Enterprise

1 Manufacturing Process Management

Automatic Control System

- works in real time
- check 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 can be caused by:

- the material flows between the devices, warehousing, stocks

  synchronization of the processes

  recycle (heat, materials)

drastically changes the time constants and flows values

- interconnection of the loops creates large systems
- the intensity of the continuous processes changes

  100 % $\rightarrow$ 2 %, startup, shutdown

Problems with Precise and complex control

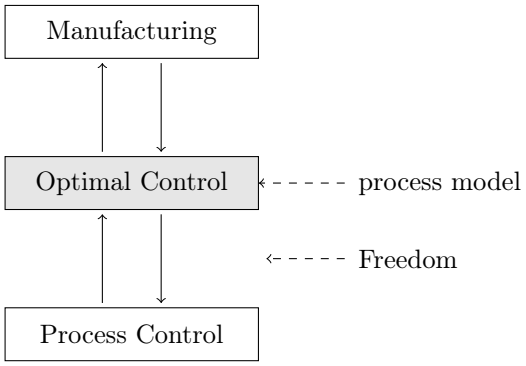
- work content and high cost to design a model
- design of the controller, usage, modification
- clarity and transparency of the control structure
- difficult to operators (complexity)

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)

2 Optimization

Complex processes give freedom to choose process' 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

3 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

Possible activities:

1. Reactive maintenance - "Do not touch if it works"
   - the event driven service / maintenance
   - searching for the error + repair
   - works arise in unappropriate time:

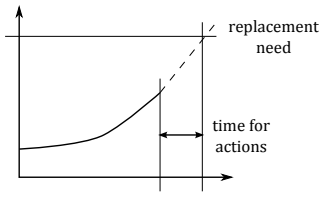
     27% of the failures take place during working hours Mon-Fri 8:00 to 17:00

     78% of the failures take place beyond working hours

     idle time costs a lot ≈ 3500 per hour
2. Preventive maintenance
   - according to the schedule with specified time intervals
   - min. expenditure
   - forced replacement of the working devices

     creates a lack of understanding with business management

     does not preclude the occasional failures
3. Predictive maintenance - 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

Safety

4 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):

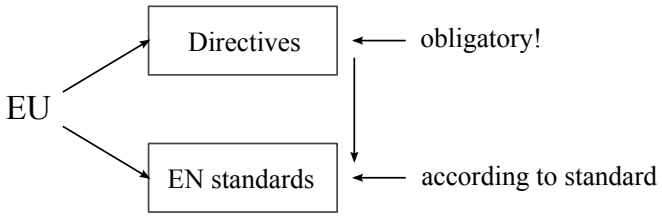
  nuclear energy, railroad systems, aviation, traffic equipment, medical equipment, chemical plants, boilers, safety devices

✓ 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

- 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".

Examples:

- 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 $0.2 \ldots 0.5$
- 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

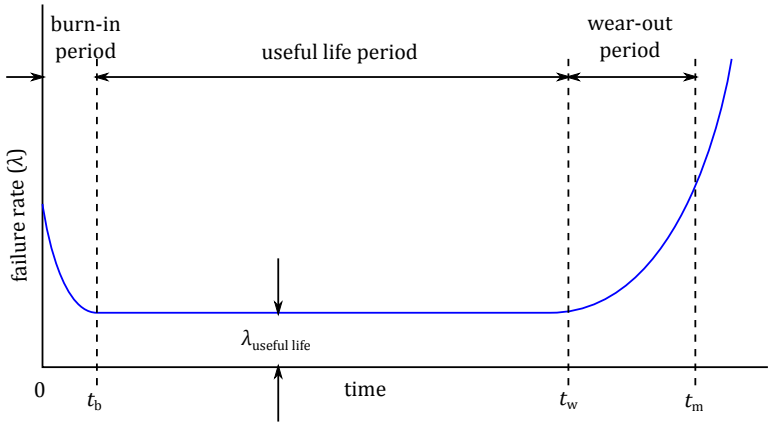
Reliability is a probability P that the device/system performs correctly(under certain conditions, during a certain period of time).
Fault rate λ "number of faults / unit of time"

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. The definition of "failure rate" for a group of components undergoing reliability tests is the instantaneous rate of failures per number of surviving components

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

where λ - failure rate,
N_f - number of components failed during testing period,
N_s - number of components surviving during testing period,
t - time.
Failure rate tends to be constant during a component's useful lifespan where the major cause of failure is random events. However, lambda does not remain constant over the entire life of the component or system. This curve profiles the failure rate of a large sample of components (or a large sample of systems) as they age. Failure rate begins at a relatively high value starting at time zero due to defects in manufacture. Failure rate drops off rapidly during a period of time called the burn-in period where defective components experience an early death. After the burn-in period, failure rate remains relatively constant over the useful life of the components, and this is where we typically define and apply the failure rate (λ). Toward the end of the components' working lives when the components enter the wear-out period, failure rate begins to rise until all components eventually fail. The average life of a component (t_m) is the time required for one-half of the components surviving up until the wear-out time (t_w) to fail, the other half failing after the mean life time [1].

In case of $\lambda = const$ Reliability (R) is the probability of a component or system will perform as designed when needed. Given the tendency of manufactured devices to fail over time, reliability



decreases with time. During the useful life of a component or system, reliability is related to failure rate by a simple exponential function

$$R(t) = e^{-\lambda t} \tag{2}$$

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

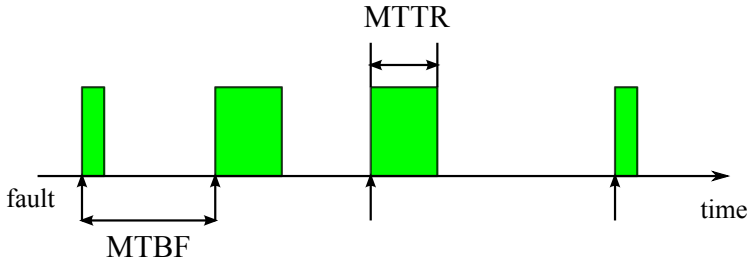
$$q = 1 - R \tag{3}$$

$$\lambda_{useful\ life} = \frac{1}{MTBF}, \tag{4}$$

where MTBF is a mean time between failures. MTBF is the correct term when talking about an item of equipment that is repairable. When we consider items that are not repaired when they fail, then Mean Time To Failure (MTTF) is the more correct term, but it does not much matter as they mean the same thing, Often MTBF is used when talking about non-repairable items too.

If $\lambda \cdot t \ll 1$, then $R \approx 1 - \lambda \cdot t$ and fault probability $q \approx \lambda \cdot t$

λ depends on the operating mode (U, t°). In case of failure system should be repaired. System



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

$$availability = \frac{MTBF}{MTBF + MTTR}, \tag{5}$$

which shows what time part system is working.

Availability is different from reliability in that it takes repair time into account. An item of equipment may not be very reliable, but if it can be repaired quickly when it fails, its availability could be high.

availability	idle time
95%	18 days
99%	4 days
99.9%	9 hours
99.99%	1 hour

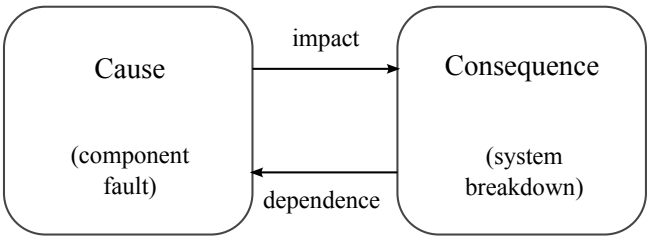
5 Safety analysis

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

- unexpected dangerous events?

Methods:

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



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

5.1 Layer of Protection Analysis (LoPA)

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.

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?

Risk tolerance criteria must be established for LoPA and they address the first issue.

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 IP:s should be used [2].

Protection Layers	Type of Device
Inherent safety in process design	Passive
Basic process control system (BPCS)	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

The Basic Process Control System (BPCS) is responsible for normal operation. If the BPCS fails to maintain control, alarms will notify operations that human intervention is needed. If the operator is unsuccessful then other layers of protection need to be in place to bring the process to a safe state and mitigate any hazards.

LoPA procedure

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).

5.2 Hazard and operability analysis (HAZOP)

Used in chemical industry - standard IEC 61822.

HAZOP is a structured and systematic technique for system examination and risk management. In particular, HAZOP is often used as a technique for identifying potential hazards in a system and identifying operability problems likely to lead to nonconforming products [3].

HAZOP procedure

1. Select a node, define its purpose and determine the process safe limits;

2. Select a process guideword;

3. Identify the hazards and their causes using the deviation guidewords;

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 guideword, or to the next node if the guideword discussion is complete.

Significantly affects the analysis:

- the source data (diagrams, drawings) quality

- qualifications of experts

5.3 Fault tree analysis (FTA)

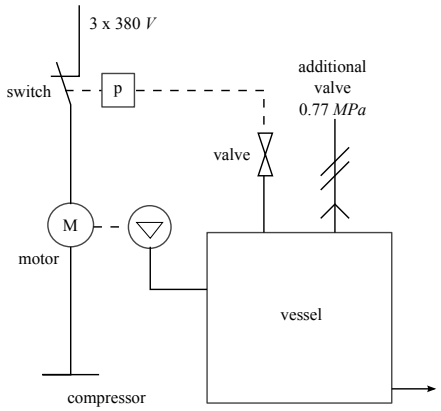
Standard IEC 61025. Dependence of a system failure on the components errors

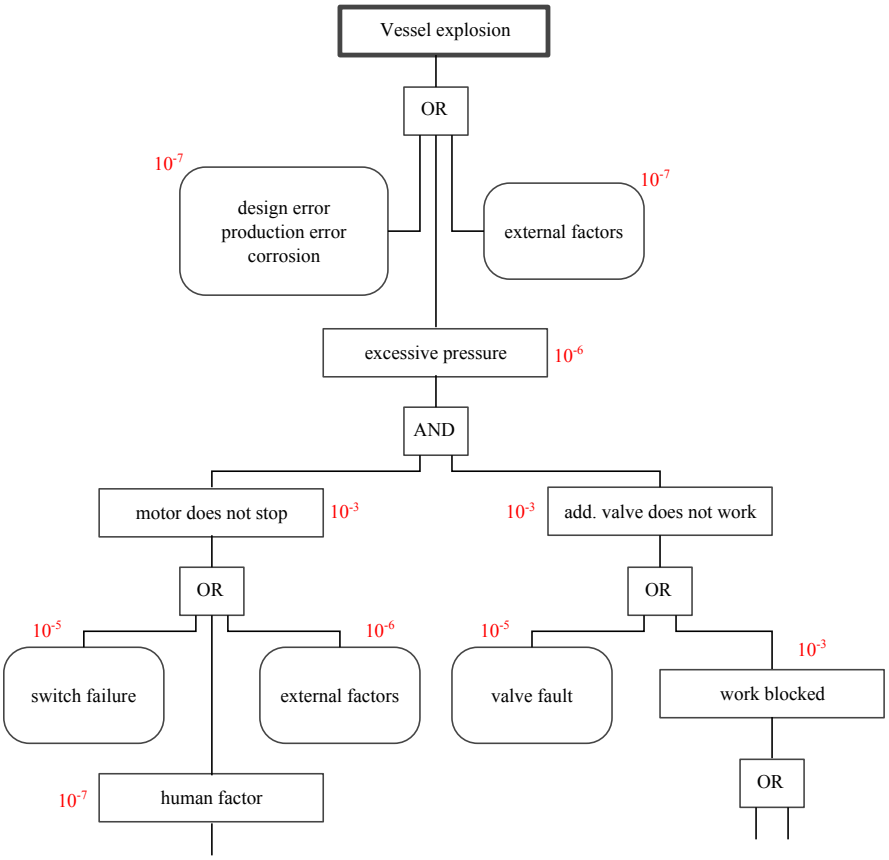
Consequence (system failure) → Causes (component failure)

- Seeking 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)

Example 1 *Air compression system*





5.4 Event tree analysis

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

Starts important parameter deviation, failure, explosion, accident, etc.

evolution branches - alternatives

branch closure the probability, loss, risk

Example 2 *Dust explosion at sawmill*

Dust explosion	Fire	Exting.	Alarm	Probability	loss	Risk
			yes	B_1 $7.9 \cdot 10^{-3}$	0.001	$7.9 \cdot 10^{-6}$
		yes	0.999			
		0.99	no	B_2 $7.9 \cdot 10^{-6}$	0.01	$7.9 \cdot 10^{-8}$
	yes		0.001			
	0.8		yes	B_3 $7.9 \cdot 10^{-5}$	0.3	$2.4 \cdot 10^{-5}$
yes		no	0.999			
0.1(1/a)		0.01	no	B_4 $8 \cdot 10^{-8}$	1	$8 \cdot 10^{-8}$
			0.001			
	no			B_5 $2 \cdot 10^{-3}$	0	0
	0.2					

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

  $SIL_1 \ldots SIL_4$

  evaluation of risk reduction

SIL is proposed for the protection circuit
It is used to describe the degree of safety protection needed by a process and consequently the safety reliability of the safety system necessary to achieve that protection. SIL1 is the lowest level of safety protection and SIL4 the highest.

Component can be certified for SILx

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	$10^{-2} \dots 10^{-1}$	$10 \dots 100$	$90\% \dots 99\%$

SIL_4 is not used in industry ("global catastrophe!")
risk reduction up to > 100000 does not exist

Probability to Fail on Demand (PFD) - 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

The 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). Protective circuit probability to fail on demand

$$PFD = \lambda \cdot T_1/2$$

Emergency probability in case of risk situation

$$P_e = PFD \cdot P_{risk}$$

6.1 Different multi-sensor architectures

Serving exactly the same purpose at the same point in the process. Possible architectures:

1. 1003
2. 2003
3. 3003

Consider Tank Reactor Fig. 1.

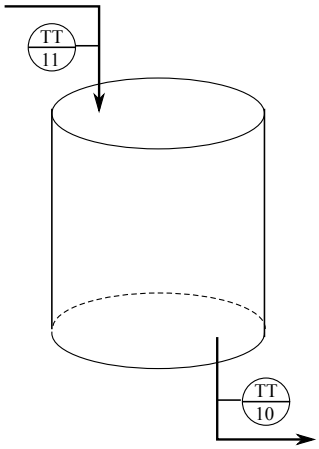


Figure 1: Tank reactor

1. Inlet temperatures: TT-11, TT-21, TT-31;
2. Outlet temperature: TT-10;
3. Voting block.

A block reliability diagram shows (see Fig. 2) how calculating the $\mathrm{PFD}_{\mathrm{AVG}}$ should be approached. Subsystems with identical components.

1oo1 $\mathrm{PFD}_{\mathrm{AVG}} = \lambda\frac{T}{2}$;

1oo2 $\mathrm{PFD}_{\mathrm{AVG}} = \frac{(\lambda T)^2}{3}$;

1oo3 $\mathrm{PFD}_{\mathrm{AVG}} = \frac{(\lambda_1 T)^3}{4}$;

MooN $\mathrm{PFD}_{\mathrm{AVG}} = (N/(M-1)/(N-M+1))(\lambda T)^{N-M+1}/(N-M+2)$;

NooN $\mathrm{PFD}_{\mathrm{AVG}} = N\lambda T/2$.

Subsystems with diverse components

1ooN $\mathrm{PFD}_{\mathrm{AVG}} = \lambda_1\lambda_2\ldots\lambda_n\frac{T^N}{N+1}$;

NooN $\mathrm{PFD}_{\mathrm{AVG}} = (\lambda_1 + \lambda_2 + \ldots + \lambda_n)\frac{T}{2}$.

Note that $\mathrm{PFD}_{\mathrm{AVG}}$ can be summed, but not multiplied.

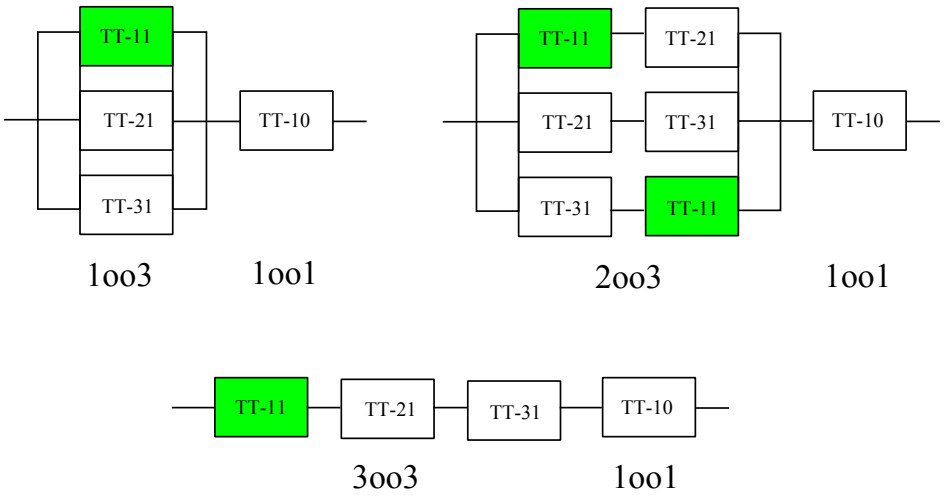


Figure 2: Reliability diagram

Bibliography

[1] Tony R. Kuphaldt, *Lessons In Industrial Instrumentation*, URL:`http://www.pacontrol.com/industrial-instrumentation.html`, 2012.

[2] Primatech, *FAQ Sheet - Layer of Protection Analysis (LoPA)*, URL:`http://www.primatech.com/docs/faq_layers_of_protection_analysis.pdf`, 22.04.2012.

[3] Product Quality Research Institute, *Risk Management Training Guides - HAZOP*, URL:`http://www.pqri.org/pdfs/MTC/HAZOP_Training_Guide.pdf`, 22.04.2012.