Chapter 3

Enterprise

1 Manufacturing Process Management

Manufacturing process management (MPM) is the discipline of defining how products are manufactured so production processes can be made more efficient and responsive. The MPM process starts with manufacturing engineers evaluating the requirements of the product design and defining the necessary production qualities, including whether partners will be involved.

The process definition is usually sent to enterprise resource planning (ERP) and manufacturing execution system (MES) or manufacturing operations management (MOM) software, which executes and monitors the production process, including outputting printed or electronic work instructions [1].

Automatic Control System

✓ works in real time;

✓ checks the safety;

✓ an accurate representation of the situation (to the operator);

✓ data representation to other systems (inside the factory)

not just one algorithm but number of interconnected functions.

Automatic control types are

- Main control (feedback),
- Procedural (sequencing),
- Coordinated (shared resources),

- Supervisory control (SP),
- Special (failures), startup, shutdown.

Idea: observe and control the processes as a whole, will give the better results. Question: how to make it?

Problems with Precise and complex control

- Work content and high cost to design a model.
- Design of the controller, usage, modification.
- Clarity and transparency of the control structure.
- Difficult to operators (complexity).

Better solution is to simplify the control actions

- Divide the process into parts with precise functions.
- For each part its own control tasks.
- Coordination of the parts (upper level, the slower time scale).

MPM focuses on *how* to manufacture a product.

Benefits of MPM include the following:

- Improved efficiency of engineering and design processes through reuse of standardized products designs and production plans;
- Faster production ramp-up through the use of digital simulation and training;
- Reduced scrap materials and rework;
- Lower costs of product-design changes [1].

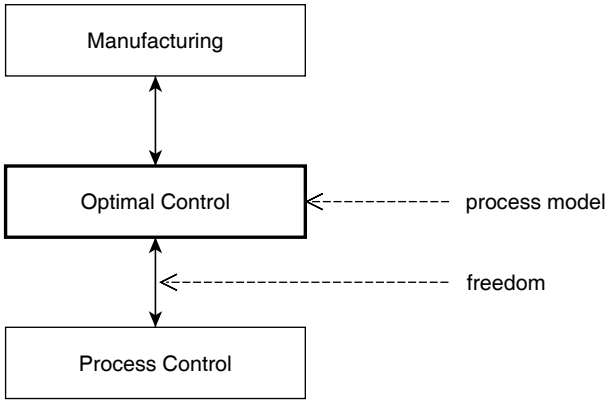
1.1 Optimization

Complex processes give freedom to choose process's parameters.

Aim: maximal profit, minimal expenses and wastes.

The hierarchy of optimization:

1. Equipment work optimization
    - objective is understood;



- does not depend on the other devices work.

2. Company's work optimization

   - confusing, requires careful work
     - provide model of the process, check the data
     - define the objective (market):
       ✓ is it possible to sell the excess product → max volume
       ✓ if only necessary amount of product could be produced → min cost

Methods: Newton, Simplex, ...
Tools: Matlab, AMPL, Octave, Scilab

2 Asset management

Company's assets are:

process equipment: buildings, machinery, boilers, etc and

controllers - 5..15% of the project cost

- PLC, PC, valves - physical assets
- distributed systems, networking - (in the accounts)
- programs, tuning - software

staff: knowledge, skills, experience

The purchase of equipment is an investment that requires intensive use of these devices. Is there justification of expenses?

ROI (Return on investment):
Keep the equipment working with the maximum efficiency

- Do the same at lower cost (time, money, energy);
- Or do more with the same amount of resources.

Work and activities:

Monitoring - states of the devices and loops, observation of the work, diagnostics, problem detection

How does it actually work?

Operation - equipment maintenance

Purpose: to keep devices working, restore to normal state throughout the equipment life cycle.

Enterprise Asset Management EAM involves the management of the maintenance of physical assets of an organization throughout each asset's lifecycle.

Streamline lifecycle management for your property, plant, and equipment assets.

Integration with Enterprise Resource Planning (ERP) and operational technology systems – and support of preventative maintenance, asset utilization, remote monitoring, real-time analytics, and more.

By helping to ensure that high-value assets operate the way they are designed to, enterprise asset management can both minimize risks and costs and optimize business value.

Failures are inevitable in complex systems, but careful design, manufacturing and maintenance policy can control their occurrence and consequences.

Design of complex equipment is trade-off between achieving the required performance and acceptable reliability.

2.1 Reactive/corrective maintenance [2]

"Do not touch if it works"

- The event driven service / maintenance;
  - Searching for the error + repair;
  - Works arise in inappropriate time:
    - ✓ 27% of the failures take place during working hours Mon-Fri 8:00 to 17:00,
    - ✓ 78% of the failures take place beyond working hours.

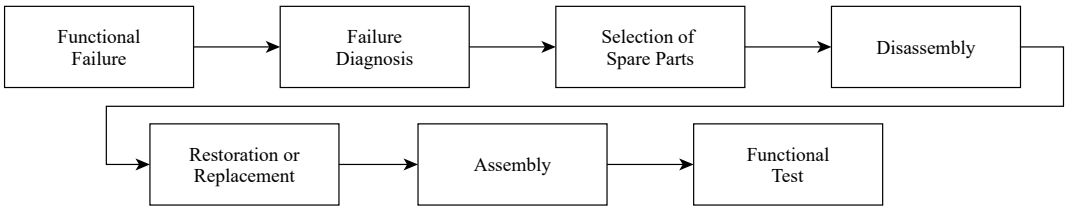


Figure 3.1: Activities of a corrective maintenance

Idle time costs a lot ≈ 3500 per hour

The basic activities are:

Most time consuming: failure diagnosis or disassembly and assembly.

Advantages:

- Lower short-term costs: no actions before the failure;
- Minimal Planning require;
- Simpler processes: easy to understand - take action then problem appears;
- Best solution in some cases: stop and repair costs in case of failure will be less than investment to preventive maintenance.

Disadvantages:

- Unpredictability;
- Paused operations: unavailability of materials and increasing equipment downtime;
- Equipment not maximized: reduces the lifetime of the assets;
- Higher long-term costs: in case of catastrophic failure it can be extremely costly.

2.2 Preventive maintenance

- According to the schedule with specified time intervals;
  - Minimal expenditure;
  - Forced replacement of the working devices
    - ✓ creates a lack of understanding with business management,
    - ✓ does not preclude the occasional failures.

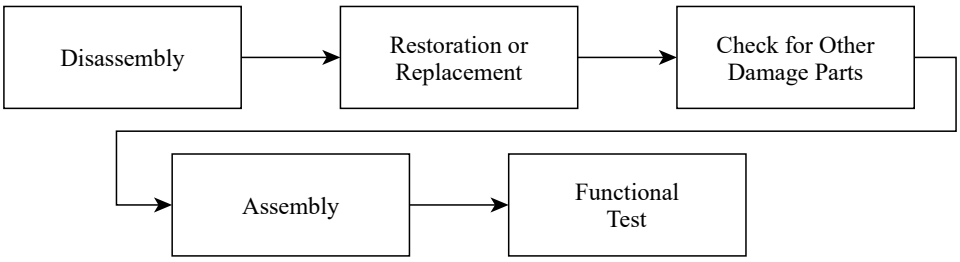


Figure 3.2: Activities of a preventive maintenance task

- Item is subject to a critical failure (major economical consequences);
- Item shows a rapid increase of failure rate.

Advantages:

- Prolonged life of company equipment;
- Less unplanned downtime;
- Fewer errors in day-to-day operations;
- Fewer expensive repairs caused by unexpected equipment failure
- Reduced risk of injury.

Disadvantages:

- Requires maintenance planning;
- Investment in time and resources;
- Equipment not maximized: parts are often replaced before end of life;
- Higher upfront costs;
- More workers: regular checks are must.

2.3 Predictive maintenance

PdM directly monitors the condition and performance of equipment during normal operation to reduce the likelihood of failures.

When error can occur in the device work?

- Monitoring of the parameters (vibrations, pressure drop, power consumption, accuracy decrease, etc.);
  - Analysis of the trends;
  - Replaced before the malfunction of the device
    ✓ we know exactly what needs to be replaced (fully depreciated!),
    ✓reduced unexpected downtime.

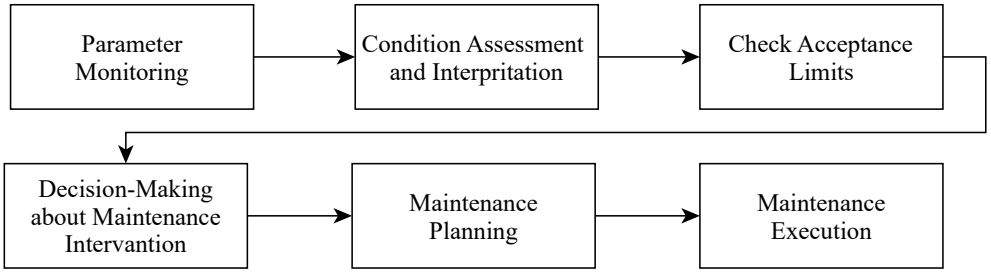


Figure 3.3: Activities of a predictive maintenance

Three criteria to be applicable:

1. Possibility to detect reduced failure resistance,
2. Possibility to define a potential failure condition,
3. Existance of interval between the time of potential failure and time of functional failure.

2.3.1 Condition monitoring

Most frequent condition monitoring techniques:

1. Vibration based
   - Equipment: pumps, compressors,turbines, el. generators and motors.
   - Used: data acquisition, signal processing system, algorithm for decision-making problem.
2. Lubrication oil analysis
   - Schedule oil change
3. Wear particle analysis

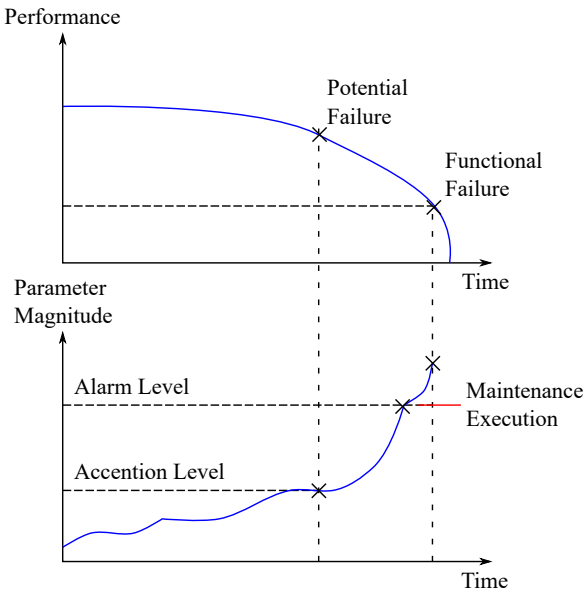


Figure 3.4: Development of a potential failure mode

- Analysis of cating oil

4. Performance monitoring
   - Diagnose the system operational condition
   - Thermometers, pressure gauges, flow meters
5. Non-destructive techniques
   - Monitor the deterioration of some components
   - Magnetic particle inspection, acoustic emission testing, radiographic, ultrasonic and thermographic inspection.

Advantages:

- Predicts failures before they occur;
- Parts will be shut down only before imminent failure;
- Saves time and money in the long run.

Disadvantages:

- Higher upfront cost: cost of equipment is high;
- Necessity of employee training: skill level and experience for condition monitoring is high;
- Time commitment to develop and implement program.

Main factors identifying which asset should be considered for PdM:

- What is the impact on production if the asset failure unexpectedly?
- Can cost-effective tasks be performed proactively to prevent the consequences of the failure?
- What is the average cost of repairing this asset?

3 Safety

Reliability-Centered Maintenance (RCM) has been so named to emphasize the role that reliability theory and practice plays in properly focusing (or centering) preventive maintenance activities on the retention of the equipment's inherent design reliability. As the name implies, then, reliability technology is at the very center of the maintenance philosophy and planning process [3].

3.1 Failure

Human life and activities are related to threats (a significant bad impact to)→ health, property, environment (is caused by) ← nature, people and technology.

- Natural disaster (earthquake, flood, ...), with the consequences
  - involved government and insurance
- Human activity can cause harm, "Security"
  - legal safeguard: police, prosecution, courts
- Accidents using the technology
  - mining, electricity, traffic, boilers, transport, etc.
  - (learn from your mistakes, but learn from the tests on the way!)

We do not like accidents, but they happen.

People do work, using technology created by people, make mistakes → probability for accidents.

Every new technology and increase in complexity raise the risks.

Some systems are particularly dangerous.

✓ So-called higher risk associated sites:

Safety Critical Systems

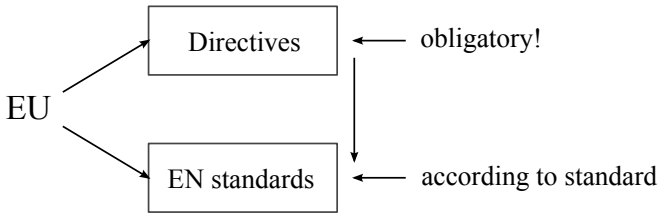
- nuclear energy, railroad systems, aviation, traffic equipment, medical equipment, chemical plants, boilers, safety devices

✓ Careless usage leads to danger,

✓ Those projects are designed and built differently.

All hazardous processes must be controlled in appropriate manner in normal as abnormal situations.

The European Union Legislation: Safety is a comprehensive and universal requirement for people and the environment must be protected against the risk.



1. EU directives

EU Directive	Eesti Vabariigi seadus (Estonian laws)
97/23/CE Pressure Equipment Directive	Surveseadmete ohutuse seadus (Pressure Equipment Safety Law)
88/609/EEC on the limitation of emissions of certain pollutants into the air from large combustion plants	Välisõhu kaitse seadus. Säästuse kompleksse vältimise ja kontrollimise seadus.

EU Safety Directive 96/082/EEC requires to

✓ Define all hazardous events and associated risks.

✓ Reduce the risk to an acceptable level.

✓ Ensure that the precautionary measures realize the risk.

✓ Ensure that safety is maintained during all operational time.

2. Standard (EN)–defines the different and significant knowledge and experience of many people

- How to do a good work
- Is not a manual for specific actions

Employer / employee responsibilities:

If an employee receives the task, you will need to take into account the knowledge of the staff (training) and skills.

Anyone who does anything should be convinced that the result of the operation is correct.

Do not put people in a dangerous situation!

✓ Safety principles are common (chemical, energy, engineering, etc).

✓ People used to expect that systems and equipment are safe, often do not know how to react when something happen.

✓ Automation increases the safety level (sometimes without automation is not possible to manage situation).

✓ The increasing complexity of safety-related systems, safety devices are "intelligent", a software and data exchange in several directions.

Statistical description of events
the probability P of event during the time t is $P = n/N$
n- number of events, N - number of observable elements
λ- the fault rate is the "probability / unit time".

Event Probabilities Human error probabilities:

- reads value inaccurately - 0.005
- driver does not notice the main road - 0.0005
- calculates incorrectly - 0.01
- does not respond to an event that took place 1 mim. ago - 0.9
- operator (in case of failure with several alarms) avoids emergency shoutdown with probability 0.2 . . . 0.5

The fatal event probabilities:

- flying $2 \cdot 10^{-6}$ $1/y$ $\quad 2 \cdot 10^{-10}$ $1/km$
- car $100 \cdot 10^{-6}$ $1/y$ $\quad 5 \cdot 10^{-10}$ $1/km$
- industry $4 \cdot 10^{-8}$ $1/h$ *or* 8000 in EU per year
- boxing $20000 \cdot 10^{-8}$ $1/h$
- swimming $1300 \cdot 10^{-8}$ $1/h$

- incidence of cancer $24 \cdot 10^{-4}$
- total: 10^{-2}

Components fault rate

- micro-processor $0.3 \cdot 10^{-6}$ $1/h$
- PLC $20 \cdot 10^{-6}$ $1/h$
- switch $0.5 \cdot 10^{-6}$ $1/h$
- valves $10 \cdot 10^{-6}$ $1/h$
- transistor faulty work 10^{-14} 1/switch
- tanker accident 0.4/1000 for refueling
- industry-pump crash: $1\times$ per 5 years

Reliability is a probability P that the device/system performs correctly (under certain conditions, during a certain period of time).

Fault rate λ "number of faults / unit of time"

unit of time: hours, 1000 hours, 10^6 hours, a year (pa "per annum")

The most fundamental measure of (un)reliability is the failure rate of a component or system of components λ.

$$\lambda = \frac{\mathrm{d}N_f}{\mathrm{d}t}\frac{1}{N_s} \approx \frac{N_f}{N_s \cdot t}, \tag{3.1}$$

where λ - failure rate, N_f - number of components failed during testing period, N_s - number of components surviving during testing period, t - time period.

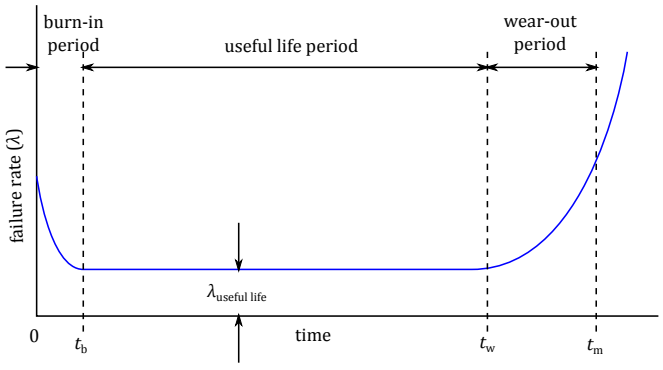


Figure 3.5: Life characteristic curve

In case of $\lambda = \text{const}$ Reliability (R) is the probability of a component or system will perform as designed when needed.

$$R(t) = e^{-\lambda t} \tag{3.2}$$

The reliability of a component over a specified time is a function of time, and not just the failure rate (λ).

Fault probability

$$q = 1 - R \tag{3.3}$$

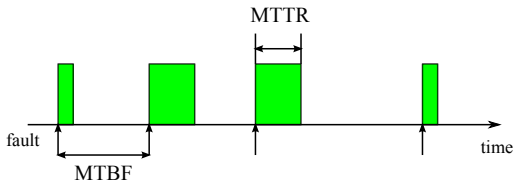
$$\lambda_{\text{useful\_life}} = \frac{1}{\text{MTBF}}, \tag{3.4}$$

where MTBF is a mean time between failures.

System is repaired during MTTR time and works further. System is characterized by availability

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}, \tag{3.5}$$

which shows what time part system is working.



availability	idle time [pa]
95 %	18 days
99 %	4 days
99.9 %	9 days
99.99 %	1 hour

3.1.1 Reliability of Series Systems

$$R_s(t) = R_1(t) \cdot R_2(t) \cdot \ldots \cdot R_n(t) = \prod_{i=1}^{n} R_i(t) \tag{3.6}$$

$$R_s(t) = e^{-t \cdot \sum_{i=1}^{n} \lambda_i} \tag{3.7}$$

The system reliability decreases rapidly as the number of components is increasing.

The purpose of a Safety Instrumented System (SIS) is to reduce the risk that a process may become hazardous to a tolerable level. The SIS does this by decreasing the frequency of unwanted accidents. The amount of risk reduction that an SIS can provide is represented by its Safety Integrity Level (SIL), which is defined as a range of probability of failure on demand [4].

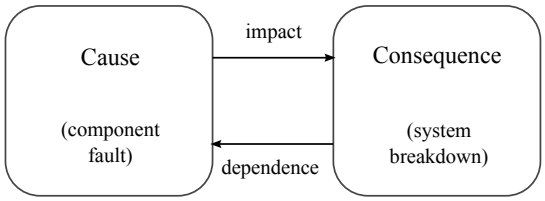
3.2 Methods

The method organizations use to select SILs should be based on their risk of accident, an evaluation of the potential consequences and likelihoods of an accident, and an evaluation of the effectiveness of all relevant process safeguards [4].

- LoPA
- HAZOP
- fault detection analysis
- fault tree analysis
- event tree analysis

Readiness to known threats. How to estimate safety and related risk.

Unexpected dangerous events?



Often it is useful to use more than one method. Hazard and risk assessment are real, but not very accurate.

At your work real problems are caused by the things you have never thought about!

3.3 Consequence Analysis

Consequence analysis is the act of estimating the damage that results from a process accident [4, 2, 5].

$$\text{Risk}\left(\frac{concequence}{time}\right)=\text{likelihood}\left(\frac{event}{time}\right)\times\text{Impact}\left(\frac{concequence}{event}\right) \tag{3.8}$$

Risk —uncertainties associated with events.

It is measured as effect distances or effect zones .

1. Qualitative Methods
2. Semi-Quantitative Methods

3. Statistical Analysis of Accidents

4. Quantitative Methods: Release Phenomena Modeling

3.3.1 Qualitative Methods

Qualitative estimation is a procedure by which an expert or a team of experts estimates the consequence of a hazard by simply using judgment based on their personal and corporate experience with the process.

- Although this method has the strength of simplicity, its drawbacks include its reliance on historical accidents and a large, broad pool of experienced personnel.
- Ineffective for processes that are new or have not had a large number of accidents.

3.3.2 Semi-Quantitative Methods

Tools for developing a general feel for the amount of risk in a process.

Semi-quantitative risk indices

- the Dow Fire and Explosion Index,
- the Dow Chemical Exposure Index.

The Fire & Explosion Index (FEI) provides a simple method to help determine the areas of greatest loss potential in a particular process. It also enables one to predict the physical damage that would occur in the event of an incident. Absolute measures of risk are very difficult to determine, but the FEI system will provide a method of ranking one hazard relative to another. It is NOT intended to define a particular design as safe or unsafe [6].

Semi-quantitative methods provide a result that combines the estimate of the consequence zone and the impact analysis within that zone.

3.3.3 Statistical Analysis of Accidents

Statistical analysis is tool used then long as sufficient data is available, which is rarely the case for process accidents.

Effective: when the data set is large;

Ineffective: in situations such as chemical releases where sufficiently large and specific data sets are unavailable.

The average consequence is determined by summing the total consequences and dividing by the total number of accidents.

The applicability of this method is narrow because extensive historical data must be amassed. It is not enough for the data set to cover a large time period; it must also contain a large number of accidents.

3.3.4 Quantitative Methods

Release phenomena modeling works by first analyzing the potential energy that a hazard contains in its pre-accident state. The method then estimates the effect of the release of that energy (potential) under the conditions that result from the loss of control of the process.

Release of

- mechanical energy,
- thermal energy,
- chemical reactive potential,
- electrical potential.

  In process plants, this release falls into three main categories: physical (such as a high-pressure vessel rupture), flammable, or toxic.

Modeling the physical and chemical phenomena surrounding a release is a very effective method, but it is also time consuming and requires a high level of expertise [4].

3.3.5 Effect zones

The consequence of an incident will depend on the size of the incident's effect zone and the zone's occupancy. Once both of these factors are known, you can integrate them into such consequence measures as Probable Loss of Life (PLL), Probable Injuries (PI), and Expected Value of loss (EV).

The occupancy for an area occupied only randomly by people is a function of the size of the effect zone.

$$O_{person} = A_{effec} \cdot \rho_{person} \tag{3.9}$$

Vulnerability is defined as the probability that a receptor, whether human or equipment, will sustain a defined level of harm when exposed to the effect of an incident [4].

For example consequence in terms of PLL can be calculated as follows

$$PLL = O_{person} \cdot V \tag{3.10}$$

3.4 Likelihood analysis

Breaking the overall failure into smaller, more quantifiable parts through a method called fault propagation modeling. These process event segments are often similar to other small process plant event segments. The more complex the system the greater the interaction between its constituent components, and the greater the need for a formal and systematic process to identify and classify effects [7].

We can then combine these small event probabilities to calculate the likelihood that the overall sequence will lead to a harmful failure of the larger system in question.

- Statistical Analysis
- Fault Propagation Modeling

The likelihood that smaller component events could occur, and thus contribute to an overall failure, is often determined by statistically analyzing historical data.

Two conditions must be met

1. There must be a sufficiently large amount of data to be analyzed.
2. All of the data must come from systems that are roughly similar so that any conclusions will be valid for the case in question.

Fault propagation modeling is the analysis of the chain of events that leads to an accident.

Fault propagation modeling techniques use the failure rates of individual components to determine the failure rate of the overall system.

Depending on the type of model used, different logical operations are allowed and thus different types of scenarios can be analyzed.

- Event Tree Analysis
- Reliability Block Diagrams
- Fault Tree Analysis
- Markov Analysis

3.4.1 Fault tree analysis

Standard IEC 61025. Dependence of a system failure on the components errors.

$$\text{Causes (component failure)} \Longrightarrow \text{Consequence (system failure)}$$

- Seeks and discovers deductively

- Detects the important phenomena for the failure
- Considers: the failures, mistakes, environment, service, etc.
- Long and slow.

Occurrence probability of events

AND: $P(A_1 \ \& \ A_2) = P(A_1) \cdot P(A_2)$

OR: $P(A_1 \vee A_2) = 1 - (1 - P(A_1)) \cdot (1 - P(A_2))$ (independent elements)

The objective of fault tree analysis is to determine the likelihood of the top event.

FTA is a top-down technique. The analysis starts with a specific failure condition (e.g., loss of power), and proceeds downward to define possible system and subsystem faults, conditions and user actions whose occurrence singly or in combination can cause this event [7].

FTA can be applied at any time during a product's life-cycle. However, it is most effective when applied:

1. During early development, based on preliminary design information.
2. After final design, prior to full scale production, based on manufacturing drawings.

3.4.2 Reliability Block Diagrams

The reliability block diagram is a more robust likelihood-modeling tool that is still relatively easy to use.

Block represents each equipment item in a system, and the arrangement of the blocks represents the logical relations between the potential failures of the components.

Items that are vertically aligned represent a parallel path (OR logic), and items that are horizontally aligned represent a series path (AND logic).

Some blocks represent complex equipment groups such as two-out-of-three voting.

3.4.3 Markov Analysis

Markov analysis is the most complex of the methods mentioned here; it is also the most accurate and flexible.

In Markov analysis there is a group of circles, each of which represents a system state.

The different states are connected by transitions.

These transitions are quantified by using either failure rates (λ), when the transition is from an OK state to a failed state, or repair rates (μ) when the transition is from a failed state back to an OK state.

$$\lambda \approx \frac{N_f}{N_s \cdot t}$$

$$A = 1 - \frac{\lambda}{\mu}$$

3.4.4 Event tree analysis

Event-driven sequence (possibly evolution of events from the initial one).
Suitable risk and loss calculation.

Starts Single initiating event: important parameter deviation, failure, explosion, accident, etc.

Evolution Branches: the different event sequence paths to the various outcomes. Each branch associates a probability of occurrence with each possible event in the branch set. Each of the events in each branch of an event tree has a probability of occurrence associated with it.

Branch closure Event tree analysis always results in multiple outcomes: the probability, loss, risk.

Example 1 *Pressure-Reducing Station*

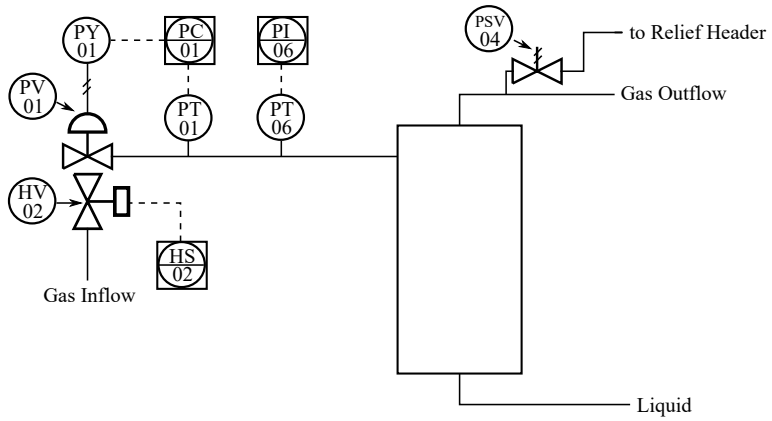


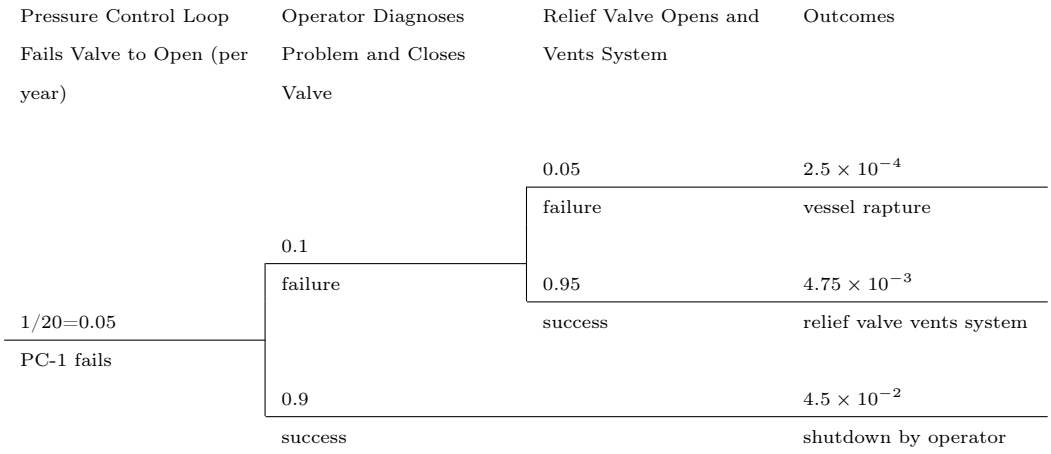
Figure 3.6: Example of pressure-reducing station [4]

Natural gas $P_{in} = 4,000kPa(g)$. The pressure is reduced to 900 kPa(g) as measured by PT-01, located downstream of the choke valve, PV-01. Piping and vessels downstream of the choke valve are designed for a $P_{max} = 1,500kPa(g)$.

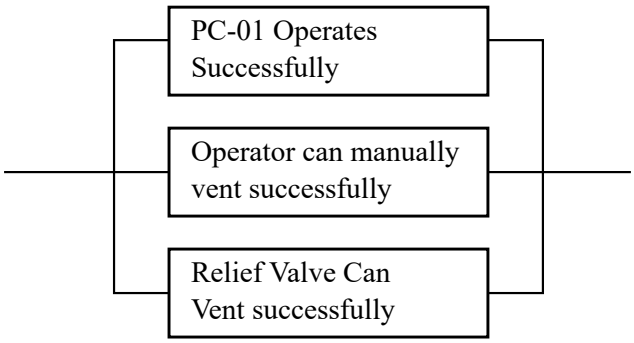
If the pressure-reduction control system fails so that the choke valve (PV-01) is in the open position, then the liquid knockout drum may rupture and cause a release of high-pressure natural

gas. This could potentially cause a fireball. The failure scenario:developing enough pressure to rupture the vessel would require at least 25 minutes. A historical reliability analysis yielded a failure rate in the open-valve position of once in twenty years.

The probability of failure for this type of relief valve in natural gas services is 0.05. The second protection layer is operator intervention. If the operator detects a high pressure from an alarm generated by PT-06 ansactivates HS-02, closing a shutoff valve upstream of the choke valve. Human error is the major contributor to the failure of this protection layer. A simplified analysis yielded a human error probability of 0.1. What is the rate at which a vessel rupture incident will occur without the addition of an SIF?



Event Tree Analysis Solution. Event tree analysis always results in multiple outcomes.



Reliability Block Diagrams Solution. All components must be described in terms of probability of success.

$$P_{s,RV} = 1 - 0.05 = 0.95 \tag{3.11}$$

$$P_{s,Man} = 1 - 0.1 = 0.9 \tag{3.12}$$

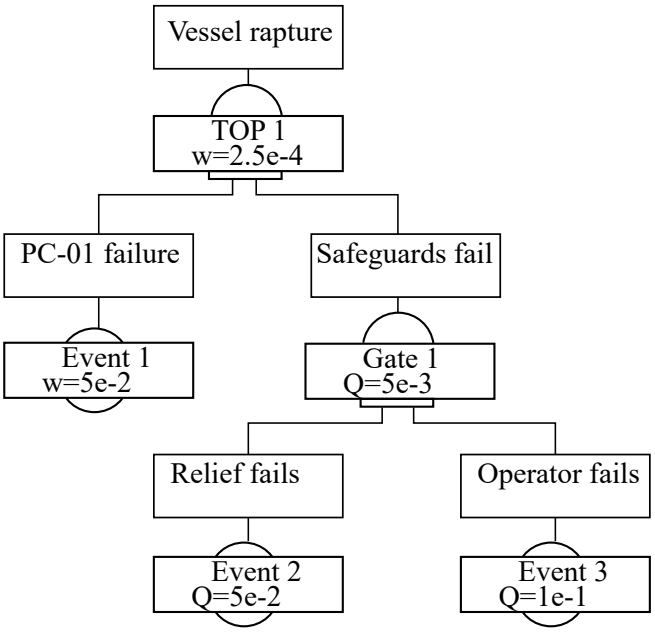
Success probability knowing failure rate

$$P_{s,PC} = e^{-\lambda t} = e^{-(1/20)\times 1} = 0.951$$

System success

$$P_{s,Sys} = 1 - [(1 - 0.95) \times (1 - 0.9) \times (1 - 0.951)] = 0.999755$$

Fault Tree Analysis Solution. The basic events are PC-01 failure, operator intervention failure, and relief valve failure. The top event of the fault tree is a vessel rupture.



3.5 Layer of Protection Analysis

LoPA is a simplified risk assessment method. Its provides a technique for evaluating the risk of hazard scenarios and comparing it with risk tolerance criteria to decide if existing safeguards are adequate, and whether additional safeguards are needed. It is a variation of event tree analysis that is limited and optimized for a specific situation.

The examples for analysis can be found on Application of LoPA: LoPa basic steps [6]. There are 3 questions to be answered for protection layers:

1. How safe is safe enough?
2. How many protection layers are needed?
3. How much risk reduction should each layer provide?

However, in LOPA the initiating events are always described in terms of frequency.

LoPA helps to decide now much risk reduction is needed and how many protection layers should be used. It does not help decide what specific IPs should be used.

Table 3.1: LoPA protection Layers

Protection Layers	Type of Device
Inherent safety in process design	Passive
Basic process control system (BPCS by PFD)	Active
Critical Alarms and Human intervention	Active/Human action
Safety instrumented functions (SIFs), e.g. Interlock	Active
Physical protection such as relief devices	Active
Post-release physical protection such as dikes	Passive
Plant Emergency Response	Human action
Community Emergency Response	Human action

BPCS is responsible for normal operation.
If the BPCS fails alarms will notify operations that human intervention is needed.
If the operator is unsuccessful then other layers are needed.

3.5.1 LoPA precedure

1. Identifying a single consequence;
2. Identifying an accident scenario/cause associated with the consequence;
3. Identifying the initiating event and estimating its frequency;
4. Identifying the protection layers for the consequence and estimate the probability failure on demand (PFD) for each layers;
5. Estimate a mitigated consequence frequency;
6. Estimate the risk by plotting the consequence versus the mitigated consequence frequency;

7. Evaluating the risk for acceptability (if unacceptable, additional layers of protection are required).

3.5.2 HAZOP precedure

Hazard and operability analysis used in chemical industry - standard IEC 61822.

1. Select a node, define its purpose and determine the process safe limits;
2. Select a process guide-word;
3. Identify the hazards and their causes using the deviation guide-words;
4. Determine how the hazard is found (how operator gets to know about it);
5. Estimate the consequences (safety, environmental, economic) of each identified hazard;
6. Identify the safeguards;
7. Estimate the frequency of occurrence of the hazard;
8. Risk rank of the hazard, with and without safeguards;
9. Develop potential recommendations.
10. Move on to the next process guide-word, or to the next node if the guide-word discussion is complete.

    HAZOP is a structured and systematic technique for system examination and risk management.

3.6 Industry process safety standards

IEC 61508	Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems
IEC 61511	Functional safety— Safety instrumented systems
IEC 61513	Nuclear Power stations

Basic Concepts:

- safety has life cycle
  - specification, design, realization, work, modification, etc.
- Safety Integrity Level (SIL)
  - $SIL_1 \dots SIL_4$
  - evaluation of risk reduction

SIL is proposed for the protection circuit component can be certified for SILx

3.6.1 Demand Mode of Operation

Table 3.2: SIL: Demand mode of operation

SIL	PFD	Risk reduction 1/PFD	Availability 1 − PFD
4	$< 10^{-4}$	> 10000	> 99.99 %
3	$10^{-4} \dots 10^{-3}$	$1000 \dots 10000$	99.9 % $\dots$ 99.99 %
2	$10^{-3} \dots 10^{-2}$	$100 \dots 1000$	99 % $\dots$ 99.9 %
1	$10^{-2} \dots 10^{-1}$	$10 \dots 100$	90 % $\dots$ 99 %

Probability to Fail on Demand (PDF)—is a statistical measurement of how likely it is that a process, system, or device will be operating and ready to serve the function for which it is intended. Among other things, it is influenced by the reliability of the process, system, or device, the interval at which it is tested, as well as how often it is required to function.

1/PFD is a risk factor reduction
1 − PFD is the availability

3.6.2 Continuous Mode of Operation

This is continuous or high-demand mode of operation.

Table 3.3: SIL: Continuous mode of operation

SIL	Frequency of Dangerous Failure Per Hour
4	$10^{-8} \dots 10^{-9}$
3	$10^{-7} \dots 10^{-8}$
2	$10^{-6} \dots 10^{-7}$
1	$10^{-5} \dots 10^{-6}$

The continuous mode is common in the machine industry and in avionics.

$$\text{SIL} = -\log_{10}(\text{PFD}_{\text{avg}}) \tag{3.13}$$

Example 2 *SIL calculation*

An SIF (safety instrumented function) is used in the demand mode of operation. SIF achieves a PFD $= 0.017$*. What is the SIL for this SIF?*

$$\text{SIL} = -\log_{10}(0.017) = 1.77$$

1. Thus, performance of SIF is closed to SIL2 category.

2. Check Demand mode of operation table.

3.6.3 Average PFD

Protective circuit probability to fail on demand

$$\mathrm{PFD}_{\max} = 1 - e^{-\lambda T} \tag{3.14}$$

The ordinary sensor does not detect its breakdown!

The actual situation of the protective circuit can be detected during technical inspection (for example, T_1 inspection interval is 6 months).

Unavailability of safety function or average probability of failure on demand

$$\mathrm{PFD}_{\mathrm{avg}} = \lambda \cdot T_1/2 \tag{3.15}$$

Note that PFD can be summed but not multiplied!

Example 3 *PFD_{max} and PFD_{avg} A relief valve has failure rate $\lambda = 1.68$ failures per 10^6 hours. Failure mode is "fails to open on demand". This valve is checked and tested annually. What is the maximum and average probability of failure on demand of this valve?*

$$\lambda = 1.68 \frac{\text{failures}}{10^6 \text{hours}} \cdot 8760 \frac{\text{hours}}{\text{year}} = 0.015 \frac{\text{failures}}{\text{year}}$$

$$\mathrm{PFD}_{\max} = 1 - e^{-0.015 \cdot 1} = 0.015$$

Thus, $\mathrm{PFD}_{\max}$ is essentially equal to the failure rate λ.

$$\mathrm{PFD}_{\mathrm{avg}} = \frac{0.015 \cdot 1}{2} = 0.0075.$$

Bibliography

[1] TechTarget. Manufacturing process management. [Accessed: April, 2018]. [Online]. Available: https://searcherp.techtarget.com/

[2] G. F. M. de Souza, Ed., *Thermal Power Plant Performance Analysis.* Springer Series in Reliability Engineering, 2012.

[3] A. M. Smith and G. R. Hinchcliffe, *RCM: Gateway to World Class Maintenance.* Elsevier Butterworth–Heinemann, 2004.

[4] E. M. Marszal, *Safety integrity level selection: systematic methods including layer of protection analysis.* ISA—The Instrumentation, Systems, and Automation Society, 2002.

[5] V. Molak, *Fundamentals of Risk Analysis and Risk Management.* CRC Press, Inc., 1997.

[6] S2S. (2003) A gateway for plant and process safety. [Accessed: May, 2018]. [Online]. Available: http://www.safety-s2s.eu

[7] R. T. Anderson, *Reliability-Centred Maintenance: Management and Engineering Methods.* ELSEVIER Applied Science, 1990.