NE529
RISK ASSESSMENT
HRA & HAZOP
6

R. A. Borrelli

University of Idaho

Idaho Falls Center for Higher Education

University of Idaho
Department of Nuclear Engineering
and Industrial Management

Learning objectives

Chapter 12 in the book

Applying HRA and HAZOP

Analyzing systems peformance

Assessing human reliability as part of risk

HAZOP is not in the book

See OER for more information

Learning nodes

Human Reliability Analysis
LOCA
Task analysis

Human error probability

Common cause

HAZOP
Flowchart
Flash drum example
Safeguards
Record keeping
Pyroprocessing
Advantages
Drawbacks

Human Reliability Analysis (HRA)

HRA is an important part of PRA

Based on human error probability

PRA $\rightarrow$ equipment failure

HRA $\rightarrow$ analyze people response to equipment failure

Though an initiating event in PRA could be due to people

HRA can identify activities where human error can be reduced

HRA 'system' is series of steps or actions that involve the potential for human failure

Pump trips in a reactor facility

Personnel would start the other pump and then maybe untrip the first one

PRA tells us the sequence resulting in the trip with an event tree maybe

HRA tells us how the personnel would screw up fixing it

What would be the best way to reduce probability of human error?

Dreamliner documentary talking about where to score drugs

LOCA

LOCA is the worst accident at the reactor

Initiating event – Rupture in coolant pipes (12.1.3)

How could that happen?

Pipe ruptures (somewhere)

Drywell pressure reaches 2 psig – provides pressure suppression system and fission product barrier BWR

Emergency Core Cooling System (ECCS) initiates

SCR signal initiates

Containment building isolates

Emergency ventilation systems start

Probably could construct and event tree since these are all success/fail

Operators have a bunch to do if a LOCA occurs

Verify ECCS inititates

SCR actions

Verify containment isolation

Verify emergency ventilation starts

Numerous manual actions all with potential for error

Passive safety therefore is a big deal at reactors

AP1000 has numerous passive safety upgrades from Generation III designs

EBR-II experiment

Operators have to act if automatic systems fails

Like turning on the emergency ventilation systems

For loss of onsite power, which would kill the pumps, someone may have to start generators

Which was hard to do at Fukushima because they were flooded

Even though these are fairly straightforward procedures there is a lot happening quickly with personnel

Which leads to error

As much passive safety as there can be, human action is always going to be required at some level

Each HRA must be ‘bounded’ and have measurable start and end states

Start point and metric for success of each step is distinctly identified

For SCR –

(1) Control rods inserted into core (automatic)
(2) Operator places reactor mode switch to shutdown position
(3) Verify all control rods fully inserted
(4) Verify reactor power is decreasing
(5) Operator inserts low power level monitors
(6) Verify reactor vessel (coolant) level to be within the correct band
(7) Verify reactor pressure to be within the correct band
(8) Verify reactor coolant pumps shift to slow speed
(9) Shift feed water control system to single element

You need an HRA for each step

Then assess total human failure probability for SCR

Same procedure for each event in the pipe rupture sequence

Then obtain failure probability of LOCA

All of this will be defined as an accident sequence in a PRA

Task analysis

‘Task analysis’ identifies personnel actions into basic steps

Derive the smallest set of actions (very detailed)

Walk through the overall procedure and list what needs to be done

Include what to do if personnel fails to achieve each step in the procedure

12.2 in the book shows how to do this for ‘verifying all rods are inserted’ (coming up next)

It seems overly much, but you need all this precise actions to get operating license

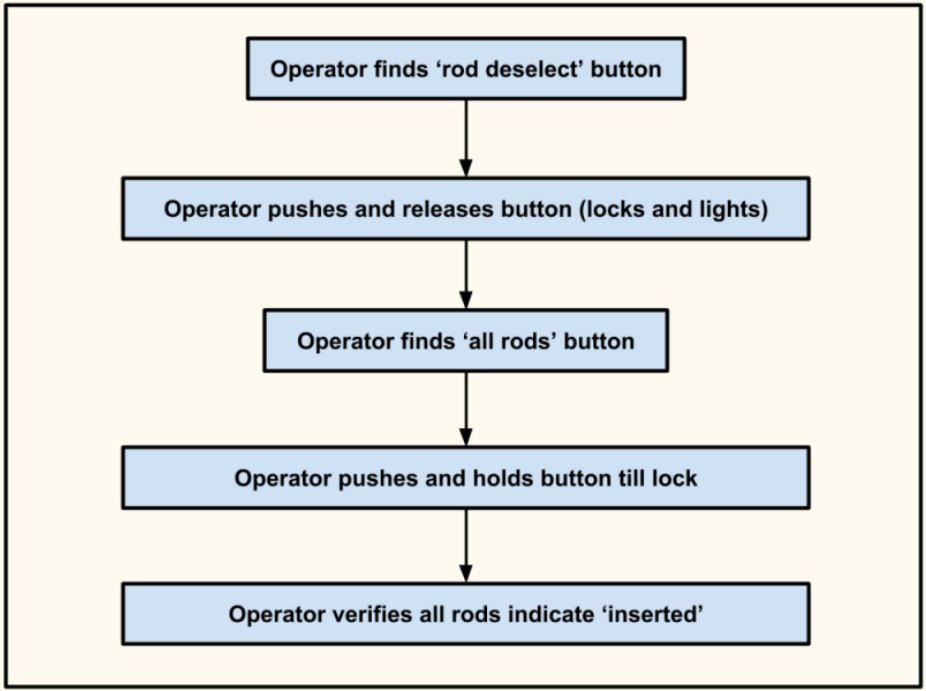
Walkthrough with experienced personnel

You don’t want to be ‘umm, what’s first now’ when an accident happens (muscle memory)

‘User error’ for a nuclear reactor accident has enormous social implications

Three Mile Island and Chernobyl

We had all this on our research reactor, but there was only one big button


Operator finds ‘rod deselect’ button
Operator pushes and releases button (locks and lights)
Operator finds ‘all rods’ button
Operator pushes and holds button till lock
Operator verifies all rods indicate ‘inserted’

Task analysis validates operator actions

Figure 12.1

Operators must validate the sequence

A lot to do in just one NPP

Why do we need to be so detailed?

What would cause a failure?

Picture break


CAUTION

Visually depict each task as a failure with applicable recovery actions

HRA model needs to visually depict each task as a failure with applicable recovery actions

Potential human errors and their mechanisms

Recovery paths if error occurs

Quantify error (frequency)

What would be the errors and recovery acts for the SCR rods sequence?

Could make an event tree or fault tree from this

Though fault tree would be just one and gate (figure 12.3) for failure to verify rod insertion

Human error probability

Human error probability is difficult to quantify

Because people generally behave stupidly even sober

Or, different responses are elicited by people in the same environment

What would be examples of human errors that could be quantified?

Astronaut behavior in normal conditions and critical conditions

Psychological stress

Performance shaping factors account for human response to stressors

hot/cold
noise level
light level (my office is dark)
vibration
ergonomics
experience and training
management
time
stress
equipment design/human machine interface

Now, we need to figure out probabilities

Each task then would have an associated probability

Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications

‘The completion cue or sign for the task or activity is simple and unambiguous.’

Not identifying buttons may be due to labeling, or whether they’re lit up

Also need to establish what everything looks like under normal operations

NPPs have certain instrumentation and processes not found in other facilities

Now what happens when control panels are digitized?

Increasing complexity with human error happens fast

THERP tables

Operator fails to find Rod Deselect button = 0.003 Table 20-12 item 2

Obtaining human error data is really the same as equipment failure rates

Search historical data for the task

Expert advice

We could ask people who have worked on manipulators for hot cells

Simulations of the activity can be performed and data collected

Now, there are tons of PRAs to study for related activities

Delphi studies

Performance shaping factors affect human error

hot/cold
noise level
light level (my office is dark)
vibration
ergonomics
experience and training
management
time
stress
equipment design/human machine interface

How can we reduce human error?

Is there a procedure that is followed?

Pre-start checklist, log, and shutdown for WPI reactor

If there is an error in reactor operation, the checklist could show that

Procedures have to be memorized though

Is there time pressure to complete the sequence?

SCR actions need to be completed in about 3 minutes

So you need to know your actions

Familiarity can lead to cutting corners and errors

Common cause

Avoid dependencies

Dependence is relationship between tasks Chapter 10 NUREG

Now we have a new problem with reactor controls going digital

New cyberattacks from new equipment

How do operators identify a cyberattack?

How do they respond?

We need to make sure we identify the most critical procedures to analyze

Don't want to waste money on simple tasks

HAZOP

HAZOP identifies hazards without waiting for an accident to occur

Developed by Imperial Chemical Industries in early 1960s

Not only for safety, but efficient operations

Accidents caused by deviations from design/operating intentions

Identifying potential hazards and operability problems caused by deviations from the design intent of both new and existing process plants

Essential feature to review process drawings and/or procedures

Identify all possible deviations from normal operation and associated hazards

‘What if’ analysis for system parameters

What if ‘temperature’ of ‘reactor’ ‘rises’?

System realization of perturbation (or sensitivity analysis)

Requires flow model of operating plant

So this is not something done too early on in design phases

But can affect design

Later on in the life cycle if facility upgrades/retrofits have been made

For use with PHA & FMEA and provides input to event trees too

Can offer some options to mitigate hazards

HAZOP seems to me to be a limited fit for industrial facilities/reactors

HAZOP is a structured and systematic technique for examining a defined system

Identify potential hazards in the system

Identifying potential operability problems with the system, causes of operational disturbances, and production deviations

Ensure that all relevant deviations of process parameters are evaluated

Causes of deviations are human error, equipment failure, external events

Deviation = Guideword + Parameter

Operability is any process inside the design envelope that would cause a shutdown

Where a shutdown could possibly lead to a violation of environmental, health or safety regulations or negatively impact profitability

Also called licensing basis envelope

More about system operation than safety

HAZOP deals with the identification of potential deviations from the design

Intent, examination of causes, and assessment of consequences

Improve operating procedures or when modifying plant

Identify possible improvements where accident rate is abnormally high

Time consuming and can be tedious (Theo from Simplot)

Generates many failure events with insignificant risk

Again, can miss common cause failures

Tends to ignore contributions that can be made by operator interventions

HAZOP has a logical structure like event and fault trees

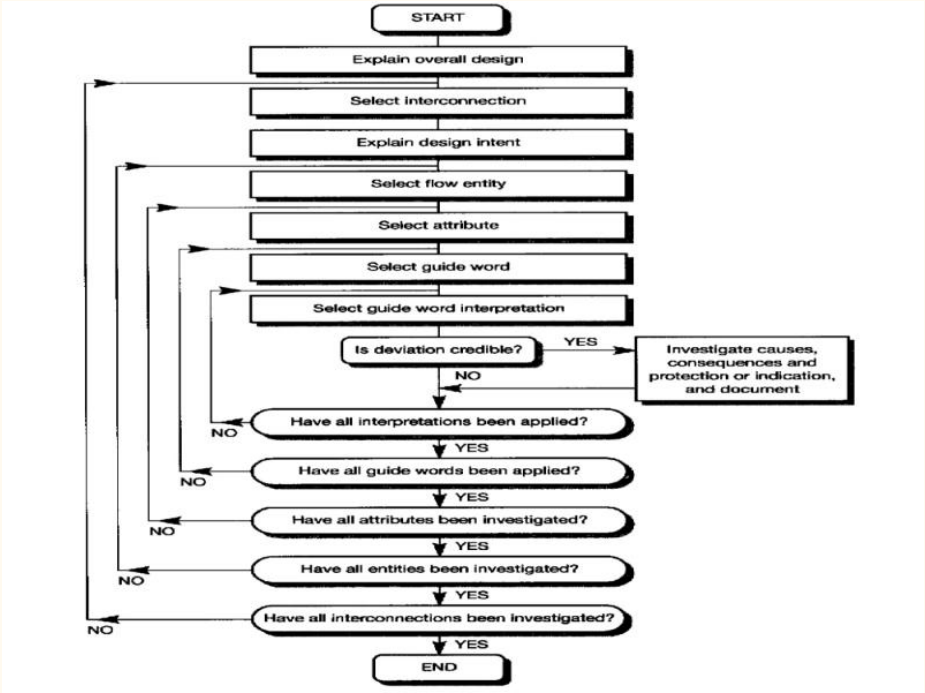
Flowing/process items are ‘entities’ (study nodes)

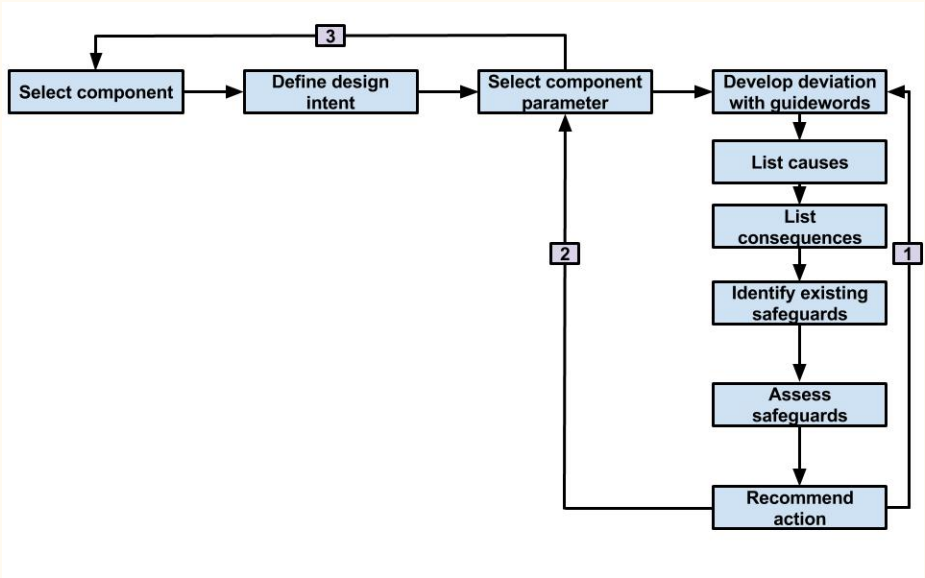
Entities have characteristic properties known as ‘attributes’

Analysis based on possible deviations of attribute values (sensitivities)

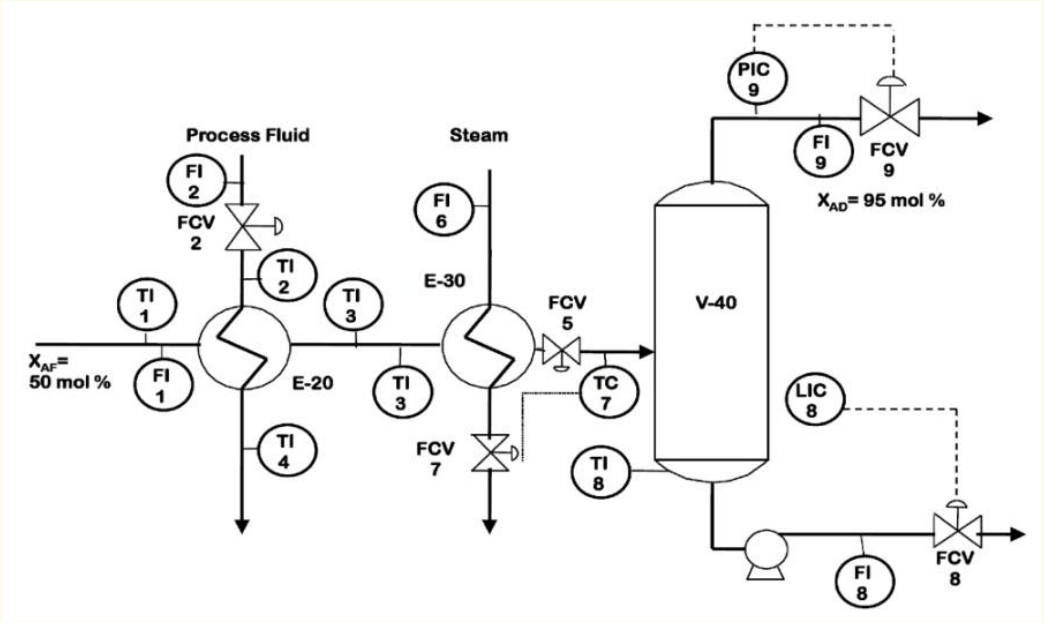
‘Guide words’ used to guide the analysis and designed to capture dimensions of variation

Flowchart


START
Explain overall design
Select interconnection
Explain design intent
Select flow entity
Select attribute
Select guide word
Select guide word interpretation
Is deviation credible?
YES
Investigate causes, consequences and protection or indication, and document
NO
Have all interpretations been applied?
NO
YES
Have all guide words been applied?
NO
YES
Have all attributes been investigated?
NO
YES
Have all entities been investigated?
NO
YES
Have all interconnections been investigated?
NO
YES
END


3
Select component
Define design intent
Select component parameter
Develop deviation with guidewords
List causes
List consequences
Identify existing safeguards
Assess safeguards
Recommend action
2
1

Flash drum example


Process Fluid
Steam
FI 2
FCV 2
TI 2
TI 1
TI 3
E-30
FI 6
FCV 5
V-40
PIC 9
FI 9
FCV 9
X_{AD}= 95 mol %
X_{AF}= 50 mol %
FI 1
E-20
TI 3
TC 7
LIC 8
TI 4
FCV 7
TI 8
FI 8
FCV 8

HAZOP analysis process for flash drum

(1) Select component – Flash drum

(2) Define design intent – The flash drum separates light and heavy materials

(3) Select component parameter – Pressure

(4a) Develop deviation with guidewords
More/high pressure

(4b) List causes – Valve is stuck closed; Feed temperature too high
Within or outside boundary
Derived from independent variables

(4c) List consequences – Explosion
Process hazards
Operability problems

HAZOP analysis process for flash drum

(4d) Identify existing safeguards – Temperature control; Pressure control
Safeguards reduce risk

(4e) Assess safeguards – Are the controls adequate? No.

(4f) Recommend action – Relief valve; Alarm
Action to remove cause, mitigate consequence

Return to 4a until all deviations have been analyzed under the component parameter

Return to 3 and identify new component parameter

Return to 1 and select new component

Safeguards

There are five types of safeguards

IDENTIFY
alarm instrumentation
human operator detection

COMPENSATE
automatic control system

PREVENT
inert blanket gas in storage of flammable substances – AP1000 water blanket

DESCALATION
trip of the activity – SCR

RELIEVE
pressure safety valves
vent systems

Record keeping

You can set up a chart

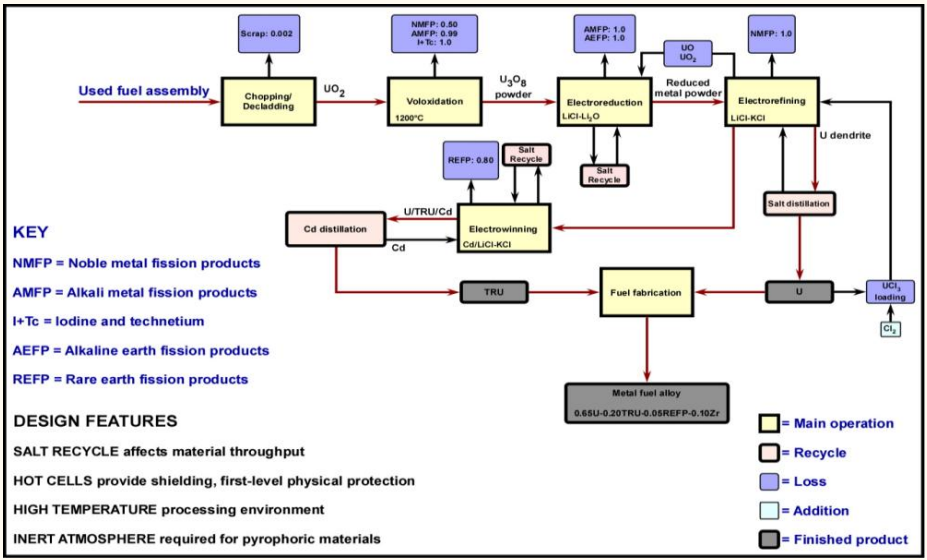
Recording sheet

Chemical reactor

Heat exchanger

P&ID schematic

Pyroprocessing


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
Electrowinning
Cd/LiCl-KCl
Cd
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

HAZOP analysis process for pyroprocessing injection casting

(1) Select component – Injection casting

(2) Define design intent – Manufacture metal fuel slugs that contain U+TRU

(3) Select component parameter – Temperature

(4a) Develop deviation with guidewords
Less temperature

(4b) List causes – Heater malfunction; Fails to start; Starts late; Power source failure
Within or outside boundary
Derived from independent variables

(4c) List consequences – Metal is not totally melted; Quartz molds break; Spill liquid metal
Process hazards
Operability problems

HAZOP analysis process for pyroprocessing injection casting

(4d) Identify existing safeguards – Unknown
Safeguards reduce risk

(4e) Assess safeguards – None

(4f) Recommend action – Instrumentation; Human detection
Action to remove cause, mitigate consequence

Return to 4a until all deviations have been analyzed under the component parameter

Return to 3 and identify new component parameter

Return to 1 and select new component

Select temperature

Deviation – LESS+TEMPERATURE — Low temperature

Causes – Heater fails to start; Heater starts late; Power source not available

Consequences – Metal not melted; Quartz molds break; Molten TRU spill

Protection – Unknown

Action – Install temperature indicator; Human detection; Positive injection operation

Select time

Deviation – LESS+TIME — Short injection time

Causes – Operator error; Motor trip

Consequences – Not enough metal injected into molds; Waste of material

Protection – Unknown

Action – Install timer; Human detection; Positive mold removal operation

Advantages

What's good about HAZOP

Considers more than failure accidents

Process and operation deviations

Can identify new hazards

Not limited to previously identified hazards

A simple method that can uncover complex accidents

Applicable to new designs and new design features

Disadvantages

What are the drawbacks?

Requires detailed plant information

Flowsheets, piping and instrumentation diagrams, plant layout

Tends to result in protective devices rather than real design changes

Relies very heavily on judgment of engineers (and?)

Unusual to consider deviations for systemic factors

Organizational, managerial factors, management systems

Difficult to apply to software (not really an automated procedure)

Human behavior reduces to compliance/deviation from procedures

Does not account for human performance factors