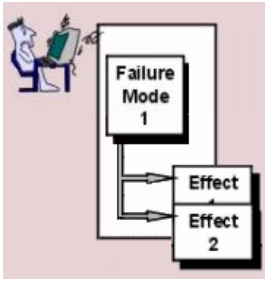
Chapter 5 Semi-quantitative Systems Risk Analysis Methods

5.1 Introduction

Compared with the approaches described in the preceding section, the methods presented here extend on one hand the scope of the hazard analysis of systems of a certain complexity, and allow on the other hand to make some evaluation of the potential effects of the system failures that these methods help identifying.

5.2 Failure Modes, Effects and Criticality Analysis (FMECA)

General presentation of the method



Failure Modes and Effects Analysis (FMEA) is an inductive analytical technique used to systematically analyze all contributing failure modes of structures, equipment or processes and identify the resulting effects of such failures on the larger systems, of which they form a part and on the surrounding systems. A *failure mode* is the particular way a given failure manifests itself (e.g. *failure to open*, *failure to close*, *failure to continue to operate*, etc.). When the criticality (criticality = probability/severity assessment) of the effects is in addition considered, the method is called *Failure Modes, Effects and Criticality Analysis* (FMECA).

Failure modes and effects analysis play an important role in the understanding of how systems are designed and how they might fail during operation. Since such an analysis requires people removed from the detailed design, a cross-functional team can do it. This work can have a significant impact on the overall design and safety of a system and in some cases can save lives. The idea behind the FMEA is to identify functions and hardware whose failure has a very undesirable effect on the safety (or safe operation) of a system or can lead to overall poor performance. The systems are identified from the top down and the failures and their consequences are identified from the bottom.

The method can be used at different system levels. Since changes as a result of a FMEA can occur, it should preferably be performed initially during the preliminary design phase of a system but can then be followed through to construction/ production. Basically, the method is designed to answer the questions: “How can the system fail?” and “What effects will such failure(s) have?”. There are variations in the application of the method and the complexity of the systems analyzed. However, the analysis normally consists in the following main stages conceived to assure that, to the possible extent, all potential failure modes and their associated causes/mechanisms have been considered and addressed:

1. The system is first broken down into its constituent units (e.g., mechanical components, motors, valves, relays, switches, instruments, etc.).
2. Failure modes are systematically identified for the various units.
3. Conceivable causes, consequences and the significance of failures are assessed for each failure mode.
4. Each cause/failure mode/effect is rated for severity, occurrence and ability to detect.
5. Recommendations for suitable control measures (action plans) are made.

Used at the design stage of a system, FMEA is a simple, structured analysis technique that gives design teams the information they need to:

- increase system reliability/safety;
- ensure the design is robust;
- reduce the number of engineering changes;
- correct design errors before construction/production starts.

The FMEA method was originally developed at the NASA (U.S. National Aeronautics and Space Administration), early in the *Apollo* space program. NASA created the tool to alleviate the stress between two conflicting mottos: "Failure is not an option" and "perfect is the enemy of good". The first meant successfully completing the mission and returning the crew safely back to Earth. The second meant that failure of at least some components was recognized unavoidable in such a novel and complex space system; the job was to predict them, prevent them when possible, plan for them and build in the ability to overcome failures. In Europe, FMEA had been extensively used in the development of the *Concorde* and *Airbus* airliners for example. Design engineers in many industrial domains today largely use it. This method is the object of many official texts, guidelines and standards (e.g. U.S. Department of Defense's MIL-STD-1629A, SAE International's J1739 and ARP5580, etc.). It is frequently selected whenever a detailed analysis involving fault trees or event tress (see chapter 6) is not required.

FMEA detailed process

The detailed step-by-step process for conducting a FMEA is outlined below. As already mentioned, there is however a great variety within industry as to the specific implementation details for individual FMEA/FMECA analyses. The different steps described here must therefore be appropriately adapted from case to case.

FMEA step-by-step process:

1. Clearly identify and describe the system or process that will be the subject of the analysis, including the functions that the system or process is expected to perform. For FMEA analysis of a system, the investigation could be performed at the system, subsystem, component or other level of the system configuration. The problems of interest for the analysis (personnel/public safety problems, environmental issues, economic impacts, etc.) should also be precised at this stage. This understanding simplifies the process of analysis by helping the engineer identify those system/process parts that fall within the scope of the study and those that fall outside.

2. Choose the type of FMEA approach – hardware approach (bottom-up), functional approach (top-down) or a combination of both - for the study. The hardware approach is normally used when hardware items can be uniquely identified from schematics, drawings, and other engineering and design data. The hardware approach typically focuses on the potential failure modes of basic components of the system. It can be difficult or inefficient, however, for use in analyzing complex systems or systems that are not well defined at the time the analysis has to be performed. The functional approach is normally used when hardware items cannot be uniquely identified or when system complexity requires progressive analysis, with each successive level of analysis focusing in more detail on only the most important contributors. This approach focuses on ways in which functional intents of a system may go unsatisfied rather than on the specific failure modes of individual equipment items. An FMEA may also begin with a functional approach and then make a transition aiming at focusing on equipment, especially equipment that directly contributes to functional failures identified as important. Traditional reliability-centered maintenance analysis uses this hybrid approach.

3. Break down the system by equipment or functions for analysis. This step defines the elements of a system that will provide the basic structure of the initial FMEA. These elements may be equipment items for a hardware approach or intended functions for a functional approach.

4. Identify the potential failure modes that could prevent or degrade the ability of the system/process to perform its designated functions. Those can for example be:
   - premature operation;
   - failure to operate at prescribed time;
   - failure to cease operation at a prescribed time;
   - intermittent operation;
   - accident of output or failure during operation;
   - degraded output or operational capability;
   - other unique failure conditions.

   The list of typical failure conditions above applies to equipment items and functional statements.

5. Identify the potential causes for each failure. In a hardware-based FMEA, the causes are typically the failure modes of equipment at the next lower level of resolution for the system, as well as human errors and external events that cause equipment problems at this level of resolution. In a function-based FMEA, the causes are typically lower-level functional failures.

6. Identify the potential effects that would result from the occurrence of each failure. It may be desirable to consider the effects at the component level (local effects), at the higher level of equipment or function (next higher level effects) and/or at the system level (end effects). The end effect normally become possible only if planned mitigating safeguards for the failure mode fail themselves.

   The figure below illustrates for a particular example the relationships between failure mode, cause and effect.

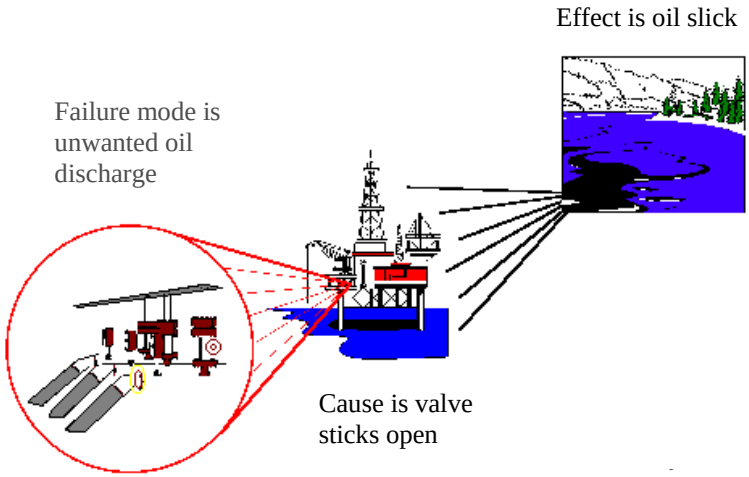


Figure 5.1 ***Illustration of failure mode, cause and effect*** **(source: GRB)**

7. Perform (semi-) quantitative evaluation if necessary. As mentioned previously, FMEA analyses often include some effort to prioritize issues. This means extending the analysis of potentially important failures by characterizing their likelihood, their severity, and the resulting levels of risks (approach refers to as FMECA, see above). The intent is to help the analyst rank the failures and address the real big concerns first.

There are many ways to characterize the criticality of a failure mode. In the industrial domain, *Risk Priority Number* (RPN) ratings and *Criticality Analysis* are common methods of prioritization.

The *Risk Priority Number system* is a relative rating system that assigns a numerical value to the issue corresponding to each of the three different risk parameters: *severity rating* (*S*), *occurrence probability or frequency* (*O*) and *detection rating* (*D*). The three ratings are multiplied together to determine the overall RPN for the issue[1]. The rating scales typically range from 1 to 5 or from 1 to 10. A five-level scaling for the *S* and *O* ratings could for example be "semi-quantitatively" defined as follows:

Table 5.1 ***Example of a five-level RPN scaling for the severity and occurrence parameters***

S scale

Catastrophic 5	*High* 4	*Moderate* 3	*Low* 2	*Negligible* 1
Fatalities	Severe injuries or disabilities	Injuries or lost time	First aid required	No or negligible concern
Catastrophic impact on habitat	Significant, irreversible impact on habitat	Significant, reversible impact on habitat	Minor impact on habitat	No measurable impact on habitat
Unable to meet regulatory obligations; shut down	Exceeds regulatory obligations more than once per year	Occasionally (< one per year) exceeds regulatory obligations	Seldom exceed regulatory obligations	Do not exceed regulatory obligations

O scale

Frequent 5	*Probable* 4	*Occasional* 3	*Remote* 2	*Improbable* 1
10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}

Example: Partial FMEA for a battery, with five-level RPN scaling (detection is assumed to be certain, i.e. *D* =1)

Device	Function	Failure Mode	Effect	*S*	Cause	*O*	*D*	RPN
Battery	Provide adequate relay voltage	Fails to provide adequate power	System fails to operate	4	Battery plates are shorted	2	1	8

Because all issues are rated according to the same set of rating scales, the resulting RPN can be used to compare and rank issues within the same analysis. However, it is generally not appropriate to compare Risk Priority Numbers resulting from ratings obtained in different analyses.

[1] It is however the author's belief that risk is, and should remain, fundamentally a two-dimensional concept (probability / severity). There is no imperative reason to add detection rating as a new dimension. An event with a different probability of detection just defines another failure mode, with a different occurrence probability and/or effect severity.

The *Criticality Analysis* (CR) approach is similar to the RPN rating system, but it calculates the rankings in a slightly different way. Criticality Analysis takes into account the device probability of failure (for the considered failure mode), *Q*, the share of the failure likelihood that can be attributed to the particular failure mode, *R*, and the probability of loss, *L*. The later is an indication of the severity of the failure effect and may be set according to the following scale:

- Actual loss → 100%
- Probable loss → 50 %
- Possible loss → 10 %
- No loss → 0 %

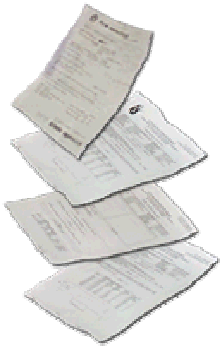
Example: consider as above a partial FMEA for a battery. The reliability of the battery at the operating time of interest and for the considered failure mode is 92%, therefore its probability of failure (unreliability) is $Q = 8\%$. The share of the device unreliability that can be attributed to the given failure mode is $R = 25\%$ (i.e., 25% of the battery failures are likely to be due to this particular failure mode). The probability of loss is $L = 100\%$ because the occurrence of the failure mode will with certainty cause a system failure. The criticality for the failure mode is thus $CR = 0.08 \cdot 0.25 \cdot 1.00 = 0.02$ or 2%. Therefore, the partial FMEA takes here the form:

Device	Function	Failure mode	Cause	*Q*	*R*	Effect	*L*	CR
Battery	Provide adequate relay voltage	Fails to provide adequate power	Battery plates are shorted	.08	.25	Systems fails to operate	1.0	.02

As with the RPN method, this Criticality value can be compared with the corresponding values for other failure modes to help making decision about the priorities of the issues that must be addressed.

8. Identify current controls (design or process). Current controls are the mechanisms that could prevent the cause of the failure mode from occurring or which detect the failure before it can cause actual damages. Each of these controls should be assessed to determine how well it is expected to identify or detect failure modes.

9. Determined recommended action(s) to address potential failure modes that have been attributed a high priority. These actions could include testing quality procedures, selection of different components or materials, limiting environmental stresses or operating range, redesign of the device to avoid the failure mode, specific inspection, monitoring mechanisms, preventive maintenance, inclusions of back-up systems or redundancy, etc. Assign responsibility and a target completion date for these actions; this makes responsibility clear-cut and facilitate tracking. Monitor the application and results of these actions to be able to propose improvements when this proves to be both feasible and desirable.



10. Document the results and conclusions of the analysis. A comprehensive FMEA report should at least include the following main chapters:
    - *Executive summary* (abstract of complete report).
    - *Scope of the analysis* (brief system description, analysis boundaries); say what is analyzed and what is not analyzed.

- *The analysis*; discuss FMEA method (strengths/limitations; state resolution level(s) used; present risk prioritization technique (if used); describe software used (if applicable); present the analysis data results.
- *Findings* (interpretation of analysis results); predominant hazards; comments on high risk hazards (- high from severity or probability? - countermeasures effective?); comments on high severity risks (probability acceptably low?); chief contributors to overall system risks.
- *Conclusions and recommendations* (interpret findings); - is overall risk under acceptable control? – is further analysis needed? – by what method?
- *Analysis worksheets* (as an appendix or attached table); these worksheets, completed throughout the whole analysis, should typically include the kind of headings shown below:

Table 5.2 ***Typical FMEA Table Template*** **(from [Mohr, 1994])**

Project No.:_____ Sheet_____of_____
Subsystem:_____ Failure Modes & Effects Analysis Date:_____
System:_____ Prep. by:_____
Operational Phase(s):_____ FMEA No.:_____ Rev. by:_____
Approved by:_____

IDENT. No.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT		RISK ASSESSMENT			ACTION REQUIRED / REMARKS
						SEV	PROB	Risk Code	

P: Personnel / E: Equipment / T: Downtime / R: Product / V: Environment

A FMEA report is in fact a living document. Throughout the system development cycle change and updates are made to the system and process. These changes can and often do introduce new failure modes. It is therefore important to review and/or update the FMEA when:

- A new system or process development is being initiated.
- Changes are made to the operating conditions the system or process is expected to function in.
- A change is made to either the system or process design.
- New regulations are instituted.
- User feedback indicates problems in the system or process.

This completes the FMEA step-by-step process description (summarized in Fig. 5.2).

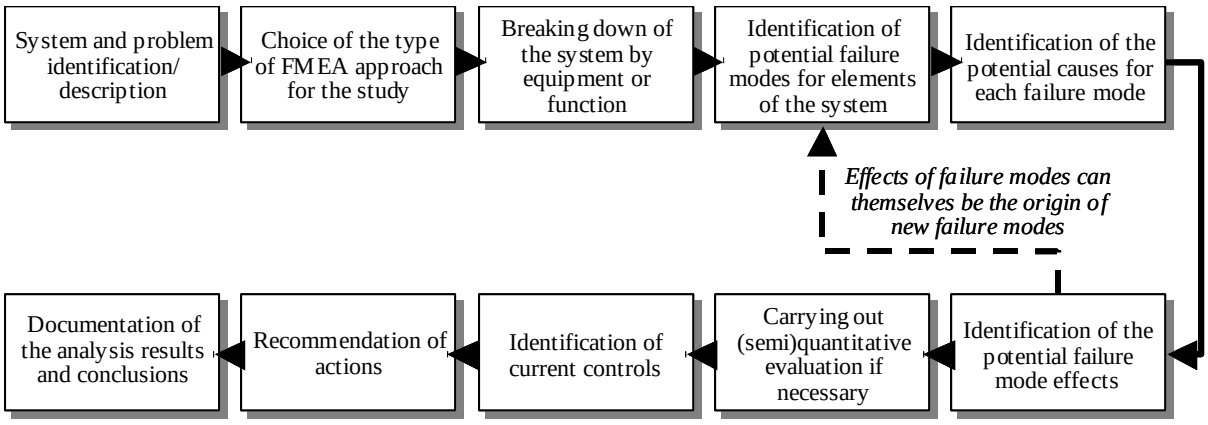


Figure 5.2 ***Block diagram of the FMEA process***

FMEA/FMECA applications

FMEA/FMECA techniques are used throughout industry for a variety of applications. These flexible analysis methods can be employed to support design, development, manufacturing, service and other activities to improve reliability and increase efficiency.

A practical application of the FMEA/FMECA techniques would involve the completion of a worksheet of the type described in the preceding page, in which the failure modes of individual components are identified, assessed and risk priority codes evaluated.

As an illustrative example, let us consider the case of the pressure cooker described below (source: American Society of Safety Engineers):

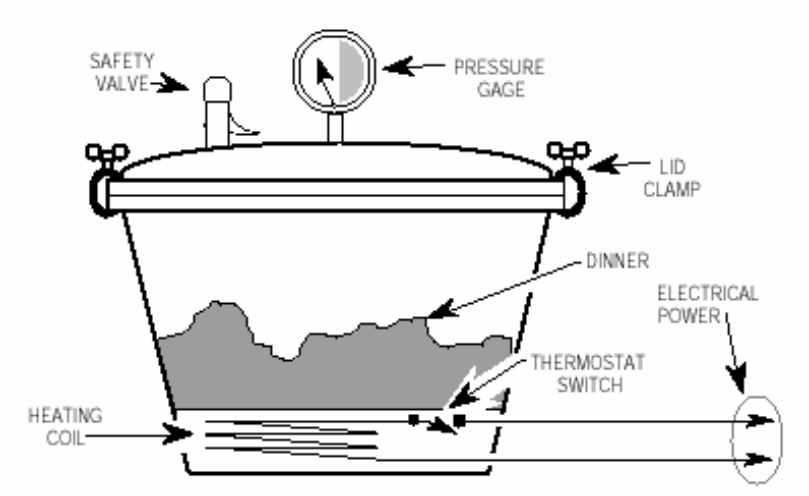


Figure 5.3 ***Pressure cooker (simple FMEA example)***

The following observations can be made about this system:

- The electric coil heats the cooker.
- The thermostat controls the cooker inside temperature; the switch opens when this temperature becomes > 120 °C.
- A spring-loaded safety valve opens on overpressure.
- Pressure gage red zone indicates overpressure.
- High temperature/pressure cooks and sterilizes food, tenderizes and protects against botulin toxin.

Moreover, the “operator” ’s process tasks are:

- to load the cooker;
- to close/seal lid;
- to connect power;
- to observe pressure;
- to time cooking at prescribed pressure;
- to offload the dinner when ready.

The objective is to prepare a FMEA at component level for cooking (after loading/closing/sealing). Targets are personnel (P), product or dinner (D), and the pressure cooker itself (C). Facility/kitchen as well as energy consumption will be ignored. Food is supposed to be for private use.

The corresponding FMEA worksheet (of the model type described on page 84) is shown in Table 5.3.

Table 5.3 ***Pressure cooker FMEA worksheet***

Project No.:_____ Sheet_____of_____
Subsystem:_____ **Failure Modes & Effects Analysis** Date:_____
System: Pressure Cooker/Food/Operator Prep. by:_____
Operational Phase(s): Cooking (after load/close/sealing) FMEA No.:_____ Rev. by:_____
Approved by:_____

IDENT. No.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT		RISK ASSESSMENT SEV	PROB	Risk Code	ACTION REQUIRED / REMARKS
SV	Safety Valve	Open	Broken Spring	Steam burns; increased production time	P D C				
		Closed	Corrosion; Faulty Manufacture; Impacted Food	Overpressure protection compromised; Thermostat Sw protects; no immediate effect (Potential explosion/burns)	P D C				
		Leaks	Corrosion; Faulty Manufacture	Steam burns; increased production time	P D C				
TSw	Thermostat Switch	Open	Defective	No heat production; mission fails	P D C	NA			
		Closed	Defective	Continuous heating; Safety Valve protects; no immediate effect (Potential explosion/burns)	P D C				
PG	Pressure Gage	False High Reading	Defective; Stuck	Dinner undercooked; bacteria/toxins not destroyed; OR…	P D C				
				Operator intervenes/ interrupts process (mission fails)	P D C	NA			
		False Low Reading	Defective; Stuck	Dinner overcooked; Safety Valve protects/releases steam if Thermostat Sw fails closed (Potential explosion/burns)	P D C				
CLMP	Lid Clamp(s)	Fracture/Thread Strip	Defective	Explosive pressure release; flying debris/burns	P D C				

Another (more "industrial") example worksheet, related to the Multi-Canister Overpack Handling Machine (MHM; a large crane in a radioactive waste storage facility) is shown below (source: ARES Ciorporation).

Table 5.4 ***Multi-Canister Overpack Handling Machine FMEA worksheet***

Subcomponent/ Subsystem	Component ID	Component Fail Rate	Failure Mode	Failure Effects Local	Failure Effects End	Failure Detection Method	Mitigation	Severity Class	Maintenance Action
Hoist Motor and Gearbox	MFPH - Hoist Motor 3 HP & Gearbox	5.5E-06	Motor fails to start/run	Cannot raise or lower Tube Plug by motor	Shutdown for repairs ~24 hours	Status light indicator	Use of handwheel for manual application	III	Replace
	BFPH - Tube Plug Hoist Brake	1.15E-05	Fails	Potential for tube plug drop	Shutdown for repairs ~24 hours. If tube plug drops then shutdown n > 1 week.	None	None	III (II if plug drops)	Replace
	PHOL - Tube Plug Hoist Motor Overload Switch EE33056-16	4.12E-06	Fails Open	Motor will not run	Shutdown for repairs ~8 hours	Status light indicator	Manual handwind	IV	Replace

It is worth noting that a FMEA cannot be conducted, as made obvious in the above examples, until design has proceeded to the point that system elements have been selected at the level the analysis is to explore. Ideally, FMEA is best done in conjunction with or soon after PHA efforts (see Chapter 4). Results can be used to identify high-vulnerability elements and to guide resource deployment for best benefit

Strengths and limitations of FMEA/FMECA

The advantage of the FMEA (or FMECA) technique lies in its explicit and systematic, component by component, consideration of the cause and effects of potential failure modes. Moreover, this method is beneficial at all stages of a system life cycle and can easily be adapted to the specificities of various case studies.

FMECA assesses risk for potential, single element, failures for each identified target, within each mission phase. Knowing this information helps to:

- optimize reliability, hence mission accomplishment;
- guide design evaluation and improvement;
- guide design of system to “fail safe” or crash softly;
- guide design of system to operate satisfactorily using equipment of low reliability;
- guide component/manufacturer selection.

Using FMEA/FMECA, high-risk hazards found in a PHA can be analyzed to the piece-part level. Hazards caused by failures identified in the FMEA/FMECA can be added to the PHA if they have not already been logged there.

Although the FMEA/FMECA methodology is highly effective in analyzing system failure modes, this technique has nevertheless some limitations:

- Examination of human errors and external influences is limited. A traditional FMEA/FMECA uses potential equipment failures as the basis for the analysis. All of the questions focus on how equipment functional failures can occur. A typical FMEA/FMECA addresses potential human errors or external influences only to the extent that such events produce equipment failures of interest.
- Focus is on single-event initiators of problems. A traditional FMEA/FMECA tries to predict the potential effects of specific equipment failures. These equipment failures are generally analyzed one by one, which means that important combinations of equipment failures may be overlooked. Such combinations of equipment failures should be examined in an extension of the FMEA/FMECA approach known as the “Combinations of Reduced Failures Method” (in French: “Méthode de combinaisons des pannes résumées” , see [Lemeur, 1988]).
- Results are dependent on the mode of operation**.** The effects of certain equipment failure modes often vary widely, depending on the mode of system operation. More than one FMEA/FMECA may, therefore, be necessary for a system that has multiple modes of operation.
- If the system is at all complex and if the analysis extends to the assembly level or lower, the FMEA/FMECA process can be tedious and time consuming. Examples of typical time requirements for a FMEA team are given in Table 5.5

Table 5.5 ***Typical time requirements for a FMEA team***

Scope	Preparation	Evaluation	Documentation
Simple/small system	2-6 hours	1-3 days	1-3 days
Complex/large system	1-3 days	1-3 weeks	2-4 weeks

- FMEA/FMECA does not directly address operability problems.

Is the "Challenger" case a "bad advertising" for the FMEA approach?

Everyone's first reaction to the Challenger event was that the design group responsible for the solid rocket boosters did not take appropriate precautions. This is, in fact, *not* the case. Morton-Thiocol engineers *did* indeed conduct a FMEA on the design of the solid rocket boosters. They also employed the PDCA discipline, which called for a forensic analysis of the boosters after each launch. In their continuously updated FMEA, they placed an extremely high risk of a "loss of vehicle and crew" (Severity=10/10) on launch where the ambient temperature was below 40 degrees.

So why was there a catastrophic failure? It came out that the pressure from NASA and Thiocol top management was so great at the time that the recommendation "not to launch in such extreme external temperature conditions" made by the engineers was overturned. The thought process was that there was no data to suggest that there could be a real problem.

The lessons to be learnt here is threefold:

1. FMEA predicted outcomes with high severity must be taken seriously.
2. Absence of data is *not* an indication that everything is OK.
3. In the pursuit of excellence, the value of experience and judgment should not be overlooked. People closest to any business process, whether it is the manager responsible for the process, the practitioner responsible for execution of the process or the ultimate beneficiary of the process outcome, will sustain the greatest loss should a failure take place. Safety, reliability and quality are thus of paramount importance.

In summary

To conclude, FMEA/FMECA is a well-suited tool for limiting the analysis work to only those things that are of significant importance to the considered system. This method can be used to help narrow the analyst's focus to what is "most" important. FMEA/FMECA thus usefully complements Fault Tree Analysis (see next chapter) and other risk analysis techniques.

5.3 Hazard and Operability Analysis (HAZOP)

A process-oriented risk analysis approach

The HAZOP (HAZard and OPerability Analysis) method was first developed in Great Britain at ICI Chemicals in 1964 for identifying potential hazards and operability problems caused by deviations from the design intent, primarily as a tool to be used in the design phase of a plant or plant upgrade. This is an important activity in Process Safety Management (PSM), which requires a significant amount of time, effort, and specialized expertise.

HAZOP is the most widely used and recognized as preferred formalized approach by the chemical process industry. It has however become apparent over time that this same basic methodology can as well be applied to many circumstances and systems, other than the classical process systems. It is now largely recommended by legislators, regulators, insurance companies and other professional institutions.

To maximize the benefit of a HAZOP study, the timing is critical. A HAZOP analysis will inevitably result in design changes. Taking into account that time is required to implement these changes, the optimum time for a HAZOP study is at the start of detail design, with completed Process Flow Diagram. It thus can provide a valuable tool, in project scheduling, to fix a "design freeze" milestone. Process changes after this time must be agreed as essential to the operation, in order to minimize cost impact.

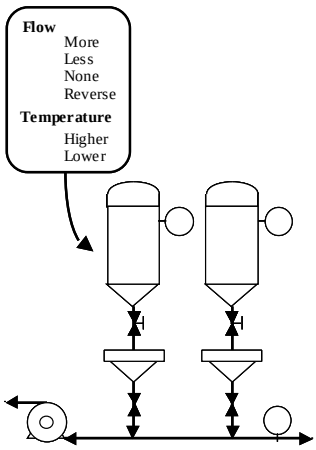
A HAZOP is carried out by a multi-discipline team having both general and specific knowledge of the system and its operation. This team should in principle include representatives from the Design, Process, Operating and Maintenance groups.

The process-general knowledge is related to the models of the process units, which are qualitative causal models expressly developed for hazard identification. The process-specific knowledge, which changes from plant to plant and is provided by the engineers responsible, consists of information about the materials used in the process, their properties (such as flammability, "corrosivity", volatility, toxicity, etc.), as well as about the piping and instrumentation of the plant.

Thus, HAZOP studies provide a well-structured brainstorming forum for specialists to use their experience and skills to assess ways in which hazards or operating problems might arise.

HAZOP detailed process

As mentioned above, the HAZOP method relies on brainstorming. Brainstorming is a very powerful technique, but it is difficult to ensure that it is sufficiently rigorous to meet the objective of not missing any significant safety or operability issues. One requirement to meet this need has already been discussed, that is the size and capability of the team. The other requirement is a suitable set of "prompts".



To this end, an agreed checklist containing basic guidewords relevant to the system should be compiled prior to the analysis. The purpose of this guidewords list is to help identifying how deviations from the design intent can occur in the system, and whether the consequences of these deviations can result in hazard(s). Basic guidewords are simple expressions such as : "*No*", "*More*", "*Less*", "*As well as*", "*Reverse*", "*Other than*", etc. They are applied to *parameters of importance* (process variables) – e.g. *Flow*, *Temperature*, *Pressure*, *Composition*, etc. - that will depend on the type of process being considered, the equipment in the process and the process intent. HAZOP focuses on specific portions of the process called "*nodes*". At a node, a process parameter is identified, say "*Flow*", and then combined with a guideword, e.g. "*No*", to give a possible deviation (in this example: "*No Flow*"). This generates a more extended checklist of generic guidewords to be used as "prompts". Generic guidewords for flow in a chemical process can be: *High Flow*, *No/Low Flow*, *Reverse Flow*, *Misdirected Flow*, *High Pressure*, *Low Pressure*, *High Temperature*, *Low Temperature*, *High Contaminants*, *Leak*, etc. (a more complete list for continuous chemical processes is given in Table 5.6). For processes utilizing energetic materials, the generic guidewords include: *Electrical Initiation*, *ESD spark*, *Impact shock*, *Friction*, *Impingement*, *Incompatibilities*, *Explosive Shock*, *Thermal Ignition*, *Propagation*, *Personnel Injury*, *Environmental Contamination*, *Equipment Damage*, *Product Damage*, etc.

Table 5.6 ***Generic HAZOP guidewords for continuous chemical processes***

No Flow	*Less temperature*	*Sampling*
Less Flow	*More temperature*	*Corrosion/Erosion*
More Flow	*Less viscosity*	*Service Failure*
Reverse Flow	*More viscosity*	*Abnormal Operation*
Less Level	*Composition Change*	*Maintenance*
More Level	*Contamination*	*Ignition*
Less Pressure	*Relief*	*Spare Equipment*
More Pressure	*Instrumentation*	*Safety*

One looks then for the credible causes (the reason why a deviation might occur) and consequences (the results of a deviation) of the identified possible deviations. Once the causes and consequences are recorded, the team identifies the existing or potential safeguards.

Safeguards are mechanisms/devices that help to reduce the occurrence frequency of the deviation or to mitigate its consequences. There are, in principle, five types of safeguards:

1. Devices that *identify* the deviation. These comprise, among others, alarm instrumentation and human operator detection.
2. Mechanisms that *compensate* the deviation (e.g. an automatic control system that reduces the feed to a vessel to prevent overfilling if the deviation is “increase of level”). These usually are an integrated part of the process control.
3. Mechanisms that *prevent* the deviation to occur (e.g. an inert gas blanket in storages of flammable substances).
4. Mechanisms that *contain* further escalation of the deviation (e.g. by total trip of the activity). These mechanisms are often interlocked with several units in the process, often controlled by logical computers.
5. Devices that "*relief*" the process from the hazardous deviation (these comprise for instance: pressure safety valves and vent systems).

Finally, recommendations are made that include design, operating, or maintenance changes able to reduce or eliminate unsafe deviations, causes and/or consequences.

The above process is repeated for all nodes, parameters and guidewords (see Fig. 5.4). Such a systematic approach, considering each node, mode of operation, and type of hazard in turn, minimizes the chance of overlooking a problem. The method can be made semi-quantitative by using a *Risk Ranking Matrix* (as in the FMEA case, see section 5.2), with estimated severity and likelihood rankings for each identified hazards.

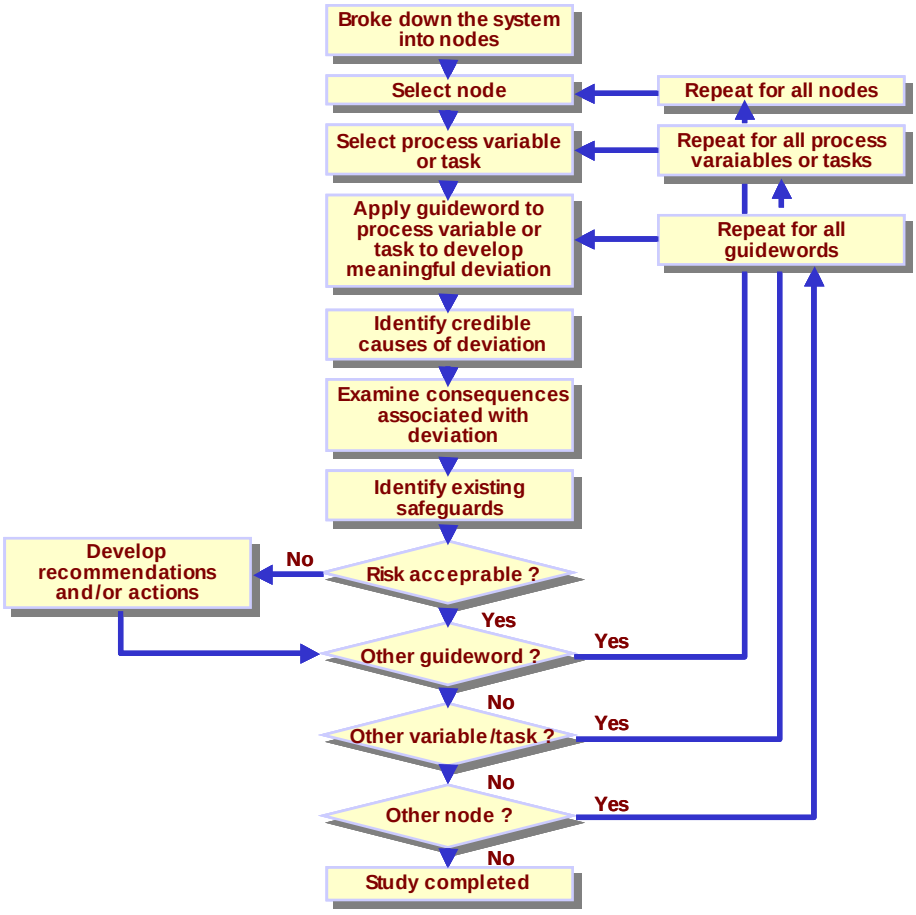


Figure 5.4 ***Block diagram of the HAZOP process***

HAZOP applications

To illustrate first the concepts used in the HAZOP method, imagine that as part of an industrial facility a cooling water system is required. This one is roughly schematized below.

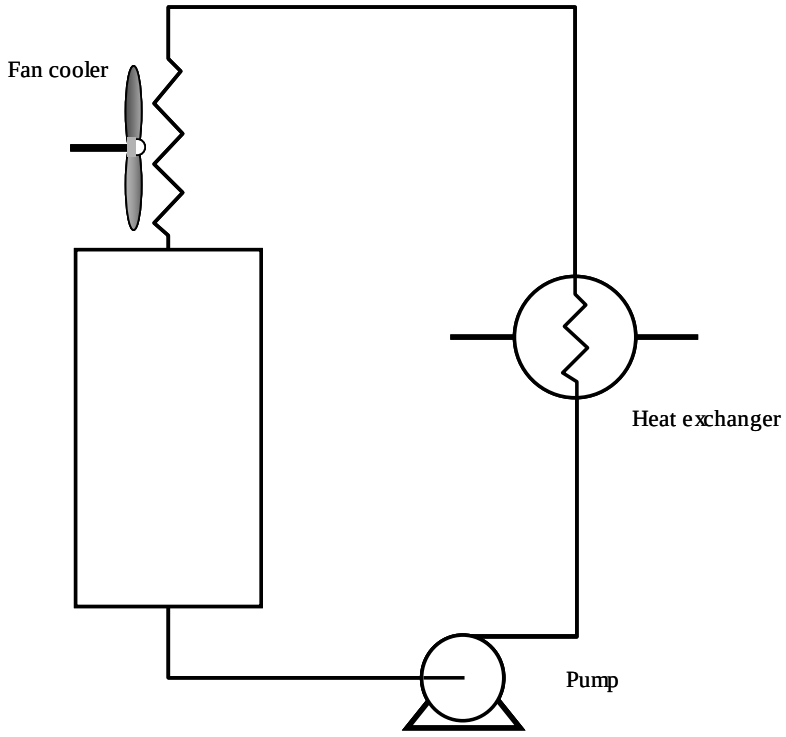


Figure 5.5 ***Cooling water system***

Table 5.7 gives in that particular case the appropriate definitions of the main terms used in HAZOP.

Table 5.7 ***Definition of HAZOP terms for the particular example of Fig. 5.5***

Node	Heat exchanger
Intent	To continuously provide cooling water at a given temperature of *x* °C and at a rate of *y* liters per hour
Parameter	Temperature
Deviation	Cooling water at too high a temperature compared with the design intent
Guideword	*Higher (more) temperature*
Causes	Failure of the fan cooler or failure of the pump
Consequence	Cooling is not assured as intended, which could result in serious damages for the facility

Note the difference between a *deviation* and its *cause(s).* In the case above, failure of the fan cooler or the pump will be causes, not deviations.

An example of a section of a HAZOP analysis table is given in Table 5.8 for the simple process system presented in Fig. 5.6 (from [Hendershot et al., 1998]).

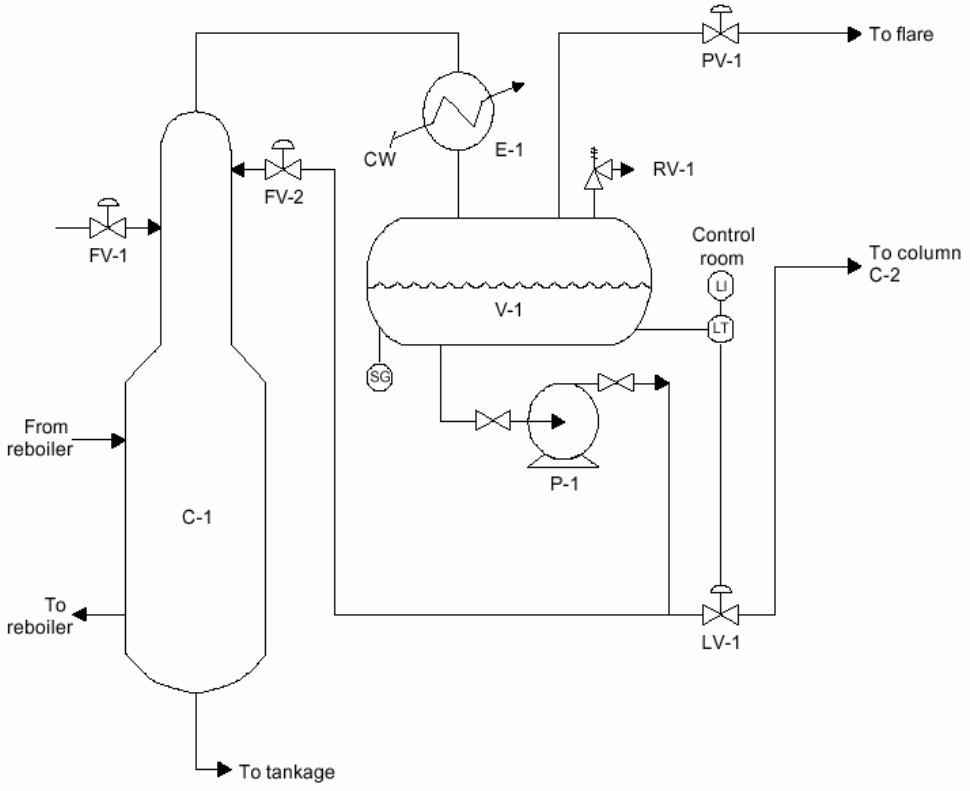


Figure 5.6 *Example system for HAZOP analysis*

Table 5.8 *Section of a HAZOP analysis table for the system shown in Fig. 5.6*

Section 5: Accumulator V-1					
Deviation	**Causes**	**Consequences**	**Safeguards**	**Risk**	**Recommendations**
High level	Insufficient flow from P-1 **(See the generic FMEA for centrifugal pumps)** Operator fails to start or inadvertently stops P-1 • • •	Overflow of V-1, possibly causing a major upset at the flare and/or in other systems connected to the flare header High pressure in C-1 (see the high pressure deviation for C-1)	Field checks of the sightglass on V-1 **(See the generic FMEA for sightglasses)** Control room indication from LT-1 **(See the generic FMEA for level control loops)**	Medium	Add independent high level switch/alarm to V-1 (Engineering)
• • •	• • •	• • •	• • •		• • •

Strengths and limitations of HAZOP

HAZOP helps to efficiently identify the steps needed to move the design and safety management process forward, and to formally record and demonstrate that safety and operability issues have been correctly addressed. This assists in formally demonstrating that hazards have been identified and avoided or the resulting risks have been reduced to an acceptable level.

More specifically, the HAZOP strengths are the following:

- HAZOP is a systematic and powerful process-engineering tool to identify hazardous deviations from an original or existing intent.
- HAZOP is a very versatile technique that can be applied to both continuous and batch processing.
- HAZOP utilizes combined experience of staff in a constructive way. It facilitates interaction between design and 'end user' personnel and is an ideal medium for process operators and line management to interact with senior management to highlight areas of concern.
- HAZOP helps establishing a milestone that permits detail design proceed unhindered.
- HAZOP can highlight where scarce capital expenditure can be directed to those areas where resources need to be applied to meet company and regulation requirements.
- HAZOP can give confirmation of plant 'fitness for purpose'- non-essential equipment and piping is avoided at design stage.
- HAZOP can identify where process operability problems exist and hence elimination of such problems can result in improved reliability of plant and cost effective modifications undertaken.
- HAZOP has proven benefits in reducing commissioning and start up delays.

In the case of existing plants that have been extensively "debottlenecked" or modified, and thus may have deviated from original design intent and safety concepts, a HAZOP study will assist in reviewing such changes.

Contrary to the FMEA, the HAZOP method does not require the systematic study of all the failure modes of the system but rather focuses on "failure events". It is however not always straightforward to attribute a well delimited part of the system to each couple "guideword-parameter", which could lead to errors in the analysis or to the risk of overlooking complex events chains.

HAZOP can be a quite time-consuming process, especially when many people are involved in the brainstorming sessions. A typical HAZOP study can take 1-8 weeks to complete, costing about $ 10'000 per week. Moreover, not always can closed recommendations for avoidance or mitigation of the observed hazards be derived within the team. The basic purpose of a HAZOP study is to identify potentially hazardous scenarios. Therefore, the team should not spend any significant time trying to engineer a solution if a potential problem is uncovered. If a solution to a problem is obvious, the team should document their recommended solution. If a solution is not obvious, they should only recommend to follows and resolves the problem outside the HAZOP study. Such recommendations will imply the instruction to have specific design items be reviewed by the design - or engineering department.