NE529
RISK ASSESSMENT
PRA Wrapup
8

R. A. Borrelli

University of Idaho

Idaho Falls Center for Higher Education

Learning objectives

Understanding the integrative nature of a PRA

Overview of chapters 17 and 19 in the book

Other material I found

This is a bit of a mash

Learning nodes

NRC use of PRA

PRA for system design

Farmer's chart

PRA space

WASH-1400
Peer review
Major findings
Recommendations
Brown's Ferry

Common cause failures

Human factors

Quantitative comparisons

Follow up to WASH-1400
1995 Policy statement

PRA challenges

Putting it all together

Narrative research

Case studies

NRC use of PRA

PRA is the NRC regulatory paradigm

Surprisingly, this is not the case with many industries

Defense-in-Depth is an element of the NRC safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility

Design Basis Accidents are postulated accidents that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to assure public health and safety

Essential to PRA

Quantitative safety goals were issued in 1986

Early and latent cancer mortality risks to an individual living near the plant should not exceed 0.1% of the background accident or cancer mortality risk

5×10^{-7} per year for early death

2×10^{-6} per year for death from cancer

The prompt fatality goal applies to an average individual living in the region between the site boundary and 1 mile beyond this boundary

The latent cancer fatality goal applies to an average individual living in the region between the site boundary and 10 miles beyond this boundary

PRA for system design

PRA can inform system or facility design

‘as-design’ trend

Facility must be operated without undue risk to public health and safety

A single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions

So don’t have something fail and the whole place blows up

Defense-in-depth mitigates single failures

For nuclear, this deals with LOCA

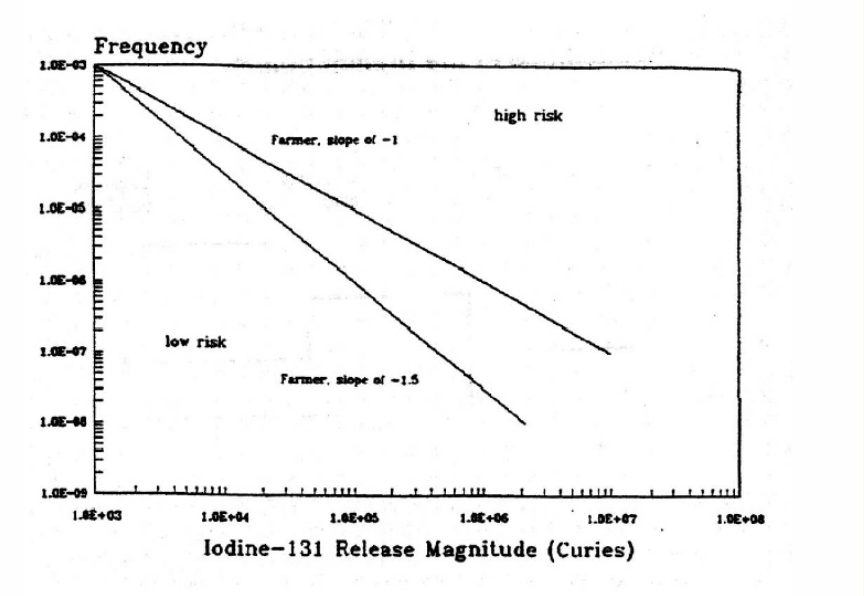
So they came up with criteria to avoid this

Need a heat sink and coolant source (Generation III+)

Cladding temperature, long term cooling, accident tolerant fuels etc.

Farmer’s chart

Farmer came up with his chart in 1967 for I-131



I-131 is a major threat to health in a nuclear plant accident

Farmer considered the public acceptability of risk

Whole spectrum of events needs to be considered

Not just worst case (which would be low frequency)

Low consequence but more probable carries equal risk

Postulated a near-inverse for acceptable risk

Events with twice the consequence must be half as frequent

There are two overall ‘spaces’ to consider with risk assessment

1. After the accident

Figure out what went wrong

Limit potential exposures and releases

Prevent future similar accidents

19.3 in the book

2. Facility/process/experimental operations

Demonstrate ahead of time what the risks are and how they meet institutional requirements

19.3.1. discusses again about the detection of small structural cracks in aircraft

You can't really establish a probability of detection of the cracks

But you can determine how experience would make detection more reliable

Knowing what parts are more prone to cracks

So you need qualitative efforts to determine this

Develop a survey to determine experience level of inspectors

Conduct a physical experiment to collect quantitative data from a lot of inspectors

WASH-1400

WASH-1400 came along in 1975

First formalized use of PRA – Fault and events trees, etc.

Dominant contributors to risk were small LOCAs and transients

Core damage frequency higher than what was thought at the time

But consquences smaller

Support systems and operator actions very important

Change in the reactor coolant system temperature, pressure, or both, attributed to a change in the reactor's power output

300 reactor-years commercial experience

WASH-1400 peer review

WASH-1400 was reviewed by experts

(1) Clarify the achievements and limitations of WASH-1400

(2) Assess the peer comments thereon, and responses

(3) Study the present state of such risk assessment methodology

(4) Recommend to NRC how (whether) such methodology can be used in the regulatory and licensing process

WASH-1400 was a conscientious and honest effort to apply the methods of fault-tree/event-tree analysis to an extremely complex system, a nuclear reactor, in order to determine the overall probability and consequences of an accident.

They identified several problems we still talk about

Inability to quantify human adaptability during the course of an accident

Inadequate treatment of common cause failure

We are unable to define whether the overall probability of a core melt given in WASH-1400 is high or low, but we are certain that the error bands are understated. We cannot say by how much. Reasons for this include an inadequate data base, a poor statistical treatment, an inconsistent propagation of uncertainties throughout the calculation, etc.

Even with all the operational history to drawn upon, they still have problems

Risk assessment itself though was considered good

We do find that the methodology, which was an important advance over earlier methodologies applied to reactor risks, is sound, and should be developed and used more widely under circumstances in which there is an adequate data base or sufficient technical expertise to insert credible subjective probabilities into the calculations.

The methodology can therefore provide a tool for the NRC to make the licensing and regulatory process more rational, in more properly matching its resources (research, quality assurance, inspection, licensing regulations) to the risks provided by the proper application of the methodology.

We find that the fault-tree/event-tree methodology is sound, and both can and should be more widely used by NRC. The implementation of this methodology in WASH-1400 was a pioneering step, but leaves much to be desired.

They didn't like how it was written

It is very difficult to follow the detailed thread of any calculation through the report.

We find that the Executive Summary is a poor description of the contents of the report, should not be portrayed as such, and has lent itself to misuse in the discussion of reactor risks.

Other major findings

(1) WASH-1400 was a substantial advance over previous attempts to estimate the risks of the nuclear option. The methodology has set a framework that can be used more broadly to assess choices involving both technical consequences and impacts on humans

(2) Made study of reactor safety more rational

(3) Established a topology of accident sequences

(4) Delineated procedures to quantify risk *for those sequences for which a database exists*

(5) Error bounds may be understated due to inadequate database

(6) Inability to quantify common cause failures

(7) Inability to quantify human adaptability during the course of an accident (as illustrated at Browns Ferry) and failure to take credit for this is a major source of conservatism

(8) Transients, small LOCA, and human errors are important contributors to overall risk, yet their study is not adequately reflected in the priorities of either the research or regulatory groups

(9) Most complete single picture of accident probabilities associated with nuclear reactors

(10) Fault/event tree approach coupled with an adequate data base is the best available tool with which to quantify these probabilities

(11) Made clear the importance to reactor safety discussions of accident consequences other than early fatalities (thyroid damage, land contamination, delayed cancers, genetic defects, etc.) for the first time

Let's look at some recommendations

(1) Incorporate lessons learned into NRC licensing criteria

(2) Use PRA to reduce uncertainties

(3) Still use PRA even if data base is inadequate

(4) Use PRA for other electric generating technologies

(5) Fault/event tree analyses should be among the principal means used to deal with generic safety issues, to formulate new regulatory requirements, to assess and revalidate existing regulatory requirements, and to evaluate new designs

And some limitations

(1) Insufficient human data for the trees (though this seems at odds with what they just said)

(2) Methodological weakness due to the difficulty of incorporating time-window information into the event trees

(3) Humans might make things worse, which is hard to analyze

(4) But they might also make things better

(5) This leads to uncertainty in assessing human factors

Recommend that the NRC undertake a systematic program to evaluate the need for better human data

Time dependencies only recently being addressed with dynamic risk assessment

It must be said at the outset that RSS represents the fruits of a praiseworthy and pioneering effort to deal in depth with an extremely complex subject. It is a monumental report, written in three years by a large number of people and (although it is difficult to count the pages because they are not consecutively numbered) is nearly a foot thick. Clearly no one person can, or did, write all of this, and the report suffers thereby from incoherence.

A specific definition of risk was not defined

But displayed its results through graphs of the probability of occurrence of an event against the consequences of that event

Other means of displaying the results could produce different risk perceptions

We know that is the definition of risk now

Establishing acceptable levels of risk is always challenging

WASH-1400 compared estimated risks with other societal risks in Chapters 6 and 7

To judge acceptability of nuclear reactors solely on the risk of early fatalities, and latent health effects, and property damage for Class 9 accidents is inappropriate

Public perception hangs heavily upon the perceived credibility of NRC

I'm actually surprised to see this statement and wonder how they arrived at it

They also considered the effects of sabotage

It is also worth noting that some features that make the plants difficult to sabotage successfully would also help to make most sabotage scenarios benign from the standpoint of public injury

It would be-much easier to sabotage the plant so as to lead to shutdown and a need for expensive repair than to produce a core melt

What about sabotage now?

Brown’s Ferry

Could PRA have predicted Brown's Ferry?

March 1975

Two BWRs

Electricians were using *candles* to test for air leaks and the sealant caught on fire

Common cause failures in a variety of otherwise independent and redundant systems

Control of 11 relief valves lost

Only source of makeup water was a control rod drive pump not intended for this purpose and of inadequate capacity for the long term

Nothing actually went wrong

Valves were repaired in 5 and a half hours

Reactor shutdown safely

Appendix XI of WASH-1400 contains a probabilistic analysis of the Browns Ferry event

Failed to estimate that last 4 valves would fail because air supply ran out

No models for repair times

Reviewers don't comment on whether the core melt probability is reasonable

Aren't particularly glowing of the assessment either

Do not think PRA captured fire as an important accident initiator

The accident was initiated by human error

Which is still hard to model

A a substantial element of conservatism in the body of WASH-1400 (other than in the analysis of Browns Ferry) lies in failing to take credit for the fact that well-trained humans provide adaptive coping capability.

This is similarly hard to model or quantify

Too little time and energy have been expenaed in using the event to help quantify some of the inputs to a reactor safety analysis which are most difficult to quantify: quality assurance, human behavior, common cause failure, etc. It is even now not too late for the NRC to have some impartial body do these things.

So, the same things as now

Common cause failures

Can PRA identify common cause failures?

Common cause failure may invalidate some of the sequential features of an event-tree, while at the same time causing failures on adjacent and apparently disparate event-trees (report)

With so many people working on all the event trees, it's easy to see how common cause failures could slip through (me)

We are unconvinced by the arguments for completeness of the report in connection with common cause failures.

Common cause failures can activate low probability accident sequences that would otherwise be overlooked

So this continues to be a problem with PRA

Principal assurance against common cause failures must lie in dealing with initiating events

(1) Fire

(2) Earthquakes

(3) Acts of violence

(4) Explosions and missiles

(5) Massive electrical failure

(6) Human error

(7) Flood, tsunamis

(8) Tornadoes, hurricanes

How do you mitigate these initating events?

Earthquake is potential initiator of a common cause failure

WASH-1400 found earthquakes to be small contributors to the total risks of core melt

Earthquake risk in nuclear plants deserves much more attention than it has received

Investigation at a level of sophistication necessary to resolve issue to our satisfaction has not yet been performed, and it is important that done

TYPES OF COMMON CAUSE FAILURES AND THEIR ASPECTS

	DEPENDENT	STRUCTURAL*	ENVIRONMENTAL	EXTERNAL*
Description of Failure Cause	Failure of an interfacing system, action or component	A common material or design flaw which simultaneously affects all components population	A change in the operational environment which affects all members of a component population simultaneously	An event originating outside the system which affects all members of a component population simultaneously
Hardware Examples	• Loss of electrical power • Loss of steam production in steam-driven feedwater system • A manufacturer provides defective replacement parts that are installed in all components of a given class	• Faulty materials • Aging • Fatigue • Improperly cured materials • Manufacturing flaw	• Dirty water in RCS with regard to pump seal • High pressure • High temperature • Vibration	• Weather: hurricanes, tornado, ice, heat, low cooling water flow • Earthquake (breaks pipe, disables cooling system, breaks containment) • Flooding→loss of electricity • Birds in engine of airplane
Human Examples	• Following a mistaken leader • An erroneous maintenance procedure is repeated for all components of a given class	• Incorrect training • Poor management • Poor motivation • Low pay	• Common cause psf's • New disease • Hunger • Fear • Noise • Radiation in control room	• Explosion • Toxic substance • Weather • Earthquake • Concern for families
Easy to Anticipate?:				
Component failure	High	Very Low	Medium	Medium
Human error	Medium	Very Low	Medium	Medium
Easy to Mitigate?:				
Component failure	High, if system designed for mitigation	Very Low, hard to design for mitigation	Low	Low
Human error	High, if feedback provided to identify the error promptly	Very Low, the factors making CCF likely also discourage being prepared for correction	Low	Low

* Usually there are no precursors

Human factors

People screwing up also cause a lot of accidents

Which is why we have the human factors field

The peer review group was not pleased about the lack of peer comment on human factors

But no one had any expertise in it either

(1) Humans operate systems during an accident to mitigate consequences

(2) Humans can make a mistakee to aggravate the situation

(3) Accidents can be initiated by humans through error

(4) Humans can inadvertantly disable safety equipment that will then be unavilable in an accident

Event and fault trees must take human intervention into account

(1) Human performance data base is weak (at the time)

(2) Human factor data used in WASH came from nonnuclear experience

(3) Event/fault trees need to be highly detailed

(4) Some human-intertention phenomena are time-dependent (hard to quantify)

(5) Uncertainties arise when expert judgment is used

WASH1400 threw human factors a bone

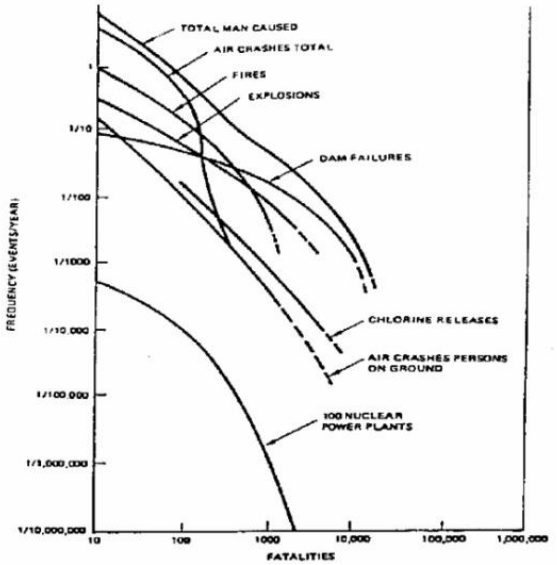
(1) Role of operators delinated better than prior to WASH1400

(2) Experience with other highly complex systems operated by well trained personnels is relevant

(3) Consensus among other experts WASH1400 estimated human error well

But they point out that a substantive review did not occur

Quantitative comparisons



Frequency of Fatalities Due to Man-Caused Events (RSS)

Courtesy of U.S. NRC.

Follow up to WASH-1400

Zion and Indian Point were the first PRAs sponsored by industry

Comprehensive analysis of uncertainties (Bayesian methods)

Detailed containment analysis (not all accidents lead to containment failure)

‘External’ events (earthquakes, fires) may be significant contributors to risk

Still have not found these reports

The follow up to WASH1400 was NUREG1150 1990

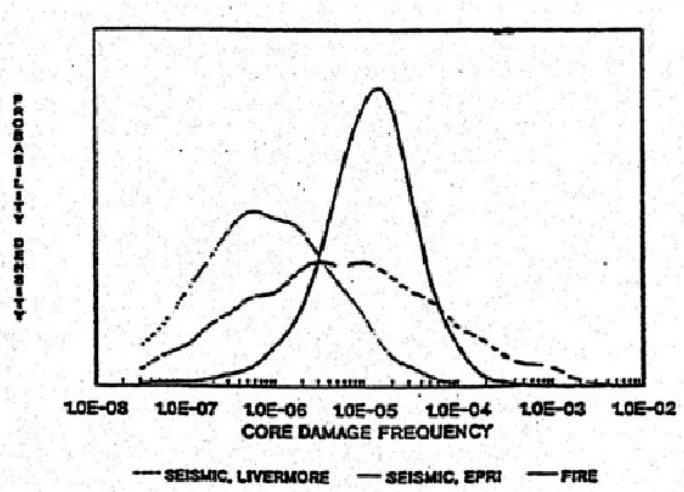
Average probability of an individual early fatality per reactor per year

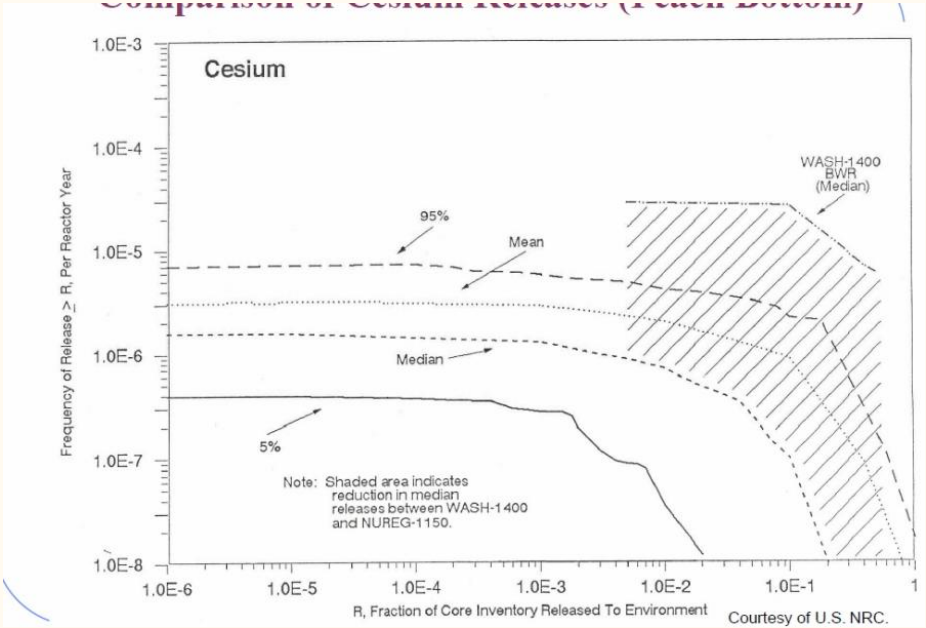
NRC Safety Goal – 5×10^{-7}

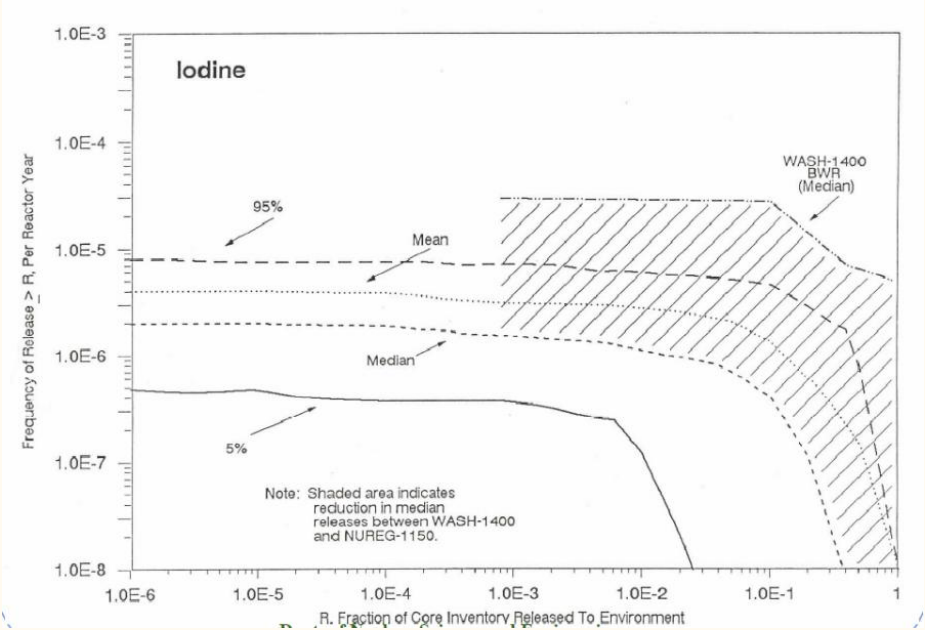
Level I PRA methods generally sound

Concerns with human reliability analysis, common cause failures, data analysis

Same things we talk about today


PROBABILITY DENSITY
1.0E-08
1.0E-07
1.0E-06
1.0E-05
1.0E-04
1.0E-03
1.0E-02
CORE DAMAGE FREQUENCY
SEISMIC, LIVERMORE
SEISMIC, EPRI
FIRE


Cesium
1.0E-3
1.0E-4
1.0E-5
1.0E-6
1.0E-7
1.0E-8
Frequency of Release ≥ R, Per Reactor Year
WASH-1400
BWR
(Median)
95%
Mean
Median
5%
Note: Shaded area indicates
reduction in median
releases between WASH-1400
and NUREG-1150.
1.0E-6
1.0E-5
1.0E-4
1.0E-3
1.0E-2
1.0E-1
1
R, Fraction of Core Inventory Released To Environment
Courtesy of U.S. NRC.


Iodine
1.0E-3
1.0E-4
1.0E-5
1.0E-6
1.0E-7
1.0E-8
Frequency of Release > R, Per Reactor Year
95%
Mean
Median
5%
WASH-1400
BWR
(Median)
Note: Shaded area indicates
reduction in median
releases between WASH-1400
and NUREG-1150.
1.0E-6
1.0E-5
1.0E-4
1.0E-3
1.0E-2
1.0E-1
1
R, Fraction of Core Inventory Released To Environment

1995 Policy statement

NRC released a policy statement 1995

Use of PRA should be increased to the extent supported by the state of the art and data and in a manner that complements the defense-in-depth philosophy

PRA should be used to reduce unnecessary conservatisms associated with current regulatory requirements

This is still kind of a problem

Insights derived from PRAs are used in combination with deterministic system analysis to focus licensee and regulatory attention on issues commensurate with their importance to safety

Use risk to inform decision making, not dictate the decision

Measurable parameters monitor plant and licensee performance

Devise objective criteria to assess system performance

Based on a combination of risk insights, deterministic analysis, and performance history

Licensee flexibility to determine how to meet established performance criteria

Failure to meet a performance criterion must not result in unacceptable consequences

NPP needs to make sure when an earthquake hits that there is no care damage or release

But how a CA plant does that v an MA plant is different

Risk informed, performance based regulations

PRA challenges

Doing a PRA is wicked hard

Models the whole system including hardware failures, human performance, and relevant physical phenomena

Which is why you need all these tools

When do you know the PRA is satisfactory, complete, comprehensive?

Knowing a priori is highly subjective and very difficult

Unknown unknowns

Still a reactive process

Failures result from events exhibiting dependencies

Or from a single shared cause and coupling factor

Sequence of item failures where the first failure shifts its load to one or more nearby items such that these fail and again shift their load to other item, etc.

Cascade

Why did the item fail?

Why were several items affected?

Identify causes as part of facility or system design

Pre-operational causes stem from design, manufacturing, construction, installation

Operational causes stem from inadequate maintenance and operational procedures, execution, competence, scheduling

Redundancy and diversity

Isolation (shielding, containment, separation)

There's lots of modeling for this (bayes and binomial distribution, tables)

Putting it all together

PRA was used by aviation and nuclear industry first, but now everyone uses it

Requires in-depth knowledge of the system or process

Tools like fault/event trees, PHA, HAZOP, FMEA all contribute

We need to know what normal operation looks like

Identify deviations

Assign frequencies (with uncertainties)

Sensitivity analysis (HAZOP)

Integrate all our tools to assess risk

Identify end states

How can radiation be released?

How could people become exposed?

How could we lose a lot of money?

Characterize the system comprehensively

You've all done some of this with all the homework projects

Identify what data is going to be needed and how you would collect it

Select initiating events (hazards)

Define scenarios linking each initiating event to the end states

Apply the trees, FMEA, HAZOP

Modeling where needed

Material flow models

Transport models

Quantify risk for each initiating event

Uncertainty and sensitivity analysis

Rank risk

Farmers chart

Regulations

Peer review

Management

We have been focused largely on qualitative risk analysis

Risk assessment matrices

Being able to do this is most of the job

Eventually, frequencies have to be developed

Parameters quantified with associated uncertainties

Models defined

More specific to the system to be analyzed

Narrative research

Narrative research can be used to determine what happened

Way of understanding experience

Determining risk by looking at an event such as an airplane crash

You already did this for several examples

Narrative research incorporates personal observation, records, videos, pictures

Mitigate risk for future events

Again, still a retrospective process though

Quantitative risk analysis is needed for the Farmer's chart and regulations

Ultimately needed for Level I,II,III PRA

We have initiating events and scenarios, including human effects

We know how to obtain failure rates and process data

Higher level statistical analysis used

Like Monte Carlo

Identify distributions for relevant parameters

Run the model

Establish confidence limits

Case studies

Case study research can be used to apply a bounded system to other problems

Hyatt

Pinto $\rightarrow$ GM ignition

Dreamliner

Bay bridge

Nuclear accidents

Takata air bags

Doesn't need to be historical

Pedagogically, you want to teach fundamental principles, existing case studies

Then develop your own

So data gathering (what/importance) is important because you aren't modeling on your own, or using existing data in a model to further analyze the case

Consider repository assessment

Wide variety of engineering and scientific disciplines to be needed

Geology, chemical engineering, environmental science, nuclear engineering

Even though we've been working on small-scale projects, you should be able to expand to this level

What is important is that risk has to be defined clearly for each system