Controlling Risks
Risk Assessment

Hazard/Risk Assessment

- Having identified the hazards, one must assess the risks by considering the severity and likelihood of bad outcomes. If the risks are not sufficiently low, then additional controls or alternate methods must be applied.

- Risk increases if either likelihood or severity [*magnitude of loss*] increases provided the other component does not decrease proportionally.

Tailoring Your Risk Definition

- No task is completely without risk
- Must develop tailored risk matrix, based upon acceptable risk, in order to identify what is considered *sufficiently low*
- Must define *"acceptable risk"*

Risk Class

- Example Risk Classification (IEC61508-5)
  - I Unacceptable
  - II Undesirable
  - III Action Recommended (ALARP)
  - IV Broadly Acceptable
- Classifications are developed inside the organization and approved by senior management

Acceptable Risk

- What is it?
  - The threshold level below which risk will be tolerated
- To whom is the risk posed?
  - Generally the risk is posed to those who are not defining it
- By whom is it judged acceptable?
  - Senior management based upon input from technical experts

Risk Assessment: Severity

- Evaluate the severity, or consequences, of each possible accident and rank order them by severity of the outcome.
  - Determine the potential negative impact of each hazard scenario on
    - Personnel
    - Equipment
    - Operations
    - Public
    - Environment
    - The system itself

Risk Assessment: Likelihood

- Likelihood, or Probability, assignment
  - Qualitative
  - Quantitative

- Estimate the probability of each possible accident.
  - Past history of accidents/incidents
  - Industry benchmarks

Likelihood/Probability Definition

- Can be defined in terms of occurrences per
  - Units of time
  - Events
  - Population
  - Items
  - Activity

Risk Assessment Tools

- To determine what actions to take to eliminate or control a hazard, a system of determining the level of risk is needed.

- Risk tool should enable you to properly understand the level of risk involved relative to what it will cost in schedule and mitigation $$

Risk Tool Development

- In early design stages, severity consideration is all that's needed since you should first try to eliminate the hazards by design
- When all hazards cannot be eliminated, probability factors become important
- General risk assessment tools are available however it's best if you use tools tailored to your individual program

Simple Probability Functions

P(Event)=P(Hazard)*P(Severity)*P(Liklihood)*P(Exposure)

The Risk/Hazard Matrix (RHM)

- Allows you to assign a risk value to each hazard scenario
- Can rank order hazard scenarios
- Identify potential mitigation alternatives
- Evaluate alternatives in terms of risk reduction (use your matrix)
- Prioritize mitigation tasks

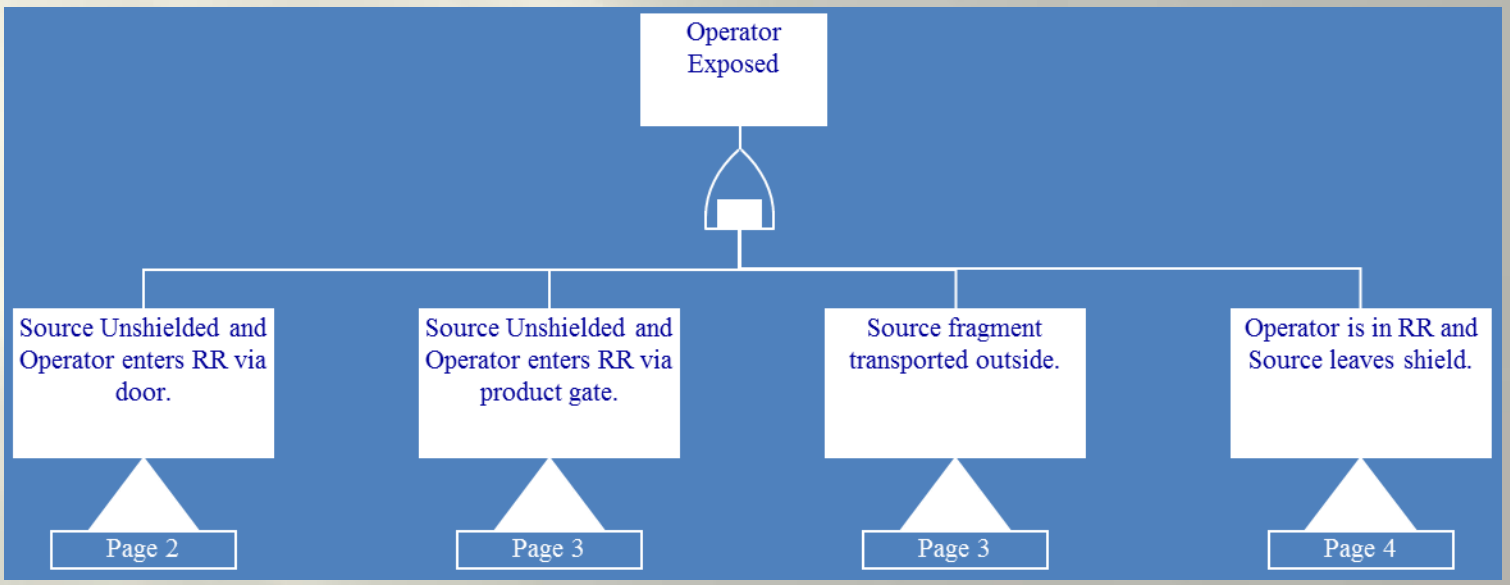
Frequency	Catastrophic	Critical	Marginal	Negligible
	Consequence			
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

	A	B	C	D	E	F	G
1	Today's Date	6/29/2004					
2							
3	Project	USPAS					
4	Evaluator	K. Mahoney					
5	Date	6/22/2004					
6	Hazard	Shock from Energized Magnets					
7	Constraint 1	50-250VDC					
8	Constraint 2	<5mA					
9							
10	Likelihood						
11	Consequence						
12							
13							User Defined Ra
14	**Risk Matrix**		**Color code**	**Intolerable**		0	4
15				**Undesirable**		4	5
16				**Tolerable**		5	7
17				**Acceptable**		7	>
18	User Defined Likelihood						
19	Immanent	**0**	**Frequent**	3	2	1	0
20	1day-1year	**1**	**Probable**	4	3	2	1
21	1-10 years	**2**	**Occasional**	5	4	3	2
22	Over life of facility	**3**	**Remote**	6	5	4	3
23	100-1000 years	**4**	**Unlikely**	7	6	5	4
24	>1000 years	**5**	**Impossible**	8	7	6	5
25				**3**	**2**	**1**	**0**
26			**Consequences**	**Minimal**	**Marginal**	**Critical**	**Catastrophic**
27				**First Aid**	**< 5 Lost Work Days**	**> 5 lost work days**	**Death or Disability**

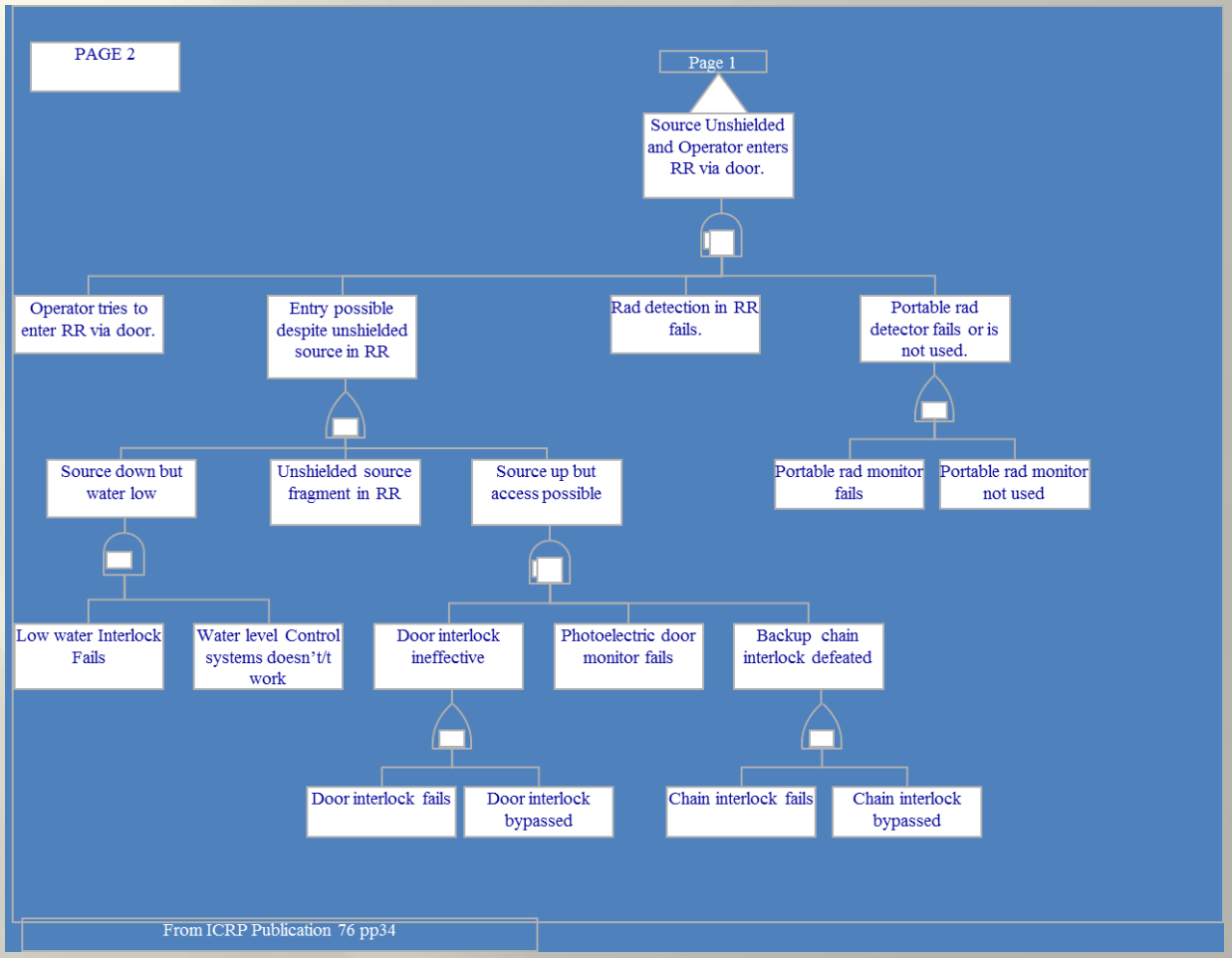
Fault Tree Analysis (FTA)

- Widely used in aerospace, electronics and nuclear industries
- Primarily a means for analyzing causes of hazards, not identifying hazards
- Top-down search method, with the top event having been foreseen
- Four basic steps: (1) system definition; (2) fault tree construction; (3) qualitative analysis; and (4) quantitative analysis

Qualitative Fault Tree



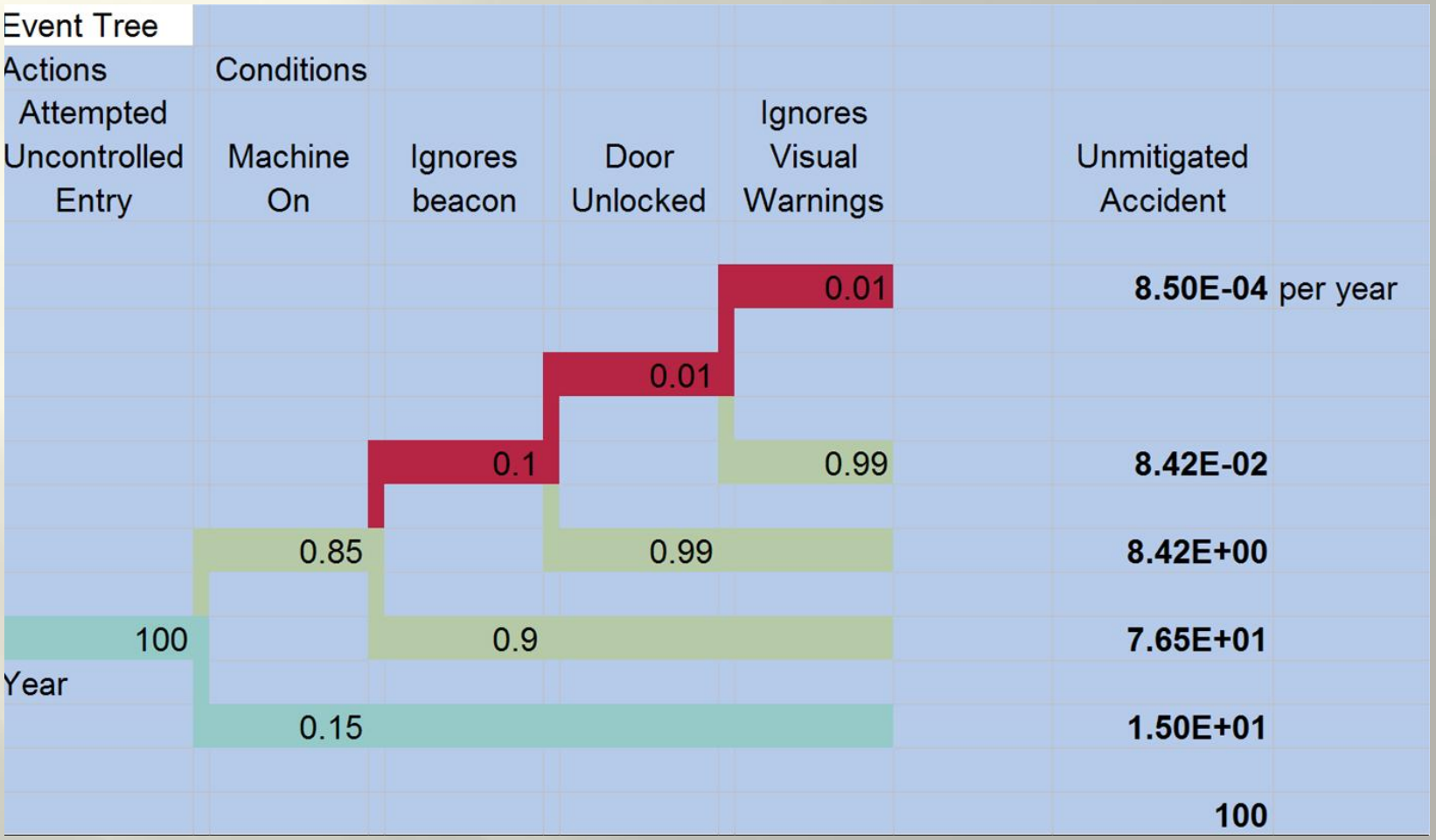
Qualitative Fault Tree



Event Tree Analysis (ETA)

- An adaptation of general decision tree whereby a problem is broken up into smaller parts to which the FTA is then applied.
- Uses forward search to identify possible outcomes of an event
- Principally used in nuclear power plants
- Drawn from left to right
- Based upon a binary state system [success or failure]
- Tend to be quite large

Example Event Tree



Failure Modes & Effects Analysis (FMEA)

- Form of reliability analysis
- Emphasizes successful functioning rather than hazards & risk
- Uses forward search based upon chain-of-events model
- All significant failure modes must be known in advance
- Doesn't consider effects of multiple failures (except for subsequent effects it might produce)

Failure Modes & Effects Analysis (FMEA)

- Analyzes single failure modes
  - Determines effects on all other system components and on overall system
  - Probabilities and seriousness of each failure mode's results are calculated
  - Critical effects are added to get failure probability for entire system
- Failures rates predicted from generic rates developed from experience over time

Failure Modes & Effects Analysis (FMEA) - Uses

- Identify redundancy and fail-safe design requirements
- Single-point failure modes
- Inspection points
- Spare parts requirements
- Strength of technique is completeness but it is also time consuming

Hazard & Operability Analysis (HAZOP)

- Primarily used by the chemical industry
- Focuses on safety & efficient operations
- Assumes accidents are caused by deviations from design or operating intent
- Systematic, qualitative technique
- Able to identify “unreviewed” safety issues
- It is labor-intensive