Hazard Log Information

- System, subsystem, unit
- Description
- Cause(s)
- Possible effects, effect on system
- Category (hazard level)
- Safety requirements and design constraints
- Corrective or preventative measures, possible safeguards, recommended action
- Operational phase when hazardous
- Responsible group or person for ensuring safeguards provided.
- Tests (verification) to be undertaken to demonstrate safety.
- Other proposed and necessary actions
- Status of hazard resolution process.

System Hazard Analysis

- Builds on PHA as a foundation (expands PHA)
- Considers system as a whole and identifies how
  system operation
  interfaces and interactions between subsystems
  interface and interactions between system and operators
  component failures and normal (correct) behavior
  could contribute to system hazards.
- Refines high-level safety design constraints
- Validates conformance of system design to design constraints
- Traces safety design constraints to individual components.
  (based on functional decomposition and allocation)
Models

- Provide a means for
  - Understanding phenomena
  - Recording that understanding so can communicate to others

- All models are abstractions
  - Omit assumed irrelevant details
  - Focus on features of phenomenon assumed most relevant
  - Selection process usually arbitrary and dependent on choice of modeler
  - Selection is critical in determining usefulness and accuracy of model

Accident models

- Underlie all attempts to engineer for safety.
- Used to explain how accidents occur.
- Assume common patterns in accidents; not just random events
  - Imposing pattern on accidents influences factors considered in safety analysis
  - Model may act as filter and bias toward considering only some events and conditions
    or
  - May force consideration of factors often omitted.
Accident models (2)

• Forms basis for:
  – Investigating and analyzing accidents
  – Preventing accidents
    • Hazard analysis
    • Design for safety
  – Assessing risk (determining whether systems are suitable for use)
  – Performance auditing and defining safety metrics

• So influences causes identified, countermeasures taken, and risk evaluation

• May not be aware using model, but always exists

Chain–of–Events Models

• Explain accidents in terms of multiple events, sequenced as a forward chain over time.
  – Simple, direct relationships between events in chain
  – Contrapositive (if A hadn’t occurred, then B would not have)

• Events almost always involve component failure, human error, or energy–related event

• Form the basis of most safety–engineering and reliability engineering analysis:
  e.g., Fault Tree Analysis, Probabilistic Risk Assessment, FMEA, Event Trees

and design:
  e.g., redundancy, overdesign, safety margins, ...
Chain–of–Events Example

Reason’s "Swiss Cheese" Model
Hazard (Causal) Analysis

• "Investigating an accident before it happens"

• Requires
  - An accident model
  - A system design model (even if only in head of analyst)

• Almost always involves some type of search through the system design (model) for states or conditions that could lead to system hazards.
  - Forward
  - Backward
  - Top–down
  - Bottom–up

• Can be used to refine high–level safety constraints into more detailed constraints.

---

Forward vs. Backward Search

<table>
<thead>
<tr>
<th>Initiating Events</th>
<th>Final States</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>W nonhazard</td>
</tr>
<tr>
<td>B</td>
<td>X HAZARD</td>
</tr>
<tr>
<td>C</td>
<td>Y nonhazard</td>
</tr>
<tr>
<td>D</td>
<td>Z nonhazard</td>
</tr>
</tbody>
</table>

Forward Search

<table>
<thead>
<tr>
<th>Initiating Events</th>
<th>Final States</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>W nonhazard</td>
</tr>
<tr>
<td>B</td>
<td>X HAZARD</td>
</tr>
<tr>
<td>C</td>
<td>Y nonhazard</td>
</tr>
<tr>
<td>D</td>
<td>Z nonhazard</td>
</tr>
</tbody>
</table>

Backward Search
Top–Down

Intermediate or pseudo-events

Basic or primary events

Bottom–Up

Component failure events
Fault Tree Analysis

- Developed originally in 1961 for Minuteman.
- Top–down search method.
- Based on converging chains–of–events accident model.
- Tree is simply a record of results; analysis done in head.
- FT can be written as Boolean expression and simplified to show specific combinations of identified basic events sufficient to cause the undesired top event (hazard).
- If want quantified analysis and individual probabilities for all basic events are known, frequency of top event can be calculated.

Example:

**Hazard:** Explosion

**Design:**
System includes a relief valve opened by an operator to protect against overpressurization. A secondary valve is installed as backup in case the primary valve failed. The operator must know if the first valve does not open so the second valve can be activated.

Operator console contains both a primary valve position indicator light and a primary valve open indicator light.
Fault Tree Example

Critical Function: RCS Jet Firing (from NSTS 22254)
Fault Tree Example

Explosion

and

Pressure too high

Relief valve 1 does not open

or

Relief valve 2 does not open

or

Valve failure

Computer does not open valve 1

or

Valve failure

Operator does not know to open valve 2

or

Operator inattentive

Sensor Failure

Computer output too late

and

Computer does not issue command to open valve 1

and

Valve 1 Position Indicator fails on

and

Open Indicator Light fails on

Example Fault Tree for ATC Arrival Traffic

A pair of controlled aircraft violate minimum separation standards

OR

Violation of minimum in–trail separation while on final approach to same runway

OR

Violation of distance or time separation between streams of aircraft landing on different runways

OR

Violation of minimum separation between arrival traffic and departure traffic from nearby feeder airports.

OR

Two aircraft on final approach to parallel runways not spatially staggered.

Two aircraft landing consecutively on different runways in intersecting or converging operations violate minimum difference in threshold crossing time.

An aircraft violates the non–transgression zone while airport is conducting independent ILS approaches to parallel runways.

An aircraft fails to make turn from base to final approach.
System Hazard Analysis

"On U.S. space programs where FTA (and FMEA) were used, 35% of actual in-flight malfunctions were not identified or were not identified as credible."

See http://sunnyday.mit.edu/nasa-class/follensbee.html (list of aircraft accidents with risk of $10^{-9}$ or greater)
Example of unrealistic risk assessment contributing to an accident

System design:
Previous overpressurization example

Events:
The open position indicator light and open indicator light both illuminated. However, the primary valve was NOT open, and the system exploded.

Causal Factors:
Post–accident examination discovered the indicator light circuit was wired to indicate presence of power at the valve, but it did not indicate valve position. Thus, the indicator showed only that the activation button had been pushed, not that the valve had opened. An extensive quantitative safety analysis of this design had assumed a low probability of simultaneous failure for the two relief valves, but ignored the possibility of design error in the electrical wiring; the probability of design error was not quantifiable. No safety evaluation of the electrical wiring was made; instead confidence was established on the basis of the low probability of coincident failure of the two relief valves.

Event Tree Analysis

- Developed for and used primarily for nuclear power.
- Underlying single chain of events model of accidents.
- Forward search
- Simply another form of decision tree.
- Problems with dependent events.
Event Tree Example

1. Pipe break
2. Electric power
3. ECCS
4. Fission product removal
5. Containment integrity

Initiating event

- Available
  - 1 - P2
  - Fails
    - P3

- Fails
  - P2
Event Trees vs. Fault Trees

- Relief valve 1
  - Opens
  - Pressure decreases
  - Fails
  - Pressure decreases
  - Fails
  - Explosion

- Relief valve 2
  - Opens
  - Pressure decreases
  - Fails
  - Explosion

- Pressure too high
  - Relief valve 1 does not open
    - Valve failure
      - Computer does not open valve 1
        - Pressure monitor failure
        - Computer output too late
        - Computer does not issue command to open valve 1
      - Valve failure
        - Valve 1 position indicator fails on
        - Open indicator light fails on
  - Relief valve 2 does not open
    - Operator does not know to open valve 2
      - Operator inattentive
ETA Evaluation

- Events trees are better at handling ordering of events but fault trees better at identifying and simplifying event scenarios.

- Practical only when events can be ordered in time (chronology of events is stable) and events are independent of each other.

- Most useful when have a protection system.

- Can become exceedingly complex and require simplication.

ETA Evaluation (2)

- Separate tree required for each initiating event.
  - Difficult to represent interactions between events
  - Difficult to consider effects of multiple initiating events.

- Defining functions across top of event tree and their order is difficult.

- Depends on being able to define set of initiating events that will produce all important accident sequences.
  
    Probably most useful in nuclear power plants where
    - all risk associated with one hazard (overheating of fuel)
    - designs are fairly standard
    - large reliance on protection systems and shutdown systems.
Cause–Consequence Analysis

- Used primarily in Europe.
- A combination of forward and top–down search.
  Basically a fault tree and event tree attached to each other
- Again based on converging chain–of–events.
- Diagrams can become unwieldy.
- Separate diagrams required for each initiating event.

---

**Cause–Consequence Diagram**

```
Uncontrolled reaction

Pressure too high

<table>
<thead>
<tr>
<th>Relief valve 1 opens?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Relief valve 2 opens?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

| Pressure reduced | Explosion |
```
FMEA or FMECA

Failure Modes and Effects (Criticality) Analysis

- Developed to predict equipment reliability.
- Forward search based on underlying single chain–of–events and failure models (like event trees).
- Initiating events are failures of individual components.

HAZOP: Hazard and Operability Analysis

- Based on model of accidents that assumes they are caused by deviations from design or operating intentions.
- Purpose is to identify all possible deviations from the design’s expected operation and all hazards associated with these deviations.
- Unlike other techniques, works on a concrete model of plant (e.g., piping and wiring diagram).
- Applies a set of guidewords to the plant diagram.
HAZOP Guidewords

<table>
<thead>
<tr>
<th>Guideword</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO, NOT, NONE</td>
<td>The intended result is not achieved, but nothing else happens (such as no forward flow when there should be)</td>
</tr>
<tr>
<td>MORE</td>
<td>More of any relevant physical property than there should be (such as higher pressure, higher temperature, higher flow, or higher viscosity).</td>
</tr>
<tr>
<td>LESS</td>
<td>Less of a relevant physical property than there should be.</td>
</tr>
<tr>
<td>AS WELL AS</td>
<td>An activity occurs in addition to what was intended, or more components are present in the system than there should be (such as extra vapors or solids or impurities, including air, water, acids, corrosive products).</td>
</tr>
<tr>
<td>PART OF</td>
<td>Only some of the design intentions are achieved (such as only one of two components in a mixture).</td>
</tr>
<tr>
<td>REVERSE</td>
<td>The logical opposite of what was intended occurs (such as backflow instead of forward flow).</td>
</tr>
<tr>
<td>OTHER THAN</td>
<td>No part of the intended result is achieved, and something completely different happens (such as the flow of the wrong material).</td>
</tr>
</tbody>
</table>

Example Entry in a HAZOP report

<table>
<thead>
<tr>
<th>Guide Word</th>
<th>Deviation</th>
<th>Possible Causes</th>
<th>Possible Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONE</td>
<td>No flow</td>
<td>1. Pump failure</td>
<td>1. Overheating in heat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Pump suction</td>
<td>exchanger.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>filter blocked</td>
<td>2. Loss of feed to reactor.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Pump isolation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>valve closed.</td>
<td></td>
</tr>
</tbody>
</table>
Task and Human Error Analyses

• Qualitative Techniques
  – Break down tasks into a sequence of steps.
  – Investigate potential deviations and their consequences.

• Quantitative Techniques
  – Assign probabilities for various types of human error.
  – Most effective in simple systems where tasks routine.
  – Not effective for cognitively complex tasks operators often asked to perform today.