Chapter 8.
Calculation of PFD using PDS method

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:

- Become familiar with the attributes of PDS method
- Become familiar with how to utilize PDS data for the analysis

The slides include topics from Chapter 8 in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

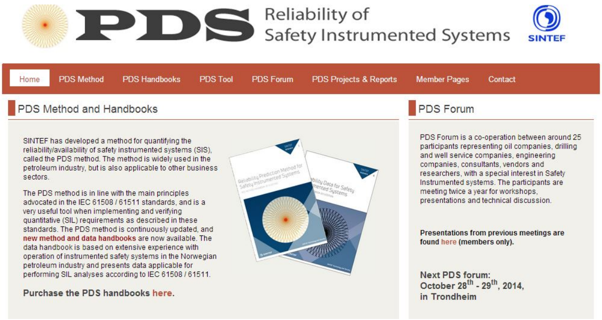
Outline of Presentation

1. Introduction
2. What is PDS and PDS Method?
3. Key Measures to Calculate

PDS in brief

Some keywords:

- PDS is a Norwegian acronym for computerized safety-systems.
- PDS relates to a forum `www.sintef.no/pds` as well as the PDS method.
- Focuses primarily on the oil and gas industry.



PDS method

The PDS method is a framework developed for calculating unavailability of safety-instrumented systems. The method is complemented by a PDS data handbook, developed jointly by PDS participants.

Some keywords:

- Focus primarily on safety-instrumented systems operating in the low-demand mode, even if some extensions have been made to also address high-demand.
- Provides formulas for calculating the critical safety unavailability (CSU), which includes PFDavg, as well as for the spurious trip rate.
- Includes an extension for how to include common cause failures (CCFs) in voted configurations

CSU

☞ Critical safety unavailability (CSU) of a safety instrumented function (SIF) is the probability that hte SIF cannot be performed if a demand occurs. CSU is defined as:

$$CSU = PFD_{avg} + DTU + P_{TIF}$$

where DTU is the downtime unavailability (due to testing and repair) and P_{TIF} is the probability of a test-independent failure.

We notice already now that the PDS method (i) separates PFD from DTU (as opposed to formulas in IEC 61508) and that a new parameter P_{TIF} has been added.

DTU

☞ Downtime unavailability (DTU): Part of the downtime due to repair or testing.

DTU may be split into two parts:

Measure	Description
DTU_R	Part of the downtime unavailability due to repair of dangerous (D) faults, resulting in a period when it is known that the SIF is unavailable.
DTU_T	Part of the downtime unavailability resulting from planned activities, such as proof-testing and planned maintenance, when it is known that the SIF is unavailable.

PFD_{avg}

The PFD_{avg} constitutes two parts:

- $\text{PFD}_{avg}^{(i)}$: This is the "traditional formula" for PFD_{avg} when only DU failures are included. Often, the factor $(1 - \beta)$ as this factor usually is close to 1.
- $\text{PFD}_{avg}^{(c)}$: This is the"traditional formula" for including CCFs using the standard beta factor model with one exception: A C_{koon} factor is introduced so that::

$$PFD_{avg}^{(c)} = C_{koon}\beta\frac{\lambda_{DU}\tau}{2}$$

For more in-depth presentation of the theory behind the C_{koon} factor, see the PDS method.

C_{koon} table

Values of C_{koon} used in the PDS method:

k/n	n=2	n=3	n=4	n=5	n=6
k=1	1.00	0.50	0.30	0.20	0.15
k=2	–	2.00	1.10	0.80	0.60
k=3	–	–	2.80	1.60	1.20
k=4	–	–	–	3.60	1.90
k=5	–	–	–	–	4.50

It may be remarked that IEC 61508 in its most recent version (2010) has included a similar table, but with slightly different calibration of the parameters.

Example

Consider a 1oo3 system. In this case the PFD_{avg} is:

$$PFD_{avg} = \frac{(\lambda_{DU}\tau)^3}{4} + C_{1oo3}\beta\frac{\lambda_{DU}\tau}{2}$$

It may be remarked that the PDS data handbooks include data for failure rates and beta values for typical SIS components.

Formulas for DTU$_R$

Probability of failure to perform while repair is onging (DTU$_r$) will depend on the operating philosophy. We assess different scenarios for illustration:

$$DTU_R \approx \Pr(\text{SIF is down due to a D failure}) \cdot \Pr(\text{Remaining components have a hidden failure})$$

Three scenarios are presented with basis in a 2oo3 system:

- Scenario 1: A repair of a **one** D failure is ongoing. No change in configuration during repair, so the SIF is now a 2oo2 in this period. The DTU$_R$ becomes:

$$DTU_R \approx [3\lambda_D MTTR] \cdot [2 \cdot \frac{\lambda_{DU}\tau}{2}]$$

Formulas for DTU_R (cont.)

Three examples are presented with basis in a 2oo3 system (cont.):

- Scenario 2: One D failure is being repaired. The SIF is reconfigured to 1oo2 in this period. In this case, there is no contribution from DTU_R as the SIF now is more reliable than with 2oo3.
- Scenario 3: **two** failures are being repaired. The SIF is reconfigured to a 1oo1 system in this period. The DTU_R becomes:

$$DTU_R \approx [(C_{2oo3} - C_{1oo3})\beta\lambda_{DU} MTTR] \cdot [\frac{\lambda_{DU}\tau}{2}]$$

The current version of the slide series do not include an explanation of DTU_T.

P_{TIF}

☞ Probability of test independent failure, P_{TIF}: Unavailability due to test independent failures.

What do we mean by “test-independent failure”?

☞ Test independent failure (TIF): A dangerous failure not revealed during a proof test.

- P_{TIF} acknowledges that a proof test may not be perfect, and P_{TIF} is a way to add a contribution fron this “imperfectness” of the test
- PDS method also suggest formulas using “proof test coverage” as an alternative.

What is best? Proof test coverage or P_{TIF}?

It is no general rule. What is important to evaluate if the regular testing has any impact at all. For example: The probability that a fire detector does not respond on demand due to wrong location may be independent of how often the fire detector is tested. Consequently, it may be argued that P_{TIF} is most suited *in this specific case*.

Other Contributions of the PDS method

The PDS method covers a number of topics beyond formulas, for example:

- On failure classification
- Handing of systematic failures
- Analysis of multiple SIFs

Visit the PDS method for more information.