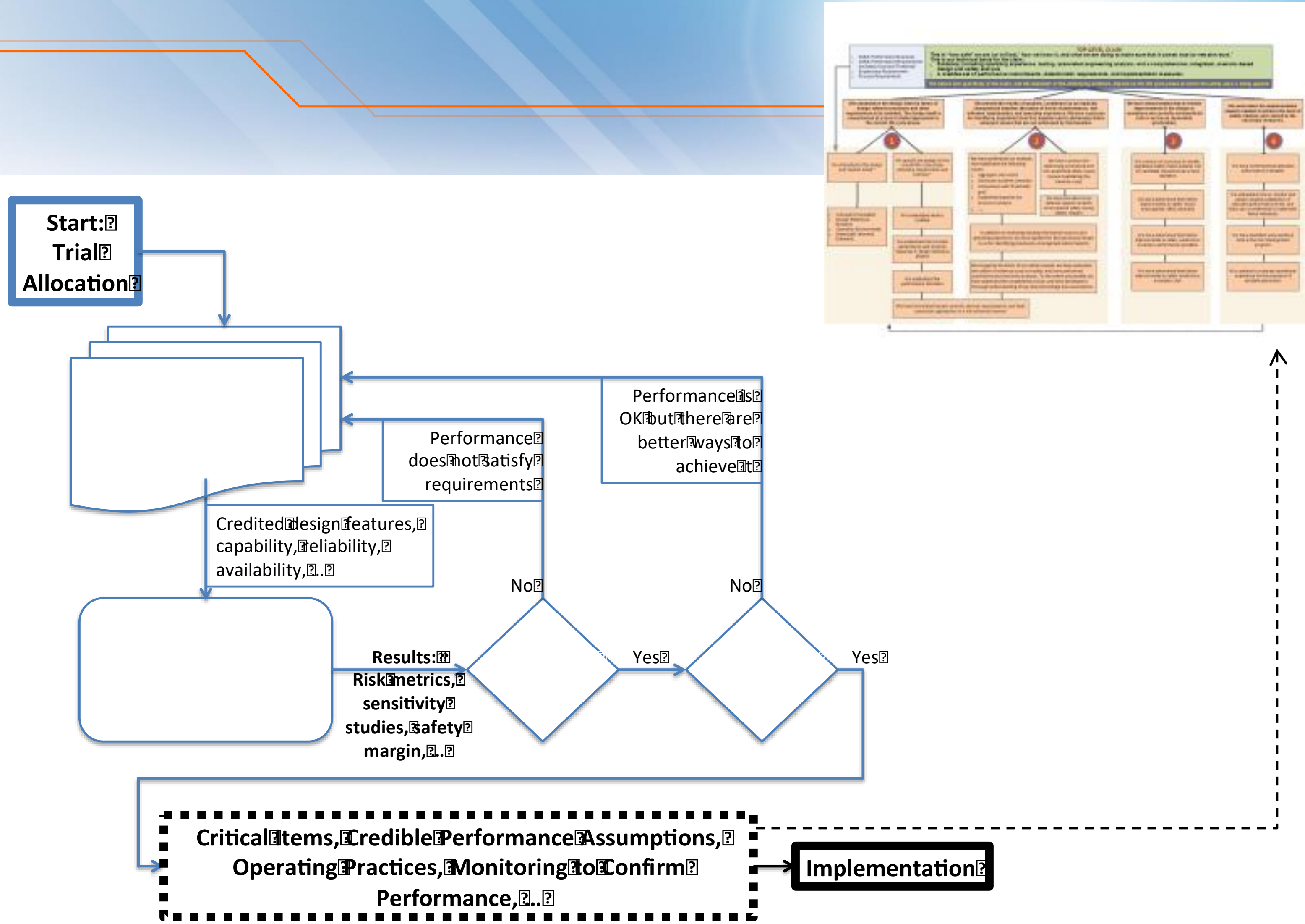


Figure 3- 1. Example Comparison of End State Distributions



Start: Trial Allocation

Credited design features, capability, reliability, availability, …

Performance does not satisfy requirements

Performance is OK but there are better ways to achieve it

No

No

Results: Risk metrics, sensitivity studies, safety margin, …

Yes

Yes

Critical Items, Credible Performance Assumptions, Operating Practices, Monitoring to Confirm Performance, …

Implementation

Figure K- 2. Process for Confirming Overall Performance Based on Items Credited in the Assurance Case

Next Generation Nuclear Plant Licensing Basis Event Selection White Paper (INL/EXT-10-19521)

Farmer

(Holbrook)

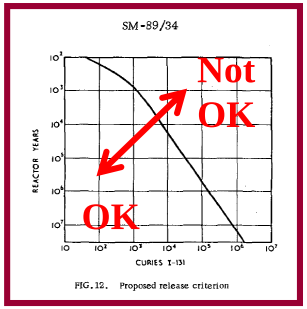
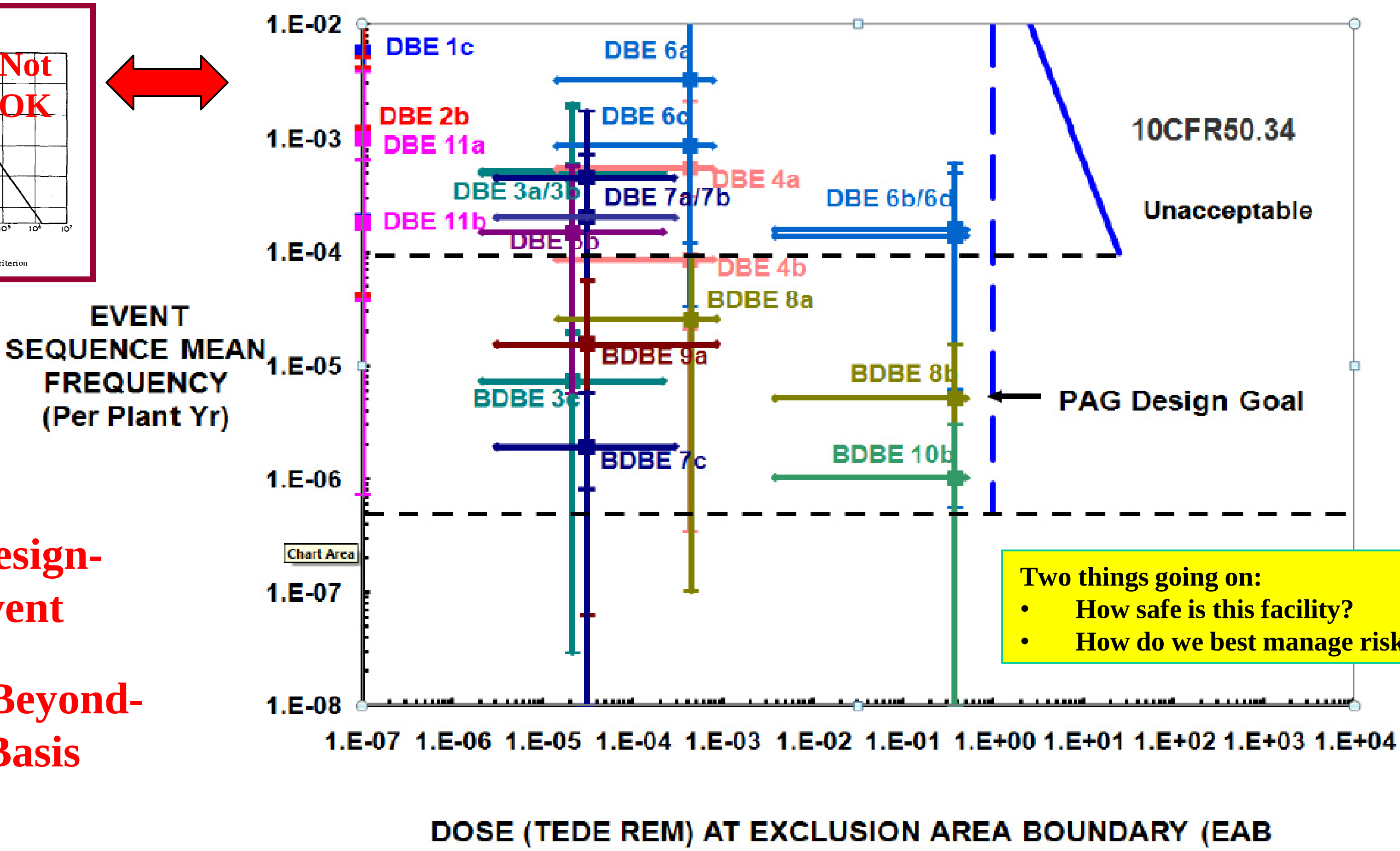


FIG. 12. Proposed release criterion



Two things going on:

- How safe is this facility?
- How do we best manage risk?

DBE: Design-Basis Event

BDBE: Beyond-Design-Basis Event

Figure 8. Use of PRA to select BDBEs.

Summary

- NASA’s Johnson Space Center (JSC) is developing a PRA Procedures Guide for BSEE, initially scoped to deal with offshore drilling
- INL is helping JSC do that
- By agreement between JSC and BSEE, the starting point for the development was NASA’s PRA Procedures Guide
  - Development of the NASA guide was initiated after Challenger
  - The NASA guide was heavily influenced by nuclear industry PRA guidance
    - Initially (2002), mostly logic modeling, which is good at functional dependency, redundancy, etc., but rather approximate in some ways
    - Later (2011), the guide paid some attention to simulation, which is better at timing, variations in event phenomenology, …
  - We are trying to be responsive to oil-industry risk modeling needs, not blindly assume nuclear/ NASA PRA techniques are optimal
- The Draft BSEE Guide addresses [or *will* address, when complete]
  - Standard high-end logic-model tools
  - More qualitative risk assessment tools
  - Simulation-enhanced PRA [placeholder for now]
  - Improved discussion of data analysis
  - Better understanding of uncertainty
  - Improved discussion of the USE of risk model results

PARKING LOT

Cross Reference Matrix showing how NASA PRA Guide corresponds to BSEE's (1 of 2)

Topic	NASA Guide Section	Draft BSEE Guide Section
Introduction	1	1
Risk Management	2	2.1
PRA Overview	3	2.2.1-2.2.5, Appendices A, B
Scenario Development	4	2.1, 2.2.1-2.2.5, Appendix C
Data Collection and Parameter Estimation	5	2.2.6, Appendix E, Appendix G (TBD)
Uncertainty Analysis	6	2.2.6, Appendices F, G
Common Cause Failures	7	Appendix D (TBD)
Human Reliability	8	Appendix L (TBD)
Software Risk	9	???
Physical and Phenomenological Models	10	2.3.1 (TBD)

Cross Reference Matrix showing how NASA PRA Guide corresponds to BSEE's (2 of 2)

Topic	NASA Guide Section	Draft BSEE Guide Section
Probabilistic Structural Analysis	11	2.3.1 (TBD)
Uncertainty Propagation	12	2.2.6
Presentation / Interpretation of Results	13	3, Appendices I, J, K
Launch Abort Models	14	N/A
Probability basics	Appendix A	???
Failure distributions	Appendix B	2.2.6
Bayesian inference	Appendix C	2.2.6, Appendices F, G
Modeling examples	Appendix D	2.2
Simulation example	Appendix E	2.3
Configuration Control	N/A	???