Chapter 11.
Imperfect Proof-Testing

Marvin Rausand Mary Ann Lundteigen

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:

- Understand why regular tests may be imperfect
- Be able to explain what the proof test coverage (PTC) is
- Be able to set up analytical formulas for PFD_{avg}
- Be able to explain how analytical formulas are adapted for partial testing
- Be able to explain some main principles for how partial testing is physically implemented
- Explain how the partial test coverage (PST) is influenced by how the partial testing is physically implemented
- Be able to determine the PST from OREDA data
- Be able to apply checklist to determine PST
- Be able to suggest how imperfect testing can be solved using Multi-Phase Markov (new)

Outline of Presentation

Assumptions Made for Perfect Testing

Many of our analytical formulas developed for PFD_{avg} assume perfect tests. This means that:

- The proof test conditions are identical to the demand conditions
- All DU failures are revealed during the test, and no new ones are introduced during the test itself
- Repair is perfect, meaning that the channels achieve an as good as new condition.

Therse are not realistic, but in some cases realistic *enough*. When the assumptions seem too unrealiztic, we consider the test as imperfect.

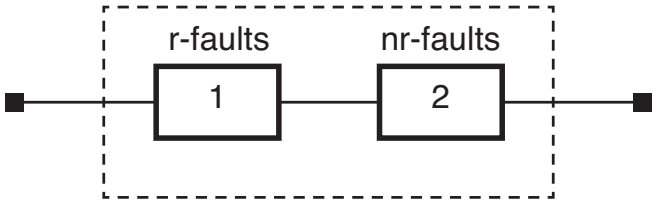
Splitting the Failure Rate

Under the imperfect test condition, we may distinguish between:

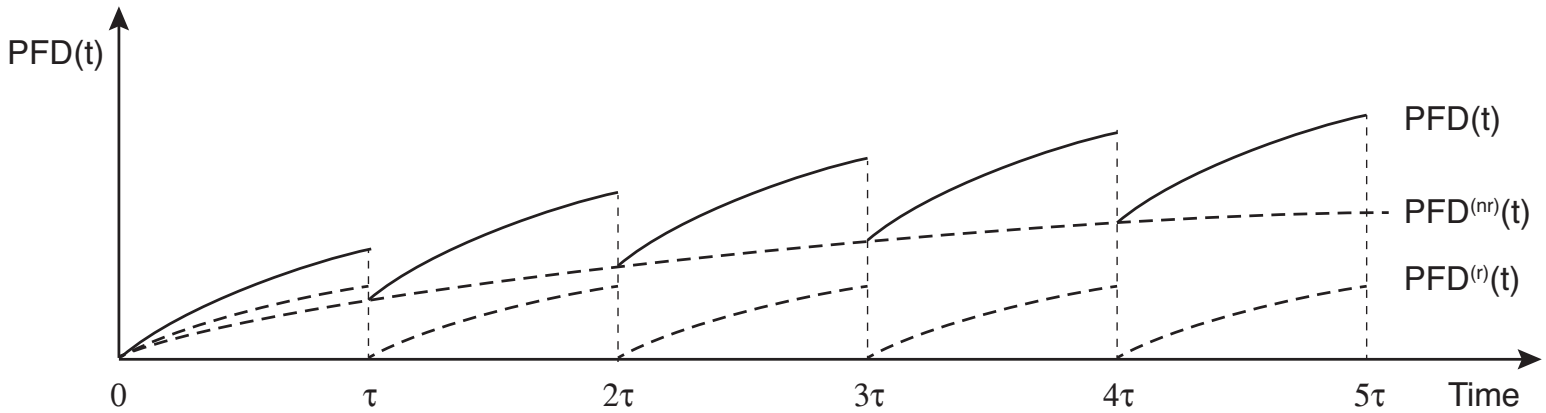
(a) DU faults that can be revealed by the proof test (r-faults), denoted by failure rate $\lambda_{DU}^{(r)}$

(b) DU faults that cannot be revealed by the proof test (nr-faults), denoted by failure rate $\lambda_{DU}^{(nr)}$

The splitting of failure rate may be illustrated as below.



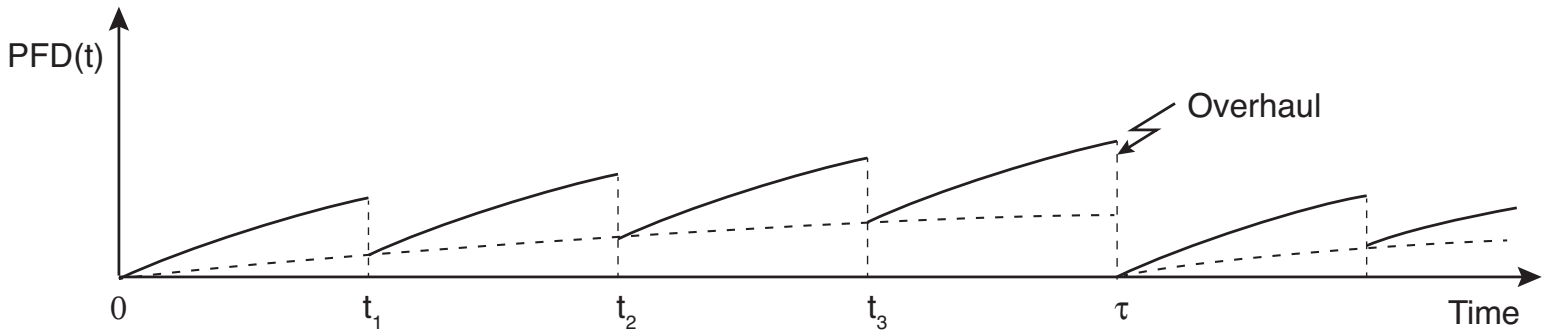
The PFD as a function of time can be illustrated as follows:



Full Renewal when Imperfect Testing

The non-revealed failures may remain hidden over the whole life of the system, unless a demand is experienced or the system is fully renewed during a scheduled overhault.

The effects of regular overhauls on the PFD may be illustrated as below.



Proof Test Coverage

The fraction between revealed and non-revealed can be expressed by the proof test coverage (PST):

☞ PST coverage is defined as:

$$\text{PTC} = \frac{\lambda_{\text{DU}}^{(\text{r})}}{\lambda_{\text{DU}}^{(\text{r})} + \lambda_{\text{DU}}^{(\text{nr})}} = \frac{\lambda_{\text{DU}}^{(\text{r})}}{\lambda_{\text{DU}}}$$

A proof test is said to be *perfect* when PST= 100% , while*imperfect* when PST $< 100\%$.

Proof test coverage

This means that the rate of r-failures and nr-failures can be expressed by the PTC and the DU failure rate.

$$\lambda_{\mathrm{DU}}^{(\mathrm{r})} = \mathrm{PTC} \cdot \lambda_{\mathrm{DU}}$$

$$\lambda_{\mathrm{DU}}^{(\mathrm{nr})} = (1 - \mathrm{PTC}) \cdot \lambda_{\mathrm{DU}}$$

Modeling of PFD with Imperfect Testing

Modeling of PFD may be done by:

- Time-dependent PFD calculations
- Average PFD

With time-dependent calculation, it is possible to achieve the socalled “saw tooth” curve, which will have increasing heith of each peak as the time goes by. Time-dependent solution may be found by:

- Numerical integration
- Multi-phase Markov models
- Simulation in combination with RBDs, FTs, or PetriNets.

In this chapter, the main focus is on determining *Average PFD* based on analytical formulas.

Analytical Formulas: Single System

We start with a single system subject to imperfect proof test with interval τ and overhaul with interval $\tilde{\tau}$. In this case, it is easy to obtain the PFDavg, considering the virtual items "r-faults" and "nr-faults":

$$\begin{aligned} \mathrm{PFD}_{\mathrm{avg}} &= \mathrm{PFD}_{\mathrm{avg}}^{(\mathrm{r})} + \mathrm{PFD}_{\mathrm{avg}}^{(\mathrm{nr})} \\ &\approx \frac{\mathrm{PTC} \cdot \lambda_{\mathrm{DU}} \tau}{2} + \frac{(1 - \mathrm{PTC}) \lambda_{\mathrm{DU}} \tilde{\tau}}{2} \end{aligned}$$

The repair-time has been disregarded here.

IEC 61508 Approach: Single System

It is not straight forward to develop analytical formulas for *koon* using reliability block diagrams. It is therefore suggested to apply the approach suggested in IEC 61508 (part 6).

Recall the basic assumptions for analytical formulas in IEC 61508 for a single system:

$$\text{PFD}_{\text{avg}} \approx \lambda_{\text{D,G}} \cdot t_{\text{GE}}$$

where $\lambda_{\text{D,G}} = \lambda_{\text{D}}$ and

$$t_{\text{GE}} = t_{\text{CE}} = \frac{\lambda_{\text{DU}}}{\lambda_{\text{D}}} \left(\frac{\tau}{2} + \text{MRT} \right) + \frac{\lambda_{\text{DD}}}{\lambda_{\text{D}}} \cdot \text{MTTR}$$

IEC 61508 Approach: Single System

When imperfect testing is introduced, we simply modify the equivalent mean downtime (t_{GE}) to recognize that nr-faults and r-faults have different downtime.

$$t_{GE} = t_{CE} = \frac{\lambda_{DU}^{(r)}}{\lambda_D}\left(\frac{\tau}{2} + MRT\right) + \frac{\lambda_{DU}^{(nr)}}{\lambda_D}\left(\frac{\tilde{\tau}}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

Here, $\tilde{\tau}/2 + MRT$ is the mean downtime of an nr-failure, and $\tau/2 + MRT$ is the mean downtime of a r-failure. The formula for PFD_{avg} becomes:

$$PFD_{avg} = \lambda_{DU}^{(r)}\left(\frac{\tau}{2} + MRT\right) + \lambda_{DU}^{(nr)}\left(\frac{\tilde{\tau}}{2} + MRT\right) + \lambda_{DD}MTTR$$

With PTC included, the formula becomes:

$$PFD_{avg} = PTC \cdot \lambda_{DU}\left(\frac{\tau}{2} + MRT\right) + (1 - PTC) \cdot \lambda_{DU}\left(\frac{\tilde{\tau}}{2} + MRT\right) + \lambda_{DD}MTTR$$

IEC 61508 Approach: 1oo2 System

For 1oo2 system, we need to modify *two* parameters in the analytical formula suggested in IEC 61508.

t_{CE}, the channel equivalent downtime:

$$t_{\mathrm{CE}} = \frac{\lambda_{\mathrm{DU}}^{(\mathrm{r})}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{2}+\mathrm{MRT}\right)+\frac{\lambda_{\mathrm{DU}}^{(\mathrm{nr})}}{\lambda_{\mathrm{D}}}\left(\frac{\tilde{\tau}}{2}+\mathrm{MRT}\right)+\frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR}$$

or

$$t_{\mathrm{CE}} = \frac{\mathrm{PTC}\cdot\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{2}+\mathrm{MRT}\right)+\frac{(1-\mathrm{PTC})\cdot\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tilde{\tau}}{2}+\mathrm{MRT}\right)+\frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR}$$

t_{GE}, the group equivalent downtime:

$$t_{\mathrm{GE}} = \frac{\lambda_{\mathrm{DU}}^{(\mathrm{r})}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{3}+\mathrm{MRT}\right)+\frac{\lambda_{\mathrm{DU}}^{(\mathrm{nr})}}{\lambda_{\mathrm{D}}}\left(\frac{\tilde{\tau}}{3}+\mathrm{MRT}\right)+\frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR}$$

or

$$t_{\mathrm{GE}} = \frac{\mathrm{PTC}\cdot\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{3}+\mathrm{MRT}\right)+\frac{(1-\mathrm{PTC})\cdot\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tilde{\tau}}{3}+\mathrm{MRT}\right)+\frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR}$$

IEC 61508 Approach: 1oo2 System

Recall that IEC 61508 suggests the following formula for a 1oo2 voted system, when CCFs are included:

$$\text{PFD}_{\text{avg}} = 2\lambda_{\text{D}}^2 \cdot t_{\text{CE}} \cdot t_{\text{GE}} + \beta\lambda_{\text{DU}}\left(\frac{\tau}{2} + \text{MRT}\right) + \beta_D\text{MTTR}$$

With imperfect testing the formula becomes:

$$\begin{aligned}\text{PFD}_{\text{avg}} = {} & 2\left[(1-\beta)\lambda_{\text{DU}} + (1-\beta_{\text{D}})\lambda_{\text{DD}}\right]^2 \cdot t_{\text{CE}} \cdot t_{\text{GE}} + \\ & \text{PTC} \cdot \beta\lambda_{\text{DU}}\left(\frac{\tau}{2} + \text{MRT}\right) + (1-\text{PTC})\beta\lambda_{\text{DU}}\left(\frac{\tilde{\tau}}{2} + \text{MRT}\right) \\ & + \beta_{\text{D}}\lambda_{\text{DD}}\text{MTTR}\end{aligned}$$

where t_{CE} and t_{GE} are given in the previous slide, to avoid a too long formula.

IEC 61508 Approach: *koon* System

For *koon* system, we need to modify *several* parameters in the analytical formula suggested in SIS textbook (IEC 61508 does not provide generalized formulas for *koon* systems).

t_{CE}, the channel equivalent downtime:

$$t_{\mathrm{CE}} = \frac{\mathrm{PTC}\cdot\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{2}+\mathrm{MRT}\right)+\frac{(1-\mathrm{PTC})\cdot\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tilde{\tau}}{2}+\mathrm{MRT}\right)+\frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR}$$

t_{GiE}, the group equivalent downtime of *degraded* states

$$t_{\mathrm{GiE}} = \frac{\mathrm{PTC}\cdot\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{i+1}+\mathrm{MRT}\right)+\frac{(1-\mathrm{PTC})\cdot\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tilde{\tau}}{i+1}+\mathrm{MRT}\right)+\frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR}$$

where $i = 2..(n-k)$

t_{GE}, the group equivalent downtime of *dangerous* state:

$$t_{\mathrm{GE}} = \frac{\mathrm{PTC}\cdot\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{n-k+2}+\mathrm{MRT}\right)+\frac{(1-\mathrm{PTC})\cdot\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tilde{\tau}}{n-k+2}+\mathrm{MRT}\right)+\frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR}$$

IEC 61508 Approach: *koon* System

Recall that the SIS textbook suggests the following formula for *koon* system:

$$\text{PFD}_{\text{avg}} = \lambda_D^{n-k+1} \cdot k \cdot n \left[\prod_{i=2}^{n-k} (n-i+1) t_{GiE} \right] \cdot t_{CE} \cdot t_{\text{GE}} + \beta \lambda_{\text{DU}} \left(\frac{\tau}{2} + \text{MRT} \right) + \beta_D \text{MTTR}$$

With imperfect testing the formula becomes:

$$\text{PFD}_{\text{avg}} = [(1-\beta)\lambda_{\text{DU}} + (1-\beta_{\text{D}})\lambda_{\text{DD}}]^{n-k+1} \cdot k \cdot n \left[\prod_{i=2}^{n-k+1} (n-i+1) t_{GiE} \right] \cdot t_{\text{CE}} \cdot t_{\text{GE}} +$$
$$\text{PTC} \cdot \beta \lambda_{\text{DU}} \left(\frac{\tau}{2} + \text{MRT} \right) + (1 - \text{PTC}) \beta \lambda_{\text{DU}} \left(\frac{\tilde{\tau}}{2} + \text{MRT} \right)$$
$$+ \beta_{\text{D}} \lambda_{\text{DD}} \text{MTTR}$$

where t_{CE}, t_{GiE} for $i = 2..(n-k)$, and t_{GE} are given in the previous slide, to avoid a too long formula.

IEC 61508 Approach: Verification

Verification of formulas for $koon$ for 1oo2 system: With imperfect testing the formula becomes:

$$\begin{aligned}\mathrm{PFD_{avg}} = &\left[(1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\right]^2 \cdot 1 \cdot 2 \cdot \left[\prod_{i=2}^{1}(n-i+1)t_{GiE}\right] \cdot t_{\mathrm{CE}} \cdot t_{\mathrm{GE}} + \\ &\mathrm{PTC} \cdot \beta\lambda_{\mathrm{DU}}\left(\frac{\tau}{2} + \mathrm{MRT}\right) + (1-\mathrm{PTC})\beta\lambda_{\mathrm{DU}}\left(\frac{\tilde{\tau}}{2} + \mathrm{MRT}\right) \\ &+ \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR}\end{aligned}$$

where t_{CE}, t_{GiE} for $i = 2..(n-k)$, and t_{GE} are given in the previous slide. This gives:

$$\begin{aligned}\mathrm{PFD_{avg}} = &\,2\left[(1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\right]^2 \cdot t_{\mathrm{CE}} \cdot t_{\mathrm{GE}} + \\ &\mathrm{PTC} \cdot \beta\lambda_{\mathrm{DU}}\left(\frac{\tau}{2} + \mathrm{MRT}\right) + (1-\mathrm{PTC})\beta\lambda_{\mathrm{DU}}\left(\frac{\tilde{\tau}}{2} + \mathrm{MRT}\right) \\ &+ \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR}\end{aligned}$$

which is the same as shown earlier.

IEC 61508 Approach: Verification

Verification of formulas for $koon$ for 2oo3 system: With imperfect testing the formula becomes:

$$\begin{aligned}\mathrm{PFD}_{\mathrm{avg}} = &\left[(1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\right]^2 \cdot 2 \cdot 3 \cdot \left[\prod_{i=2}^{1}(n-i+1)t_{GiE}\right] \cdot t_{\mathrm{CE}} \cdot t_{\mathrm{GE}} + \\ &\mathrm{PTC} \cdot \beta\lambda_{\mathrm{DU}}\left(\frac{\tau}{2} + \mathrm{MRT}\right) + (1-\mathrm{PTC})\beta\lambda_{\mathrm{DU}}\left(\frac{\tilde{\tau}}{2} + \mathrm{MRT}\right) \\ &+ \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR}\end{aligned}$$

where t_{CE}, t_{GiE} for $i = 2..(n-k)$, and t_{GE} are given in the previous slide. This gives:

$$\begin{aligned}\mathrm{PFD}_{\mathrm{avg}} = &\,6\left[(1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\right]^2 \cdot t_{\mathrm{CE}} \cdot t_{\mathrm{GE}} + \\ &\mathrm{PTC} \cdot \beta\lambda_{\mathrm{DU}}\left(\frac{\tau}{2} + \mathrm{MRT}\right) + (1-\mathrm{PTC})\beta\lambda_{\mathrm{DU}}\left(\frac{\tilde{\tau}}{2} + \mathrm{MRT}\right) \\ &+ \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR}\end{aligned}$$

which is the same as shown earlier.

IEC 61508 Approach: Verification

Verification of formulas for *koon* for 1oo3 system: With imperfect testing the formula becomes:

$$\begin{aligned}\mathrm{PFD}_{\mathrm{avg}} = {} & [(1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}]^3 \cdot 1 \cdot 3 \cdot \left[\prod_{i=2}^{2}(n-i+1)t_{GiE}\right] \cdot t_{\mathrm{CE}} \cdot t_{\mathrm{GE}} + \\ & \mathrm{PTC} \cdot \beta\lambda_{\mathrm{DU}}\left(\frac{\tau}{2} + \mathrm{MRT}\right) + (1-\mathrm{PTC})\beta\lambda_{\mathrm{DU}}\left(\frac{\tilde{\tau}}{2} + \mathrm{MRT}\right) \\ & + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR}\end{aligned}$$

where t_{CE}, t_{GiE} for $i = 2..(n-k)$, and t_{GE} are given in the previous slide. This gives:

$$\begin{aligned}\mathrm{PFD}_{\mathrm{avg}} = {} & 6\,[(1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}]^3 \cdot t_{\mathrm{CE}} \cdot t_{\mathrm{G2E}} \cdot t_{\mathrm{GE}} + \\ & \mathrm{PTC} \cdot \beta\lambda_{\mathrm{DU}}\left(\frac{\tau}{2} + \mathrm{MRT}\right) + (1-\mathrm{PTC})\beta\lambda_{\mathrm{DU}}\left(\frac{\tilde{\tau}}{2} + \mathrm{MRT}\right) \\ & + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR}\end{aligned}$$

Here, t_{G2E} and t_{GE} are:

$$\begin{aligned} t_{\mathrm{G2E}} &= \frac{\mathrm{PTC} \cdot \lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{3} + \mathrm{MRT}\right) + \frac{(1-\mathrm{PTC}) \cdot \lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tilde{\tau}}{3} + \mathrm{MRT}\right) + \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR} \\ t_{\mathrm{GE}} &= \frac{\mathrm{PTC} \cdot \lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{4} + \mathrm{MRT}\right) + \frac{(1-\mathrm{PTC}) \cdot \lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tilde{\tau}}{4} + \mathrm{MRT}\right) + \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR} \end{aligned}$$

Multi-phase Markov

Multi-phase Markov models may be used to plot PFD as a function of time, considering the effects of imperfect testing.

The basic approach is as follows:

1. Set up the Markov model for r- and nr-states without including return rates that involve regular proof tests and overhauls
2. Multi-phase Markov splits the analysis into phases. One phase can correspond to the time between imperfect proof tests
3. At the end of each phase, it is necessary to define what happens in the transition from one phase to the next. For this purpose we need a linking matrix (also called "Repair matrix")

Example of the set-up of a linking matrix is:

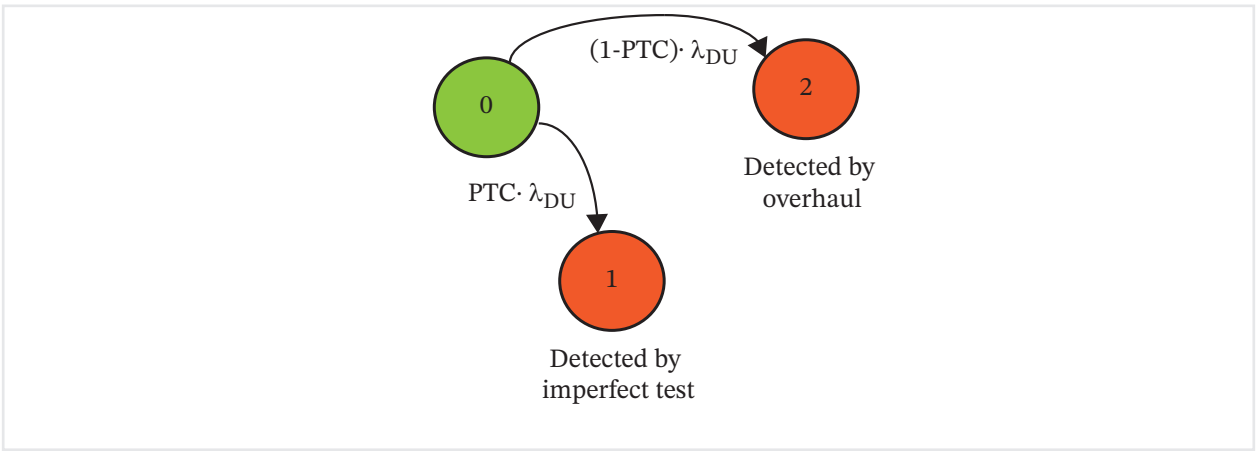
State before linking	State after linking	Probability

An example is provided.

Multi-Phase Markov: 1oo1 System

We consider a 1oo1 voted system that is subject to imperfect testing (with coverage PST interval τ) and overhaul (with interval $\tilde{\tau}$, where $\tau < \tilde{\tau}$. We want to plot PFD(t) in the interval of the overhaul, and splits into phases with length τ.

The corresponding Markov model becomes:



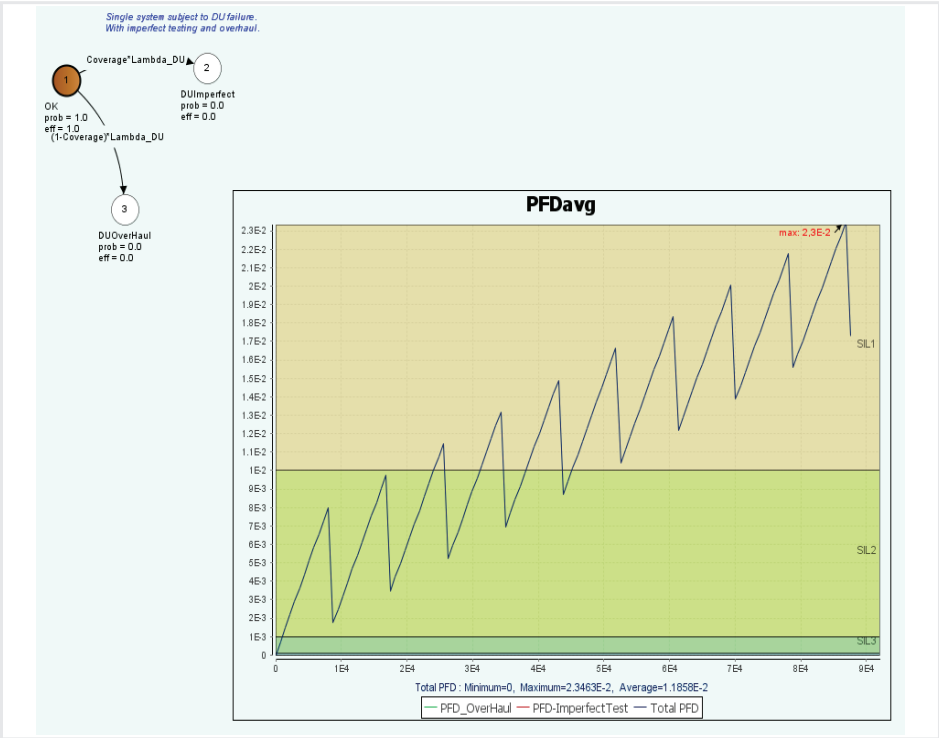
Each time the calculation reaches a proof test, it is necessary to judge what happens using the linking matrix. In this case, we suggest:

State before linking	State after linking	Probability
0	0	1.0
1	0	1.0
2	2	1.0

Multi-Phase Markov: 1oo1 System (cont.)

There are several ways to solve the Markov model. One option is to use Grif Workbench, accessible from `http://grif-workshop.com/`.

The 1oo1 system was implemented using Grif Markov package with PST= 80% , $\lambda_{\mathrm{DU}} = 1 \cdot 10^{-6}$ per hour, $\tau = 8760$ hours, and $\tilde{\tau} = 10 \cdot \tau$.



Partial Proof Testing

A partial proof test is a similar concept as imperfect testing, but is not exactly the same.

The main characteristics of a partial proof test are:

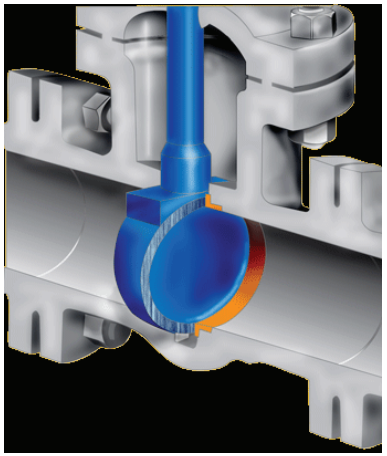
- The partial test is *planned* or designed to reveal *some*, but not all DU failure modes
- The motivation for introducing a partial test is that the test does not interfere with the normal operation
- The partial test is normally carried out more often than the proof test
- A dedicated coverage factor is suggested (we use Θ_{PST}, to distinguish it from PTC)
- In principle, it is possible to include then effects of partial proof tests, imperfect proof tests, and overhauls.

One example of a partial proof test is partial stroke testing of valves. Here the valve is only subject to a partial movement, in a way that does not require any stop of the production, e.g. from 0% to 20% closure of a shutdown valve that is normally in open position.

In the following, we use partial stroke testing as the main example.

Partial Stroke Testing of Valves

- Partial stroke testing is (automatic or mechanical) means to used to reveal certain dangerous failures which are otherwise only revealed during a function test
- During a partial stroke test, the valve is moved a certain distance to wards the position which the valve is intended to operate during a real demand (usually the fail-safe position)
- The movement may for example be from 0-15% (of a total of 100% travel distance); that is *long enough* to (hopefully) identify whether or not the valve is stuck, and *short enough* to avoid process disturbances

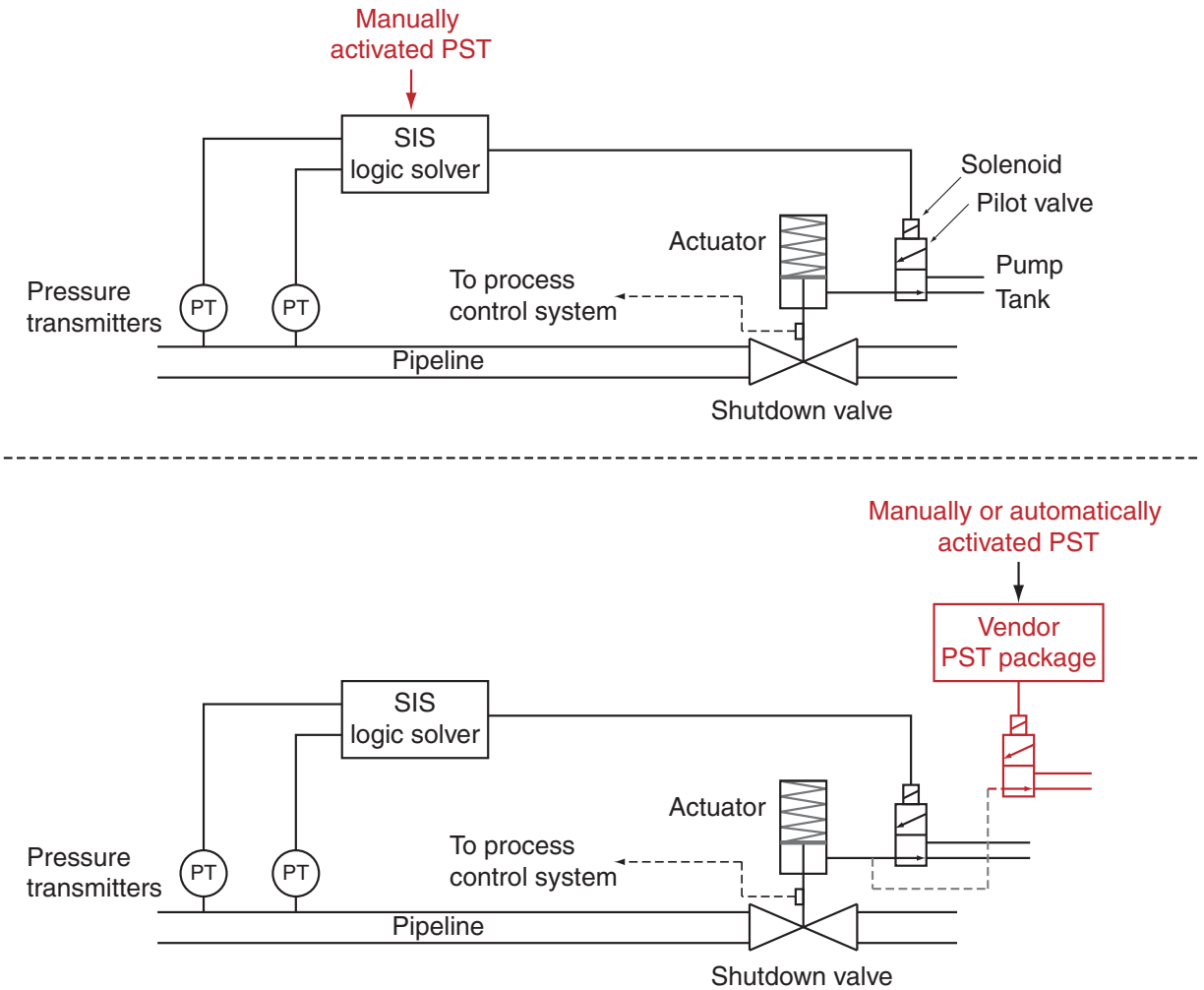


www.franklinvalve.com

Partial stroke testing is introduced to allow earlier detection of (dangerous undetected) failures.

Physical Realization

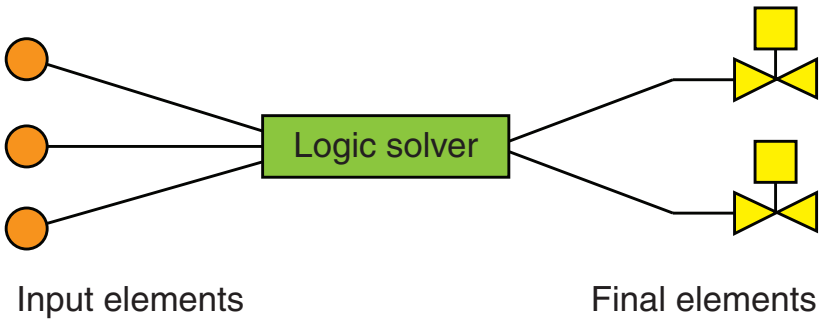
Partial stroke testing may be physically implemented in the following way:



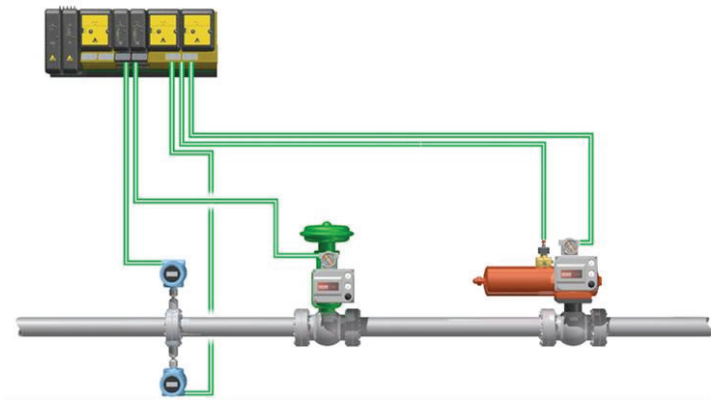
The physical implementation may impact the coverage factor.

Why Partial Stroke Testing?

Full operation of valves often require a plant shutdown. This is costly, and may also increase the risk associated with the required shutdown and start-up.



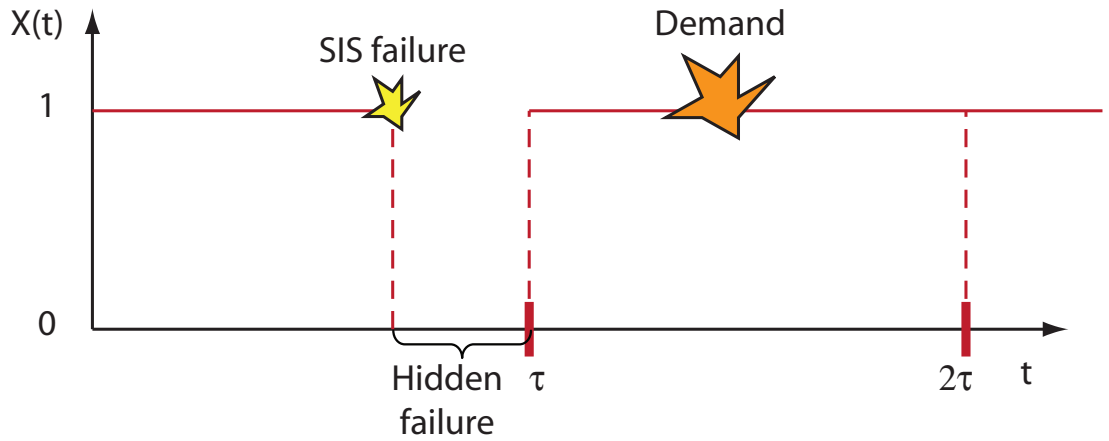
Example:



http://www.puffer.com/

Why Partial Stroke Testing?

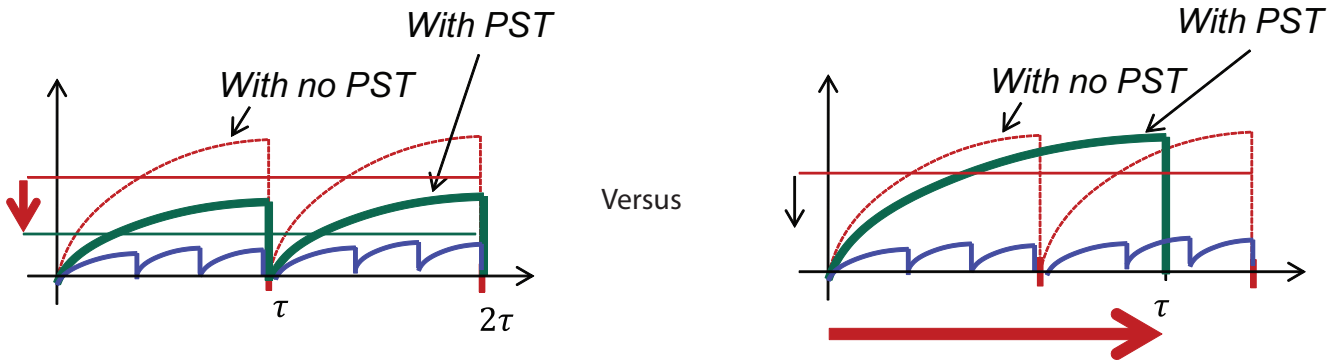
- Most valves are in *open* position during normal operation
- While in open position, it is almost impossible to reveal failures by diagnostics
- A failure may therefore be hidden until there is a demand for closing or until a functional (full stroke) test
- A functional test of a valve often requires partial or full process shutdown
- Shutdown and restart of a plant is always associated with some additional risk.



Two Main Strategies

In practice, we see that partial stroke testing is introduced to reduce costs *or* improve safety.

- Improve safety:
  - Partial stroke testing is added while maintaining current interval for full stroke testing
  - PFD_{avg} is reduced compared to having only full stroke testing
- Reduce costs:
  - Partial stroke testing is added with the motivation to extend interval between full stroke testing
  - PFD_{avg} is maintains same value as before, but the operating costs are reduced due to less frequent full stroke testing



Partial Stroke Testing and PFD

The approach to calculate the PFD_{avg} with partial stroke testing included is the same as for imperfect testing. However, the meaning of the parameters are different.

We consider a single system, with partial stroke test coverage Θ_{PST}, partial stroke test (PST) interval τ_{PST}, and full stroke (FT) (proof) test interval τ. The corresponding formula becomes:

$$\begin{aligned}\text{PFD}_{\text{avg}} &= \text{PFD}_{\text{avg}}^{(\text{PST})} + \text{PFD}_{\text{avg}}^{(\text{FT})} \\ &\approx \frac{\Theta_{\text{PST}} \cdot \lambda_{\text{DU}} \tau_{\text{PST}}}{2} + \frac{(1 - \Theta_{\text{PST}}) \lambda_{\text{DU}} \tau}{2}\end{aligned}$$

The repair-time has been disregarded here.

Partial Stroke Testing and PFD

We consider now a 1oo2 system, with partial stroke test coverage Θ_{PST}, partial stroke test (PST) interval τ_{PST}, and full stroke (FT) (proof) test interval τ.

- The corresponding channel and group equivalent downtimes become: t_{CE}, the channel equivalent downtime:

$$t_{\text{CE}} = \frac{\Theta_{\text{PST}} \cdot \lambda_{\text{DU}}}{\lambda_{\text{D}}} \left(\frac{\tau_{\text{PST}}}{2} + \text{MRT} \right) + \frac{(1 - Theta_{\text{PST}}) \cdot \lambda_{\text{DU}}}{\lambda_{\text{D}}} \left(\frac{\tau}{2} + \text{MRT} \right) + \frac{\lambda_{\text{DD}}}{\lambda_{\text{D}}} \text{MTTR}$$

  t_{GE}, the group equivalent downtime:

$$t_{\text{GE}} = \frac{\Theta_{\text{PST}} \cdot \lambda_{\text{DU}}}{\lambda_{\text{D}}} \left(\frac{\tau_{\text{PST}}}{3} + \text{MRT} \right) + \frac{(1 - Theta_{\text{PST}}) \cdot \lambda_{\text{DU}}}{\lambda_{\text{D}}} \left(\frac{\tau}{3} + \text{MRT} \right) + \frac{\lambda_{\text{DD}}}{\lambda_{\text{D}}} \text{MTTR}$$

  The PFD_{avg} becomes:

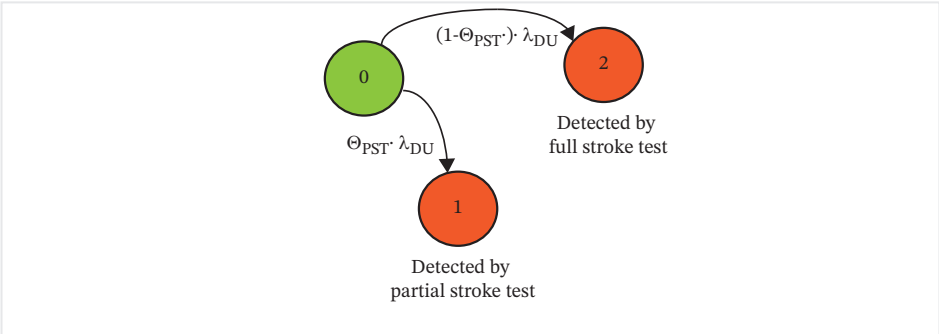
$$\begin{aligned} \text{PFD}_{\text{avg}} = {} & 2 \left[(1 - \beta) \lambda_{\text{DU}} + (1 - \beta_{\text{D}}) \lambda_{\text{DD}} \right]^2 \cdot t_{\text{CE}} \cdot t_{\text{GE}} + \\ & \Theta_{\text{PST}} \cdot \beta \lambda_{\text{DU}} \left(\frac{\tau_{\text{PST}}}{2} + \text{MRT} \right) + (1 - \Theta_{\text{PST}}) \beta \lambda_{\text{DU}} \left(\frac{\tau}{2} + \text{MRT} \right) \\ & + \beta_{\text{D}} \lambda_{\text{DD}} \text{MTTR} \end{aligned}$$

The repair-time has been disregarded here.

Multi-Phase Markov: 1oo1 System

There are several ways to solve the Markov model. One option is to use Grif Workbench, accessible from `http://grif-workshop.com/`.

The 1oo1 system was implemented using Grif Markov package with PST= 80% , $\lambda_{DU} = 1 \cdot 10^{-6}$ per hour, $\tau_{PST} = 1460$ hours, and $\tilde{\tau} = 8760$ hours.



Multi-Phase Markov: 1oo1 System (cont.)

Compared to imperfect testing,we run the simulation over several proof test intervals. We need to introduce two linking matrices, one for what is happening at each partial stroke test and one for what is happening at each full stroke test.

At each partial stroke test, the linking matrix is:

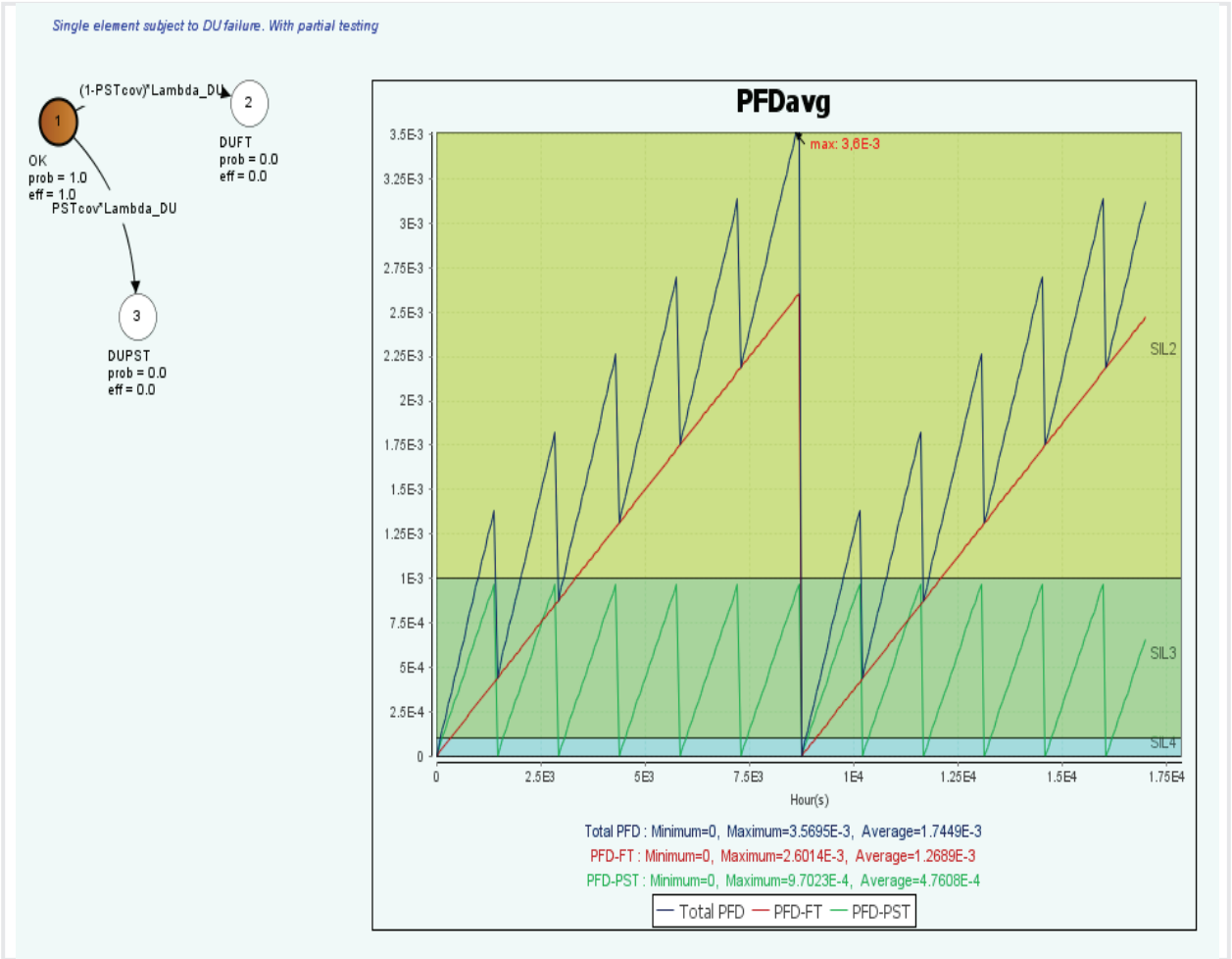
State before linking	State after linking	Probability
0	0	1.0
1	1	1.0
2	0	1.0

At each full stroke test, the linking matrix is:

State before linking	State after linking	Probability
0	0	1.0
1	0	1.0
2	0	1.0

Multi-Phase Markov: 1oo1 System (cont.)

The results using Grif Markov package becomes:



Value of Θ_{PST}

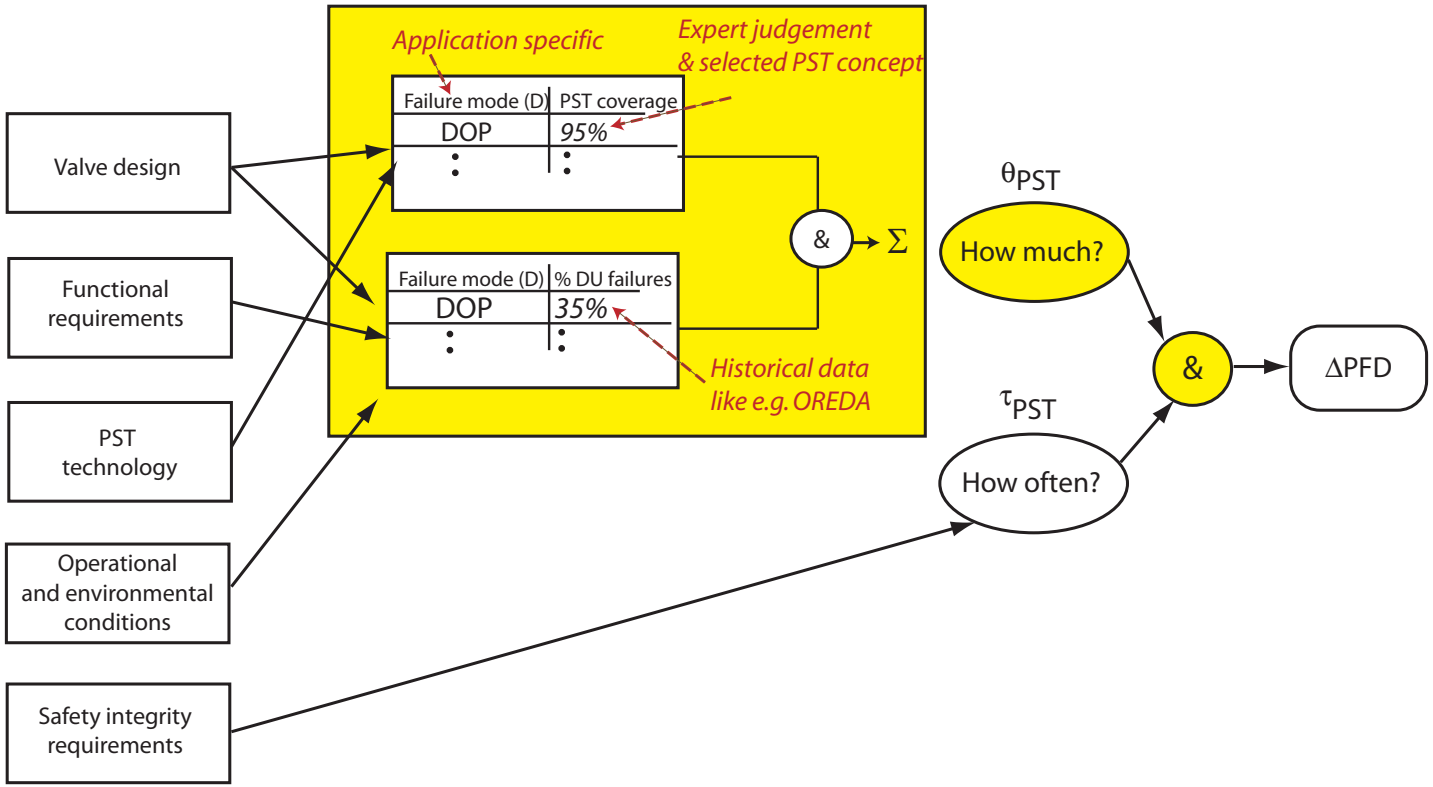
A "perfect" formula for PFD_{avg} cannot compensate for an unrealistic value of Θ_{PST}. It is therefore important to have systematic process for determining the Θ_{PST}.

- The question is: How can this value be selected, or determined?

The following slides outlines some useful approaches.

Approach I: Use of Historical Data

Historical data, like presented in OREDA data handbooks, can provide useful insight about the dangerous failure modes. This information may be complemented by judging of how likely it is that these failure modes can be detected by partial stroke testing, as shown below.



Approach II: Use of Checklists

Checklists can be an alternative approach to determine the value of the partial stroke test coverage factor. This checklist which is based on the following paper, see `https://doi.org/10.1016/j.jlp.2008.04.007` is based on an analysis of what influences the coverage factor. Note that this paper used PTC instead of Θ_{PST} as the name of the coverage factor.

Recall that PTC may have two interpretations (and now we relate this to PST in particular):

- **A fraction:** The PST coverage is the fraction of DU failures detected by PST relative to the total number of DU failures:

$$\text{PTC} = \frac{\lambda_{\text{DU,PST}}}{\lambda_{\text{DU}}}$$

- **Conditional probability:** The probability that a dangerous undetected failure is detected by the PST once a dangerous undetected failure is present (conditional probability)

$$\text{PTC} = \Pr(\text{Detect DU failure by PST} \mid \text{DU failure is present})$$

Remark: The first interpretation denotes a constant value of PTC, while the last may open up for a discussion whether it takes the same value every time a DU failure occurs. In the following, we disregard this issue.

Approach II: Use of Checklist

Starting point is to say that:

$$\text{PTC} = \frac{\Pr\left(\text{Detect DU failure by PST} \cap \text{DU failure is present})\right)}{\Pr\left(\text{DU failure is present}\right)}$$

Let $\text{FM}_1, \text{FM}_2, \ldots \text{FM}_n$ be the relevant DU failure modes. We may assume that they do not occur at the same time ("mutually exclusive"):

$$\text{PTC} \approx \sum_{i=1}^{n} \frac{\Pr\left(\text{Detect FM}_i \mid \text{FM}_i \text{ is present}\right) \cdot \Pr\left(\text{FM}_i \text{ is present}\right)}{\Pr\left(\text{DU failure is present}\right)}$$

Here, we may consider the PTC_i of failure mode i as:

$$\text{PTC}_i = \Pr\left(\text{Detect FM}_i \mid \text{FM}_i \text{ is present}\right)$$

with weight w_i:

$$w_i = \frac{\Pr\left(\text{FM}_i \text{ is present}\right)}{\Pr\left(\text{DU failure is present}\right)}$$

Approach II: Use of Checklist

The PST coverage can therefore be expressed as

$$\text{PTC} = \sum_{i=1}^{n} \text{PTC}_i \cdot w_i$$

Note:

- The first factor, PTC_i is mainly influenced by how suitable or capable PST is for revealing failures for a particular type of valve
- The second factor, w_i may be deduced from databases such as OREDA.

Approach II: Use of Checklist

It is not straight forward to select "reasonable" PTC_i, we first split PTC_i into *two* sub-factors:

- **PST Revealability ($\mathrm{PST}_{\mathrm{Rev},\,i}$):** To what extent the failure mode is *revealable* during a partial stroke operation,
- **PST reliability ($\mathrm{PST}_{\mathrm{Rel},\,i}$):** To what extent the test results are reliable ("trustable"), such that the announced results reflect the valve condition.

This implies that:

$$\mathrm{PTC}_i = \mathrm{PST}_{\mathrm{Rev},\,i} \cdot \mathrm{PST}_{\mathrm{Rel},\,i}$$

For simplicity, it is assumed that PST reliability is the same for all failure modes, so that:

$$\mathrm{PTC}_i = \mathrm{PST}_{\mathrm{Rev},\,i} \cdot \mathrm{PST}_{\mathrm{Rel}}$$

Approach II: Procedure

A procedure for determining the PST coverage (PTC) has been suggested by Lundteigen and Rausand in https://doi.org/10.1016/j.jlp.2008.04.007:

- Step 1: Familiarization with the implementation of PST
- Step 2: Analyze the PST hardware and software
- Step 3: Determine PST reliability - PST_{Rel}
- Step 4: Determine PST revealability - $\text{PST}_{\text{Rev},\,i}$
- Step 5: Determine the failure mode weights - w_i
- Step 6: Determine the PST coverage - PTC

Step 1: Familiarization with the implementation of PST

The objective of Step 1 is to collect relevant information on the PST implementation and the application specific conditions, including:

1. Which SIS components that are operated during a PST
2. The functional safety requirements of the SIS components, like valve closing time and maximum allowed leakage in closed position
3. How PST is initiated and controlled by dedicated hardware and software
4. The PST interface to the SIS and other systems, like the process control system
5. The operational and environmental conditions under which the SIF operates, including fluid characteristics, temperature, and pressure

Step 2: Analyze the PST hardware and software

The objective of Step 2 is to do a more thorough analysis of hardware and software dedicated for the execution of PST:

- Identify and analyze how PST hardware and software failures affect the PST execution and the SIS itself:
  - How has the hardware and software been verified, tested, and documented?
  - To what extent are the operators and other personnel involved familiar with the PST implementation and procedures?
  - How are failures revealed after a PST reported?
- Use this information as basis for answering checklist questions

The information may be identified by performing, or by review of an existing failure modes and effects analysis (FMEA).

Step 2: Use of FMEA

A small sample from an FMEA is shown below (just invented for this purpose):

Description of component			**Failure and the failure effects**		
Component	**Type**	**Function**	**Failure mode**	**Effect on PST**	**Effect on SIS**
Test initiator	SW	To initiate a PST	Fail to initiate	No execution of PST	None
Timer	SW	Deactivate output according to timer setpoint	Fail to start	No execution of PST	None
			Fail to reset	Valve not returned to initial position	Spurious valve closure
Position indicators	HW	Measure valve position	No signal	PST may be executed, but valve position indicator does not show that the valve moves.	Repair must be initiated to correct position indicators
			Wrong signal	May fail to announce the correct valve position	SIS may be left with unrevealed failures.

Step 3: Determine the PST reliability

The main purpose of Step 3 is to assess the trustworthiness of information provided by the PST, using expert judgment.

No	Question	Answer	Weight	Credit
1	Have success criteria for the partial stroke test been clearly defined?	Y	10	0.14
2	Has an FMEA been performed to identify the SIS failure modes, and to what extent the the failure modes can be detected during a partial valve operation?	Y	10	0.14
3	Have potential failures of the PST hardware and software been identified and analyzed?	N	10	0.07
4	Have potential secondary effects of PST on the reliability of valve, actuator and control devices (e.g., solenoid operated valves) been analyzed?	N	5	0.04
5	Is the actual stem movement measured (in %), as opposed to just verifying that the valves leaves and returns to the initial position?	Y	5	0.07
6	Is additional instrumentation installed, and is it capable of providing more insight to failure causes?	N	1	0.01
7	Is the PST hardware and software regularly inspected and tested (or otherwise verified)?	Y	5	0.07
8	Is the feedback from PST recorded and further analyzed?	Y	10	0.14
9	If short closure time is required: Has it been analyzed if the PST is able to provide useful information?	Y	10	0.14
10	Are means implemented to verify that the position indicators are reliable?	Y	5	0.07
		Sum:	71	0.89

Step 4: Determine the revealability factor

In Step 4, the purpose is to extend the FMEA sheet, in combination with using expert judgment to assign revealability factors.

FAILURE MODE	SUB-FAILURE MODES	REVEALABILITY FACTOR
Fail to close	Fail to start moving	100%
	Starts, but does not reach end position	0%
Delayed operation	Delayed start	100%
	Starts, but uses too long closing time	70%
Leakage in closed position	Minor leakage	0%
	Major leakage	0%

Step 5: Determine the failure mode weights

In Step 5, it is proposed to extend the FMEA further by assigning failure mode weights w_i. The values are selected in combination with expert judgments and available data, e.g. from OREDA.

Failure mode	Weight	Refinement Sub failure modes	Split	Resulting weight
Fail to close	40%	Fail to start moving Starts, but does not reach end position	80% 20%	32% 8%
Delayed operation	40%	Delayed start Too long travel time	40% 60%	16% 24%
Leakage in closed position	20%	Minor leakage Major leakage	60% 40%	12% 8%

The percentages added here have been derived from OREDA in combination with some expert judgments.

Step 6: Calculate the PST coverage

The main purpose of Step 6 is to determine the value of the PTC, based on the results of steps 3, 4 and 5. The following formula applies:

$$\mathrm{PTC} = \mathrm{PST}_{\mathrm{Rel}} \sum_{i=1}^{n} \mathrm{PST}_{\mathrm{Rev},\,i} \cdot w_i$$

Advantages and disadvantages

PST is used to improve safety:

- \+ Improved safety
- \+ More frequent testing for dangerous failure modes
- \+ Less sticking seals
- ÷ Process disturbances due to function tests not reduced
- ÷ More wear on components (e.g. solenoids)
- ÷ New dangerous failure causes or existing ones more likely to occur?
- ÷ Added complexity:
  - More spurious operations?
  - New dangerous failure causes introduced?

PST is used to extend proof test interval:

- \+ Reduced wear on e.g. valve seat
- \+ Less sticking seals
- ÷ Added complexity (as above)
- ÷ More wear on components (e.g. solenoids)
- ÷ Increased failure rate for those failure modes that are seldom tested (fail to close or seal completely)