In the following:

- Presentation of analytical techniques for identifying and classifying hazards.
  - Non-formal, but systematic methods.
  - Tools support for all those techniques exist.

Techniques considered are:

- Event tree analysis (ETA).
- Hazard and operability studies (HAZOP).
- Failure modes and effects and criticality analysis (FMECA).
- Fault tree analysis (FTA).
- Fault tree analysis (FTA).
- Failure modes, effects and criticality analysis (FMECA).

Techniques developed in general engineering, especially in the chemical and armaments industry.

- Tool support for all those techniques exist.
- Non-formal, but systematic methods.
- Presentation of analytical techniques for identifying and classifying hazards.

In the following:

A2. Hazard Analysis
FMEA identifies all ways a particular component can fail and the effects of a failure on the system. Since a failure does not have to occur for a hazard to be present in a system, FMEA is preliminary an engineering tool, not a safety analysis tool. Therefore FMEA is not a safety analysis tool. Example: A rocket is by its nature hazardous, even if it operates correctly.
Process of FMEA

Define scope and boundaries of the main system and of this analysis.

Break the main system down into subsystems.

Assess each subsystem, and determine, whether the failure of the subsystem would affect the main system.

If it wouldn’t, ignore that subsystem.

Otherwise, break this subsystem into further subsystems and repeat the above, until the component level is reached.
Process of FMEA (Cont.)

For each component identified as above, do the following:

- Look at the component’s failure modes = the ways the component can fail. 
- Assess the failure’s effects.
- Usually the worst-credible case with consequence severity and probability of occurrence is assessed, if this is possible to calculate.
- Identity whether the failure is a single-point failure.
- Identify, whether the failure is a single-point failure. (Single point failure = failure of a single component that could bring down the entire system.)
- Determine its mission phase (installation, operation, maintenance, repair).
- Usually the worst-credible case with consequences severity and probability of occurrence is assessed, if this is possible to calculate.
- Assess the failure’s effects.
- Look at the component’s failure modes = the ways the component can fail.
- Determine methods of corrective action.
- Determine methods of corrective action.

(C) Anton Setzer 2003 (except for pictures)
Document the results in an FMEA worksheet.

Process of FMEA (cont.)
|-----------------------------------|-------------------------|------------------------|---------------------|--------------------------|--------------------------|---------------------------------|---------------------|-----------------------------------------------------|
Solenoid Valve

Hydraulic Valve

Hydraulic Liquid

Pressurized Air

Solenoid Valve

Hydraulic Liquid

Solenoid Valve

Hydraulic Valve

Critical Systems, CS-411, Lentterm 2003, Sec. A2

A2-7

(c) Anton Setzer 2003 (except for pictures)
<table>
<thead>
<tr>
<th>Alignment sleeve</th>
<th>Signal pneumatic pilot due to inappropriate through pneumatic flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spring-plunger correct and smooth</td>
<td>or deactivation valve activation</td>
</tr>
<tr>
<td>Regularly: Assure inspect and test</td>
<td>rendered useless</td>
</tr>
</tbody>
</table>

| Leak detection for leaks: from source: inlet pressure | Working fluid due to loss of signal sent to hydraulic valve, |
| Verify air supply | No pneumatic fluid |

<table>
<thead>
<tr>
<th>Manually operate valve 4C</th>
<th>Continuous possible hydraulic</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Failure class</th>
<th>Failur e point</th>
<th>Failur e location</th>
<th>Single failure risk</th>
<th>Failure effects</th>
</tr>
</thead>
</table>

- **Page**: 13
- **Analyst**: John Doe
- **Date**: 10/13/96
FMEA is primarily designed to create products which are **correct**, not to **safe**. Example: If we apply FMEA to a gun, we obtain a gun, which has no **failures**. However, the fact that if you direct it against a human being you can kill him, is a hazard, but no failure of the gun. So e.g. the barrel doesn’t suddenly explode.

In general hazards need not be the result of a failure. Example: If we apply FMEA to a gun, we obtain a gun, which has no failures. We can of course extend FMEA to treat all situations in which a gadget is used and find out failures in that constellation.

But that is in most cases **infeasible**.

**Limitations of FMEA**
Limitations of FMEA (cont.)

Direct hazard analysis will in the case of the gun immediately identify the global hazard.

We see that FMEA is an excellent engineering tool for creating perfectly functioning gadgets.

This contributes to but doesn't guarantee safety.
Further FMEA investigates only single failures.

Often accidents have the origins in a combination of multiple failures, each of which on its own wouldn't have such severe consequences.
As FMEA, but additionally determine (or estimate) for each failure:

1. The probability of its occurrence.
2. The probability of the occurrence of the consequences, provided the failure has occurred.
3. A number measuring the criticality of the failure.

The product of the 3 factors measures the risk associated with that failure. If the risk exceeds a certain number, action has to be taken.
Explanation of the Measure above

The product of the first 2 factors measures the probability of occurrence of this deviation followed by the consequence, i.e., of this kind of accident.

Since risk = product of probability of occurrence and consequence,

Therefore the product of all 3 factors is the product of the probability of occurrence of the consequence and of a measure of the consequences.

The product of the first 2 factors measures the probability of the occurrence of this deviation followed by the consequence, i.e., of this kind of accident.

\[ \text{Risk} = \text{probability of occurrence} \times \text{probability of consequence} \]
Technique developed and used mainly in chemical industries.

HAZOP (c) Hazard and Operability Studies

Studies to apply it to computer based systems have been carried out.

Underlying systems theory model:

HAZOP considers systematically each process unit in the design and each possible deviation.

If there is no flow or no control signal, although there should be one.

E.g.: Accidents caused by deviations from the design or operating intentions.

Deviations are identified by using the guide words of HAZOP.

- Developments are identified by using the guide words of HAZOP.

- Underlying systems theory model.
HAZOP carried out by a team.
General Procedure of HAZOP

1. Define objectives and scope of the analysis.

2. Select a HAZOP team.
   - Requires a recorder, who documents the process of HAZOP.
   - Requires a leader, who knows HAZOP well.

3. Dissect design into nodes and identify lines into those nodes.

4. Analyze deviations for each line and identify hazard control methods.

5. Document results in a table.

6. Track hazard control implementation.
Nodes and Lines

- Node = location, where process parameters can change. Examples:
  - A chemical reactor
  - Pipe between two units
  - Pump
  - Sensor
  - Electrical power supply of a pump
  - Signals from a sensor to a computer
  - Signals from a computer to an actuator
  - Pipe feeding into a reactor
  - A chemical reactor

- Line = interface between nodes
  - Electrical power supply of a pump
  - Signals from a sensor to a computer
  - Signals from a computer to an actuator
  - Pipe feeding into a reactor
  - Pipe between two units
  - Pump
  - A chemical reactor
  - Sensor

Nodes and Lines
<table>
<thead>
<tr>
<th>Guide Word</th>
<th>Chemical Plant</th>
<th>Computer-based System</th>
</tr>
</thead>
<tbody>
<tr>
<td>More</td>
<td>Quantitative increase in the physical quantity</td>
<td>Signal magnitude or data exchanged.</td>
</tr>
<tr>
<td>Less</td>
<td>Quantitative decrease in the physical quantity</td>
<td>No data or control signal.</td>
</tr>
<tr>
<td>No</td>
<td>No part of intended result achieved.</td>
<td>Rate too low.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rate too high.</td>
</tr>
</tbody>
</table>

Guide Words of HAZOP and Possible Interpretations.
<table>
<thead>
<tr>
<th>Computer-based System</th>
<th>Chemical Plant</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Guide Word</strong></td>
<td><strong>Chemical Words of HAZOP (cont.)</strong></td>
</tr>
<tr>
<td>Incorrect.</td>
<td></td>
</tr>
<tr>
<td>Data complete but</td>
<td></td>
</tr>
<tr>
<td>transmitted.</td>
<td></td>
</tr>
<tr>
<td>Changes reversed.</td>
<td></td>
</tr>
<tr>
<td>Polarity of magnitude</td>
<td></td>
</tr>
<tr>
<td>transmitted.</td>
<td></td>
</tr>
<tr>
<td>Incomplete data</td>
<td></td>
</tr>
<tr>
<td>Addition to intended value.</td>
<td></td>
</tr>
<tr>
<td>Redundant data sent in.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other than</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Reverse</td>
</tr>
<tr>
<td>Opposite of what is intended activity occurs, e.g. reverse flow within a pipe.</td>
</tr>
<tr>
<td>Only part of intended activity occurs.</td>
</tr>
<tr>
<td>Activity occurs but with additional results.</td>
</tr>
<tr>
<td>Only part of intended activity occurs.</td>
</tr>
<tr>
<td>No part of intended activity occurs.</td>
</tr>
<tr>
<td>Something else happens instead.</td>
</tr>
<tr>
<td>Data complete but incorrect.</td>
</tr>
</tbody>
</table>

(C) Anton Setzer 2003 (except for pictures)
<table>
<thead>
<tr>
<th>Computer-based System</th>
<th>Chemical Plant</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Before</strong></td>
<td>Not used</td>
</tr>
<tr>
<td>After</td>
<td>Not used</td>
</tr>
<tr>
<td>Early</td>
<td>Not used</td>
</tr>
<tr>
<td>Late</td>
<td>Not used</td>
</tr>
</tbody>
</table>

**Guide Word**

- Signal arrives too early w.r.t. clock time.
- Signal arrives too late w.r.t. clock time.
- Signal arrives within a sequence intended earlier than clock time.
- Signal arrives within a sequence intended later than clock time.
Steps in the HAZOP Process

For all lines.

For all keywords and associated deviations e.g.:
No...".

Prevent deviation, make it less likely or mitigate its effects.

Identity changes in plant or methods which make him/her recognize that.

Identity, which changes in the plant will.

If the operator cannot recognize this deviation.

If that cause is hazardous or prevents efficient operation.

For all possible causes of that deviation.

E.g.: "No flow"

For all key words and associated deviations
Steps in the HAZOP Process (Cont.)

For each such change
If cost or change is justified
Agree to changes.
Agree who is responsible for action.
For each such action has been taken.
Follow up to see that action has been taken.
<table>
<thead>
<tr>
<th>Line</th>
<th>Attribute</th>
<th>Guide word</th>
<th>Cause</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor supply line</td>
<td>Supply voltage</td>
<td>No</td>
<td>Regulator or cable fault detected and system shuts down</td>
<td>Lack of sensor signal detected and system shuts down</td>
</tr>
<tr>
<td>Sensor supply line</td>
<td></td>
<td>More</td>
<td>Regulator fault</td>
<td>Damage to sensor</td>
</tr>
<tr>
<td>Sensor supply line</td>
<td></td>
<td>Less</td>
<td>Regulator fault</td>
<td>Incorrect temperature reading</td>
</tr>
</tbody>
</table>

Example: Temperature sensor.
Start with faults, which can cause accidents (e.g. broken pipe). Draw a decision tree in order to identify sequences of faults resulting in accidents. For each such sequence determine its outcome.

Probabilities can be assigned to each event to determine the likelihood of that scenario. The product of the failures on each path is the probability of that event.

• Draw a decision tree in order to identify sequences of faults resulting in accidents.
• For each such sequence determine its outcome.
• Probabilities can be assigned to each event to determine the likelihood of that scenario. The product of the failures on each path is the probability of that event.
• Sequence: Product of the failures on each path is the probability of that event.
Since probability of failure is usually very low, probabilities of success are usually almost 1 and can be ignored in the product.
Example: Loss of coolant accident in a nuclear power station

(EDCS = Emergency Core Cooling System)
Evaluation of Event Tree Analyses

**ETA handles continuity of events well.**

In general, ETA's tend to become very big.

- It is necessary to cut away subtrees which don't result in an accident.
  
  ETA becomes unnecessarily big.
  
  \[
  \Rightarrow \quad E \text{TA becomes unnecessarily big.}
  \]

However, in the tree usually many events which don't result in an accident occur.

ETA is good for calculation of probability of events.

ETA handles continuity of events well.
Fault Tree Analysis (FTA)

Whereas ETA starts with faults and determines resulting accidents (events), FTA starts with a possible accident and determines sequences of faults resulting in that event.

FTA is drawn using logical gates:

- If all of the conditions are satisfied the event occurs, or
- If one of the conditions is satisfied the event occurs.

Usually these conditions are disjunctive.

The FTA is drawn using logical gates.
Primary Laser Activated

- Incorrectly
- Failure

Primary Laser System applies Voltage to Input

- Voltage on Control Input

- Primary Cable Fault

- Relay Contacts closed

- Microswitch Contacts closed

- Control Input Voltage on

- Laser Activated Incorrectly
Fault Tree Symbols

- Fault event resulting from other event
- Fault event not fully traced
- Fault event not taken as input but causes unknown
- Basic event
- Taken as input from other event
- Fault event resulting from other event
Event occurs if at least one input occurs

Event occurs if all inputs occur

Output to other fault tree

Fault Tree Symbols (Cont.)
Fault Tree Symbols (Cont.)

Official Symbol

Meaning

Control

In

Out

t depending on

Event occurs

control condition
Fault trees can be written as Boolean formulas (take and/or as Boolean). Fault trees can be unfolded if Cond1 or Cond2 contain or/s. Boolean formulas can then be rewritten in disjunctive normal form (ie. as or an of ands).

Laser Example:

\[
((\text{Relay Contacts Closed} \text{ and Cond1}) \lor \text{Micro Switch Contacts Closed} \lor \text{Cond2}) \lor \text{Primary Cable Fault} \lor \text{Primary Laser Failure}
\]

(where Cond1 and Cond2 are conditions identified by continuing the fault trees below the rhombuses).
These conjunctions are called cut sets.

Each conjunction determines a minimal sequence of events resulting in an accident.

- In \((A \land B) \lor (B \lor C)\) and \((B \land C) \land (B \lor C)\),
- E.g.,
- Now omit conjunctions, which are implied by shorter ones.

Cut Sets (Cont.)
Cut Sets (Cont.)

Shortcut sets indicate particular weaknesses of the system.

If the cut sets are independent, the probability of the events in one cut set occurring is the product of the probabilities of the individual events. If the faults in a cut set are independent, the probability of the accident occurring is the sum of the probabilities of the individual events. If the cut sets are independent, the probability of the accident occurring is the product of the probabilities of the individual events.
• Cut sets can be generated automatically.

Risk estimates:

– Common mistake to overlook independence, which results in too low
  risk estimates.
– Assumes that the probability of them occurring is much higher.

• Often however the events in one cut set are not independent.

(C) Anton Setzer 2003 (except for pictures)
We have studied 5 techniques for Hazard analysis.

- **FMEA and FMECA.**
  - Starts from accidents. *Seems to be most suitable technique in order to identify hazards.*
  - Concentration on avoidance of failures. *Does not necessarily identify all hazards.*

- **HAZOP.**
  - Use of guide words. *Adaptation to computer systems still in experimental state.*

- **ETA.**
  - Event trees might grow too big. *Starts from faults.*

- **FTA.**
  - Event trees might grow too big. *Starts from accidents. Seems to be most suitable technique in order to identify hazards.*

- **ETA.**
  - Adaption to computer systems still in experimental state. *Use of guide words.*

**Summary**