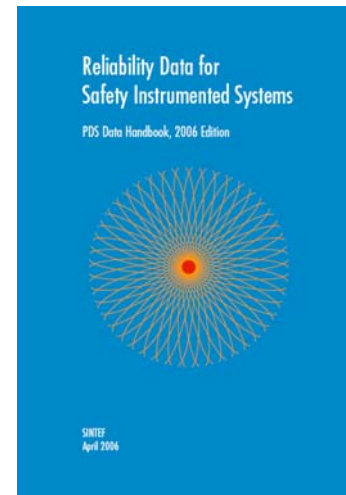
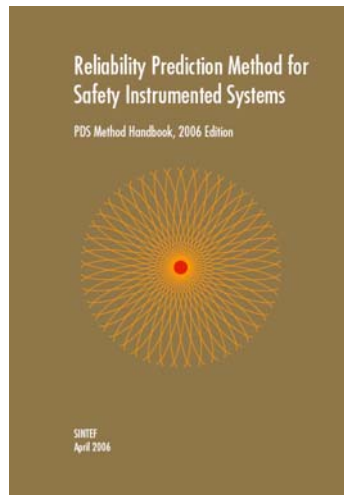


The updated PDS method

With a focus on systematic failures



ESReDA, 07. June 2006

Stein Hauge, SINTEF

Content

1. Introduction - what is PDS?
2. Related standards
3. Systematic failures in PDS
4. Summary

What is PDS?

- PDS is a method used to quantify the safety unavailability and production loss for Safety Instrumented Systems (SIS)
- The PDS method is documented mainly through a method handbook and a related data handbook
- The method is widely used in the Norwegian oil and gas industry
- The method and data are continuously updated through the PDS Forum

PDS forum

Oil Companies/Operators

- Norske Shell
- BP Norge
- Eni Norge
- Norsk Hydro
- PGS Production
- ConocoPhillips Norge
- Statoil
- TOTAL E&P NORGE

Engineering Companies and Consultants

- Aker Kværner Engineering & Technology
- Det Norske Veritas
- Nemko
- Safetec Nordic
- Scandpower Risk Management

Control and Safety System Vendors

- ABB
- FMC Kongsberg Subsea
- Honeywell
- Invensys Systems Norge
- Kongsberg Maritime
- Saas System
- Siemens
- Simrad Optronics

Governmental bodies

- Petroleum Safety Authority Norway (observer)
- Directorate for Civil Protection and Emergency Planning (observer)

Main features of the PDS method

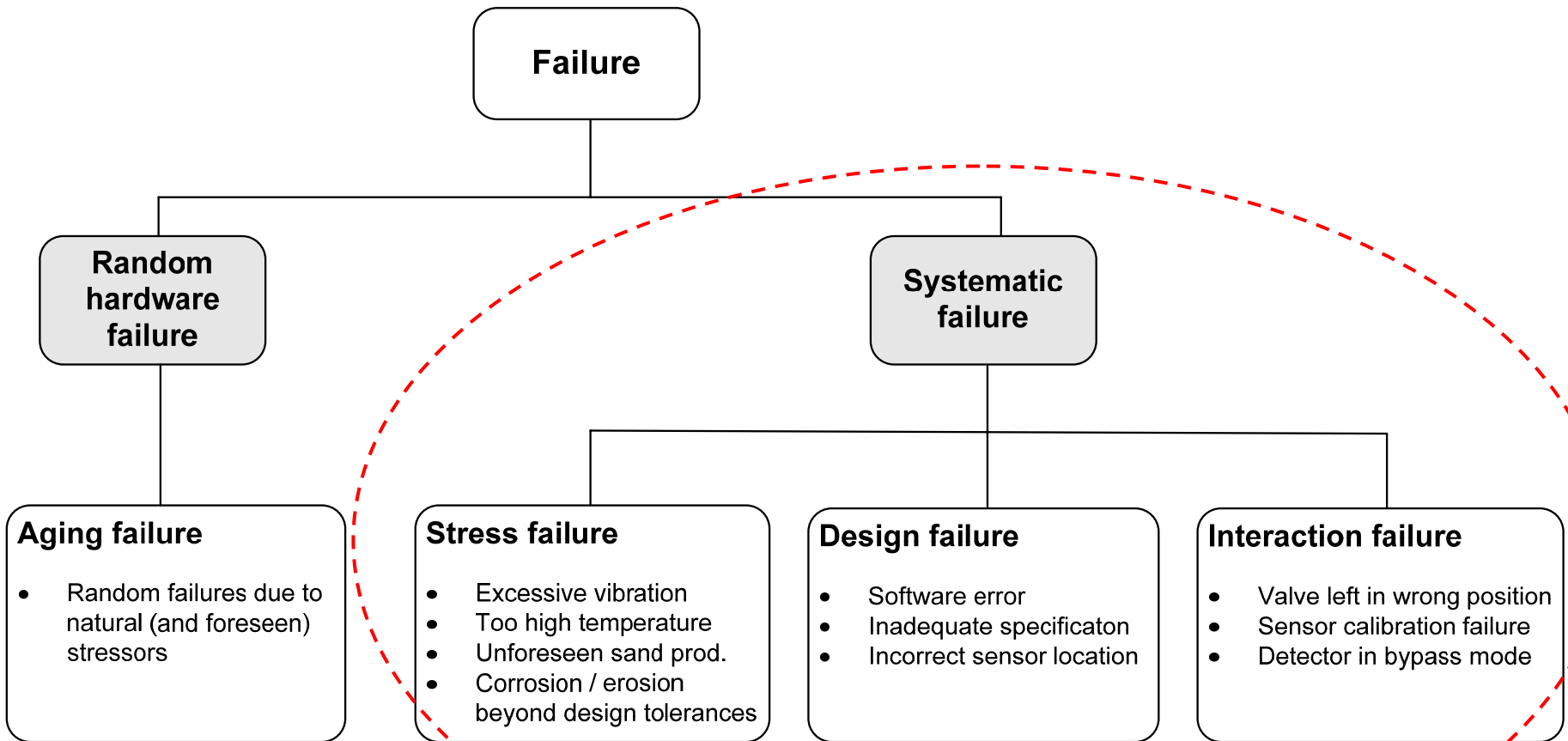
- present simple calculation formulas together with generic reliability data;
- include the entire "loop" of the safety function, i.e. field sensor, logic and the final element;
- include "all" realistic failure causes and failure modes;
- **model and quantify systematic failures in a comprehensible manner;**
- include various means of testing and detection of failures;
- provide simplified models for calculating application specific parameters.

IEC 61508 and IEC 61511

- The increased use of safety instrumented safety systems has resulted in functional safety standards like IEC 61508 and IEC 61511
- IEC 61508 and IEC 61511 provide a basis for specification, design and operation of SIS
- The PDS method is in line with the main principles advocated in these standards
- For some areas, like modelling of systematic failures, the PDS method offers an approach somewhat different from IEC 61508

The PDS method focuses on the quantitative part of IEC 61508 / 61511

Failure classification by cause of failure



- Valve failure due to wear and tear on ball and seat
- Valve failure due to natural corrosion on ball and seat
 - Valve failure due to solenoid valve wear-out



- Valve failure due to incorrect actuator installation
- Actuator failure due to corrosion caused by improper material selection
 - Stuck valve stem due to improper tightening after maintenance
 - Valve failure due to insufficient actuator force (design error)

Systematic failures

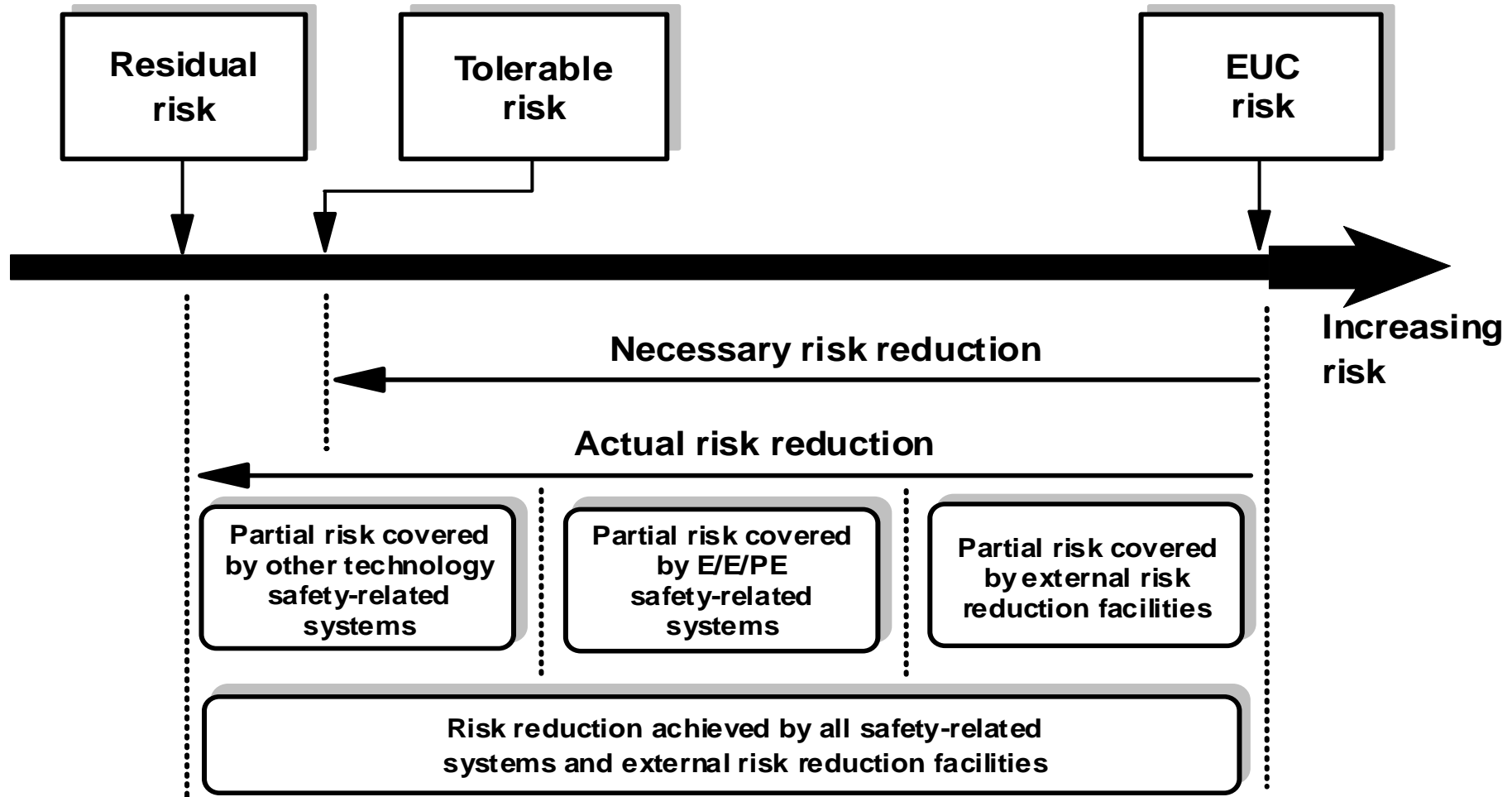
IEC 61508

Systematic failures are treated qualitatively by means of checklist

PDS

Systematic failures are modelled and quantified as part of the critical safety unavailability

Framework for risk reduction



Quantification of failure probability

Will also contribute to the failure probability

Aging failure

- Random failures due to natural (and foreseen) stressors

Stress failure

- Excessive vibration
- Too high temperature
- Unforeseen sand prod.
- Corrosion / erosion beyond design tolerances

Design failure

- Software error
- Inadequate specification
- Incorrect sensor location

Interaction failure

- Valve left in wrong position
- Sensor calibration failure
- Detector in bypass mode

IEC 61508

Single component: $PFD \approx \lambda_{DU} \cdot \tau/2$

$$\lambda_{DU} = \lambda_{DU-RH} + \lambda_{DU-S}$$

λ_{DU-S}

Contribution from systematic failures, i.e. failures related to incorrect design, use, maintenance or environment.

- Not included in λ_{DU} by strict interpretation of IEC 61508
- Heavily influenced by operational measures
- Will give rise to common cause failures

λ_{DU-RH}

Contribution from random hardware failures, i.e. failures due to natural aging and “tear & wear”.

- Corresponds to λ_{DU} as described in IEC 61508
- Will not give rise to common cause failures

Three major contributors towards the CSU

1. Random hardware failures detectable by functional testing (of rate λ_{DU-RH})
2. Systematic failures detectable by functional testing (of rate λ_{DU-S})
3. "Test independent failures" only occurring upon a true demand, of probability P_{TIF}

Single component: $CSU = (\underbrace{\lambda_{DU-RH} + \lambda_{DU-S}}_{\lambda_{DU}}) \cdot \tau/2 + P_{TIF}$

Quantification in PDS

- An accompanying PDS data handbook is issued suited for PDS (and IEC) calculations
- Data is based on OREDA[®], RNNS, expert judgements, etc.
- Includes proposed data for SIS equipment and all relevant PDS parameters
- Simplified application specific models are proposed in order to adjust the generic values

Summary - why quantify systematic failures?

- Often we want to predict the “actual” field performance (and the actual risk reduction);
- Systematic failures are a main contributor towards the failure probability of the safety function;
- In order to highlight the actual importance of these failures;
- Generic / historic failure data based on operational experience frequently include also systematic failures;
- When introducing measures to avoid and control systematic failures, we want to quantify the effect of these measures (also for single systems).

For more information about PDS

please visit:

www.pds.sintef.no