ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Risk Analysis of Highly-integrated Systems

RA I: Methods (HAZOP, FMEA, Master Logic Diagram)

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Hazard and Operability Study (HAZOP)

Goals and purposes of a HAZOP:

- Qualitative analysis of processes in a chemical engineering system (continuous or "batch" operation) based on given guide words, which highlight causes and consequence of deviations from desired physical parameters, i.e.
  - o identification of hazards within the system and caused by the system
  - o identification of causes of operational disturbances and deviations in the production, which can lead to defective products
- Fulfilment of regulatory requirements and recommendations

Working steps of a HAZOP:

1. Preparation: definition of focus of the analysis, guide words, process variables, etc.
2. Selection of the team members
3. Collection of plant data and information
4. Completing the HAZOP-form which summarizes the results

(1) Preparation

Identification of deviations from the target state by linking guide words with process variables, e.g.

- No/less/more mass flow
- More/less system constituents (corrosion products, multi phase flow, etc.)
- Other operational states than foreseen, e.g. maintenance instead of normal operation.

(2) Selection of the team members (example)

- Independent chairman, expert in HAZOP
- Company experts: design engineer, process engineer, commissioning manager, instrument design engineer
- About 5 to 7 persons depending on facility size, type and/or state of design realisation.

(3) Plant data and information

Comprehensive data of:

- “Plant- and system hardware”, like piping and instrument drawings, plant models, procedures, safety analysis reports
- “Plant- and system software”, like operation instruction, operation manuals

The data and information must be:

- up to date
- sufficiently detailed and must going into the same depth
- without contradictions/conflicts

(4) HAZOP-form

Guide word	Deviation	Possible cause	Consequences	Action required

Advantages of a HAZOP

- Guided systematic approach
- Interdisciplinary analysis of a facility
- Intensive use of facility specific data/information and expert judgment
- Internationally established method, applicable within the StFV*

Disadvantages

- Dangerous combinations of events may remain undetected
- No thorough examination of external events (mostly)
- Less suitable for analysis of small facility modifications
- No systematic analysis and collection of component failures
- Strong dependence on expert knowledge and experience
- Labour intensive and time consuming (may range up to months)

* Störfallverordnung

Failure Mode and Effects Analysis (FMEA)

Goals and purposes for applying a FMEA

- Qualitative analysis of units in respect to various failure modes and the impacts to superordinated systems (inductive questioning)
- Realisation of company goals (high quality products, etc.), customers increasing demands (conditions of use, service, etc.)
- Fulfilment of regulations and standards

Working steps of a FMEA

(1) Listing of failure modes of all units

(2) Identification of all potential failures for each listed unit and of the criticality of the facility caused by the specified failure modes

(3) Classification of each failure according to hazard and consequence

(4) Determination of procedures to reduce failure frequency and consequence (risk)

(5) Completing the FMEA-form which summarizes the results of steps 1 to 4

(1) Listing of failure modes of all units

Functions	Types of failure
Closing	Fails open Only partly closed
Opening	Fails closed Only partly opened
Remain closed	Opens completely Partly opens
Remain opened	Closes completely Partly closes
Enclose a medium	External leakage Internal leakage

(3) Classification of consequences

Class	Consequence	The failure of a unit leads to ...
I	Catastrophic	… a total failure of the system and may cause deaths
II	Critical	… major system damage and may cause severe injuries
III	Marginal	… minor system damage and may cause minor injuries
IV	Minor	… no serious system damage or injuries

(4) Classification of the event frequencies

Class	Failure frequency
Frequent	1x failure in less than 10^4 hours of operation
Reasonably probable	1x failure between 10^4 and 10^5 hours of operation
Rare	1x failure between 10^5 and 10^7 hours of operation
Extremely unlikely	1x failure in more than 10^7 hours of operation

$1 year \mathrel{\hat{=}} 8760 h \approx 10^4$

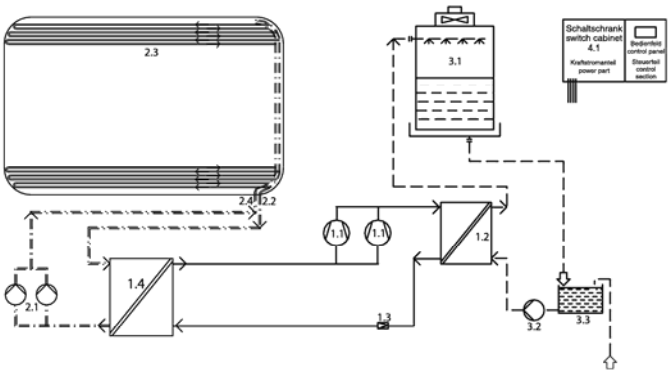
Example: Skating rink

An (older) outdoor skating rink is located in a residential area. About 10 tons of ammonia (NH_3) are used as cooling liquid. The facility is subject to the Swiss Ordinance of Protection against Major Accidents established in 1991. The question is, whether the risk due to the operation of the skating rink is acceptable or a complete revision is necessary.

General conditions:

- The skating rink is only operated in winter.
- System boundaries are proposed to be the technical facilities including the skating rink
- Cooling facility with direct cooling liquid evaporation

System layout



Flow diagram for a refrigeration plant with secondary refrigeration – cooling carrier: brine
refrigerant: ammonia (NH_3)

1.0	refrigerant circuit	1.4	evaporator	2.3	piping system	3.2	cooling water pumps
1.1	compressor with motor drive	2.0	cooling carrier circuit	2.4	return main	3.3	cooling water sump
1.2	condenser	2.1	cooling carrier pumps	3.0	cooling water circulation	4.0	electrical installations
1.3	expansion valve	2.2	supply main	3.1	cooling tower	4.1	switch cabinet

(5) Completing the FMEA-form (example: skating rink)

System: Skating rink

Initial state:
Normal daily routine

Environmental conditions:
Temperature 8°

Documentation:
Plans, system specifications, ...

Nr.	Unit	Failure mode of *(b)*	Class: Frequency of *(c)*	Failure recognition of *(c)*	Countermeasures against *(c)*	Failure effect of *(c)* on the adjoined units	Comments *(g)*	Class: Effect / facility state
(a)	***(b)***	***(c)***	*(d)*	*(e)*	*(f)*	***(g)***	*(h)*	*(i)*
1								
2								
3								

Advantages of a FMEA

- Systematic approach
- Interdisciplinary assessment of a facility
- Intensive use of facility documentation and expert judgment
- Internationally accepted method; applicable for an analysis within the StFV

Disadvantages

- Dangerous “event chains” may remain undetected
- No thorough examination of external events (mostly)
- Strong dependence on expert knowledge and experience
- Labour intensive and time consuming (“paper mill”).

Summary

HAZOP	**FMEA**
→ Hazards / operational disturbances	→ Possible failure modes of single units and related effects
• Definition of guide words / process variables • Continuous / discontinuous processes	• Listing of units / failure types • Classification of system states and effects • Classification of event frequencies
• Entries in tables; only discrete failures are considered, no event chains	

Master Logic Diagram

Purpose

• Identification of causes (of failures) of an undesired event („top event“)

Methodology

• definition of an unwanted top event
• build up detailed sub-events / categories
• cut off at basic events
• assign event frequency (failure probability or rate) to basic event
• summation of all parameters (if independent from each other)

Example: Master Logic Diagram