NTNU
Norwegian University of
Science and Technology

PK 5170: On industrial practices and use of the PDS method

Mary Ann Lundteigen
Mary.a.Lundteigen@ntnu.no

(Revision: 27. September 2016)

Keywords

CSU

β

CF

DTU_T

PFD

Systematic failure

C_{MooN}

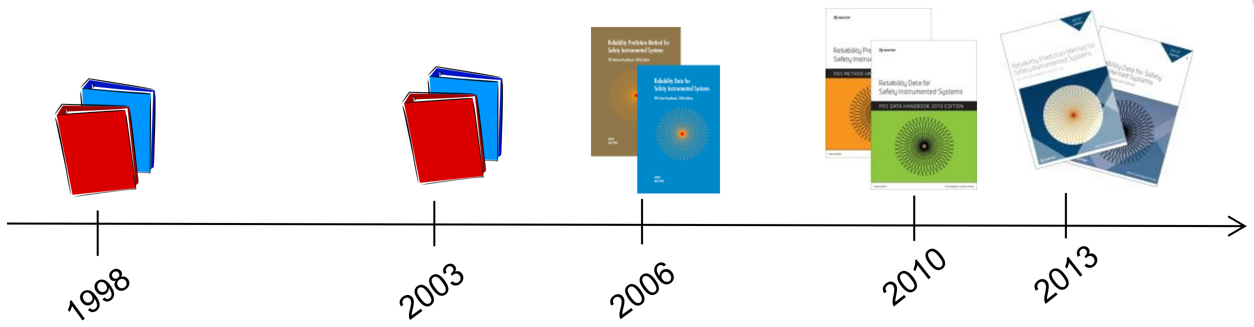
P_{TIF}

β_2

DTU_R

Random hardware failure

PDS method – brief history



- Initial development by NTNU/SINTEF
- Further improvements and alignment with standards through research projects funded by the Norwegian Research Council and the PDS forum. Headed by SINTEF.
- http://www.sintef.no/pds

PDS forum

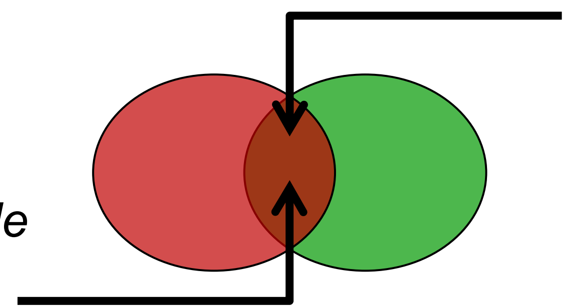

PDS
Reliability of Safety Instrumented Systems
SINTEF
Home
PDS Method
PDS Handbooks
PDS Projects & Reports
PDS Forum
NTNU Course
Contact
You are here: Home / PDS Forum
What is PDS forum
Participating companies
PDS forum meetings
PDS forum membership
PDS working committee
070 Guidelines for the Application of IEC 61508 and IEC 61511 in the petroleum activities on the continental shelf
PDS Forum
"PDS Forum" is a co-operation between oil companies, engineering companies, drilling contractors, consultants, vendors and researchers, with a special interest in safety instrumented systems.
There are more than 20 participating companies in the forum, meeting twice a year for workshops, presentations and technical discussions.
The main objective of the PDS Forum is to maintain a professional meeting place for exchange of experience between vendors and users of control and safety systems. The primary focus is on safety and reliability aspects of such systems. Topics of the forum are:
• Exchange of experience and ideas related to design and operation of instrumented safety systems
• Exchange of information on new field developments and SIS application areas
• Use of new standards for control and safety systems
• Development of guidelines for the use of these standards
• Exchange and use of reliability field data
The official language of the forum is Norwegian.
8
Published July 4, 2007
Norwegian centre of force for developing Safety Instrumented Systems (SIS) in the petroleum industry
ABB
origo
ConocoPhillips
Eni Norge
FMC
DNV·GL
Honeywell
KONGSBERG
SAFETEC
Lilleaker Consulting a.s.
TOTAL
SIEMENS
ENGIE
Statoil
Lloyd's Register Consulting
AkerSolutions
SIMTRONICS group
REPSOL
Lundin Norway
SINTEF
The Research Council of Norway
NTNU – Trondheim Norwegian University of Science and Technology

PDS method – MAIN objectives

Main objectives:
- Quantify the safety unavailability, *AND*
- Quantify loss of production

Safety unavailability: The safety function not being able to function on demand

Production stopped due to spurious (false) activations



Production stopped while SIS down for repair

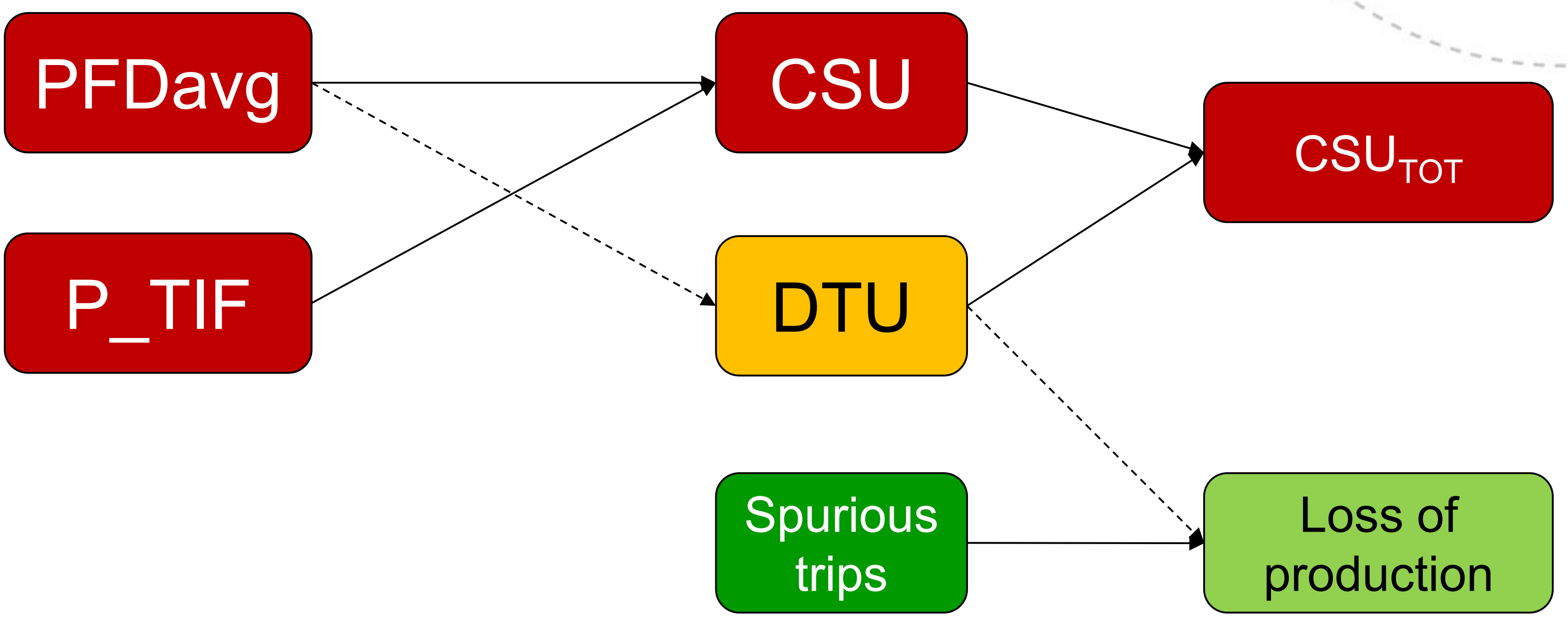
PDS method – other objectives

Other objective: Provide ``realistic" estimates for safety unavailability by:

- Overcoming some weaknesses in the IEC 61508 standard related to:
  - Common cause failures
  - Failure classification
- Presenting data that corresponds to the "best knowledge" in the oil and gas industry

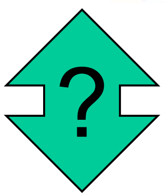
Measure of safety unavailability - CSU

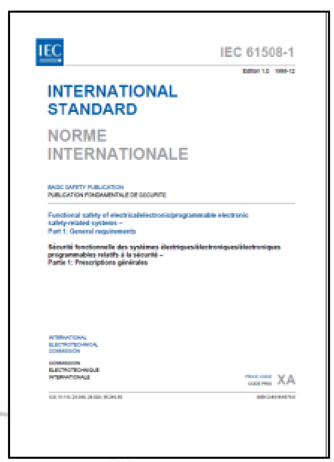
Safety unavailability is called "critical safety unavailability" (CSU)



DTU: Downtime unavailablity, P_TIF: Probability of test independent failure

PDS method versus IEC 61508





PDS and IEC 61508 differs (slightly) in their approach to:

- Failure classification and what failures to include in quantification of PFD/CSU
- Modeling of CCFs
- Approach to incorporation of downtime due to repair
- Treatment of imperfect testing
- Alternative proposals for how to treat special cases (e.g. dependencies between multiple SISs)

FAILURE CLASSIFICATION

NTNU
Norwegian University of
Science and Technology

Failure classification - application

λ

λ_{crit}

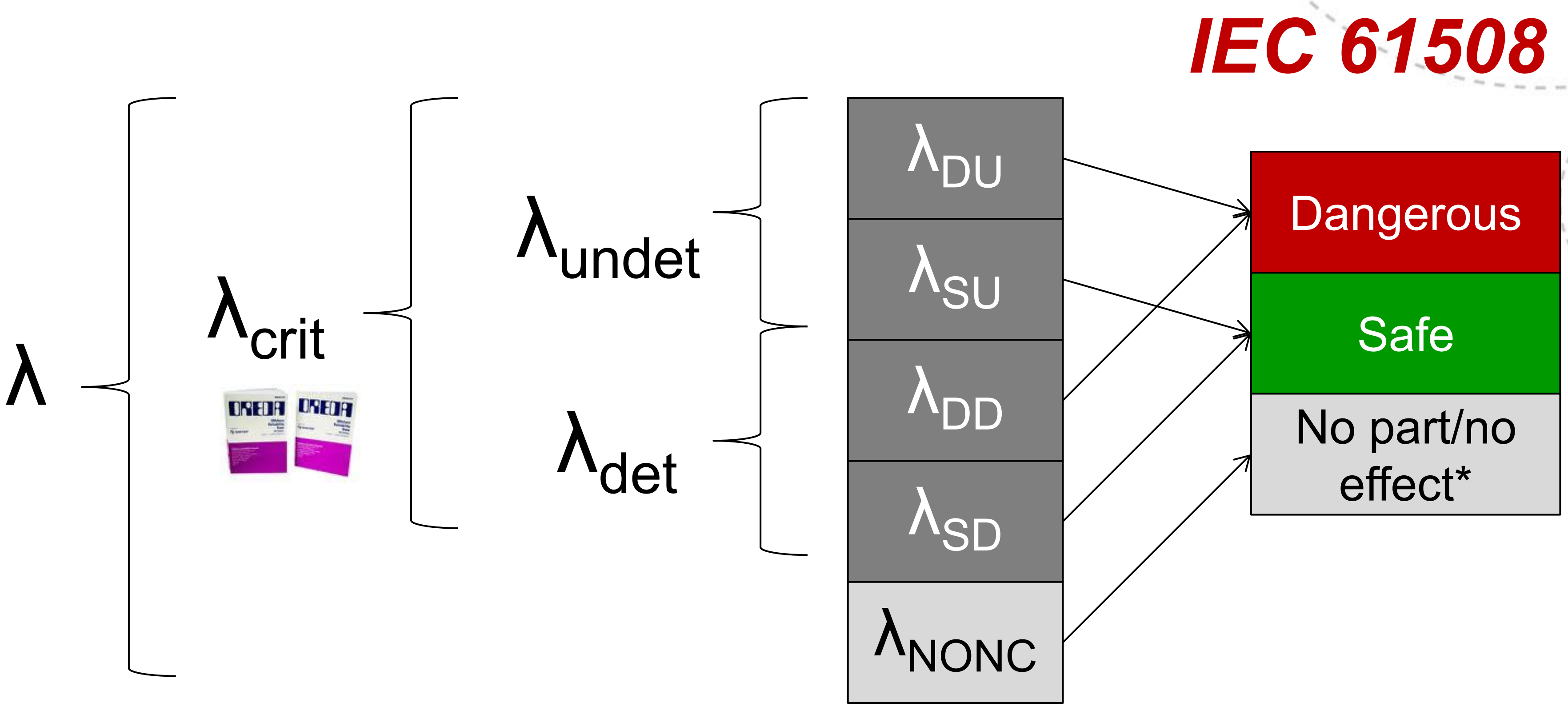
OREDA classi- fication

λ_{undet}

λ_{det}

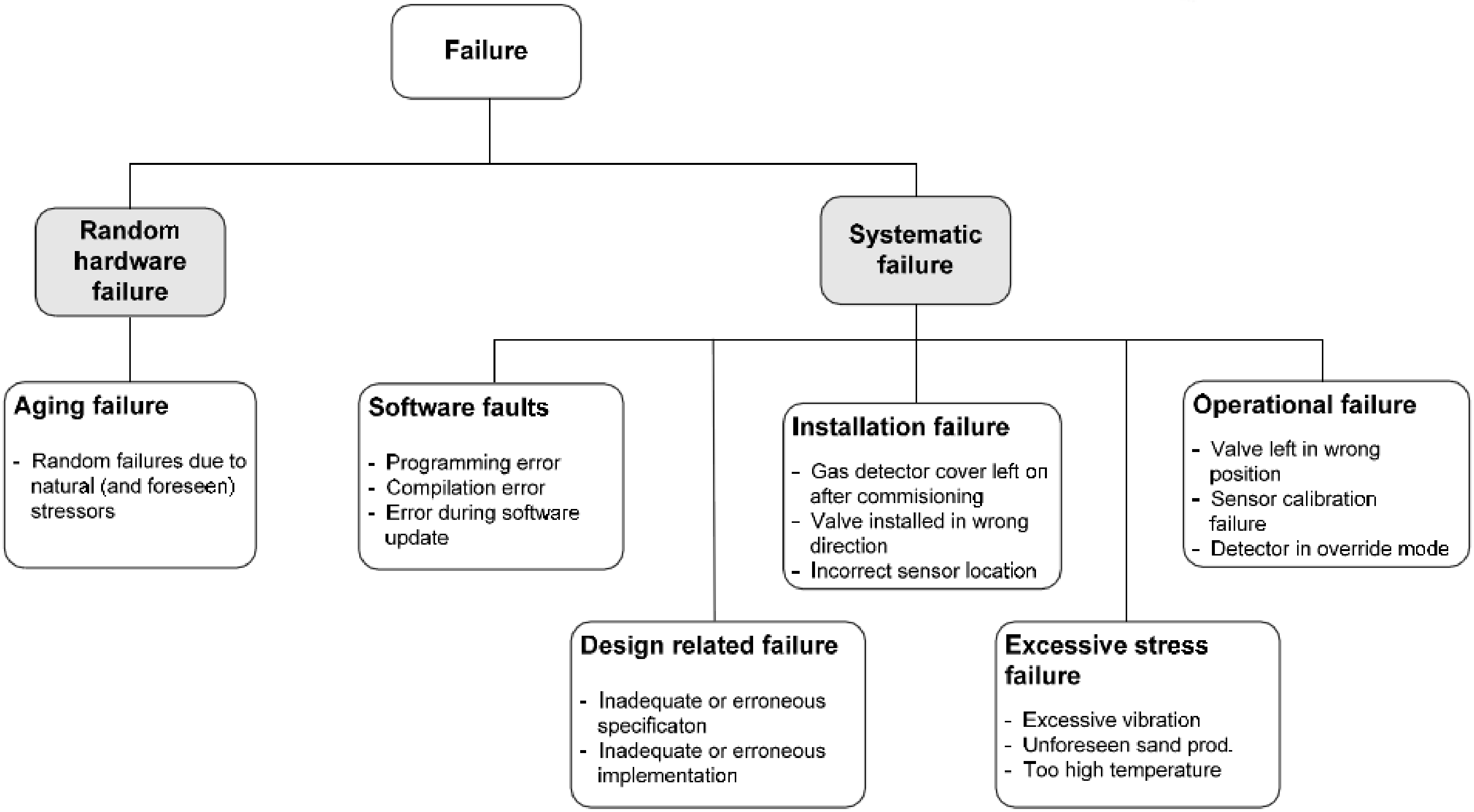
λ_{DU}
λ_{SU}
λ_{DD}
λ_{SD}
λ_{NONC}

Failure classification - application



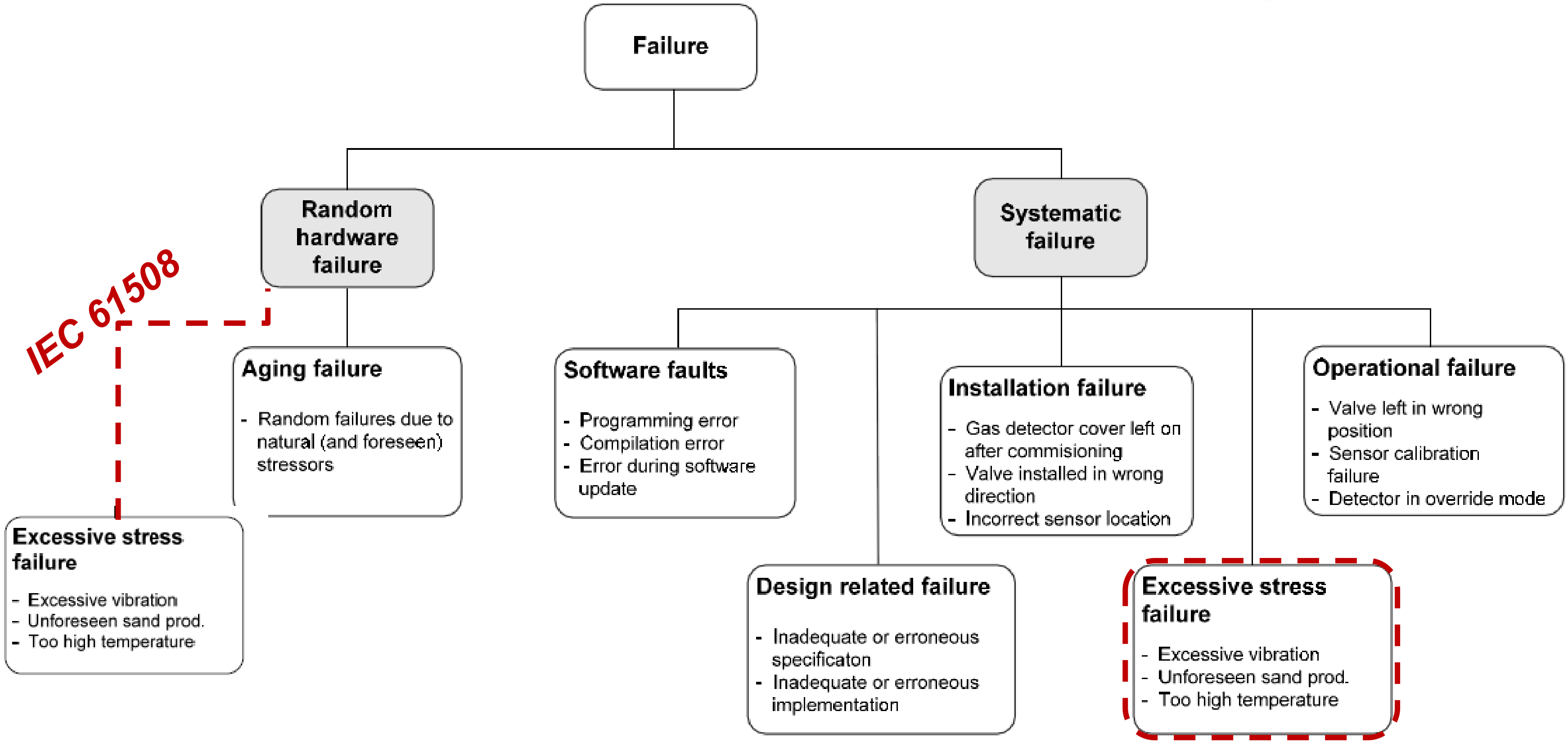
**New failure category in IEC 61508, 2010 edition*

Failure classification in PDS



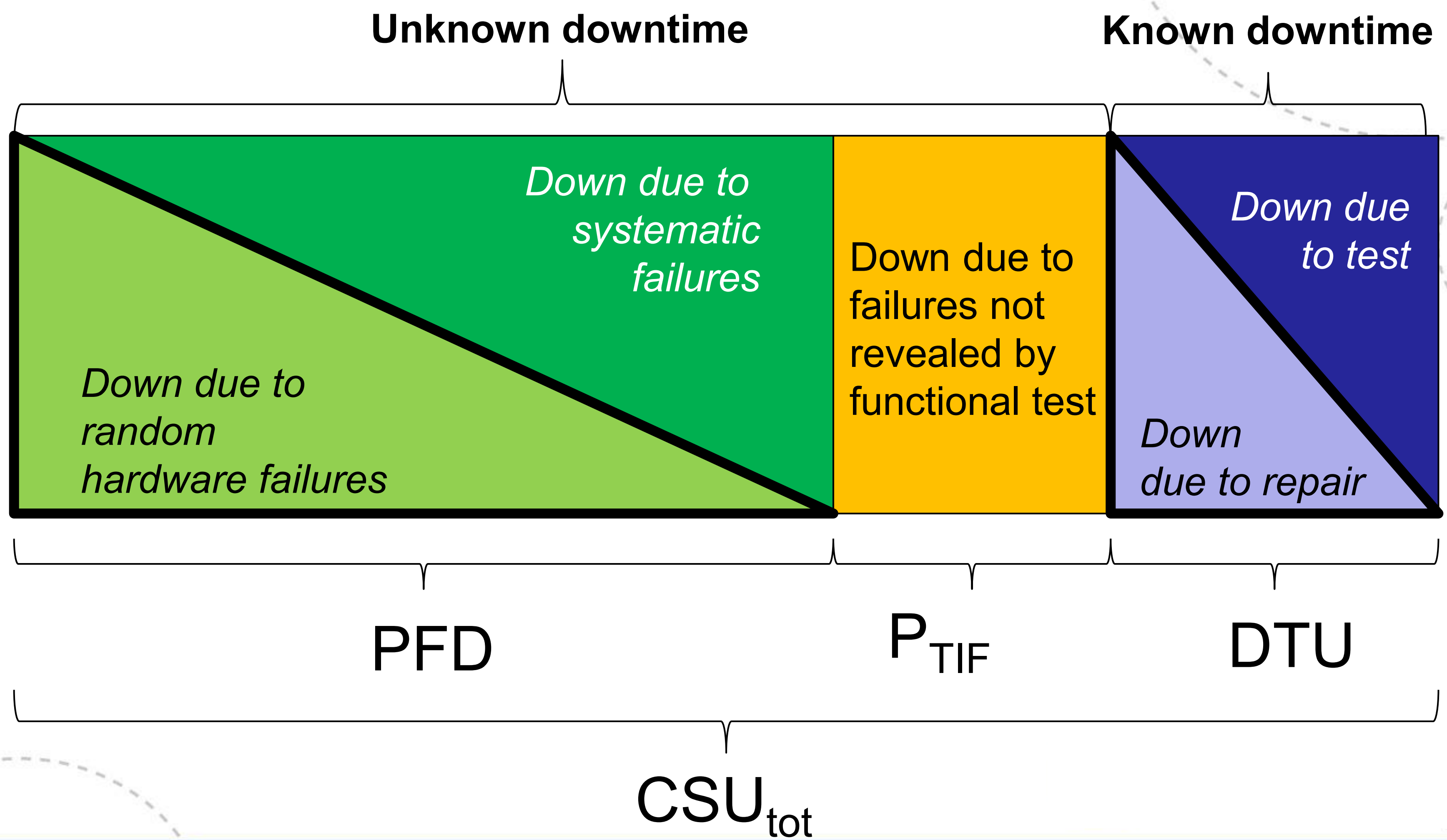
Ref: PDS method (2010)

Failure classification in PDS/ IEC 61508

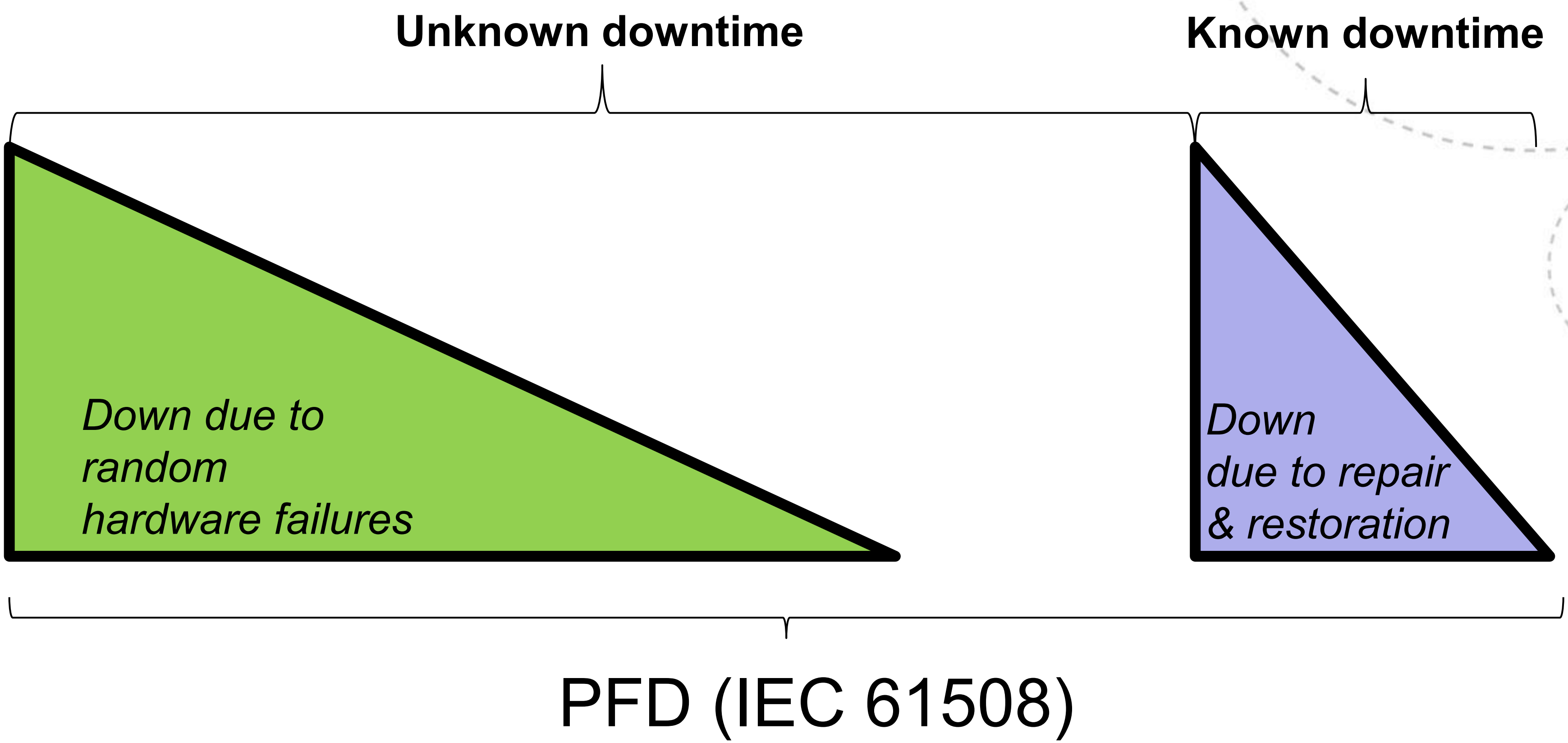


Ref: PDS method (2010)

Contributions to safety unavailability

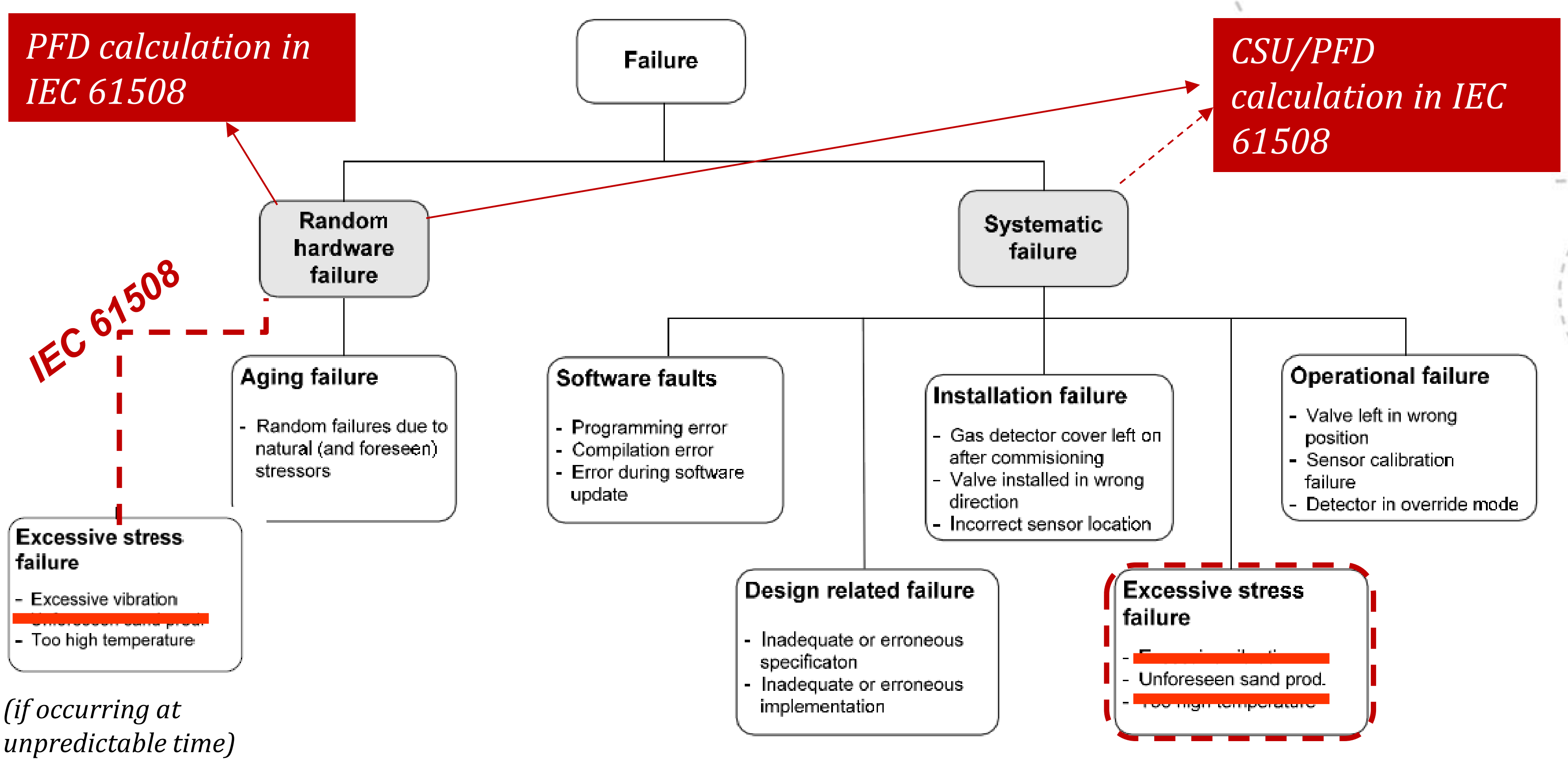


CSU versus PFD in IEC 61508 (simplified formulas)



Estimates of PFD using the PDS approach may therefore be different from estimates based on PFD in IEC 61508

Failure classification in PDS/ IEC 61508



Ref: PDS method (2013)

Best alternative? ISO TR 12489

ISO/TR 12489:2013(E)

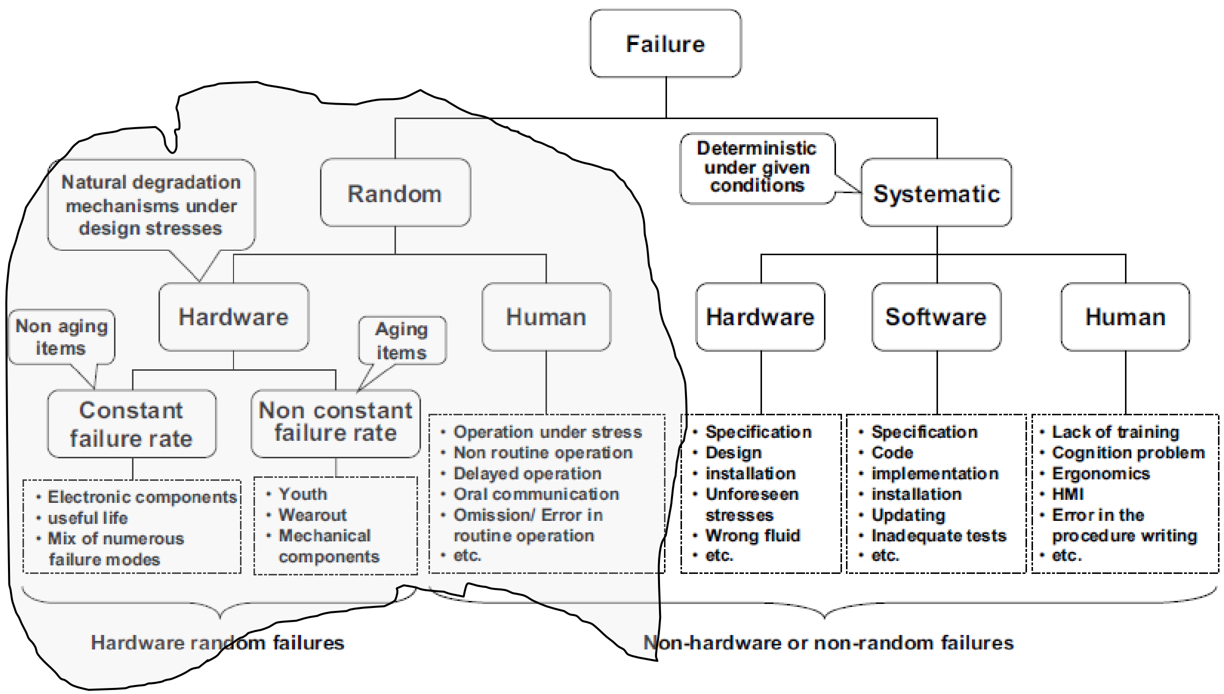


Figure B.5 — Random versus systematic failures

Failures being quantified

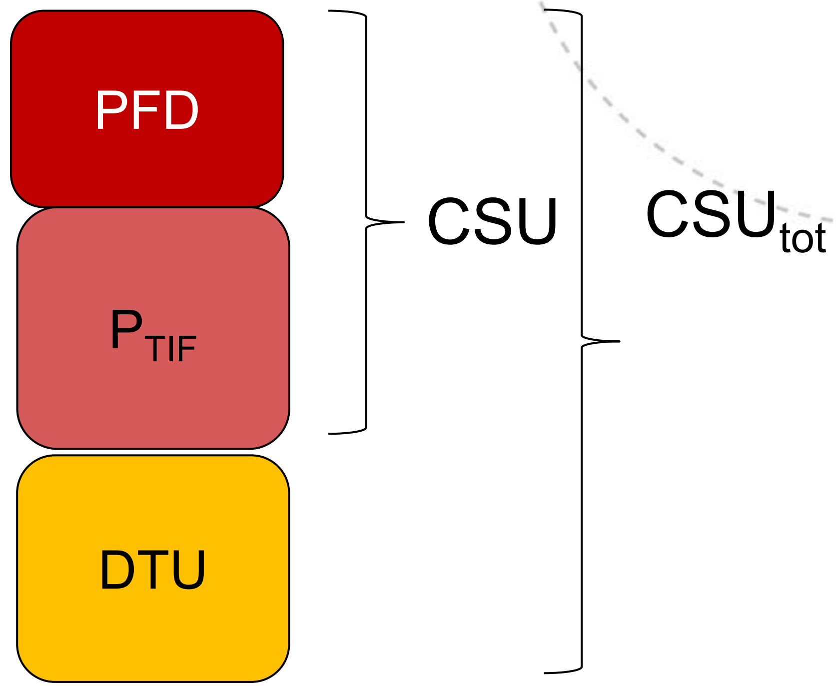
HIGH LEVEL VIEW ON CSU

Quantification of safety unavailability

Unknown *downtime due to DU failures*

Unknown *downtime due to failures that <u>cannot</u> be detected by a functional test, only a real demand*

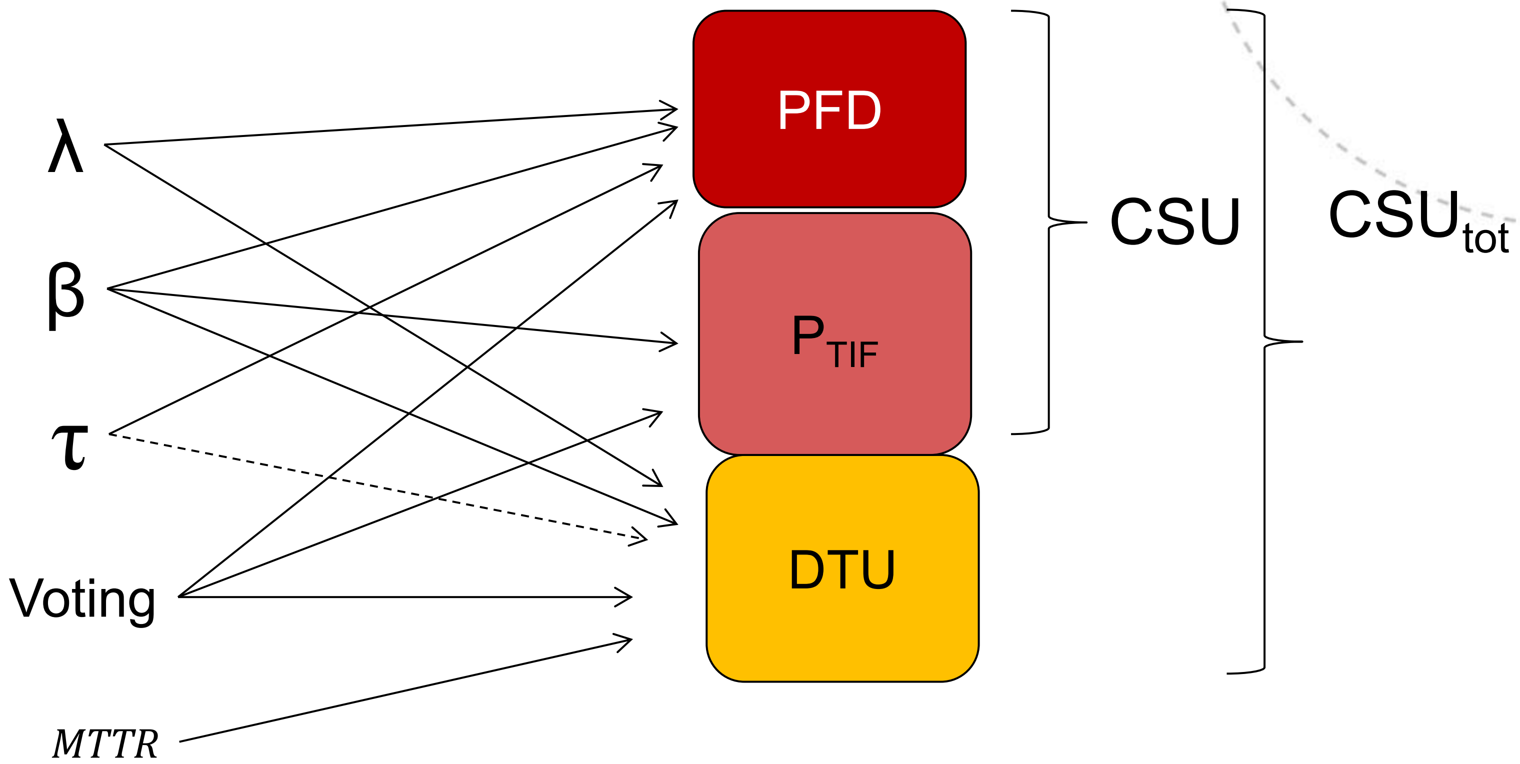
Known *downtime, due to testing and repair of detected and undetected failures*



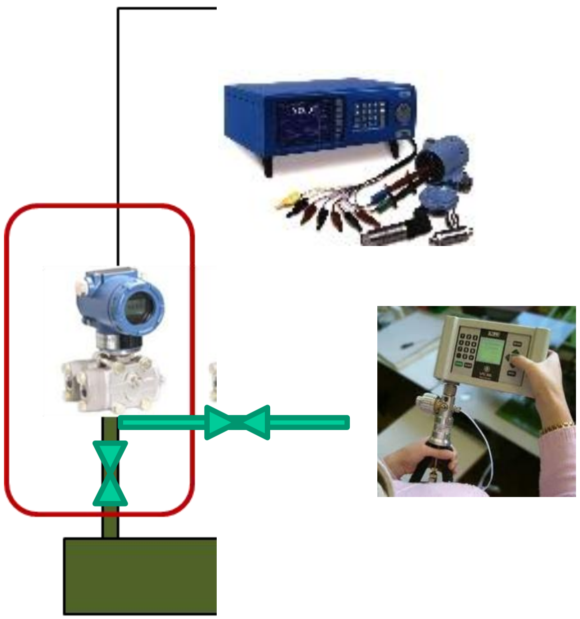
$$CSU = PFD + P_{TIF}$$

$$CSU_{tot} = PFD + P_{TIF} + DTU$$

Quantification of safety unavailability



P_{TIF} – failures not revealed during a test

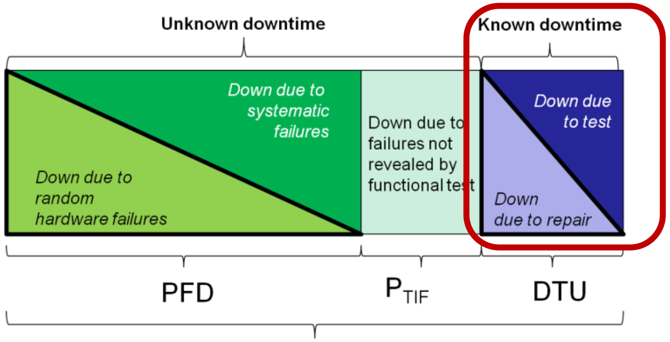


There are many "good" reasons for why a functional test is different from a real demand situation.

P_{TIF}: *The Probability that the component/system will fail to carry out its intended function due to a (latent) failure not detectable by functional testing (therefore the name "test independent failure")*

Often a systematic type of failure.

Downtime unavailability (DTU)

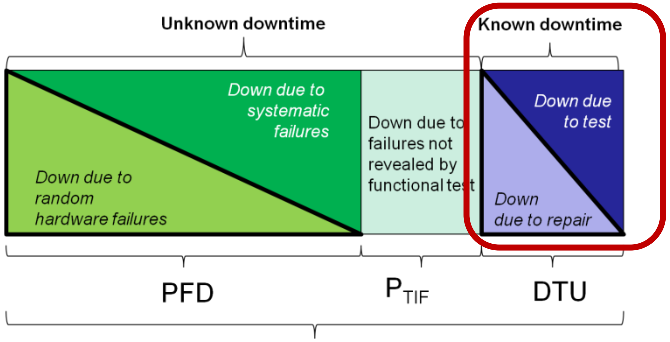


$$DTU = DTU_R + DTU_T$$

DTU_R: ***(Unplanned) Downtime*** *unavailability due to* ***repair of dangerous failures of rate λ_D****, resulting in a period when it is known that the function is unavailable (i.e. category 3a above). The average duration of this period is the mean restoration time (MTTR); i.e. the time from the failure is detected until the safety function is restored;*

DTU_T: *Planned downtime (or inhibition time) resulting from activities such as testing and planned maintenance (i.e. category 3b above).*

Downtime unavailability (DTU)



$$DTU = DTU_R + DTU_T$$

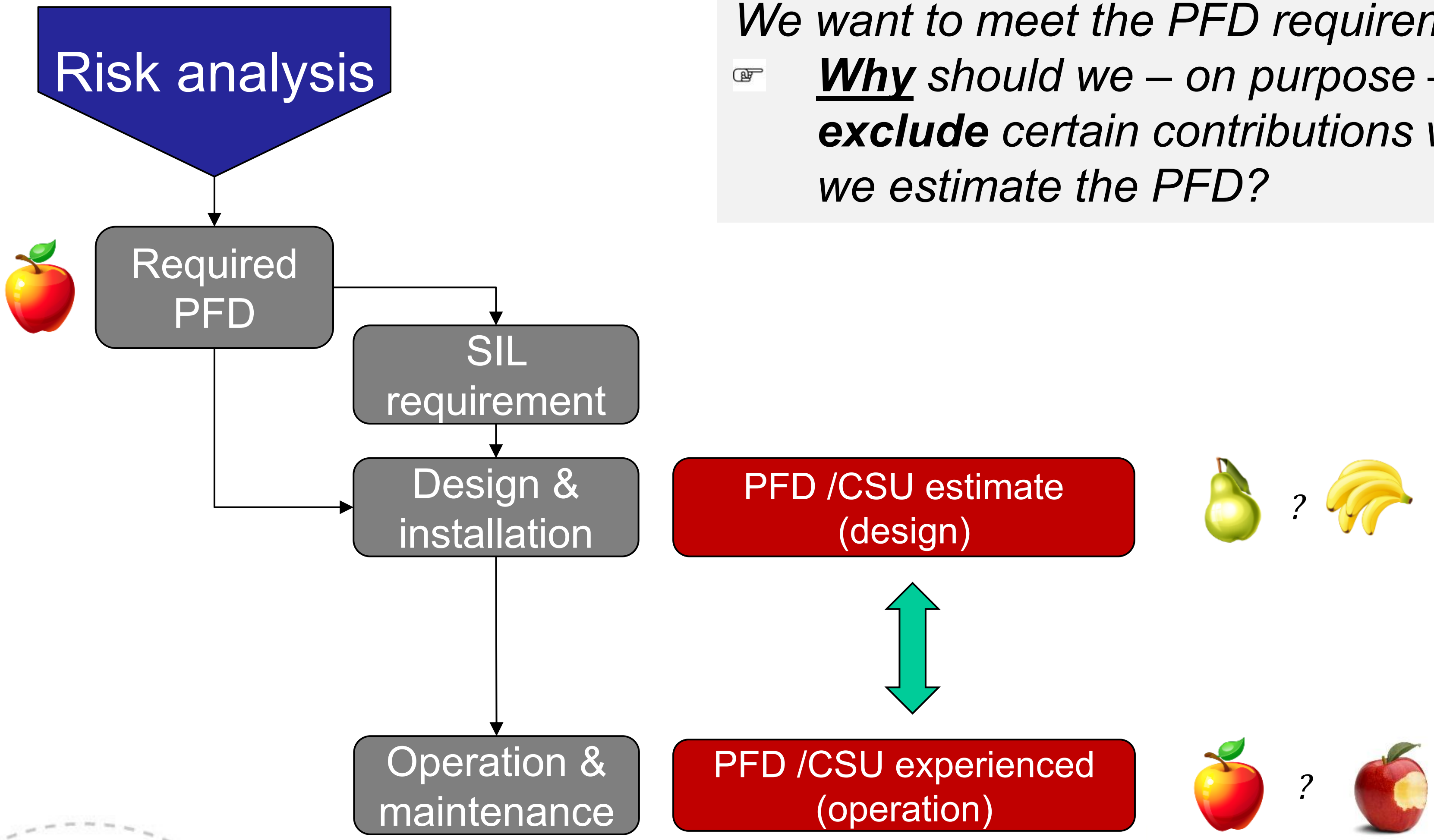
DTU_R: ***(Unplanned) Downtime*** *unavailability due to* ***repair of dangerous failures of rate λ_D****, resulting in a period when it is known that the function is unavailable (i.e. category 3a above). The average duration of this period is the mean restoration time (MTTR); i.e. the time from the failure is detected until the safety function is restored;*

DTU_T: *Planned downtime (or inhibition time) resulting from activities such as testing and planned maintenance (i.e. category 3b above).*

CSU/PFD as decision support

We want to meet the PFD requirement.

☞ ***Why** should we – on purpose – **exclude** certain contributions when we estimate the PFD?*



FORMULAS

Formulas for PFD (wrt DU failures)

Table 3 Summary of simplified formulas for PFD

Voting	PFD calculation formulas		
	Common cause contribution		Contribution from independent failures
1oo1	-		$\lambda_{DU} \cdot \tau / 2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$[\lambda_{DU} \cdot \tau]^2 / 3$
2oo2	-		$2 \cdot \lambda_{DU} \cdot \tau / 2$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$[\lambda_{DU} \cdot \tau]^3 / 4$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$[\lambda_{DU} \cdot \tau]^2$
3oo3	-		$3 \cdot \lambda_{DU} \cdot \tau / 2$
1ooN; N = 2, 3,…	$C_{1ooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$\frac{1}{N+1} \cdot (\lambda_{DU} \cdot \tau)^N$
MooN, M<N; N = 2, 3,..	$C_{MooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$\frac{N!}{(N-M+2)! \cdot (M-1)!} \cdot (\lambda_{DU} \cdot \tau)^{N-M+1}$
NooN; N = 1, 2, 3, …	-		$N \cdot \lambda_{DU} \cdot \tau / 2$

Note: The (1-β-part) has been omitted.

New parameter. Correction factor for other voting than 1oo2. Will be explained later!

Formula for DTU_R

Starting point:

- Dangerous failures come as random events
- When a dangerous failure occur, it needs repair.
- While dangerous detected (DD) failures are repaired "immediately", DU failures are repaired when revealed.
- The critical situation if the SIS is unable to function while the repair is ongoing.

Strategy 1: The plant is always shutdown while repairing a failed component.

Result: No contribution to DTU_R.

Strategy 2: It is possible to operate the plant while the SIS is in a ``degraded mode''.

Result: Contributes to DTU_R

Strategy 3: The plant is always operated while the repair is ongoing, even if the SIS is unable to function.

Result: Contributes to DTU_R

Downtime unavailability for repair (DTU_R)

Contribution to DTU when the SIS has a DU failure at the same time a repair is carried out

Table 6 Formulas for DTU_R for some voting logics and operational philosophies

Initial voting logic	Failure Type	Contribution to DTU_R for different operational/repair philosophies [1]	
		Degraded operation	**Operation with no protection**
1oo1	Single failure	N/A	$\lambda_D \cdot MTTR$
1oo2	Single failure	Degraded operation with 1oo1: $2 \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	N/A
	Both components fail	N/A	$\beta \cdot \lambda_D \cdot MTTR$
2oo3	Single failure	Degraded operation with 2oo2 [2] $3 \cdot \lambda_D \cdot MTTR \cdot 2 \cdot \lambda_{DU} \cdot \tau/2$	N/A
	Two components fail	Degraded operation with 1oo1: $(C_{2oo3} - C_{1oo3}) \cdot \beta \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	N/A
	All three components fail	N/A	$C_{1oo3} \cdot \beta \cdot \lambda_D \cdot MTTR$

[1] Note that the formulas provided here do not distinguish between the MTTR for one or two (three) components

[2] Degradation to a 1oo2 voting gives no contribution to the DTU, since a 1oo2 voting actually gives increased safety as compared to a 2oo3 voting

Downtime unavailability for repair (DTU_R)

- Give attention to note 2)
- Contribution to DTU when a repair is ongoing while there is a DU failure in *either* of the other two components.

Table 6 Formulas for DTU_R for some voting logics and operational philosophies

Initial voting logic	Failure Type	Contribution to DTU_R for different operational/repair philosophies [1]	
		Degraded operation	**Operation with no protection**
1oo1	Single failure	N/A	$\lambda_D \cdot MTTR$
1oo2	Single failure	Degraded operation with 1oo1: $2 \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	N/A
	Both components fail	N/A	$\beta \cdot \lambda_D \cdot MTTR$
2oo3	Single failure	Degraded operation with 2oo2 [2]: $3 \cdot \lambda_D \cdot MTTR \cdot 2 \cdot \lambda_{DU} \cdot \tau/2$	N/A
	Two components fail	Degraded operation with 1oo1: $(C_{2oo3} - C_{1oo3}) \cdot \beta \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	N/A
	All three components fail	N/A	$C_{1oo3} \cdot \beta \cdot \lambda_D \cdot MTTR$

[1] Note that the formulas provided here do not distinguish between the MTTR for one or two (three) components

[2] Degradation to a 1oo2 voting gives no contribution to the DTU, since a 1oo2 voting actually gives increased safety as compared to a 2oo3 voting

Downtime unavailability for repair (DTU_R)

- Contribution to DTU when exactly two DD failures are under repair (due to a CCF) and the third component has a DU failure.

Table 6 Formulas for DTU_R for some voting logics and operational philosophies

Initial voting logic	Failure Type	Contribution to DTU_R for different operational/repair philosophies [1)]	
		Degraded operation	Operation with no protection
1oo1	Single failure	N/A	$\lambda_D \cdot MTTR$
1oo2	Single failure	Degraded operation with 1oo1: $2 \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	N/A
	Both components fail	N/A	$\beta \cdot \lambda_D \cdot MTTR$
2oo3	Single failure	Degraded operation with 2oo2 [2)] $3 \cdot \lambda_D \cdot MTTR \cdot 2 \cdot \lambda_{DU} \cdot \tau/2$	N/A
	Two components fail	Degraded operation with 1oo1: $(C_{2oo3} - C_{1oo3}) \cdot \beta \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	N/A
	All three components fail	N/A	$C_{1oo3} \cdot \beta \cdot \lambda_D \cdot MTTR$

1) Note that the formulas provided here do not distinguish between the MTTR for one or two (three) components
2) Degradation to a 1oo2 voting gives no contribution to the DTU, since a 1oo2 voting actually gives increased safety as compared to a 2oo3 voting

C_{2oo3}: Correction factor when CCF involve the failure of two or three components (since two and three failures lead to system failure)
C_{1oo3}: Correction factor when CCF involve the failure of three components (since three failures lead to system failure)

C_{2oo3}- C_{1oo3}: The CCF involve exactly two failures

Downtime unavailability for repair (DTU_R)

- Contribution to DTU when *all* components have failed due to a DD failure.

Table 6 Formulas for DTU_R for some voting logics and operational philosophies

Initial voting logic	**Failure Type**	**Contribution to DTU_R for different operational/repair philosophies** [1]	
		Degraded operation	**Operation with no protection**
1oo1	Single failure	N/A	$\lambda_D \cdot MTTR$
1oo2	Single failure	Degraded operation with 1oo1: $2 \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	N/A
	Both components fail	N/A	$\beta \cdot \lambda_D \cdot MTTR$
2oo3	Single failure	Degraded operation with 2oo2 [2]: $3 \cdot \lambda_D \cdot MTTR \cdot 2 \cdot \lambda_{DU} \cdot \tau/2$	N/A
	Two components fail	Degraded operation with 1oo1: $(C_{2oo3} - C_{1oo3}) \cdot \beta \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	N/A
	All three components fail	N/A	$C_{1oo3} \cdot \beta \cdot \lambda_D \cdot MTTR$

[1] Note that the formulas provided here do not distinguish between the MTTR for one or two (three) components
[2] Degradation to a 1oo2 voting gives no contribution to the DTU, since a 1oo2 voting actually gives increased safety as compared to a 2oo3 voting

C_{1oo3}: The CCF involve the failure of three components (since three failures lead to system failure)

Downtime unavailability for test (DTU_T)

Starting point:

- The downtime due to test is deterministic! (Testing is not random events)
- In a test interval, the downtime is $\frac{t}{\tau}$
- The critical situation occurs if a test is performed with plant operating and the SIS becomes unable to function.

Strategy 1: The plant is always stopped while testing.

Result: **No** contribution to DTU_T.

Strategy 2: It is possible to operate the plant while a component is being tested (if the system can still operate in degraded mode).

Result: Contributes to DTU_T

Strategy 3: The plant is always operated during a test, even if the SIS is unable to function.

Result: Contributes to DTU_T

Downtime unavailability for test (DTU_T)

- Contribution to DTU only when all components are out for testing.

Table 7 Formulas for DTU_T for some voting logics and operational philosophies

Initial voting logic	Number of components tested simultaneously	Contribution to DTU_T for different operational/testing philosophies: Degraded operation	Contribution to DTU_T for different operational/testing philosophies: Operation with no protection [1)]
1oo1	One at a time	N/A	t/τ
1oo2	One at a time	$t \cdot \lambda_{DU}$	N/A
	Both tested simultaneously	N/A	t/τ
2oo3	One at a time	Degradation to 2oo2 [2)] $t \cdot 2 \cdot \lambda_{DU}$	N/A
	All three tested simultaneously	N/A	t/τ

[1)] Note that the formulas provided here do not distinguish between the testing time t for one component and simultaneous testing of two (or three) components. The total testing time without protection should therefore be used
[2)] Degradation to a 1oo2 voting gives no contribution to the DTU, since a 1oo2 voting actually gives increased safety as compared to a 2oo3 voting

Downtime unavailability for test (DTU_T)

Contribution to DTU when either one of the components has a DU failure at the same time as the other component is tested.

- DTU_{T1}: When the failure (of the still untested component) occurs while testing
- DTU_{T2}: When a failure of the already tested component occurs while testing the other

Table 7 Formulas for DTU_T for some voting logics and operational philosophies

Initial voting logic	Number of components tested simultaneously	Contribution to DTU_T for different operational/testing philosophies	
		Degraded operation	Operation with no protection [1]
1oo1	One at a time	N/A	t/τ
1oo2	One at a time	$t \cdot \lambda_{DU}$	N/A
	Both tested simultaneously	N/A	t/τ
2oo3	One at a time	Degradation to 2oo2 [2] $t \cdot 2 \cdot \lambda_{DU}$	N/A
	All three tested simultaneously	N/A	t/τ

[1] Note that the formulas provided here do not distinguish between the testing time t for one component and simultaneous testing of two (or three) components. The total testing time without protection should therefore be used

[2] Degradation to a 1oo2 voting gives no contribution to the DTU, since a 1oo2 voting actually gives increased safety as compared to a 2oo3 voting

$$DTU_{T1} = \frac{t}{\tau}(1 - e^{\lambda_{DU} \cdot (\tau + t)}) \approx \frac{t}{\tau} \lambda_{DU} \cdot (\tau + t) \approx \frac{t}{\tau} \lambda_{DU} \cdot \tau = \lambda_{DU} \cdot t$$

$$DTU_{T2} = \frac{t}{\tau}(1 - e^{-\frac{t}{2}\lambda_{DU}}) \approx 0 \quad \textit{(t/2 is very small also)}$$

t= test time

Downtime unavailability for test (DTU_T)

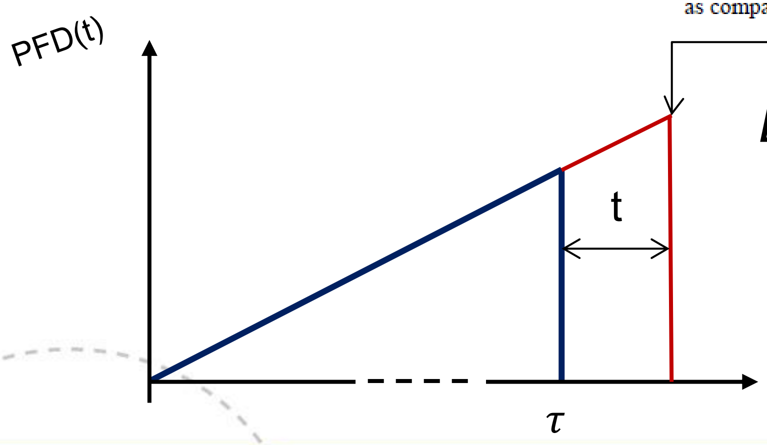
First give attention to note 2)

Contribution to DTU a component is being tested at the same time as the other (still untested) components have a DU failure.

Table 7 Formulas for DTU_T for some voting logics and operational philosophies

Initial voting logic	Number of components tested simultaneously	Contribution to DTU_T for different operational/testing philosophies	
		Degraded operation	Operation with no protection [1]
1oo1	One at a time	N/A	t/τ
1oo2	One at a time	$t \cdot \lambda_{DU}$	N/A
	Both tested simultaneously	N/A	t/τ
2oo3	One at a time	Degradation to 2oo2 [2] $t \cdot 2 \cdot \lambda_{DU}$	N/A
	All three tested simultaneously	N/A	t/τ

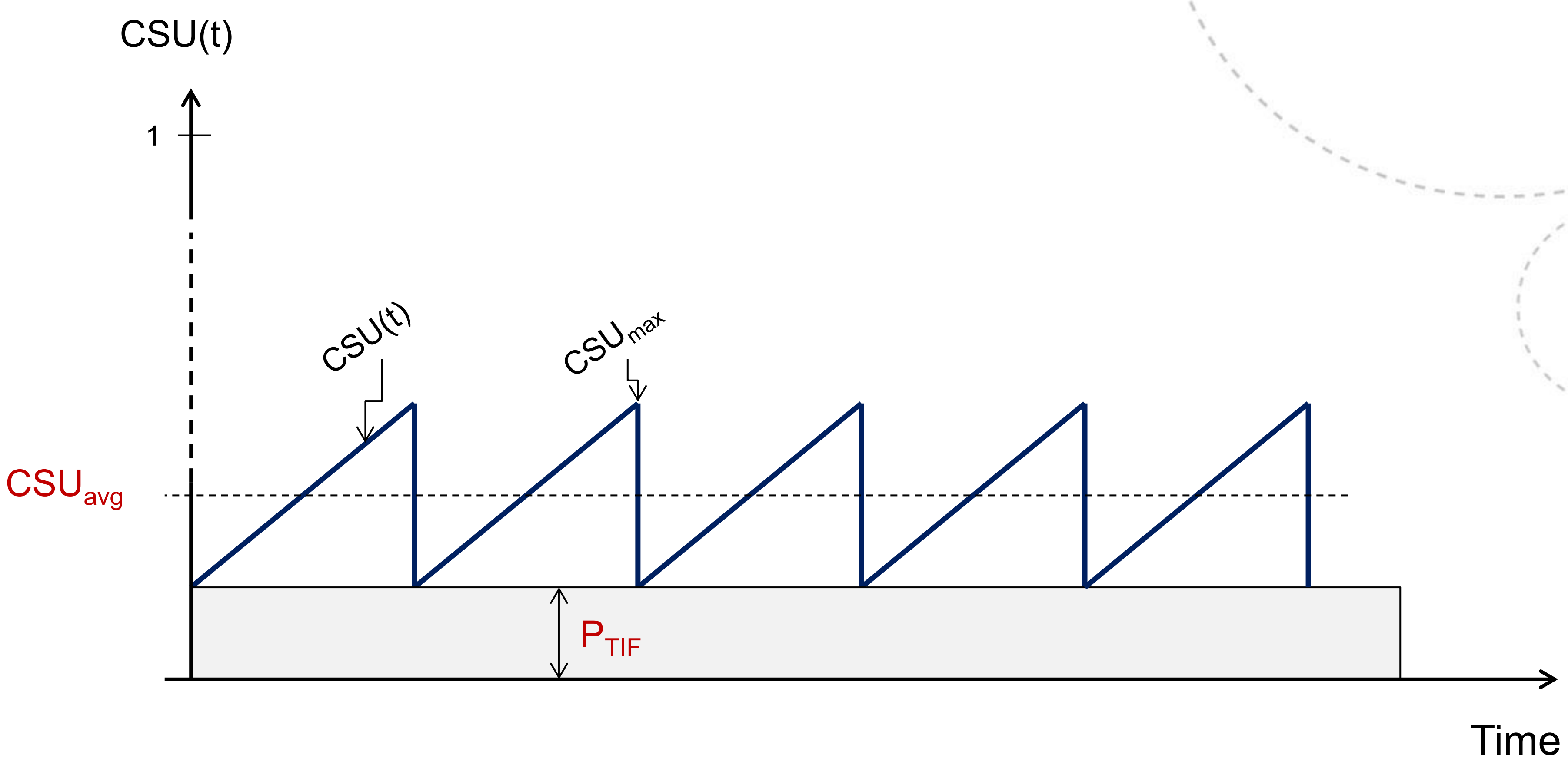
[1] Note that the formulas provided here do not distinguish between the testing time t for one component and simultaneous testing of two (or three) components. The total testing time without protection should therefore be used
[2] Degradation to a 1oo2 voting gives no contribution to the DTU, since a 1oo2 voting actually gives increased safety as compared to a 2oo3 voting



$$DTU_T = \frac{t}{\tau} \boxed{\cdot 2\lambda_{DU}(\tau + t)} \approx \frac{t}{\tau} \cdot 2\lambda_{DU}\tau = 2\lambda_{DU} t$$

(Simplified compared to previous slide)

P_TIF: Alternative 1. Fixed value



Test independent failures (P_{TIF})

Definition - interpretation:

- Probability that a component just being functionally tested, fails to perform on demand (irrespective of the interval of functional testing).
- Probability that the component/system will fail to carry out its intended function due to a (latent) failure not detectable by functional testing.
- Pragmatic, rather than theoretically funded measure
- The parameter P_{TIF} for a single component is usually set equal to $5 \cdot 10^{-4}$.
- The P_{TIF} of a subsystem is:

$$P_{TIF}^{SYS} = f(P_{TIF}, \beta, \text{voting})$$

Table 5 Formulas for P_{TIF}, various voting logics

Voting	TIF contribution to CSU for MooN voting
1oo1	P_{TIF}
1oo2	$\beta \cdot P_{TIF}$
MooN, M<N	$C_{MooN} \cdot \beta \cdot P_{TIF}$
NooN, (N= 1, 2, …)	$N \cdot P_{TIF}$

P_TIF: Alternative 2. As imperfect test

When incorporating the PTC the rate of dangerous undetected failures can be regarded as having two constituent parts:

1. Failures *detected* during proof testing: with rate $\mathrm{PTC} \cdot \lambda_{\mathrm{DU}}$ and proof test interval τ, and
2. Failures *not detected* during proof testing: with rate $(1 - \mathrm{PTC}) \cdot \lambda_{\mathrm{DU}}$ and "test interval" T.

Here τ is the proof test interval and T is the assumed interval of complete testing. T may for example be the interval of a complete component overhaul when it is the assumed that the residual failure modes will be detected. If some failure modes are never tested for, then T should be taken as the lifetime of the equipment. For a 1oo1 voting the PFD is then given as:

$$\mathrm{PFD}_{1\mathrm{oo}1} = \mathrm{PTC} \cdot \left(\lambda_{\mathrm{DU}} \cdot \frac{\tau}{2}\right) + (1 - \mathrm{PTC}) \cdot \left(\lambda_{\mathrm{DU}} \cdot \frac{T}{2}\right)$$

We see that the above expression becomes identical to the simplified formula given for $\mathrm{PFD}_{1\mathrm{oo}1}$ in section 5.2.1 when the proof test coverage, PTC = 1 (= 100 %), i.e., when the functional test is perfect. This was also illustrated in Figure 5 where the average PFD (or CSU) is the same in all test intervals. However, if PTC < 1, the average PFD for a test interval will increase in subsequent test intervals, as illustrated in Figure 7.

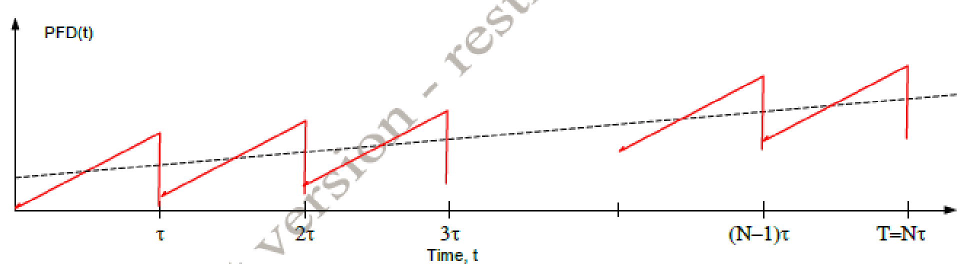


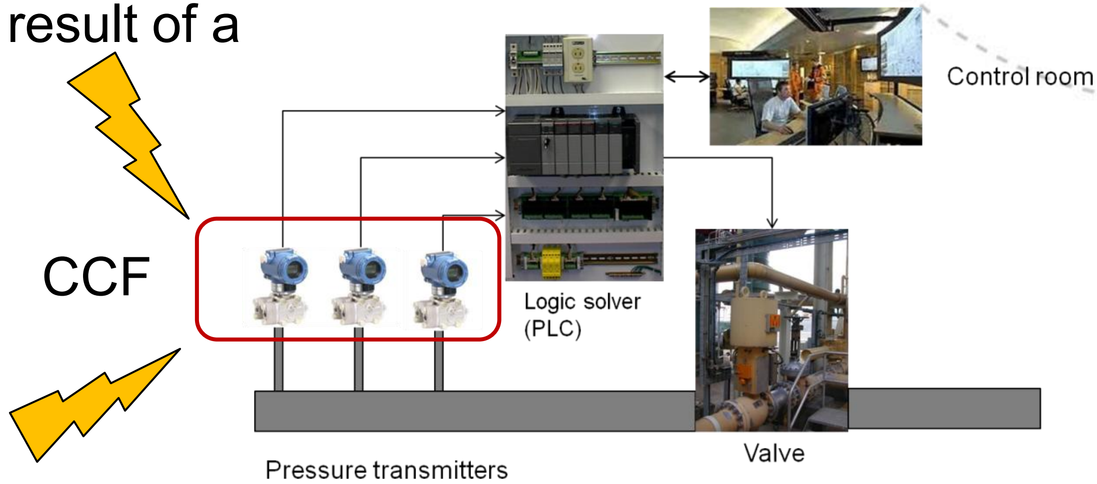
Figure 7: Time dependent PFD with PTC < 100 %

Remark:
Note that PFD_{1oo1} gives average value for a given combination of τ and T, and not the curves indicated in figure 7!

C_{MOON}-FACTOR

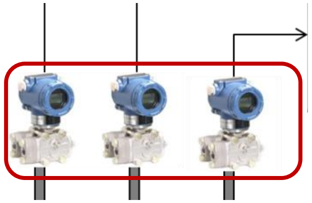
Inclusion of CCFs

IEC 61508: **All** redundant components as the result of a CCF



PDS method: From **two to *n*** components may fail as the result of a CCF. What failure combinations that contribute to the safety unavailability depends on how the components are voted

Inclusion of CCFs

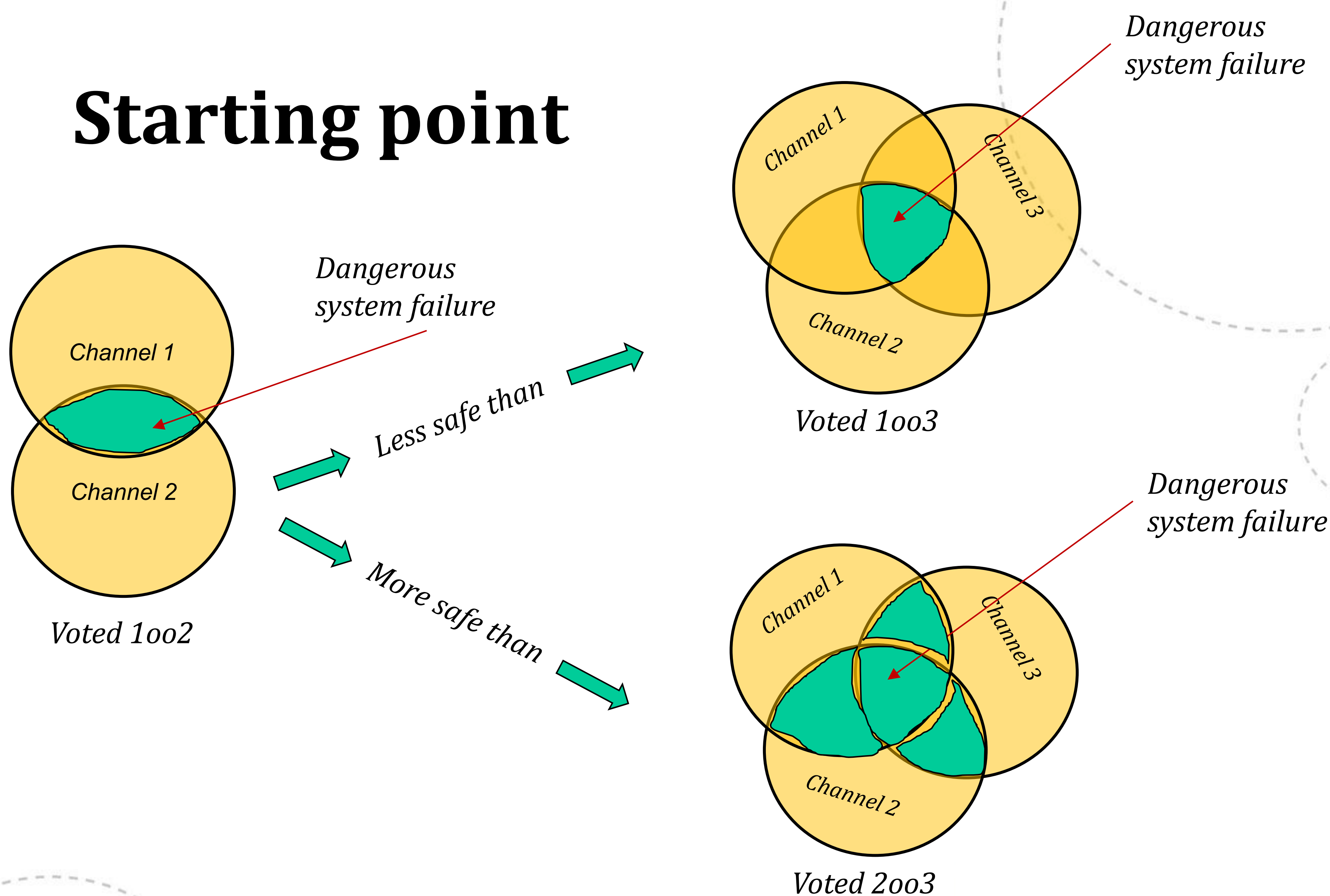


	1oo3	2oo3
IEC 61508	$PFD_{CCF} \approx \frac{\beta \lambda_{DU} \tau}{2}$	$PFD_{CCF} \approx \frac{\beta \lambda_{DU} \tau}{2}$
PDS	$PFD_{CCF} \approx \frac{C_{1oo3} \beta \lambda_{DU} \tau}{2}$	$PFD_{CCF} \approx \frac{C_{2oo3} \beta \lambda_{DU} \tau}{2}$

$C_{1oo3} = 0.5$
$C_{2oo3} = 2.0$

→ According to IEC 61508, there is no benefit (in reducing the PFD) from using 1oo3 compared to 2oo3.

Starting point



Multiplicity of failures

Probability that *j* specific channels fail due to a CCF (in a system of n components):

$$g_{j,n} = \Pr\left(A_1 \cap A_2 \cap \ldots \cap A_j \cap A_{j+1}^* \cap \ldots \cap A_n^*\right)$$

Probability that exactly *j* out of *n* components fail (all combinations, assuming symmetry):

$$f_{j,n} = \binom{n}{j} g_{j,n}.$$

Probability that the system fail due to a CCF is when n-k+1 or more components are involved in CCF:

$$\begin{aligned} Q_{koon} &= \Pr(At\ least\ n-k+1\ channels\ failed\ in\ CCF) \\ &= \sum_{j=n-k+1}^{n} f_{j,n}. \end{aligned} \quad (4)$$

Ref: Hokstad et al (2006)

Inclusion of CCFs - rationale

Probability that *j* specific channels fail due to a CCF (in a system of n components):

$$g_{j,n} = \Pr\left(A_1 \cap A_2 \cap \ldots \cap A_j \cap A^*_{j+1} \cap \ldots \cap A^*_n\right)$$

Probability that exactly *j* out of *n* components fail (all combinations, symmetry):

$$f_{j,n} = \binom{n}{j} g_{j,n}.$$

Probability that the system fail due to a CCF is when n-k+1 or more components are involved in CCF:

$$Q_{koon} = \Pr(At\ least\ n-k+1\ channels\ failed\ in\ CCF)$$

$$= \sum_{j=n-k+1}^{n} f_{j,n}.$$

Will eventually give

$$\boxed{Q_{koon} = C_{koon} \cdot \beta \cdot Q}$$

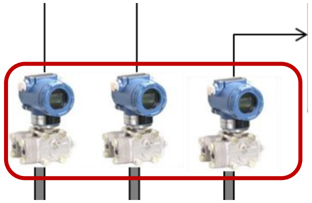
Ref: Hokstad et al (2006)

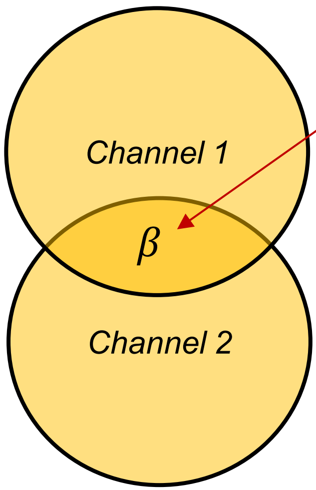
Need for new parameters

- β: Probability that a specific second channel fails, given that a channel has failed.
- β_2: Probability that a third channel fails, given that two specific channels have failed
- β_k: Probability that a (*k+1*)th channel fails, given that *k* specific channels have failed
- Symmetry is assumed, so that all combinations of multiplicities of channel failures have same probability

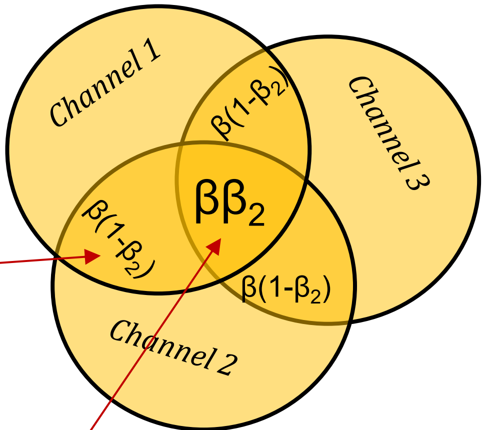
NTNU
Norwegian University of Science and Technology

Two and three channel example



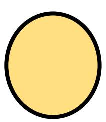


β: Probability two specific channels fail (channel 1 fails, when also channel 2 is failed, and visa verse)



$\beta(1-\beta_2)$: *Probability that two specific channels are involved in a CCF (Channel 1 and 2, but NOT channel 3)*

$\beta\beta_2$: *Probability that three specific channels are failed.*



*Representing **total** probability that a channel fails*

Three channel example: Details

Probability that three ***specific*** channels fail ($g_{3,3}$):

$$\Pr(C1^* \cap C2^* \cap C3^*) = \Pr(C1^* \mid C2^* \cap C3^*) \cdot \Pr(C2^* \cap C3^*)$$

$$= \Pr(C1^* \mid C2^* \cap C3^*) \cdot \Pr(C2^* \mid C3^*) \cdot \Pr(C3^*)$$

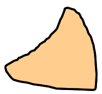
$$= \beta_2 \beta Q$$

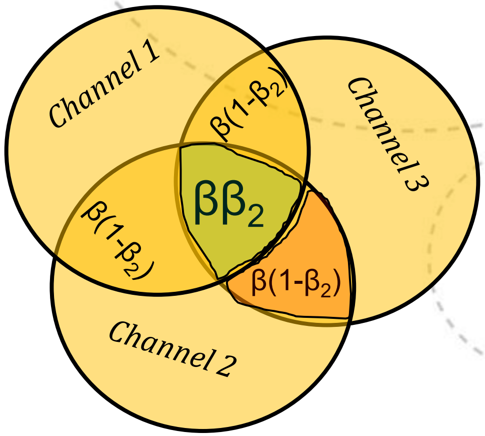
Probability that two ***specific*** components fail ($g_{2,3}$): :

$$\Pr(C1 \cap C2^* \cap C3^*) = \Pr(C1 \mid C2^* \cap C3^*) \cdot \Pr(C2^* \cap C3^*)$$

$$= (1 - \Pr(C1^* \mid C2^* \cap C3^*) \cdot \Pr(C2^* \mid C3^*) \cdot \Pr(C3^*)$$

$$= (1 - \beta_2) \beta Q$$



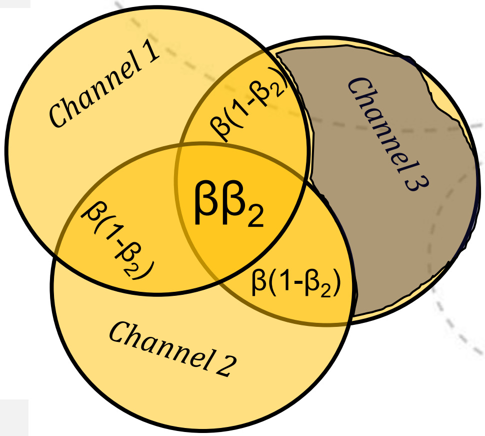


Ref: *Hokstad et al (2006), Hokstad and Rausand (2008)*

Inclusion of CCFs - rationale

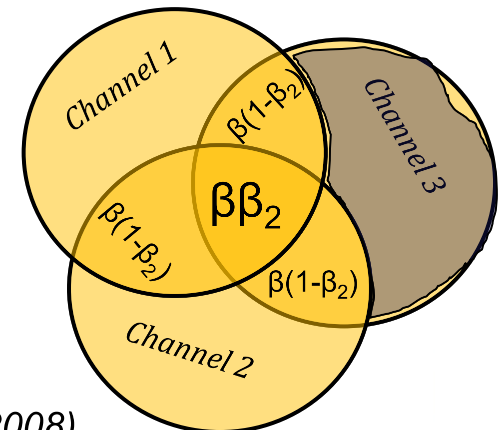
Probability that one ***specific*** component has failed ($g_{1,3}$): :

$$
\begin{aligned}
\Pr(C1 \cap C2 \cap C3^*) &= \Pr(C1 \cap C2 \ \mid C3^*) \cdot \Pr(C3^*) \\
&= \left[1 - \Pr(C1^* \cup C2^* \mid C3^*)\right] \cdot \Pr(C3^*) \\
&= \left[1 - [\Pr(C1^* \mid C3^*) + \Pr(C2^* \mid C3^*) - \Pr(C1^* \cap C2^* \cap C3^*)]\right] \cdot \Pr(C3^*) \\
&= [1 - (\beta(1-\beta_2) + \beta(1-\beta_2) - \beta\beta_2)] \cdot Q \\
&= [1 - (2-\beta)\beta_2] \cdot Q
\end{aligned}
$$



Probability that exactly 1,2, and 3 components fail out of n:

$$f_{1,3} = 3[1-(2-\beta_2)\beta]Q$$
$$f_{2,3} = 3(1-\beta_2)\beta Q$$
$$f_{3,3} = \beta_2\beta Q$$



Ref: Hokstad et al (2006), Hokstad and Rausand (2008)

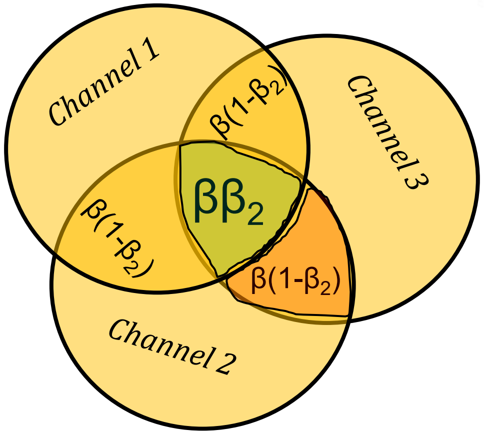
Inclusion of CCFs - rationale

Note that system has a CCF when (n-k+1) or more components fail:

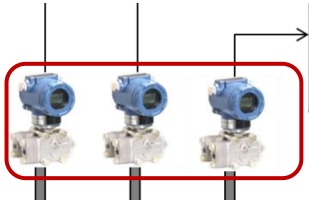
$$Q_{2oo3} = Q_{2oo3} = f_{2,3} + f_{3,3} = (3-2\beta_2)\beta Q = C_{2oo3}\beta Q$$  + 3 · 

$$Q_{1oo3} = f_{3,3} = \beta_2 \beta Q = C_{1oo3}\beta Q$$ 

$$Q_I = 1-(2-\beta_2)\beta Q$$ 3 · 



C_{MOON} - explanation



$$Q_{2oo3} = f_{2,3} + f_{3,3} = (3-2\beta_2)\beta Q = C_{2oo3}\beta Q$$

$$Q_{1oo3} = f_{3,3} = \beta_2 \beta Q = C_{1oo3}\beta Q$$

With $\beta_2 = 0.5$, we get:

$$C_{2oo3} = 2.0$$

$$C_{1oo3} = 0.5$$

Table B.2: Updated C_{MooN} factors for different voting logics

$M \setminus N$	$N = 2$	$N = 3$	$N = 4$	$N = 5$	$N = 6$
$M = 1$	$C_{1oo2} = 1.0$	$C_{1oo3} = 0.5$	$C_{1oo4} = 0.3$	$C_{1oo5} = 0.2$	$C_{1oo6} = 0.15$
$M = 2$	-	$C_{2oo3} = 2.0$	$C_{2oo4} = 1.1$	$C_{2oo5} = 0.8$	$C_{2oo6} = 0.6$
$M = 3$	-	-	$C_{3oo4} = 2.8$	$C_{3oo5} = 1.6$	$C_{3oo6} = 1.2$
$M = 4$	-	-	-	$C_{4oo5} = 3.6$	$C_{4oo6} = 1.9$
$M = 5$	-	-	-	-	$C_{5oo6} = 4.5$

Ref: Hokstad et al (2006), Hokstad and Rausand (2008)

Generalized

Let C_{MooN}* be the C_{MooN} factor calculated using generalized formula for C_{MooN}. Then the new C_{MooN} becomes:

$$C_{MooN} = q + (1-q)C^*_{MooN}$$

The fraction q of the CCF can be described as "lethal shocks" (causing all N components to fail), and the fraction $1-q$ follow the logic of the previous CCF model of PDS.

The old C_{MooN} factor was rather complex. In the most recent version, due to some unfortunate effects of the old formula, the new proposal is:*

$$C^*_{MooN} = \beta_2 \sum_{j=N-M+1}^{N} \binom{N}{j} \theta^{j-3}(1-\theta)^{N-j}; \quad M = 1,2,\dots,N-2$$

This formula relies on some new important assumption: the β_k's (for $k \geq 3$) are constant, i.e., $\beta_k = \theta$; $k \geq 3$. Provided $\theta \geq \beta_2$, it can be proved that we then get acceptable (non-negative) C_{MooN}* values.

*$\theta \geq \beta_2$ means that the probability of having a **forth** failure, if three have already failed **is greater** than having a **third** failure in a n channel system, that the probability of having a fifth failure, if the four have already failed than having a forth failure in case three components have failed in a n channel system etc – which is reasonable.*

Current values of C_{MooN} table assumes q=0.05, β_2 = 0.5 and θ=0.6

Verify?

Table B.2: Updated C_{MooN} factors for different voting logics

$M \setminus N$	$N = 2$	$N = 3$	$N = 4$	$N = 5$	$N = 6$
$M = 1$	$C_{1oo2} = 1.0$	$C_{1oo3} = 0.5$	$C_{1oo4} = 0.3$	$C_{1oo5} = 0.2$	$C_{1oo6} = 0.15$
$M = 2$	-	$C_{2oo3} = 2.0$	$C_{2oo4} = 1.1$	$C_{2oo5} = 0.8$	$C_{2oo6} = 0.6$
$M = 3$	-	-	$C_{3oo4} = 2.8$	$C_{3oo5} = 1.6$	$C_{3oo6} = 1.2$
$M = 4$	-	-	-	$C_{4oo5} = 3.6$	$C_{4oo6} = 1.9$
$M = 5$	-	-	-	-	$C_{5oo6} = 4.5$

$$C^{*}_{MooN} = \beta_2 \sum_{j=N-M+1}^{N} \binom{N}{j} \theta^{j-3} (1-\theta)^{N-j}; \;\; M = 1,2,\dots,N-2$$

Current values of C_{MooN} table assumes q=0.05, β_2 = 0.5 and θ=0.6

Some remarks

Table 3 Summary of simplified formulas for PFD

Voting	PFD calculation formulas: Common cause contribution		PFD calculation formulas: Contribution from independent failures
1oo1	-		$\lambda_{DU} \cdot \tau / 2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$[\lambda_{DU} \cdot \tau]^2 / 3$
2oo2	-		$2 \cdot \lambda_{DU} \cdot \tau / 2$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$[\lambda_{DU} \cdot \tau]^3 / 4$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$[\lambda_{DU} \cdot \tau]^2$
3oo3	-		$3 \cdot \lambda_{DU} \cdot \tau / 2$
1ooN; N = 2, 3,…	$C_{1ooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$\frac{1}{N+1} \cdot (\lambda_{DU} \cdot \tau)^N$
MooN, M<N; N = 2, 3,..	$C_{MooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$\frac{N!}{(N-M+2)! \cdot (M-1)!} \cdot (\lambda_{DU} \cdot \tau)^{N-M+1}$
NooN; N = 1, 2, 3, …	-		$N \cdot \lambda_{DU} \cdot \tau / 2$

Note that the independent failure rate is not corrected for CCFs

If independent failures were detailed

Voting	Formula for PFD
1oo1	$\lambda_{DU} \cdot \tau /2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau /2$ $+ [(1-\beta)\cdot\lambda_{DU}\cdot\tau]^2/3$
2oo2	$(2-\beta) \cdot \lambda_{DU} \cdot \tau /2$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$ $+ [\boxed{(1-1.5\cdot\beta)}\cdot\lambda_{DU}\cdot\tau]^3/4$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$ $+ [(1-1.5\cdot\beta)\cdot\lambda_{DU} \cdot \tau]^2$
3oo3	$(3-2.5\cdot\beta) \cdot \lambda_{DU} \cdot \tau /2$

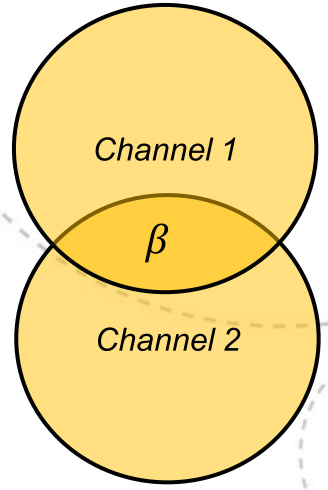
$Q_I = (1-(2-\beta_2)\beta Q$

With $\beta_2 = 0.5$, we get:

$Q_I = (1-1.5\beta)Q$

Formulas for CCFs

Voting	Formula for PFD
1oo1	$\lambda_{DU} \cdot \tau /2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau /2$ $+ [(1-\beta) \cdot \lambda_{DU} \cdot \tau]^2/3$
2oo2	$\boxed{(2-\beta)} \cdot \lambda_{DU} \cdot \tau /2$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$ $+ [(1-1.5 \cdot \beta) \cdot \lambda_{DU} \cdot \tau]^3/4$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$ $+ [(1-1.5 \cdot \beta) \cdot \lambda_{DU} \cdot \tau]^2$
3oo3	$(3-2.5 \cdot \beta) \cdot \lambda_{DU} \cdot \tau /2$

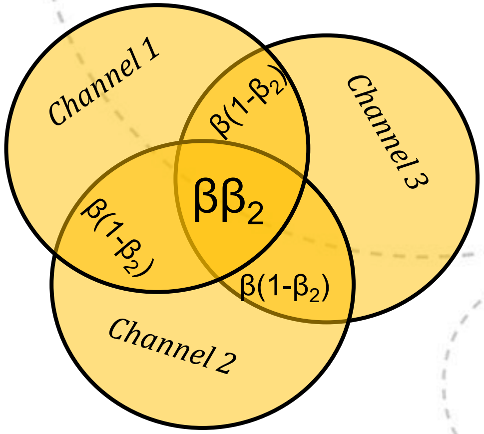


Total failure rate:
$[2(1-\beta)+\beta]\,\lambda$
$=[2-\beta]\,\lambda$

Remark: Somewhat odd to extract CCFs here since NooN. More reasonable to use $2\lambda_{DU}\tau/2$

Formulas for CCFs

Voting	Formula for PFD
1oo1	$\lambda_{DU} \cdot \tau / 2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau / 2 + [(1-\beta) \cdot \lambda_{DU} \cdot \tau]^2 / 3$
2oo2	$(2 - \beta) \cdot \lambda_{DU} \cdot \tau / 2$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2 + [(1-1.5 \cdot \beta) \cdot \lambda_{DU} \cdot \tau]^3 / 4$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2 + [(1-1.5 \cdot \beta) \cdot \lambda_{DU} \cdot \tau]^2$
3oo3	$\boxed{(3 - 2.5 \cdot \beta)} \cdot \lambda_{DU} \cdot \tau / 2$



Total failure rate:

$$3([1-(2-\beta_2)\beta] + 3(1-\beta_2)\beta + \beta_2\beta)\lambda$$
$$= [3-(3-\beta_2)\beta]\ \lambda$$
$$= (3\text{-}2.5\beta)\ \lambda$$

(Still odd to extract CCFs here for NooN)

Formulas for CCFs - important to note!

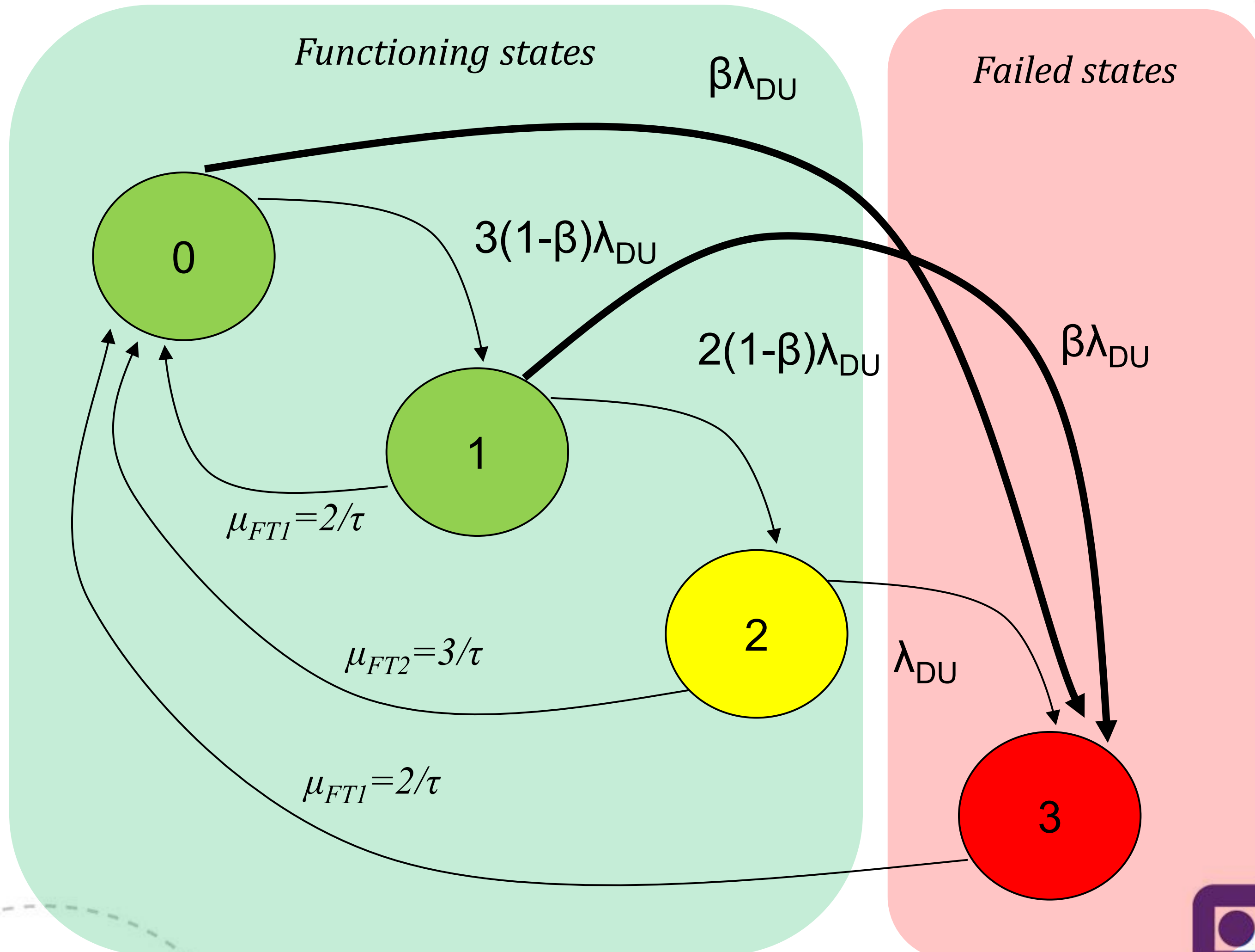
Note that β in the PDS method is only related to the ***probability of having a second failure of a structure of redundant components, given that a failure has occurred***.

In the standard beta-factor model, β is the ***probability that <u>all</u> redundant components fail, given that a failure has occurred***.

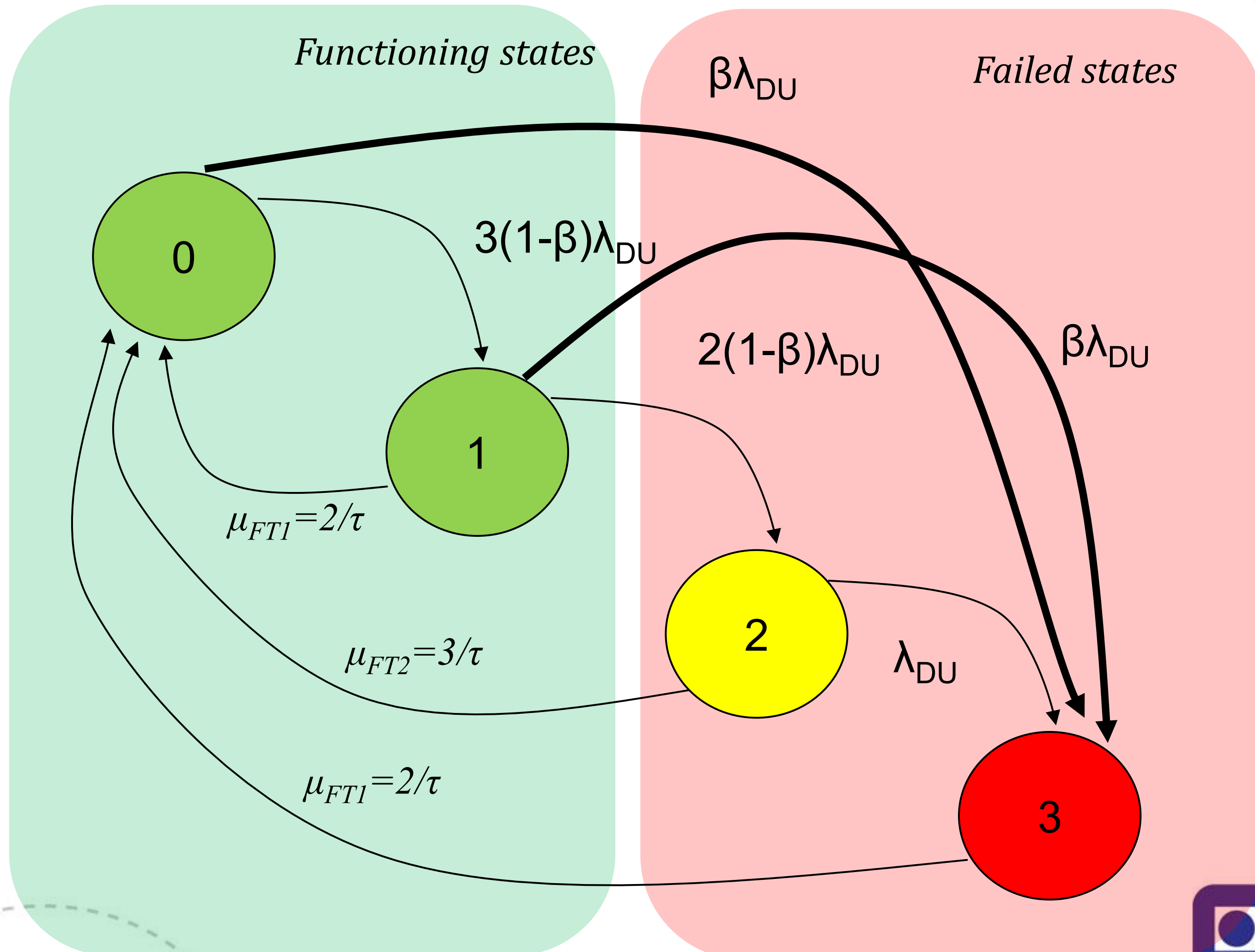
β is not only β

PDS METHOD WITH MARKOV

Standard beta factor model: 1oo3 system

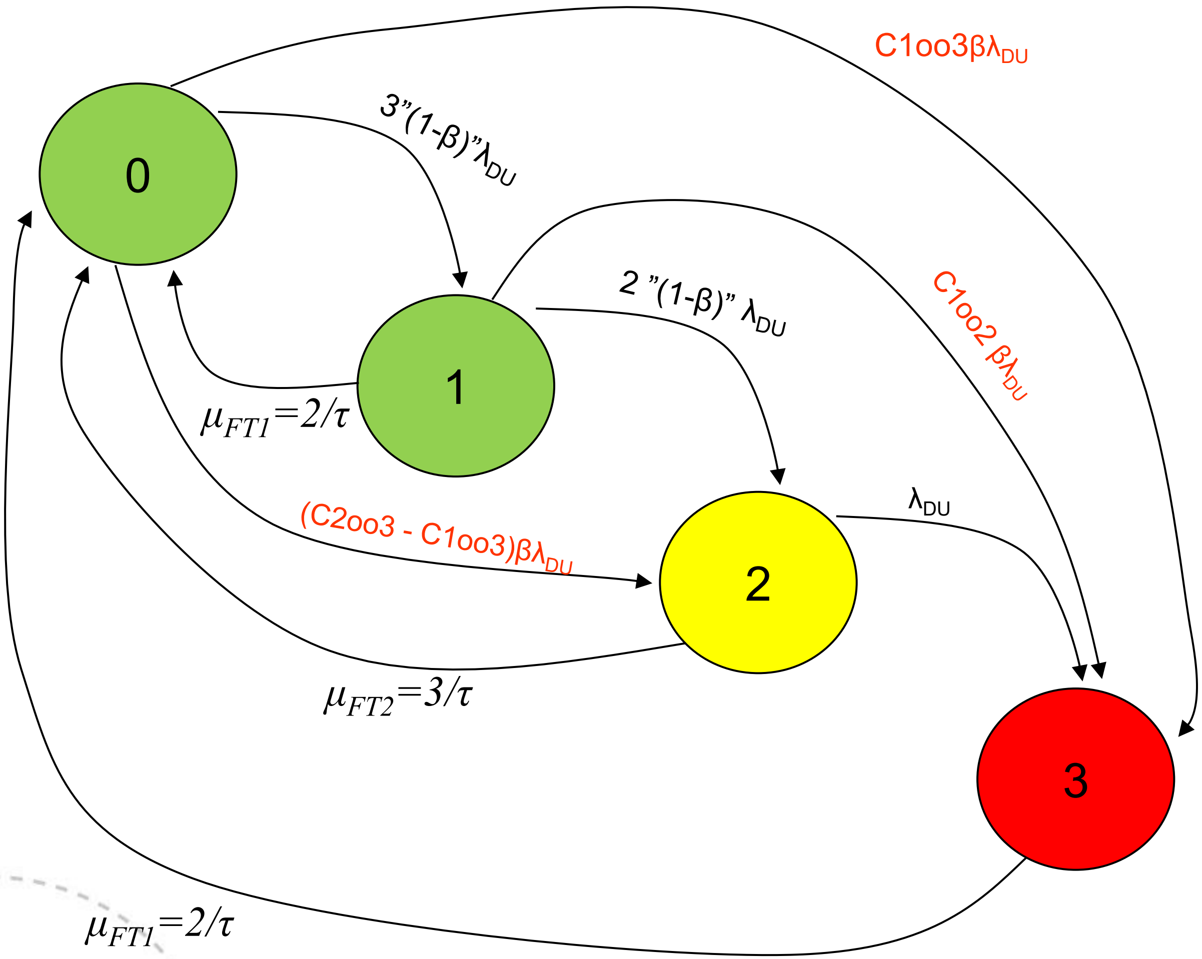


Standard beta factor model: 2oo3 system



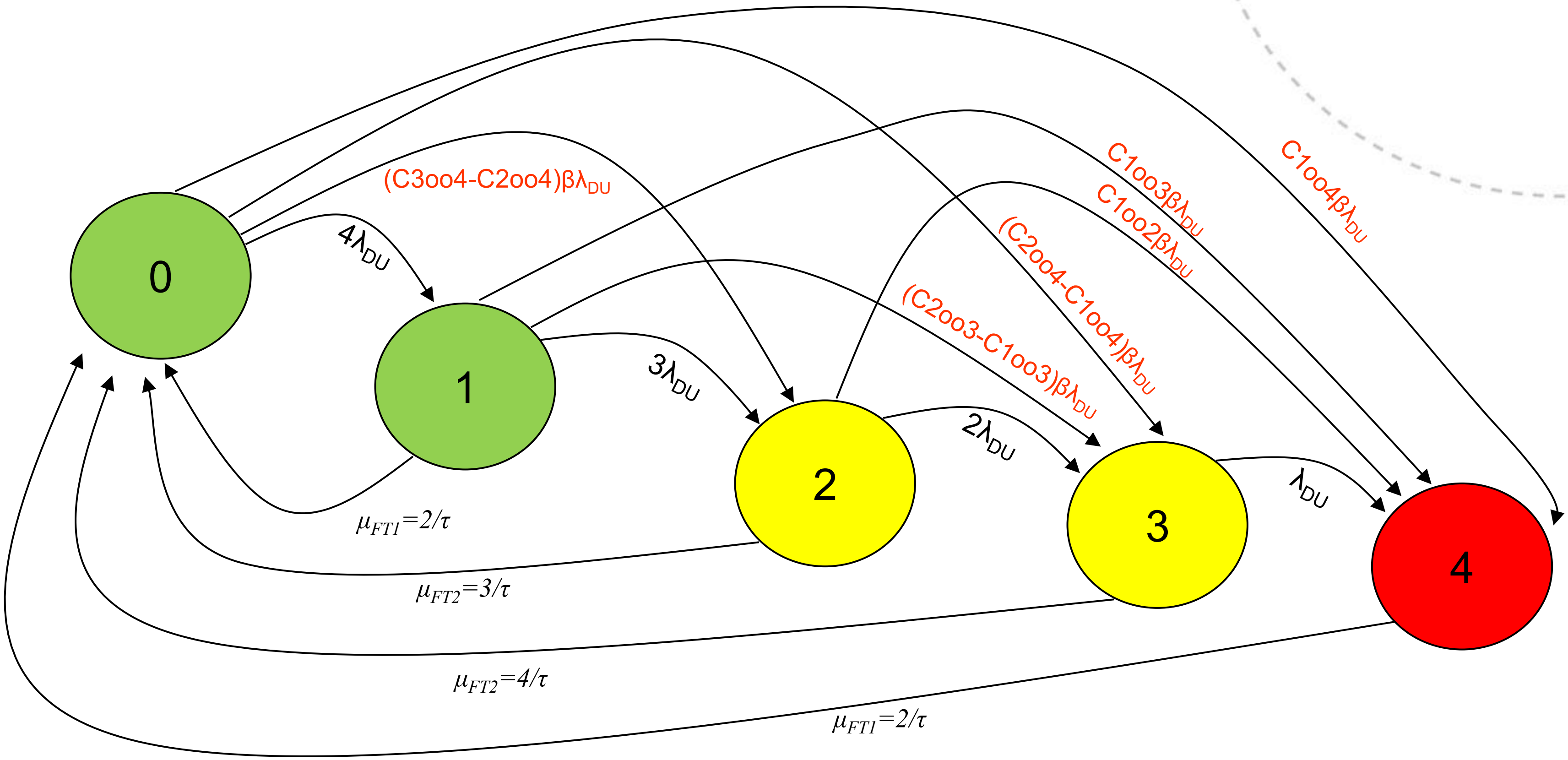
NTNU
Norwegian University of
Science and Technology

PDS method: xoo3 system

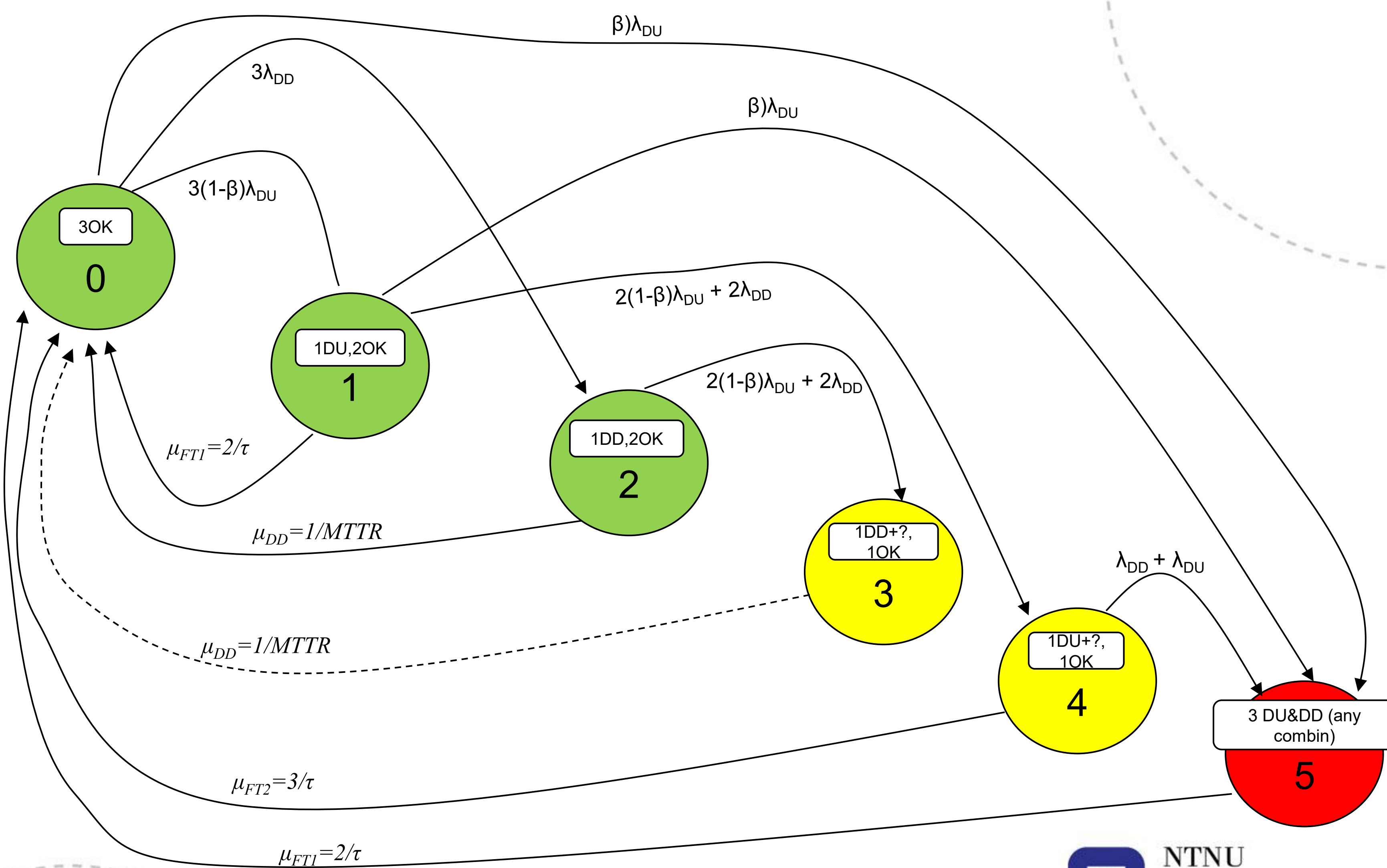


Remark:
PDS method often skips "(1-β)»

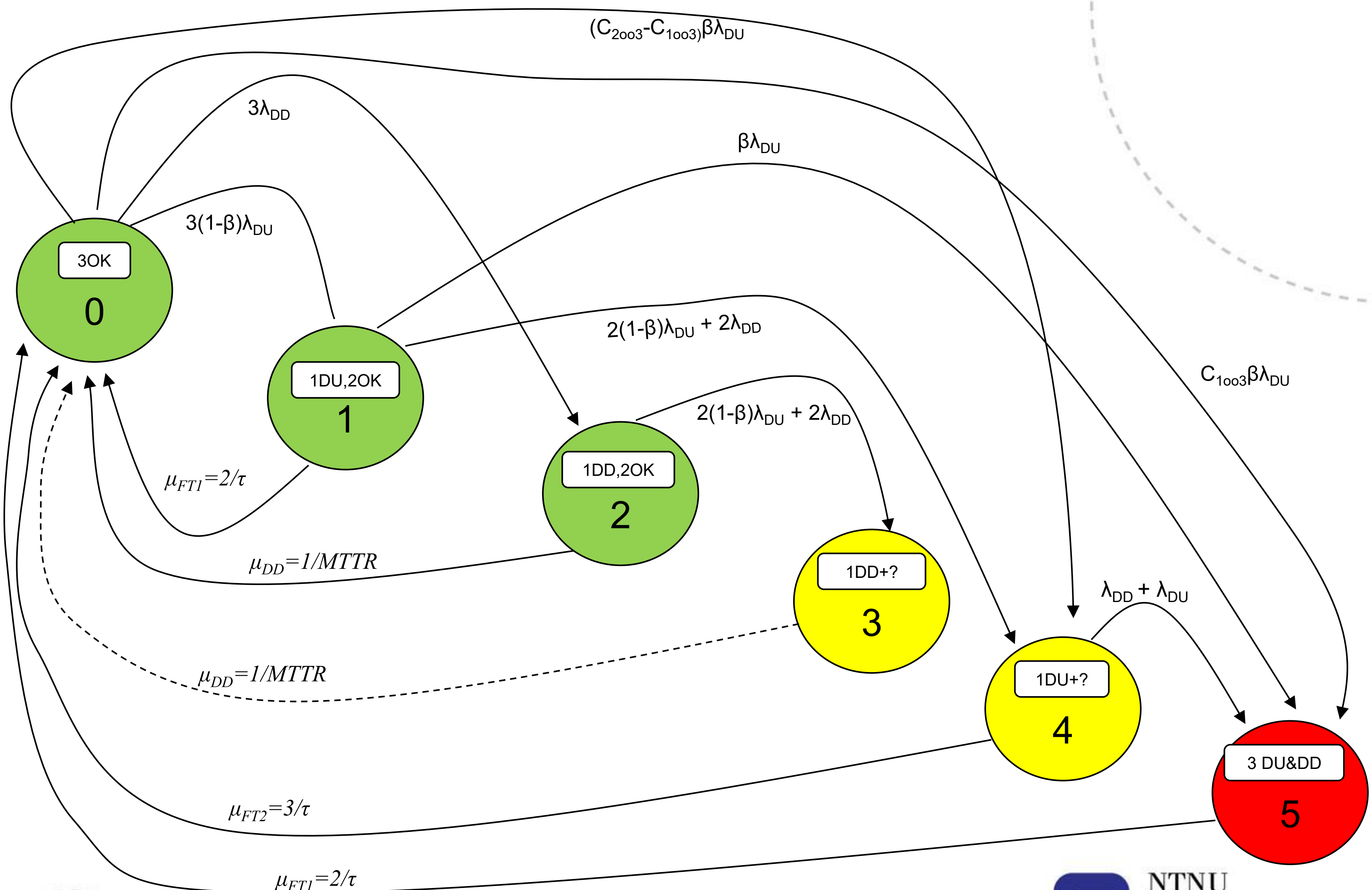
PDS method: xoo4 system



Standard beta factor: xoo3 system DU & DD



PDS method: xoo3 system DU & DD



NTNU
Norwegian University of
Science and Technology

DIAGNOSTIC COVERAGE AND SAFE FAILURE FRACTION

(Diagnostic) coverage (C_D)

In the PDS method, "diagnostic coverage" c_d denotes the diagnostic coverage, while DC is used in IEC 61508.

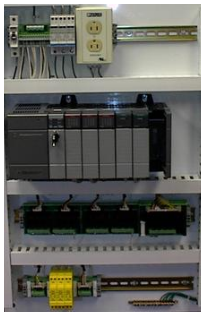
$$c_d = \frac{\lambda_{DD}}{\lambda_D}$$

Fraction of dangerous failures detected by automatic self tests.

OR

Probability that a dangerous failure is detected by self test, given that a failure has occurred.

Safe failure fraction (SFF)



PDS used to have a different definition of SFF than IEC 61508. Non-critical failures were excluded.

$$SFF = \frac{\uparrow \lambda_{DD} + \lambda_S \downarrow}{\lambda_{crit} \downarrow} = 1 - \frac{\lambda_{DU}}{\lambda_{crit}}$$

The new 2010 edition of IEC 61508 is now more in line with the PDS definition, as they now also recommend to exclude no-part /no-effect failures.

SUMMING UP – QUANTIFICATION OF SAFETY UNAVAILABILITY

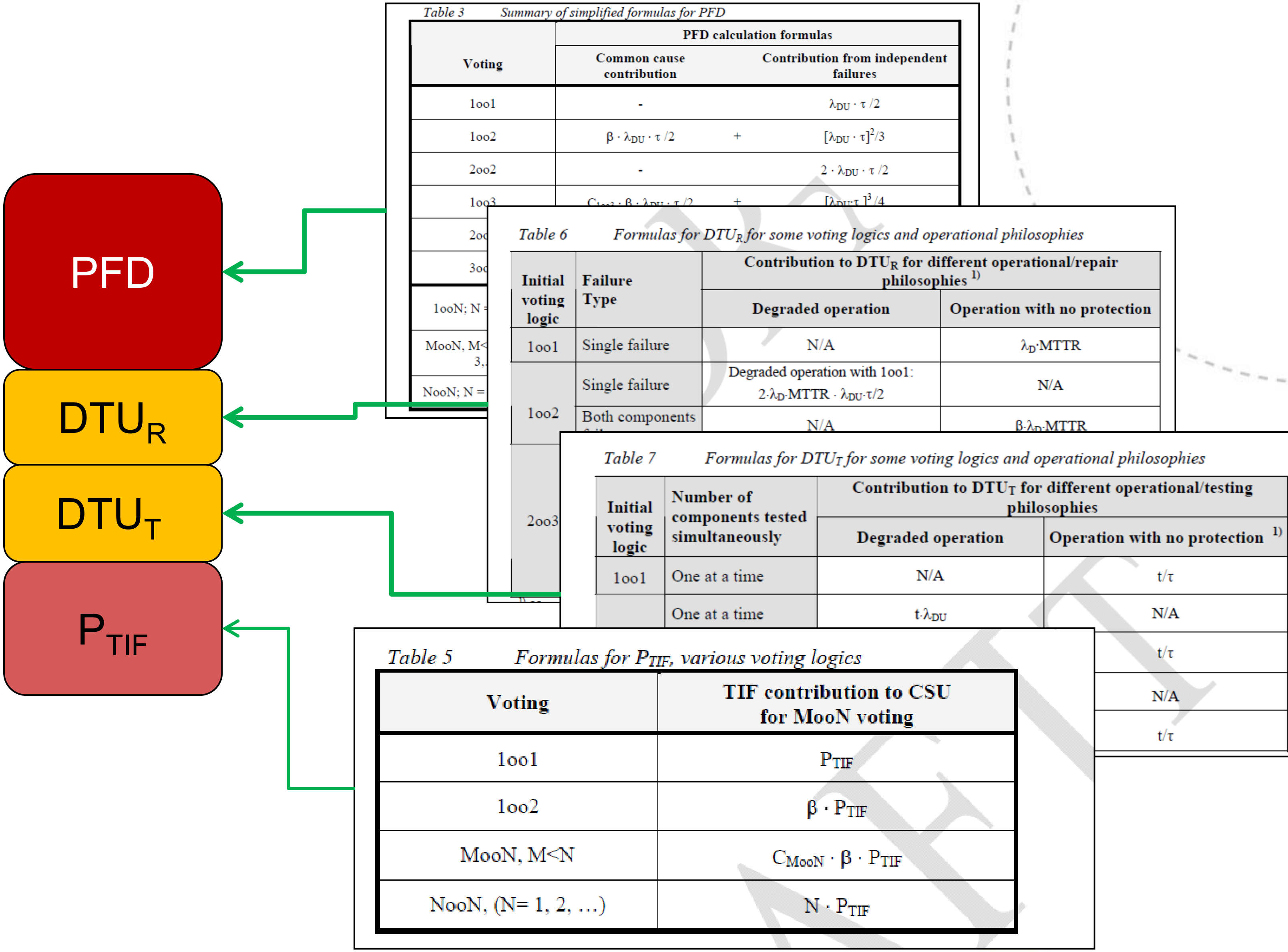


Table 3 Summary of simplified formulas for PFD

Voting	PFD calculation formulas: Common cause contribution		Contribution from independent failures
1oo1	-		$\lambda_{DU} \cdot \tau / 2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$[\lambda_{DU} \cdot \tau]^2 / 3$
2oo2	-		$2 \cdot \lambda_{DU} \cdot \tau / 2$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2$	+	$[\lambda_{DU} \cdot \tau]^3 / 4$
2oo			
3oo			
1ooN; N =			
MooN, M< 3,.			
NooN; N =			

Table 6 Formulas for DTU_R for some voting logics and operational philosophies

Initial voting logic	Failure Type	Contribution to DTU_R for different operational/repair philosophies [1]: Degraded operation	Operation with no protection
1oo1	Single failure	N/A	$\lambda_D \cdot MTTR$
1oo2	Single failure	Degraded operation with 1oo1: $2 \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	N/A
	Both components	N/A	$\beta \cdot \lambda_D \cdot MTTR$
2oo3			

Table 7 Formulas for DTU_T for some voting logics and operational philosophies

Initial voting logic	Number of components tested simultaneously	Contribution to DTU_T for different operational/testing philosophies: Degraded operation	Operation with no protection [1]
1oo1	One at a time	N/A	t/τ
	One at a time	$t \cdot \lambda_{DU}$	N/A
			t/τ
			N/A
			t/τ

Table 5 Formulas for P_{TIF}, various voting logics

Voting	TIF contribution to CSU for MooN voting
1oo1	P_{TIF}
1oo2	$\beta \cdot P_{TIF}$
MooN, M<N	$C_{MooN} \cdot \beta \cdot P_{TIF}$
NooN, (N= 1, 2, …)	$N \cdot P_{TIF}$

NTNU
Norwegian University of Science and Technology

QUANTIFICATION OF SPURIOUS TRIP RATE

NTNU
Norwegian University of Science and Technology

Spurious trip rate

Table 8 Formulas for STR [1)]

Voting	STR
1oo1	λ_{SU}
1oo2	$2 \cdot \lambda_{SU}$
2oo2	$\beta \cdot \lambda_{SU}$
1oo3	$3 \cdot \lambda_{SU}$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{SU}$
3oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{SU}$
1ooN; N = 1, 2, 3, …	$N \cdot \lambda_{SU}$
MooN; $2 \leq M \leq N$; N = 2, 3, ..	$C_{(N-M+1)ooN} \cdot \beta \cdot \lambda_{SU}$

[1)] These formulas account for CCF only, (except for 1ooN configurations). Note that shutdowns can also be initiated as a result of dangerous failures, ref. discussion in section 5.3.4.

A spurious trip occurs if any of the components send a spurious signal

A spurious trip occurs only if (N-M+1)=2 components send a spurious signal

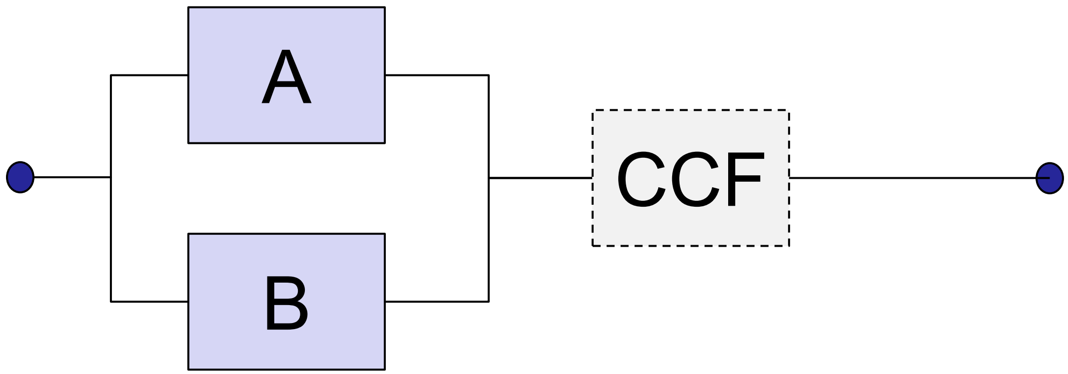
A spurious trip occurs only if <u>all</u> components send a spurious signal

SPESIAL TOPICS: INCLUSION OF CCFS IN «SPECIAL CASES»

Not updated per 13.7.16. Revise according to appendix D in 2013 version.

NTNU
Norwegian University of Science and Technology

Special case 1: CCFs if non-identical components



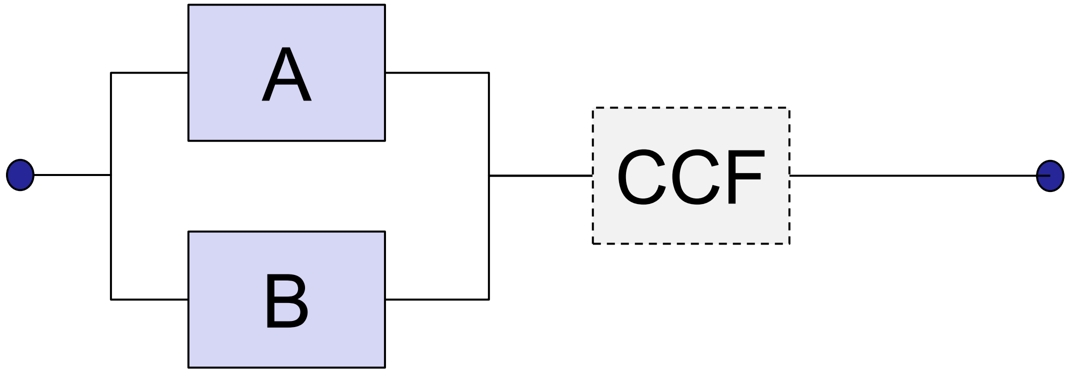
PFD due to independent failures:

$$PFD_{1oo2}^{Ind} = \frac{1}{\tau}\int_0^{\tau}[(1-e^{(1-\beta)\lambda_{DU,A}\cdot t})(1-e^{(1-\beta)\lambda_{DU,A}\cdot t})dt \approx \frac{1}{\tau}\int_0^{\tau}(1-\beta)\lambda_{DU,A}\cdot t\cdot(1-\beta)\lambda_{DU,B}\cdot t]dt$$

$$= \frac{1}{\tau}\frac{(1-\beta)^2\lambda_{DU,A}\cdot\lambda_{DU,B}\cdot\tau^3}{3} = \frac{(1-\beta)^2\lambda_{DU,A}\cdot\lambda_{DU,B}\cdot\tau^2}{3}$$

But what is β, and what failure rate and test interval should we use for the CCFs?:

Special case 1: CCFs if non-identical components



Regarding failure rate: Geometric mean is suggested:

$$\bar{\lambda}_{DU,AB} = \sqrt{\lambda_{DU,A} \cdot \lambda_{DU,B}}$$

Regarding functional test interval: *If* different, use arithmetic mean:

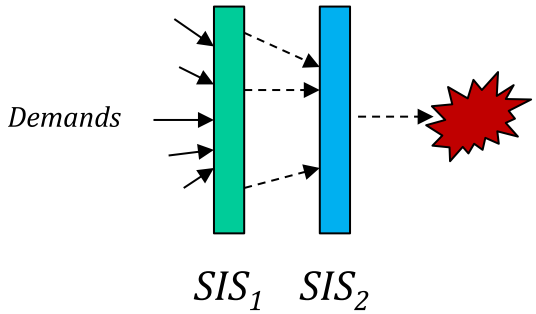
$$\bar{\tau} = \frac{\tau_A + \tau_B}{2}$$

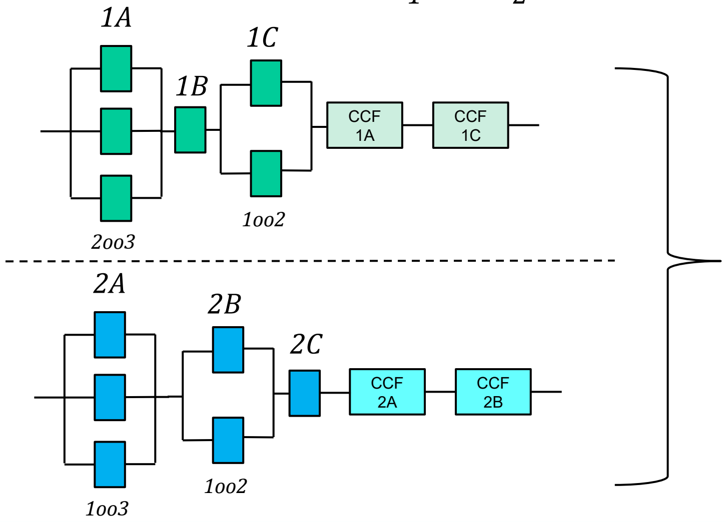
Regarding β, it must be judged from case to case, but:

$$\beta_{AB} \le \min(\beta_A, \beta_B)$$

Special case 2: Multiple SISs

- What do we mean by multiple SISs?





What is the PFD?

NTNU
Norwegian University of Science and Technology

Special case 2: Multiple SISs

- PDS proposes 6 different approaches to how

Table D.1: Possible approaches to determining the appropriate CF for a multiple SIS

	Approach	SIS element structure	Element PFD contribution	Conservative or realistic	Approximate or accurate	Calcu-lation effort	Dominant single elements
1	"Global"	Unknown/ disregarded	Unknown/ disregarded	Realistic	Approximate	Low	Yes
2	"Maximal order"	Known	Unknown/ disregarded	Conservative	Approximate	Low	No
3	"Minimal order"	Known	Unknown/ disregarded	Realistic	Approximate	Low	Yes
4	"Dominant element"	Known	Known	Realistic	Approximate	Low	No
5	"Structural average"	Known	Known	Conservative Realistic	Accurate	Medium	No
6	"Cut set"	Known	Known	Conservative Realistic	Accurate	High	No

Maximal order

Steps:

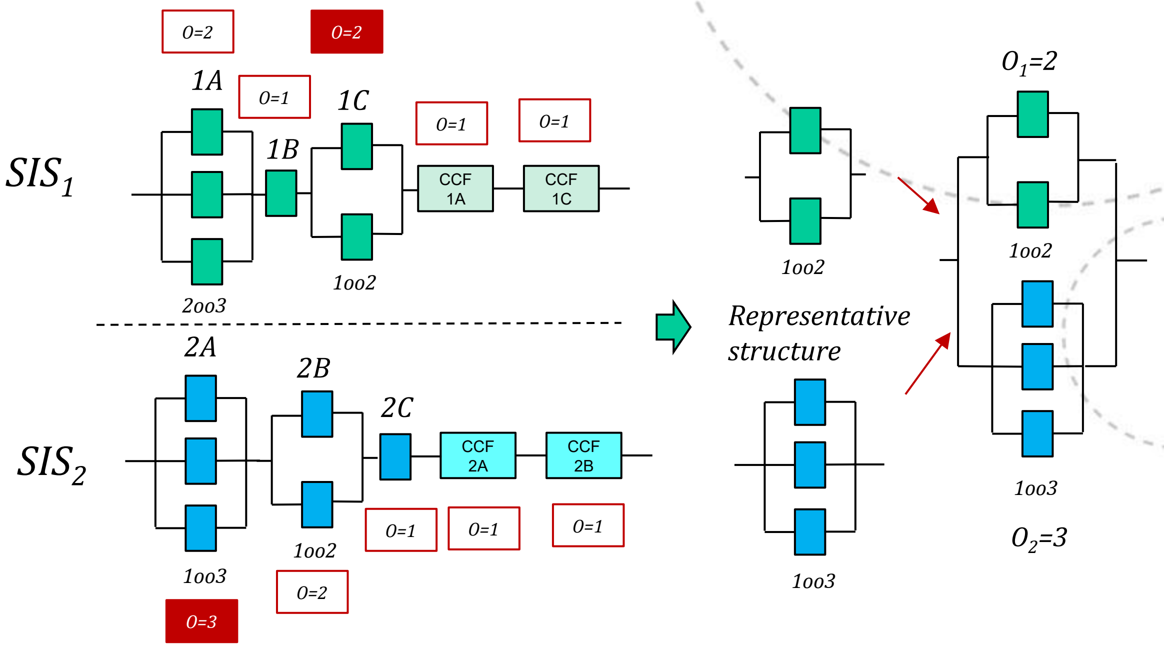
1. *Identify the order "o" of each subsystem (n-m+1)*
2. *Select simplest structure with **highest** order for each SIS: O_k, where k is SIS_k*
3. *Calculate correction factor (CF) by:*

$$CF = \frac{\prod_{k=1}^{N}(O_k + 1)}{1 + \sum_{k=1}^{N} O_k}$$

Note: N is here number of SISs. Somewhat unfortunate notation, but I use same as in the PDS method book.

4. *Multiply the total PFD as:*

$$PFD_{tot} = CF \cdot \prod_{k=1}^{N} PFD_k$$



Example above:

$$CF = \frac{(2+1)\cdot(3+1)}{1+(2)+(3)} = \frac{12}{6} = 2$$

Minimal order

Steps:

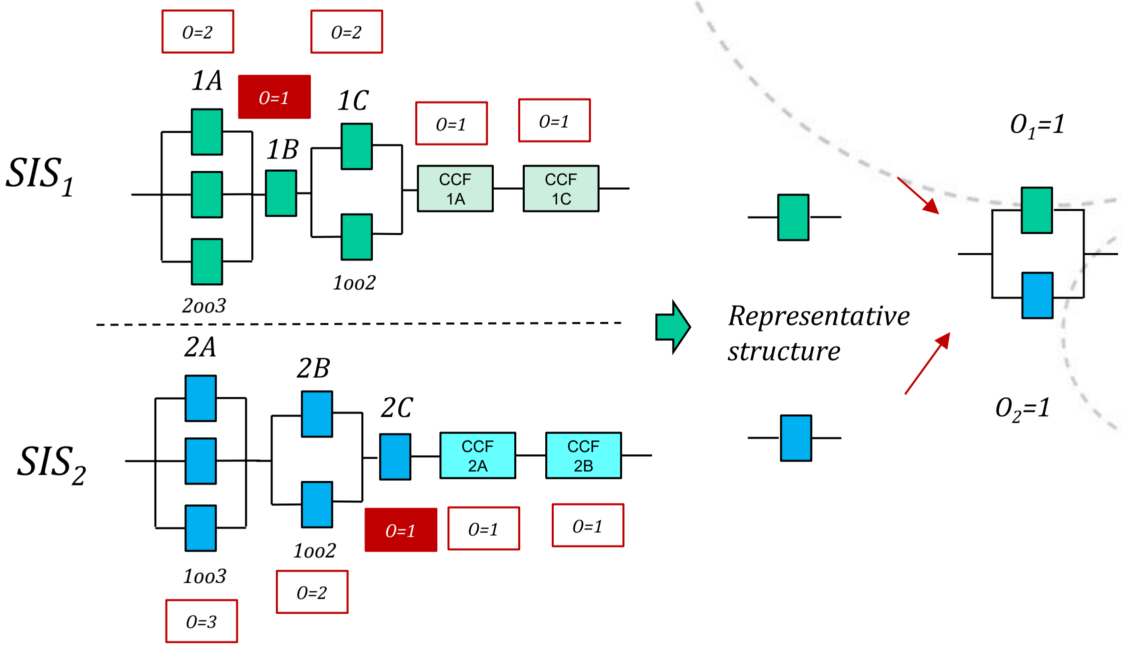
1. *Identify the order "o" of each subsystem (n-m+1)*
2. *Select simplest structure with* ***lowest*** *order for each SIS: O_k, where k is SIS_k*
3. *Calculate correction factor (CF) by:*

$$CF = \frac{\prod_{k=1}^{N}(O_k + 1)}{1 + \sum_{k=1}^{N} O_k}$$

Note: N is here number of SISs. Somewhat unfortunate notation, but I use same as in the PDS method book.

4. *Multiply the total PFD as:*

$$PFD_{tot} = CF \cdot \prod_{k=1}^{N} PFD_k$$



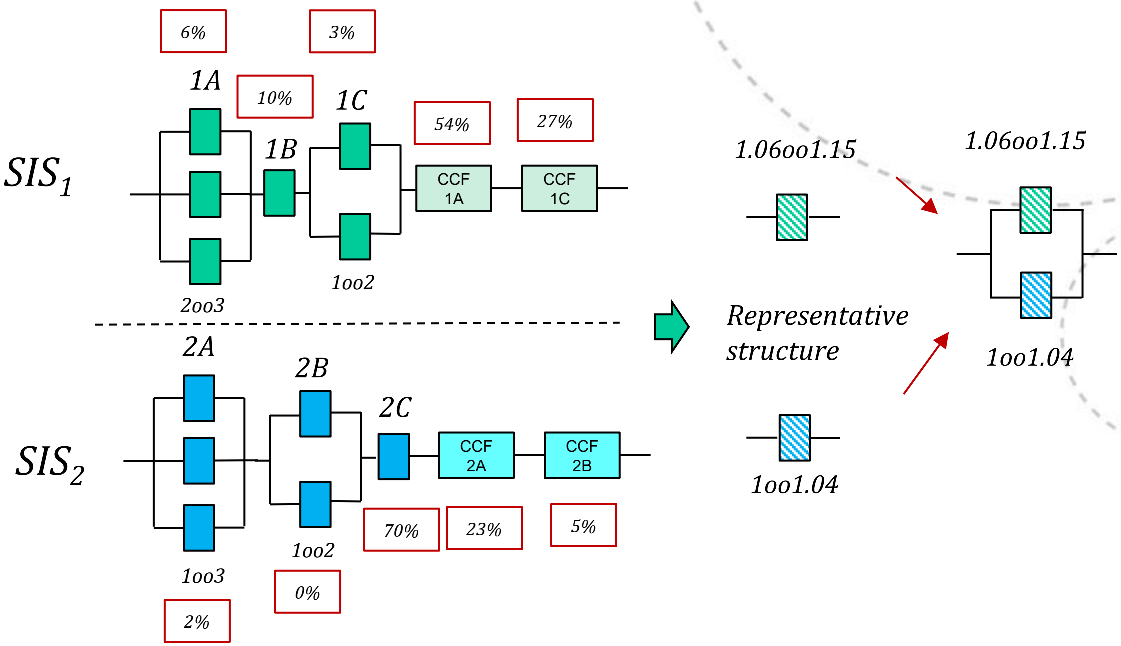
Example above:

$$CF = \frac{(1+1)\cdot(1+1)}{1+(1)+(1)} = \frac{4}{3}$$

Structural average

Steps:

1. *Do the following per subsystem (for each SIS):*
    a) *Calculate the PFD*
    b) *Determine the relative weight*
    c) *Determine the representative structure*
2. *Determine the representative structure for each SIS*
3. *Calculate the CF (using formula already introduced)*
4. *Calculate total PFD with CF (as already shown)*



Example: (SIS_1)

Table D.4: Calculation for finding the representative *m*-oo-*n* structure for SIS_1

Element	Structure			PFD [%]	Weighted structure	
	m-oo-n	*m*	*n*		*m*	*n*
1A	2oo3	2	3	6	0.12	0.18
1B	1oo1	1	1	10	0.1	0.1
1C	1oo2	1	2	3	0.03	0.06
CCF 1A	1oo1	1	1	54	0.54	0.54
CCF 1C	1oo1	1	1	27	0.27	0.27
Total				**100**	**1.06**	**1.15**

$$O_1 = 1.15 - 1.06 + 1 = 1.09$$

$$O_1 = 1.0 - 1.04 + 1 = 0.96$$

$$CF = \frac{(1+1.09)\cdot(1+0.96)}{1+(1.09)+(1.96)} = 1.34$$

Discussion

- Maximal order: Assumes that the sub-structure with the highest redundancy is the most important contributor. Not so realistic, unless <u>*very*</u> reliable single elements…
- Minimal order: Assumes that the sub-structure with the lowest redundancy is the most important contributor. Perhaps more realistic.
- Structural average: Not so intuitive. Advantage is that the sub-structure with the highest weight will influence the most on the representative structure

NTNU
Norwegian University of Science and Technology

Keywords (revisited)

β

CSU

CF

DTU_T

PFD

Systematic failure

C_{MooN}

P_{TIF}

β_2

DTU_R

Random hardware failure