# Chapter 7.
# Demand Modes and Performance Measures for Reliability

Mary Ann Lundteigen  Marvin Rausand

RAMS Group
Department of Mechanical and Industrial Engineering
NTNU

(Version 0.1)

**NTNU – Trondheim**
Norwegian University of
Science and Technology

# Learning Objectives

The main learning objectives associated with these slides are to:

- Introduce the concept of demand modes
- Describe various operational strategies in response to SIS failures
- Present different reliability measures applicable for the analysis of SIS reliability

The slides include topics from Chapter 7 in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

# Outline of Presentation

# Demand Mode

A SIS is designed to respond to certain events, called *demands*, so that the equipment under control (EUC) achieves a safe state.

IEC 61508 classifies the frequencies of demands into three categories, called *demand modes* of operation:

- Low-demand: Demands occur less than once per year.
- High-demand: Demands occur more than once per year.
- Continuous mode: Demands are always present. Part of "normal operation.

# Why Demand Mode Categories?

Why is the frequency of demands of importance for the reliability of a SIS?

| Mode | Characteristics | Implications for reliability |
|---|---|---|
| Low-demand | ▶ A response by the SIS is seldom required<br>▶ A dangerous failure may remain hidden for some time<br>▶ A SIS being in the failed state is not hazardous unless a demand occur | ▶ Interested in the probability that the SIS is in a failed state when a demand occur |
| High/cont. demand | ▶ A response by the SIS is frequently or constantly required<br>▶ A dangerous failure of the SIS may directly result in an hazardous event | ▶ Interested in how often the SIS fails. |

# Reasonable?

IEC 61508 suggests:

- A split between high and low-demand systems at one demand per year
- Using the same reliability measure (average faiure frequency) for high- and continuous mode

## Discussion issue

- Why the borderline "'once per year"?
- Why using different reliability measure of low demand and high demand?
  - Why is failure frequency a more appropriate measure than the probability of failure to perform on demand?
  - It has been shown that reliability measure for low-demand may be used also in the "upper" range of high-demand mode

# Demand Modes and Industry Sectors

**Process industry**:

- Low-demand mode applies to SIS. A separate system - the process control system (PCS) - is used to ensure stable production and processing during normal operation. SIS to respond in case of a failure of the PCS, or an event not managed by the PCS (e.g. fire).

**Machinery systems**:

- Continuous demand /high-demand applies to SIS. Many safety functions are implemented into the machinery control system, and the machinery control system is therefore referred to as safety-related electrical control system in machinery standards like IEC 62061.

**Railway signaling systems:**

- Continuous demand applies to SIS. Operation of light signals and rail switches are all safety-critical functions and part of normal operation.

# SIFs versus Demand Modes

The classification of mode of operation may be used to suggest the two following categories of SIFs:

- **Safety-related protective functions**: SIFs that are dormant during normal operation, and responds to process events and deviations that are or may develop into dangerous situations
- **Safety-related control function**: SIFs need to operate continuously to ensure that dangerous situations are avoided

Remark: The explanation deviates slightly from the textbook.

# Reliability and High/Low Demand Mode

- Low-demand:
  - Detection time of dangerous undetected (DU) failures can be long
  - Regular tests introduced to reveal dangerous undetected (DU) failures "as early as possible"
  - Still, DU failures contributes to unreliability
  - Detection and restoration time for DD failures is normally small, so their contribution to unreliability is negligible

  High-demand:

  - Any dangerous failure (DU and DD) of the SIF may result in an hazardous event
  - The effect of DD failures on unreliability may be neglected if the SIS makes an automatic transition to the safe state within due time

# Reliability Measures

There are several relevant reliability measures in relation to SIS:

- Average probability of (dangerous) failure on demand ($PFD_{avg}$)
- Average frequency (per hour) dangerous failures(PFD)
- Hazardous event frequency (HEF)
- Risk-reduction factor (RFF)
- Spurious (unintentional) trip rate (STR)
- Safe failure fraction (SFF)
- Diagnostic coverage (DC)

(We could probably have added even more measures)

# Average Probability of Failure on Demand

The *average probability of (dangerous) failure on demand ($PFD_{avg}$)* is considered as an appropriate reliability measure for SIFs operating in the low-demand mode.

☞ $PFD_{avg}$: The average probability that the item (SIS, subsystem, voted group or channel) is not able to perform its specified safety function if a demand occur.

$$PFD_{avg} = \frac{1}{\tau}\int_0^{\tau} PFD(t)\,dt \tag{1}$$

where $\tau$ is the regular test interval and PFD(t)[1] is the time dependent probability of failure in a test interval.

[1] i.e. $\Pr(T < t)$

# Average Frequency (per hour) of Dangerous Failures

The *average frequency of a dangerous failure per hour*, called $PFH_{avg}$[2] is considered as an appropriate reliability measure for SIFs operating in the high and continuous demand mode.

☞ $PFH_{avg}$: The average frequency of dangerous failures (of the SIF) to perform a specified safety function of a given period of time.

$$PFH_{avg} = \frac{1}{t_0} \int_0^{t_0} PFH(t)\,dt \tag{2}$$

where $\tau$ is the regular test interval and PFH(t) is the time dependent failure frequency. When $t_0 \to \infty$, we may assume that we get a long-term PFH. However, it is not obvious (nor the case) that $PFH_{0,t_0}$ approaches such a limit.

[2] Previously called average probability of dangerous failure per hour

# Average Frequency (per hour) of Dangerous Failures

What is PFH(t)?

- A SIS is a repairable system, and when failures occur we may assume that they are repaired within relatively short time
- As such, we understand that the rate of SIS failures is the same as the *rate of occurence of failures* (ROCOF), denoted here as $\omega(t)$.
- More precisely, we can say that PFH(t) is the same as the $\omega_D(t)$ when only dangerous (D) failures are considered

# Hazardous Event Frequency

The *hazardous event frequency* (HEF) is applicable measure for both high- and low-demand SIFs.

☞ HEF: The average frequency of hazardous events.

For a low-demand SIF with no demand duration included, the HEF is:

$$HEF = PFD_{\text{avg}}\lambda_{\text{de}} \tag{3}$$

where $\lambda_{\text{de}}$ is the demand rate. For a high-demand SIF with no demand duration included, the HEF fulfills the following criterion:

$$HEF \leq PFH \tag{4}$$

# Risk Reduction Factor (RRF)

The *risk reduction factor* (RRF) is sometimes used as an alternative measure to PFDavgf for SIS operating in the low-demand mode in the process industry

☞ RRF: A reduction factor - showing how much the frequency of demands on the next protection layer or hazardous event frequency (if SIF is the ultimate protection layer) is reduced compared to initial demand frequency. (Note: This is not a formal definition.)

RRF can be calculated as:

$$RRF = \frac{\lambda_{\text{de}}}{\lambda_{\text{de}} PFD_{\text{avg}}} = \frac{1}{PFD_{\text{avg}}}$$

Example: A SIL 2 function shall provide a risk reduction factor of 100-1000.

# Spurious Trip Rate

The *spurious trip rate* (STR) is often used to also study the impact of SIS on production performance.

☞ STR: Unintended activation of a SIF or a SIF subsystem.

It is often aimed for keeping the STR as low as possible, because:

- Spurious trips often interrupts the production or service provided by the EUC
- The trip and start-up after the trip may introduce hazardous events

# Spurious Trip Rate

## Example

A spurious trip of the railway signaling system will result in manual control of trains for a period until full overview of the situation has been gained. In this phase, we are more prone to human errors, like a wrong decision where two trains are allowed to enter the same rail section.

# Spurious Trip Rate

The *spurious trip rate*, sometimes called STR, may be a reliability measure that supplement PFD and PFH.

☞ STR: Unintended activation of a SIF or a SIF subsystem.

The reliability measure is useful for high as well as low-demand SISs.

$$STR = \frac{E[N_{ST}(t)]}{t} \tag{5}$$

where $E[N_{ST}(t)]$ is the expected number of spurious trip failures in an interval $t$.

# Safe Failure Fraction

The *safe failure fraction* (SFF) has been introduced by IEC 61508 as a measure of safety-performance in the presence of a failure.

☞ SFF: The ration of the failure rates of safe and DD failures of an element relative to the average rate of all safe and dangerous failures of the same element.

The reliability measure is useful for high as well as low-demand SISs.

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \tag{6}$$

The suitability of this reliability measure has been debated, see e.g. in Lundteigen and Rausand (2008)[3].

[3] http://dx.doi.org/10.1016/j.ress.2008.06.003

# PFD or PFH?

The following table summarizes the applicability of reliability measures:

| Measure | Mode of operation | | Level | |
|---|---|---|---|---|
| | LD | HD | SIF | Element |
| PFD | X | | x | X |
| PFH | | X | X | X |
| RRF | X | | X | (X) |
| HEF | X | X | | |
| STR | X | X | X | (X) |
| SFF | X | X | | X |
| DC | X | X | | X |

LD: Low-demand, HD: High-demand/continuous demand

# PFD or PFH?

I want to calculate or study the ...

| **Example** | **Measure suggested** |
|---|---|
| Reliability of an emergency shutdown function | $PFD_{avg}$ |
| Reliability of a railway signaling function that control the position of a rail switch | PFH |
| Regularity problems due to downtime of railway signaling system | STR and PFH |
| Reliability of a fire pump system | $PFD_{avg}$ and Pr(Pump survives $T_{min}$), $T_{min}$ is the specified running time |