NE529
RISK ASSESSMENT
Preliminary hazards analysis
3

R. A. Borrelli

University of Idaho

Idaho Falls Center for Higher Education

Learning objectives

Interpeting PHA within the context of risk assessment

Applying PHA to engineering problems and work environment

Developing a systematic approach to risk assessment

Chapter 6 in the book

Learning nodes

Defining hazards

Risk assessment flowchart

Identifying hazards

OSHA

PHA framework
Hazards
Consequences
Procedures

Pyroprocessing example

Analysis methods
Forward
Backward
Top down
Bottom up

Lifecycle considerations

Preliminary risk quantification
Frequency estimation
Consequence estimation

Common cause failures

Visualizing risk

Hazard elimination

Criticisms

What is a hazard?

Preliminary Hazards Analysis (PHA) is a semi-quantitative analysis tool

Line item tabular inventory of non trivial system hazards and countermeasures

Best applied in the design and development stage

Early phase risk assessment tool

Identify all potential hazards and intiating events that may lead to an accident

Rank the identified events according to their severity

Can be drawn from the risk assessment matrix from before

Identify required hazard controls and follow-up actions

Systematic process to identify hazards, prioritize, and propose mitigation

Produce a Preliminary Hazard List

Leading to deeper analytical tools

Rapid risk ranking

Hazard identification

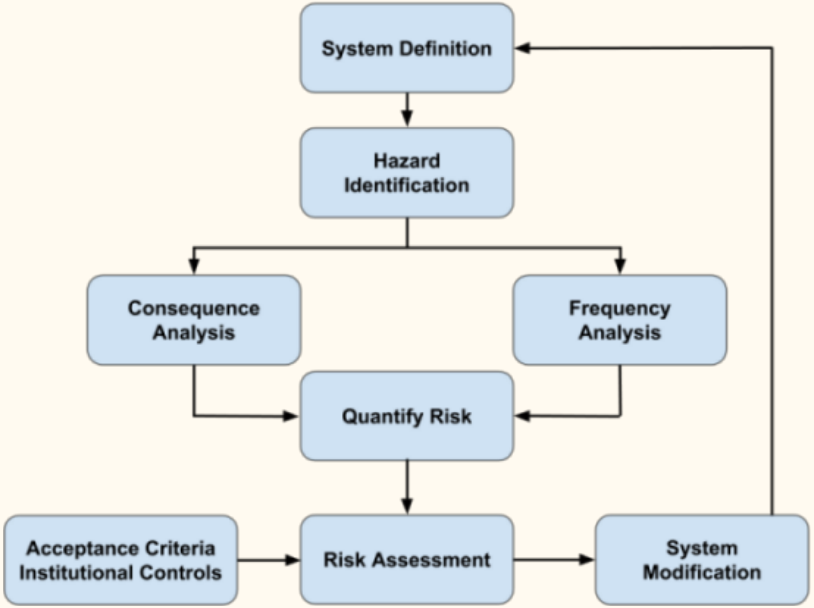
Failure Modes & Effects Analysis (FMEA)

Hazard & Operability Analysis (HAZOP)

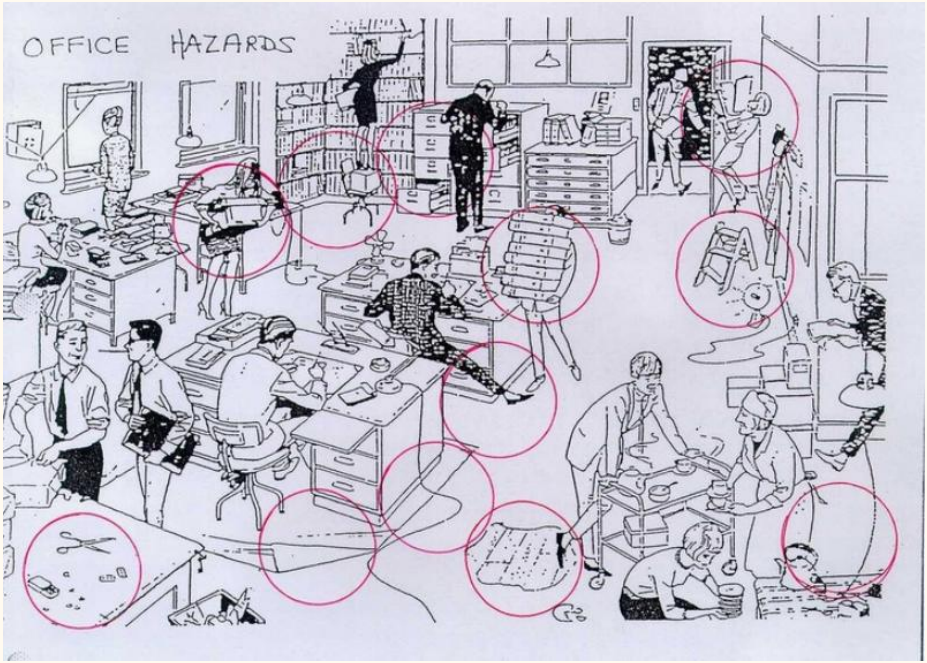
Human error analysis

Risk assessment requires continual refinement

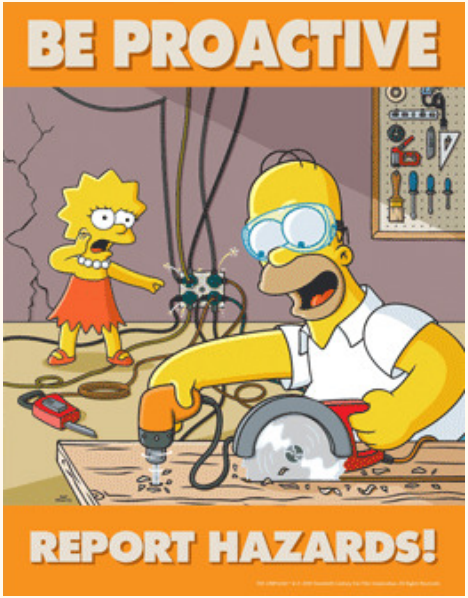
Overall risk assessment flowchart



Identify the hazards in this office space


OFFICE HAZARDS

Risk assessment is everyone's responsibility



What are some hazards OSHA might cite?

OSHA top 10 warehouse citations

(1) Forklifts
(2) Hazard communication
(3) Electrical – wiring methods
(4) Electrical – system design
(5) Guarding floor, wall openings, holes
(6) Exits
(7) Mechanical power transmission
(8) Lockout, tagout
(9) Respiratory protection
(10) Portable fire extinguishers


Check your workplace for hazards
overhead services
entry/exit access
surrounding structures
dangerous materials
facilities
people
obstructions
other equipment
www.easyguides.com.au

PHA framework

PHA is used as an initial risk study in the early stages of the project

Initially developed by US Army

‘Army had half day, Mother!’

Used to review process areas of energy released in uncontrolled manner

Identify hazards and consequences

Start as early as possible in system life cycle

Adapt PHA to the system under study

Not everything is applicable to every system

Identify hazardous components or system elements

Facility related hazards and surrounding property

Interfaces between system elements related to safety (software)

Operational & supporting equipment

Safety equipment and related safeguards

Environmental & operational constraints

Leading to potential malfunctions to system and components

Hazards

Identify potential hazards where energy may be released

Mechanical moving parts

Material incompatibilities

Nuclear radiation

Electromagnetic radiation (laser, radio, UV)

Collisions from movement of personnel, equipment, automation

Toxic materials, corrosive liquids; gases stored, generated

All sorts of deterioration

Subsonic or supersonic noise

Biological, bacterial growth

Human error

Software, network, cyber-based

Identify hazardous states of a system as part of the conceptual design phase

Inputs

Boundaries between the system(s)

System interaction and dependencies

System domain

System functionality for each component and holistically

Layout

Process flow

Output

Identify where each hazard will occur

Significance

Method to eliminate or mitigate

How associated risk will be controlled

Consequences

Identify consequences that may occur from each hazard

Estimate frequency of hazards

Estimate of the severity of each event

Compare initial design concepts

Focus on important risk issues

You might be able to easily mitigate some events right at the start

Consider PHA to be the base level of risk analysis

It is not sufficient but a necessary start

Assign each consequence a severity categorization

Quantify frequency of each accident sequence

Assign each hazard a preliminary random and systematic probability target

Propose safety features needed during the design and development phase

You want to be able to head off low risk that can be mitigated by design and high risk that needs more work

Procedures

Identify procedures related to operations, testing, maintenance, system diagnostics, emergencies

Obtain potential related data cohorts

Reports, accident statistics, regulatory reviews if you know someone

Or existing systems and PHAs

Bring in some experts for an outside review

Model energy or material flow in the system and develop operational modes

Review facility technical specifications if they are available

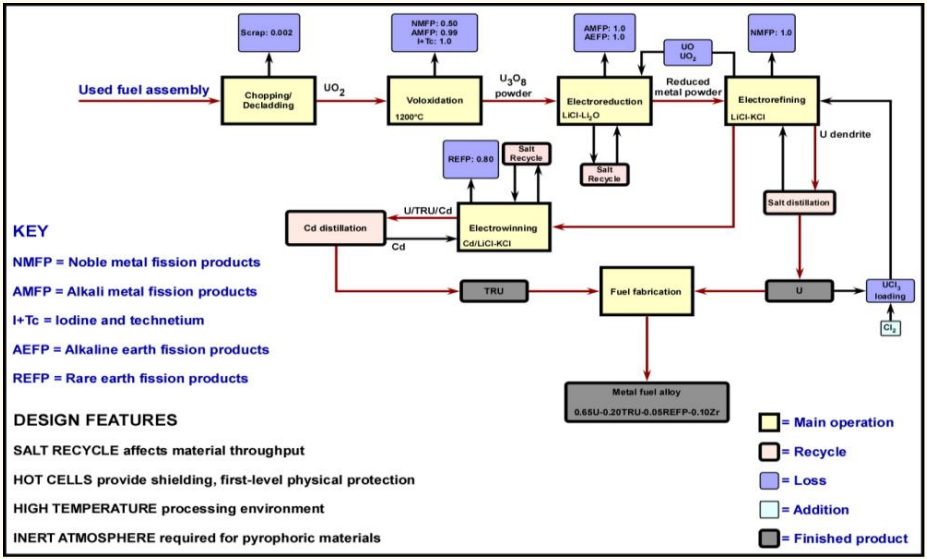
Not so easy even though ‘qualitative’

PHA is most effectively used during the initial development of a process and the procedures for performing that process

List the hazards and not to analyze each step in the procedure

Very top-level analysis, but when done properly, very useful for more comprehensive PRA

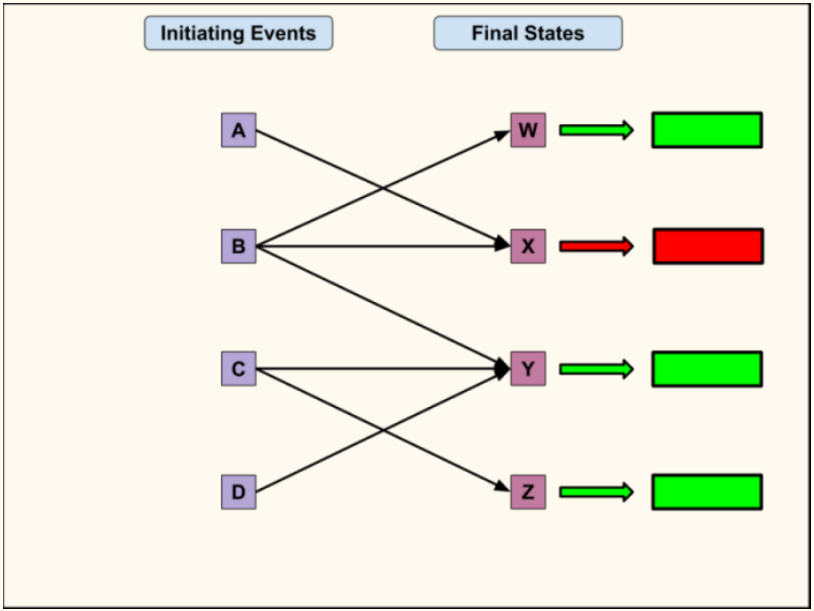
Would we really need this with mature systems?


Scrap: 0.002
NMFP: 0.50
AMFP: 0.99
I+Tc: 1.0
AMFP: 1.0
AEFP: 1.0
UO
UO2
NMFP: 1.0
Used fuel assembly
Chopping/
Decladding
UO2
Voloxidation
1200°C
U3O8
powder
Electroreduction
LiCl-Li2O
Reduced
metal powder
Electrorefining
LiCl-KCl
U dendrite
REFP: 0.80
Salt
Recycle
Salt
Recycle
Salt distillation
U/TRU/Cd
Cd distillation
Cd
Electrowinning
Cd/LiCl-KCl
KEY
NMFP = Noble metal fission products
AMFP = Alkali metal fission products
I+Tc = Iodine and technetium
AEFP = Alkaline earth fission products
REFP = Rare earth fission products
TRU
Fuel fabrication
U
UCl3
loading
Cl2
Metal fuel alloy
0.65U-0.20TRU-0.05REFP-0.10Zr
DESIGN FEATURES
SALT RECYCLE affects material throughput
HOT CELLS provide shielding, first-level physical protection
HIGH TEMPERATURE processing environment
INERT ATMOSPHERE required for pyrophoric materials
= Main operation
= Recycle
= Loss
= Addition
= Finished product

Analysis methods

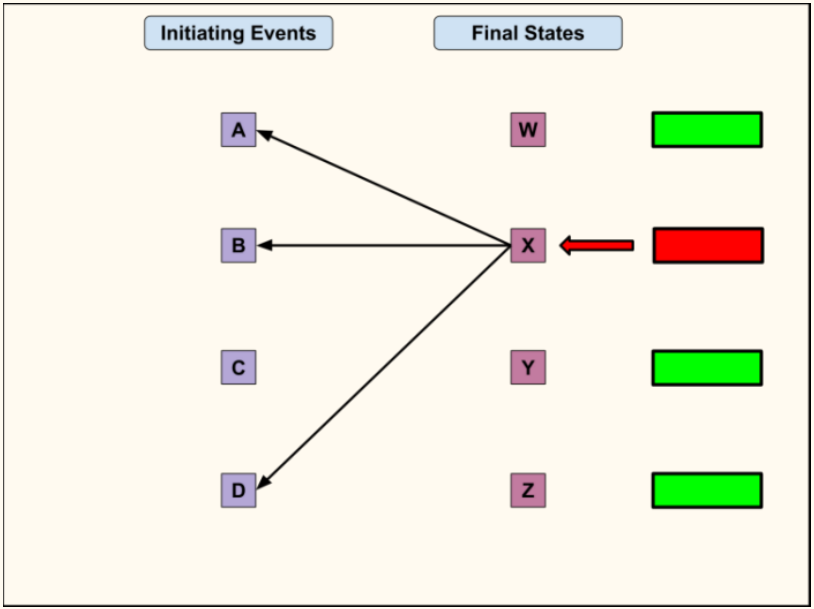
Forward

Forward analysis identifies events then consequences



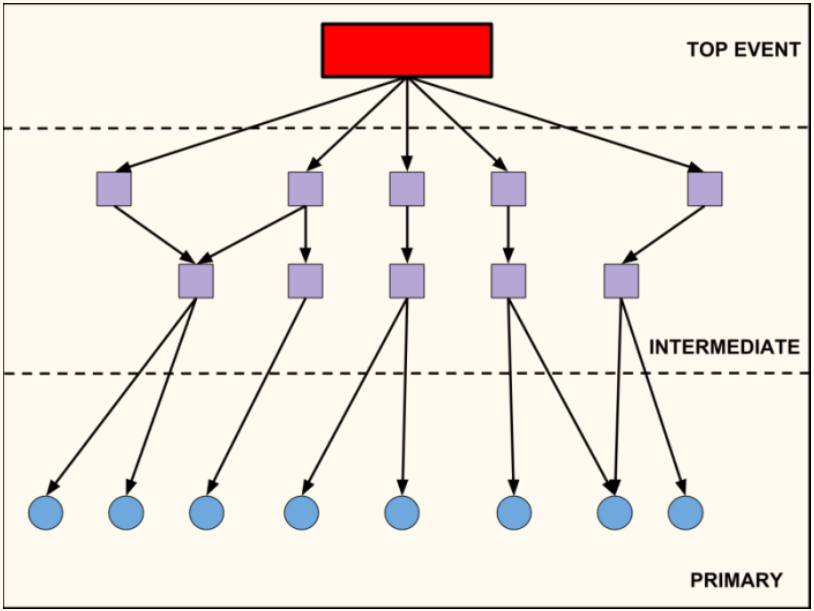
Backward

Backward analysis identifies hazards to find events



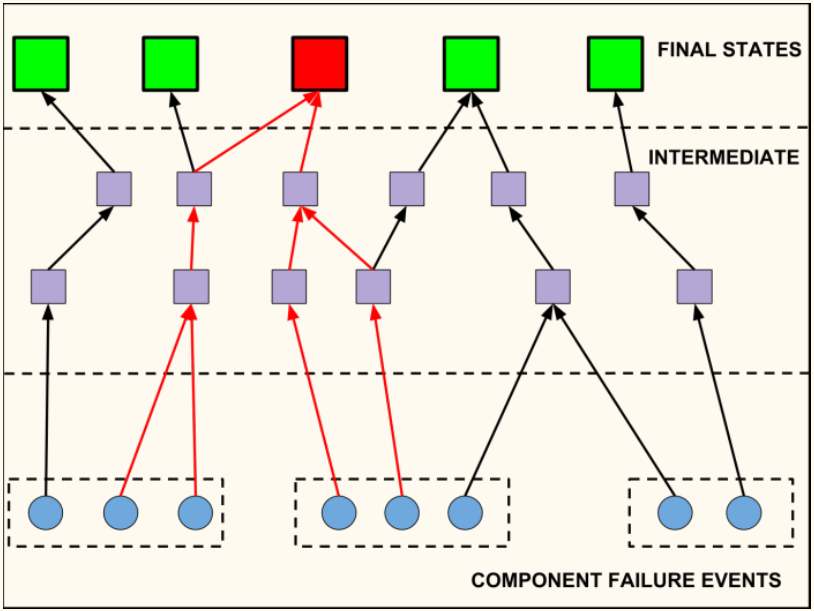
Top down

Use top down analysis to decompose the events



Bottom up

Use bottom up analysis to decompose the hazard



Lifecycle considerations

PHA should take place during different stages in the lifecycle

New facilities as part of design before committing resources

During construction, things are going to come up that were not anticipated

We know what we know
We know what we don't know
We don't know what we don't know

Operational readiness must be conducted prior to system start up

Periodic analysis during operational lifetime

Maybe due to regulations

Anytime there is a modification

Safety analysis at USA nuclear plants after Fukushima

NRC regulations for technical specification, performance based goals, best practices

Finally, when decommissioning new hazards will arise

Disposal of materials, chemicals, etc.

Preliminary risk quantification

Frequency estimation

Estimate probability of occurrence

$< 10^{-6}$ – less than credible

Not expected during facility lifetime

$10^{-6} - 10^{-4}$ – credible and extremely unlikely

Probably not occur during facility lifetime

$10^{-4} - 10^{-2}$ – credible and unlikely

May occur once during facility lifetime

Natural phenomena

Trained worker error

$10^{-2} - 10^{-1}$ – very likely

Events may often occur

You can just guess at the start

Frequent – occurs often

Likely – occurs several times

Occasional – occurs sporadically

Seldom – not negligible but unlikely

Unlikely – neglibible

Consequence estimation

Rank hazards in terms of qualitative consequences or severity

Class I – Negligible

Worst case effects cause less than minor injury, occupational illness, system damage

Class II – Marginal effects

Worst case effects cause minor occupational illness, system damage

Class III – Critical

Worst case effects cause severe (nondisabling) personnel injury, severe occupational illness, major system damage

Class IV – Catastrophic

Worst case effects cause death, disabling injury, system loss

Most reliable solution is to eliminate source of hazard

Common cause failures

Beware common cause events or multiple consequences

Different events may lead to similar consequences

Ranking hazards needs a normalized metric

So severity must be carefully determined

Consequences should be characterized as precisely or descriptively as possible

Estimate the frequency that initiating event produces a specific consequence

This means that for each initiating event, there might be several consequences with associated frequencies

Example for a typical warehouse environment

Worker (sober) falls off a ladder

Risk = low severity but moderate frequency

Could be fatal, but low frequency, not negligible

Both should be considered in PHA

How can this risk be mitigated?

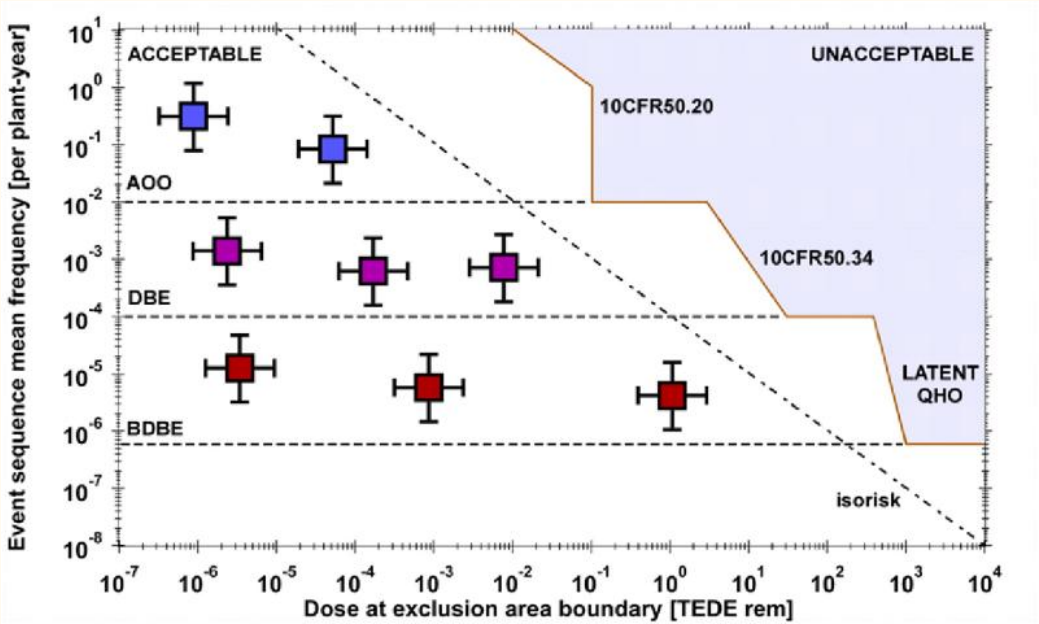
Maybe you have a separate section where fatalities are considered

How else could this be classified?

Visualizing risk

Clearer comparisons can be made now

0 – 5 = Low Risk 6 – 10 = Moderate Risk 11 – 15 = High Risk 16 – 25 = extremely high unacceptable risk		Severity of the potential injury/damage				
		Insignificant damage to Property, Equipment or Minor Injury **1**	Non-Reportable Injury, minor loss of Process or slight damage to Property **2**	Reportable Injury moderate loss of Process or limited damage to Property **3**	Major Injury, Single Fatality critical loss of Process/damage to Property **4**	Multiple Fatalities Catastrophic Loss of Business **5**
Likelihood of the hazard happening	Almost Certain **5**	5	10	15	20	25
	Will probably occur **4**	4	8	12	16	20
	Possible occur **3**	3	6	9	12	15
	Remote possibility **2**	2	4	6	8	10
	Extremely Unlikely **1**	1	2	3	4	5


ACCEPTABLE
UNACCEPTABLE
10CFR50.20
10CFR50.34
AOO
DBE
BDBE
LATENT
QHO
isorisk
Event sequence mean frequency [per plant-year]
Dose at exclusion area boundary [TEDE rem]
10^{1}
10^{0}
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
10^{-7} 10^{-6} 10^{-5} 10^{-4} 10^{-3} 10^{-2} 10^{-1} 10^{0} 10^{1} 10^{2} 10^{3} 10^{4}

Hazard reduction

How can hazards be eliminated?

Substitution

Use safe materials

Simple hardware devices may be safer than using a computer

No technological imperative that says we MUST use computers to control dangerous devices

Introducing new technologies increases unknowns

Simplify

Limit process states

Easily understood and readable

Interactions between components are limited and straightforward

Code includes only minimum features and capability required by system

No unnecessary, undocumented features, unused executable code

Worst case timing is determinable

Design so that structural decomposition matches functional decomposition

How else can hazards be eliminated?

Decouple
Tightly coupled system is one that is highly interdependent
Failure or unplanned behavior in one can rapidly affect status of others
System accidents caused by unplanned interactions
Coupling creates increased number of interfaces and potential interactions

Passive safeguards
Fail to a safe state

Redundancy and diversity

Human error

Criticisms

What's so good about PHA?

Helps ensure that the system is safe

Modifications are less expensive and easier to implement in earlier design stages

Decreases design time by reducing the number of surprises

Identifies and provides a log of primary system hazards and corresponding risks

Provides systematic evaluation early enough to allow for design mitigation (Rokkasho)

Provides information to management to make decisions to allocate resources to reduce risk

Provides relatively quick review of most significant system risks

What's not so good about PHA?

Hazards must be foreseen by the analysts

Effects of interactions between hazards are not easily recognized

You don't know what you don't know

Can fail to assess risks well of combined hazards of common failure modes

Then underrepresent overall system risk

Insufficient or inappropriate targets chosen; assessment is flawed

Garbage in = garbage out

Wrong assumptions for unknown data, etc.

Too many targets, PHA becomes large and costly

Which misses the point