NTNU | Norwegian University of Science and Technology

TPK 5170 - DESIGN AND RELIABILITY ANALYSIS OF DIGITALIZED SAFETY SYSTEMS

Introduction

Jørn Vatn/August 2020

Course content

This course focuses on the application of standards that are framing design, operation, and reliability assessment of (safety) *critical systems*.

The main focus area is standards for technical systems that employ electrical/electronic/programmable electronic technology for the purpose of preventing or acting upon hazardous situations occurring in e.g., process plants, machinery, control of trains, avionic and air traffic management systems, critical infrastructure, and in relation to car driving.

Course content, cont

The main idea is to introduce key concepts and methods under the framework of key standards, like IEC 61508 and standards that are based on this one for adaption in specific industry sectors.

Topics include: Purpose of standards, including key concepts used, lifecycle phases and management, and methods advocated for RAMS assessments of critical functions (low-demand, high-demand). Choice of modeling approach and reliability measures in light of operational conditions and requirements are discussed.

Todays lecture

- Recap of chapter 10 in textbook used in TPK4120
- Basic concepts, like SIS, SIF, SIL, PFD, Risk reduction, ALARP, RAC
- We will also repeat some of the basic for quantification
- Quantificaiton is not the main issue of TPK5170
- Main focus is on ensuring a process to develop safe enough systems

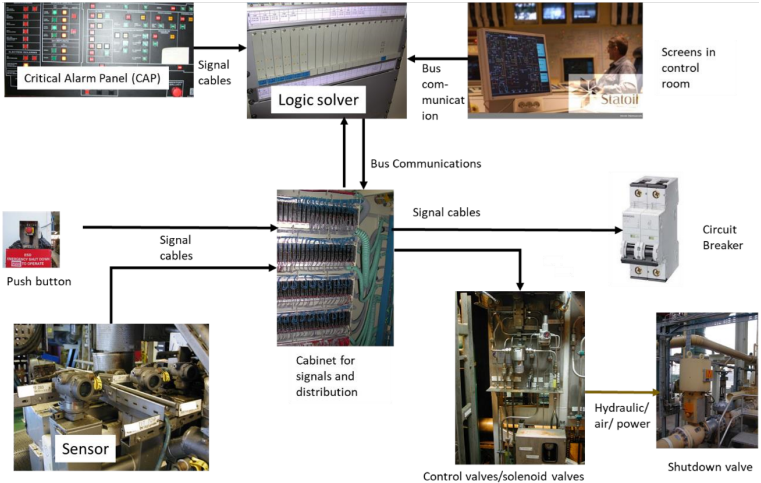
Safety Instrumented Systems

SIS

A safety instrumented system (SIS) is an independent protection layer that is installed to mitigate the risk associated with the operation of a specified hazardous system, which is referred to as the equipment under control (EUC). An example of an EUC is a process vessel.

A SIS is composed of *sensors* often referred to as *input elements*, *logic solvers* and *actuating items* often referred to as *final elements*.

Safety Instrumented Systems - Overview



Safety Instrumented Functions

SIF

A safety instrumented function (SIF) is a function that is implemented by a SIS and that is intended to achieve or maintain a safe state for the EUC with respect to a specific process demand such as high pressure in the vessel.

A SIS has two main system functions:

1. When a predefined process demand occurs in the EUC; the deviation shall be detected by the SIS sensors, and the required actuating items shall be activated and fulfil their intended functions
2. The SIS shall not be activated spuriously, that is, without the presence of a predefined process demand in the EUC

Demand

- A *demand* is defined as: An event or a condition that requires a SIF to be activated (i) to prevent an undesired event from occurring or (ii) to mitigate the consequences of an undesired event
- In the process industry, a demand is also called a *process upset* or a *process deviation*
- For an anti-lock braking system (ABS) on a car, a demand is a situation where the driver press the breaking pedal so hard that wheels are locked
- For the process industry, a demand could be high pressure in a vessel

SIS performance

- Should we put some performance requirements to the SIS?
- How to measure the performance of the SIS?

SIS performance

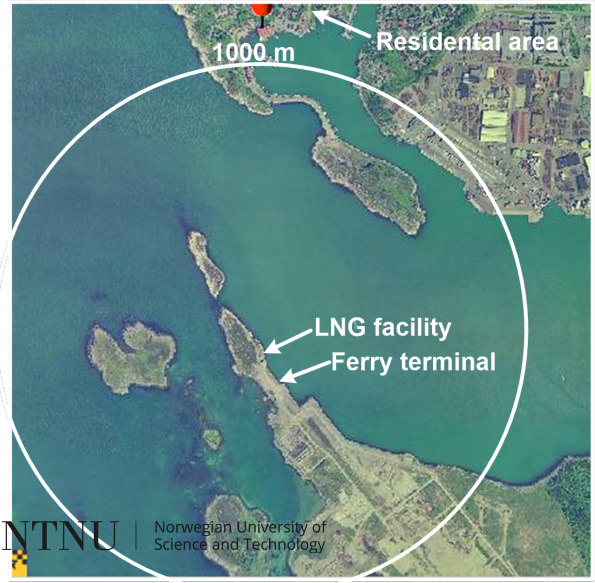
- Should we put some performance requirements to the SIS?
- How to measure the performance of the SIS?

- RAC = Risk Acceptance Criteria (TPK5160 = Risk analysis)
- PFD = Probability of Failure on Demand (TPK4120)

Example: Risavika LNG factory

- The local energy provider Lyse was developing an LNG (liquefied natural gas) facility at Risavika outside Stavanger in Norway
- Natural gas from the North Sea is transported through pipelines to shore, and then being liquefied at a process plant before it is stored in a huge tank
- The LNG is distributed from the facility to local consumers by LNG tankers and LNG lorries
- The localisation of the plant has been a hot issue in the region

Localization of the LNG factory



ALARP /RAC

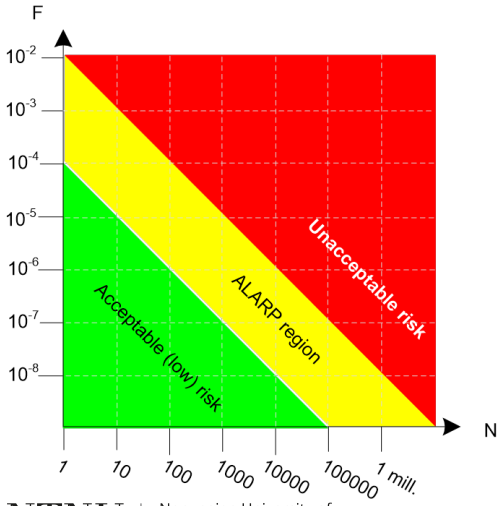
- ALARP= As Low As Reasonably Practicable
- RAC = Risk Acceptance Criteria

ALARP /RAC

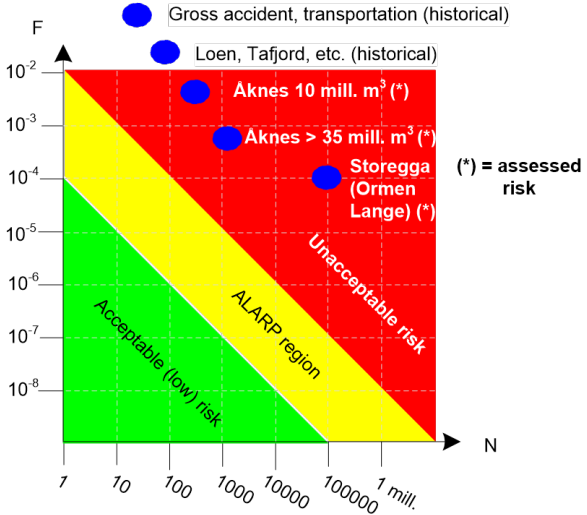
- ALARP= As Low As Reasonably Practicable
- RAC = Risk Acceptance Criteria

- Who should define the risk acceptance criteria (RAC)?
- What should the RAC be?
- How to formulate RAC, individual risk, f-N curves etc
- What is the relation beteen the RAC and the SIS performance?

Example RAC

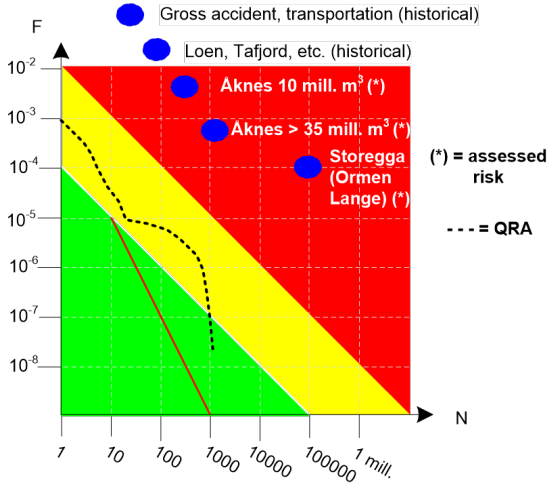

F
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
Unacceptable risk
ALARP region
Acceptable (low) risk
N
1
10
100
1000
10000
100000
1 mill.

Reasonable RAC?

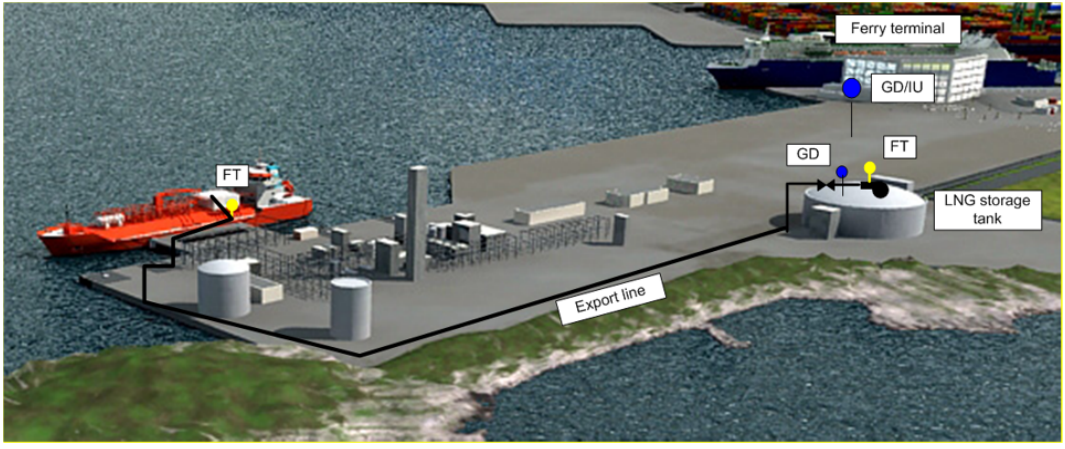


Results from the quantitative risk analysis (QRA)

- The results from the QRA shows that the risk is in the ALARP region
- The main contributor to the risk is the ferry terminal
- An ALARP process was run to obtain efficient risk reducing measures
- The red curve is level used in the Netherlands.....



Plant Layout



Risk reduction

- To reduce risk, i.e., bring risk into the green zone, it was proposed to install a gas detector (GD) connected to an ignition unit (IU) to ensure that any potential gas cloud drifting towards the ferry terminal will be ignited
- This is challenging from an ethical point of view (travelers vs workers at the plant)
- At the end the idea was not pursued further
- But if such a SIS should be implemented, the PFD should be so low that we were able to bring the risk into the green zone
- Note that often, the approach is just to bring risk from the red zone to the yellow zone....
- These type of arguments are used to define SIS performance requirements

More on SIS performance and performance modelling

A SIS is often a passive system that is activated only when a demand occurs. Failures may therefore occur and remain hidden until the system is demanded or tested. We often referred to two main categories of testing:

- *Proof Testing*. To verify that a SIS is able to perform its SIFs, the system is usually proof tested at regular intervals of length τ. The time interval between two consecutive proof tests is often called the proof test interval. Proof testing is also called functional testing. Dangerous failures detected by proof testing are called dangerous undetected (DU) failures.
- *Diagnostic testing*. A diagnostic test is an automatic partial test that uses built-in self-test features to detect failures. Dangerous failures detected by a diagnostic test are called dangerous detected (DD) failures. The identified faults are announced as alarms, locally at the equipment and in the control room.

Safety Integrity Levels (SILs)

- The IEC 61508 standard uses safety integrity as a performance measure for a SIF
- Safety integrity is the probability of a SIS satisfactorily performing the specified SIFs under all the stated conditions within a stated period of time
- IEC 61508 does not specify detailed probability values, but divides the requirements into four safety integrity levels, SIL 1, SIL 2, SIL 3, and SIL 4, with SIL 4 being the most reliable and SIL 1 being the least reliable

Probability of Failure on Demand

The probability of (dangerous) failure on demand, $\mathrm{PFD}(t)$ is the probability that the SIS has a dangerous fault and that it is not able to perform its SIFs at time t, i.e.,

$$\mathrm{PFD}(t) = \mathrm{Pr}(\text{The SIS is not able to perform its SIF at time } t)$$

irrespective of whether a demand occurs or not. If a demand should occur at time t, $\mathrm{PFD}(t)$ is the probability that the SIS fails to perform its SIF. In many cases, it is not necessary to determine the PFD as a function of time and we can suffice with an average value. If the SIF is proof tested after regular intervals of length τ and the system is considered to be as-good-as-new after each proof test, the long-term average probability of failure on demand can be expressed as

$$\mathrm{PFD} = \frac{1}{\tau}\int_0^{\tau} \mathrm{PFD}(t)dt$$

Average Frequency of Dangerous Failures per Hour

- For SIFs that are operated in high-demand or continuous mode, IEC 61508 requires that the reliability is specified by the average frequency of dangerous failures (PFH) where the frequency is given as number of dangerous failures per hour
- The idea behind using the PFH as a reliability metric is that demands will occur so often that when a dangerous failure of the SIF occurs, it is most likely that a demand will occur and a hazardous event will be manifested before we can bring the EUC to a safe state
- Examples:
  - A railway signalling system
  - ABS = Anti-lock breaking system for a very offensive driver

Spurious Trip Rate and related concepts

The spurious trip rate, (STR) is the rate of spurious trips of a specified SIF per hour.
There are three main types of spurious activation:

- *Spurious operation*. A spurious operation (SO) is an activation of the safety function of a individual component (channel) without the presence of a specified process demand
- *Spurious trip*. A spurious trip (ST) is an activation of a SIF without the presence of a specified process demand
- *Spurious shutdown*. A spurious shutdown is a partial or full process shutdown without the presence of a specified process demand.

Reliability Metrics and SIL

To fulfil the requirements of a safety integrity level, a SIF in low-demand mode must have a PFD in the corresponding interval specified below. Similarly, a SIF in high-demand or continuous mode must have a PFH in the corresponding interval specified in the same table.

SIL	**Low demand mode of operation** (Average probability of failure to perform its design function on demand)	**High demand mode of operation** (Average probability of failure per hour to perform its design function)
4	$10^{-5} \leqslant$ PFD <10^{-4}	$10^{-9} \leqslant$ PFH <10^{-8}
3	$10^{-4} \leqslant$ PFD <10^{-3}	$10^{-8} \leqslant$ PFH <10^{-7}
2	$10^{-3} \leqslant$ PFD <10^{-2}	$10^{-7} \leqslant$ PFH <10^{-6}
1	$10^{-2} \leqslant$ PFD <10^{-1}	$10^{-6} \leqslant$ PFH <10^{-5}

Why do we need SIL?

- For a SIS we need to specify it's performance, i.e., what reliability do we need to achieve sufficient risk reduction to cope with e.g., the risk acceptance criteria
- For example, we might need a reliability corresponding to $\mathrm{PFD} \leq 0.003$
- Why then just ask for this when you order the SIS?
- The argument is now that it is easier to ensure a safety demonstration process with a limited number of requirements, i.e., SIL1, SIL2, etc:
  - In addition to quantification in terms of PFD/PFH we need
  - Hardware fault tolerant criteria (redundancy)
  - Requirements for software development, usually not quantified
  - To be discussed in detailed later in the course

PFD calculations for systems

To obtain PFD for a system we may follow the following procedure:

1. Find PFD for the system as a function of t in an interval, i.e., $0 \leqslant t \leqslant \tau$, and denote the result $\mathrm{PFD}(t)$
2. To obtain $\mathrm{PFD}(t)$ we often utilize the system survivor function, say $R(t)$
3. Find the average $\mathrm{PFD}(t)$ by integration:

$$\mathrm{PFD} = \frac{1}{\tau}\int_0^{\tau} \mathrm{PFD}\,(t)\,dt = 1 - \frac{1}{\tau}\int_0^{\tau} R\,(t)\,dt$$

Example: 1oo1-system

The classical example is one component proof tested at point of times τ,2τ,3τ,..., and time to failure is exponentially distributed, i.e., $R(t) = e^{-\lambda t}$.

$$\begin{aligned}\mathrm{PFD} = 1 - \frac{1}{\tau}\int_0^\tau R(t)dt = 1 - \frac{1}{\tau}\int_0^\tau e^{-\lambda t}dt = 1 + \frac{1}{\lambda\tau}\int_0^\tau -\lambda e^{-\lambda t}dt \\ = 1 + \frac{1}{\lambda\tau}e^{-\lambda t}\Big|_0^\tau = 1 + \frac{1}{\lambda\tau}\left(e^{-\lambda\tau} - 1\right)\end{aligned}$$

If $\lambda\tau$ is small, i.e., (<0.01) we utilize that $e^{-x} \approx 1 - x + x^2/2$, and inserting in the expression for $\mathrm{PFD}(t)$ yields:

$$\mathrm{PFD} = 1 + \frac{1}{\lambda\tau}\left(e^{-\lambda\tau} - 1\right) \approx 1 + \frac{1}{\lambda\tau}\left(1 - \lambda\tau + (\lambda\tau)^2/2 - 1\right) = \lambda\tau/2$$

*k*oo*n* systems

In more general, we find that the PFDs of some *k*oo*n* systems of identical and independent components with constant failure rate λ and test interval τ are:

$k \backslash n$	1	2	3	4
1	$\frac{\lambda\tau}{2}$	$\frac{(\lambda\tau)^2}{3}$	$\frac{(\lambda\tau)^3}{4}$	$\frac{(\lambda\tau)^4}{5}$
2	–	$\lambda\tau$	$(\lambda\tau)^2$	$(\lambda\tau)^3$
3	–	–	$\frac{3\lambda\tau}{2}$	$2(\lambda\tau)^2$
4	–	–	–	$2\lambda\tau$

Numerical integration

If $R(t)$ is reasonable smooth in $[0, \tau]$ numerical integration is straight forward. Assume that we are able to calculate $R(t)$ `=Rfunc(t)` for our system at any point of time $t \in [0, \tau]$. The following pseudo-code will then help us with the PFD-calculation ($\mathrm{PFD} = 1 - \frac{1}{\tau} \int_0^\tau R\,(t)\, dt$):

```
Function PFD(Rfunc, tau, nSteps)
dt = tau / nSteps
s = 0
For i = 1 To nSteps
  s = s + dt * 0.5 * (Rfunc((i - 1) * dt) + Rfunc(i * dt))
Next i
PFD = 1 - s / tau
End Function
```

Challenges

- If we need a specific $R(t)$-function, how to pass this function to our PFD function?
- How to calculate the $R(t)$-function for complex systems?
- Other issues, how to be “smart” to avoid unnecessary calculations?

Markov approach

- For SIS systems some failures are only detected by proof-tests at point of times $\tau, 2\tau, \ldots$, whereas diagnostic tests reveal the failures immediately
- For this Markov modelling is appropriate
- This presentations deviates slightly from the presentation in the textbook
- In TPK4120 We have seen that the Markov equations may be written on matrix form:

$$\mathbf{P}(t) \cdot \mathbf{A} = \dot{\mathbf{P}}(t)$$

Markov approach, cont

which may be approximated by:

$$\dot{\mathbf{P}}(t) \approx \frac{\mathbf{P}(t+\Delta t) - \mathbf{P}(t)}{\Delta t} \approx \mathbf{P}(t) \cdot \mathbf{A}$$

yielding

$$\mathbf{P}(t+\Delta t) \approx \mathbf{P}(t) \cdot [\mathbf{A}\Delta t + \mathbf{I}]$$

where $\mathbf{I}$ is the identity matrix. This equation may now be used iteratively with a sufficient small time interval Δt and starting point $\mathbf{P}(0)$ to find the time dependent solution. Only simple matrix multiplication is required for this approach. Note that there is not much gain in using exponential of matrices, since we in any case need to go in small steps for the integration.

PFD

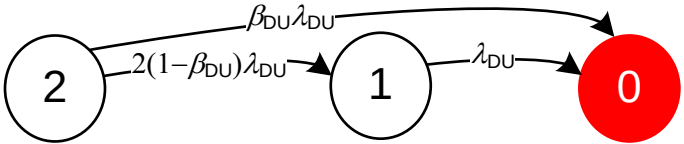
- Assume that we know the state vector $\mathbf{P}(0)$ just after a proof test, and that we have established a Markov transition model for the SIS with respect to a given SIF
- The elements of the $\mathbf{P}(t)$-vector within a proof test interval is found by $\mathbf{P}(t + \Delta t) \approx \mathbf{P}(t) \cdot [\mathbf{A}\Delta t + \mathbf{I}]$
- Let F be the set of failed states with respect to the actual safety function of the SIS. We then have:

$$\mathrm{PFD} = \frac{1}{\tau}\int_0^\tau \mathrm{PFD}(t)dt = \frac{1}{\tau}\int_0^\tau \sum_{i\in F} P_i(t)dt$$

The integral is replaced by a sum in the numerical calculations since we are already solving the time dependent solution iteratively by time steps Δt.

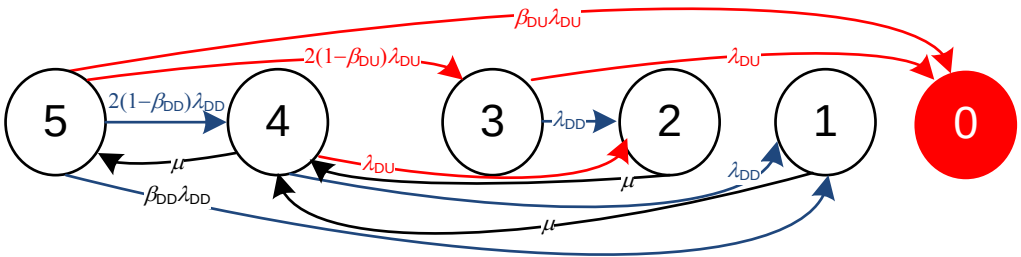
Markov diagram

The following figure shows the Markov diagram for a 1oo2 system considering DU-failures only (DU=Dangerous Undetectable, detected only by proof tests):



Note that whereas the closed form formulas for PFD presented earlier only takes DU failures into account. With the Markov approach, DD failures may also be included (DD = Dangerous Detectable, detected immediately)

The Markov diagram for the 1oo2 with DD & DU



where the following system states are defined: 5: Both components OK, 4: One OK, one DD-failure, 3: One OK, one DU-failure, 2: One DU-failure and one DD-failure, 1: Two DD-failures, and 0: Two DU-failures.

PFH = Average Probability of Failure per Hour

The procedure is now similar to the approach for PFD, but we are seeking a rate, i.e., the rate of transition from a functioning state to a fault state for the SIS safety function is found by averaging:

$$\mathrm{PFH} = \frac{1}{\tau}\int_0^{\tau} \mathrm{PFH}(t)dt = \frac{1}{\tau}\int_0^{\tau} \sum_{i\notin F}\sum_{j\in F} a_{ij}P_i(t)dt$$

where a_{ij} is the transition rate from state i to state j measured in expected number of transitions *per hour*

$P_i(t)$ is found by the regime: $\mathbf{P}(t+\Delta t) \approx \mathbf{P}(t)\cdot[\mathbf{A}\Delta t + \mathbf{I}]$

STR = Spurious Trip Rate

The procedure for the spurious trip rate is now similar to the approach for PFH, but we need to consider the spurious trip system failure mode. Let F be the set of system failure states representing a spurious trip state. STR is found by averaging:

$$\mathrm{STR} = \frac{1}{\tau}\int_0^{\tau} \mathrm{STR}(t)dt = \frac{1}{\tau}\int_0^{\tau} \sum_{i\notin F}\sum_{j\in F} a_{ij}P_i(t)dt$$

The transition rates for spurious trips are reflecting “safe” failures, i.e., those that will not directly affect safety. We thus have to draw a new Markov diagram with these rates.

Thank you for your attention