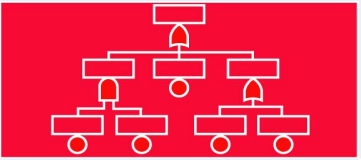
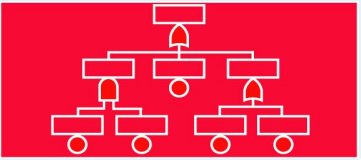
Spurious activation
Concepts and formulas

Mary Ann Lundteigen

Department of Production and Quality Engineering
Norwegian University of Science and Technology
mary.a.lundteigen@ntnu.no

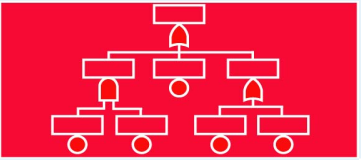


Overview

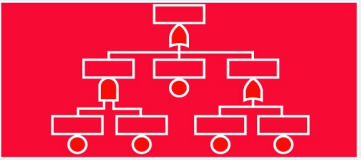


Content

1. Background
2. Spurious activation concepts and definitions
3. Spurious activation causes
4. Failure allocation
5. Formulas for calculating the spurious trip rate

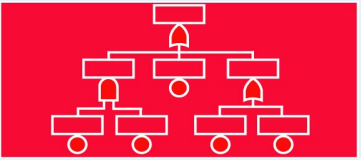


Background

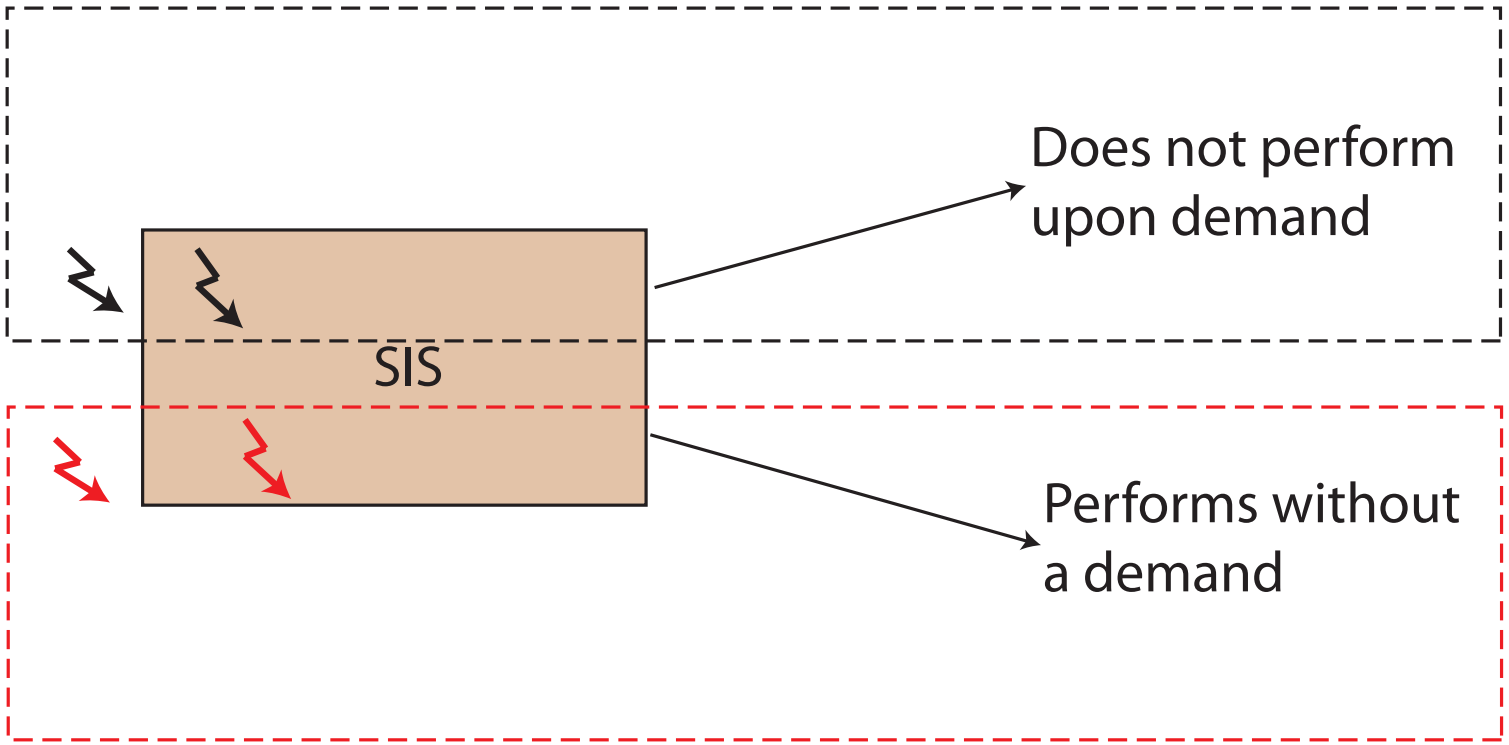


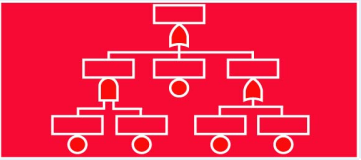
Basis for presentation

- Article written by Mary Ann Lundteigen and Marvin Rausand
- Submitted to the Safecomp 2007 - The 26th international Conference on Computer Safety, Reliability and Security (18-21.09.07, Nuremberg, Germany)



What are we talking about?

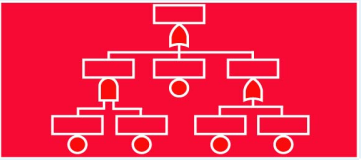




Why are spurious activations a concern

Normally, fail safe design prevent immidiate hazardeous situations upon spurious demands. But:

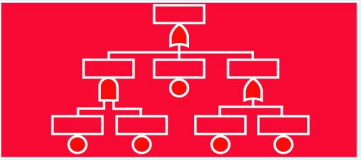
- Spurious shutdowns may lead to uncessessary production losses



Why are spurious activations a concern

Normally, fail safe design prevent immidiate hazardeous situations upon spurious demands. But:

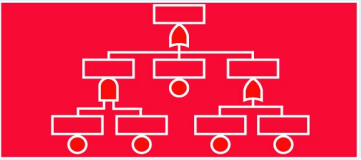
- Spurious shutdowns may lead to uncessessary production losses
- Additional risk during shutdown and the following start-up



Why are spurious activations a concern

Normally, fail safe design prevent immidiate hazardeous situations upon spurious demands. But:

- Spurious shutdowns may lead to uncessessary production losses
- Additional risk during shutdown and the following start-up
- Additional stress on components and systems

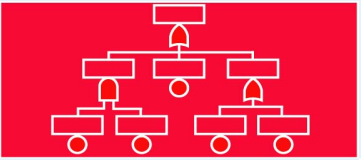


Why are spurious activations a concern

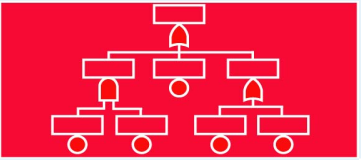
Normally, fail safe design prevent immidiate hazardeous situations upon spurious demands. But:

- Spurious shutdowns may lead to uncessessary production losses
- Additional risk during shutdown and the following start-up
- Additional stress on components and systems

In addition, the IEC 61511 requires that a maximum spurious trip rate is specified and the design verified against these constraints

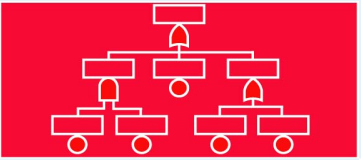


Definitions



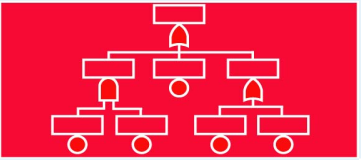
What is meant by spurious activation?

- No unique or commonly accepted concept or defintion, e.g.,
  - Spurious trip
  - Spurious stop
  - Nuisance trip
  - False trip
  - Premature closure



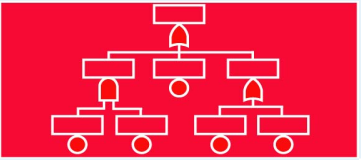
What is meant by spurious activation?

- No unique or commonly accepted concept or defintion, e.g.,
  - Spurious trip
  - Spurious stop
  - Nuisance trip
  - False trip
  - Premature closure
- Definitions may be found in:
  - ISA/TR 84.00.02-part 4
  - The PDS method
  - ISO 14224



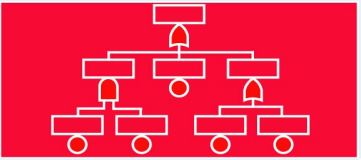
Existing concepts and definitions

- ISA/TR 84.00.02 - part 4:
  - *A spurious trip is a non-intended process shutdown*
- PDS method:
  - *A spurious trip is a spurious activation of a single SIS element or of a SIF*
- ISO 14224:
  - Fire and Gas detectors: *The detector gives an alarm signal when it is not exposed to relevant stimulus. The failure mode is normally observed during operation and logged by control room personnel*
  - Used otherwise: *Unexpected operation, fails to operate as demanded, false demand*



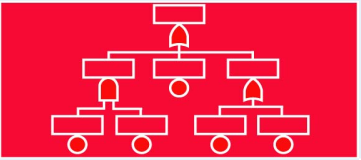
Differences between various concepts and definitions

- Do we talk about spurious activation of components or systems (e.g., the SIS)?
- Does always spurious activation lead to process shutdowns?



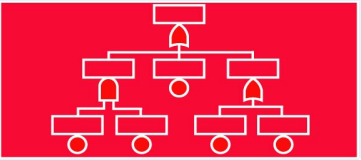
Proposed defintions and concepts

- It is suggested to differentiate between:
  - Spurious operation
  - Spurious trip
  - Spurious shutdown



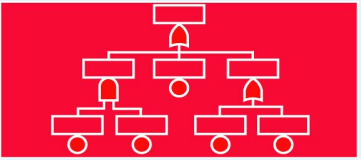
Proposed defintions and concepts

- Spurious operation:
  - A spurious operation is an activation of a SIS element without the presence of a specified process demand.



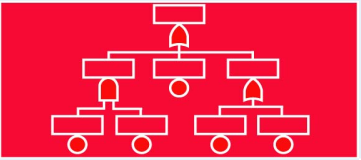
Proposed defintions and concepts

- Spurious operation:
  - A spurious operation is an activation of a SIS element without the presence of a specified process demand.
- Spurious trip:
  - A spurious trip is activation of one or more SIS elements such that the SIS performs a SIF without the presence of a specified process demand SIS element without the presence of a specified process demand.

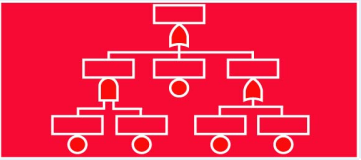


Proposed defintions and concepts

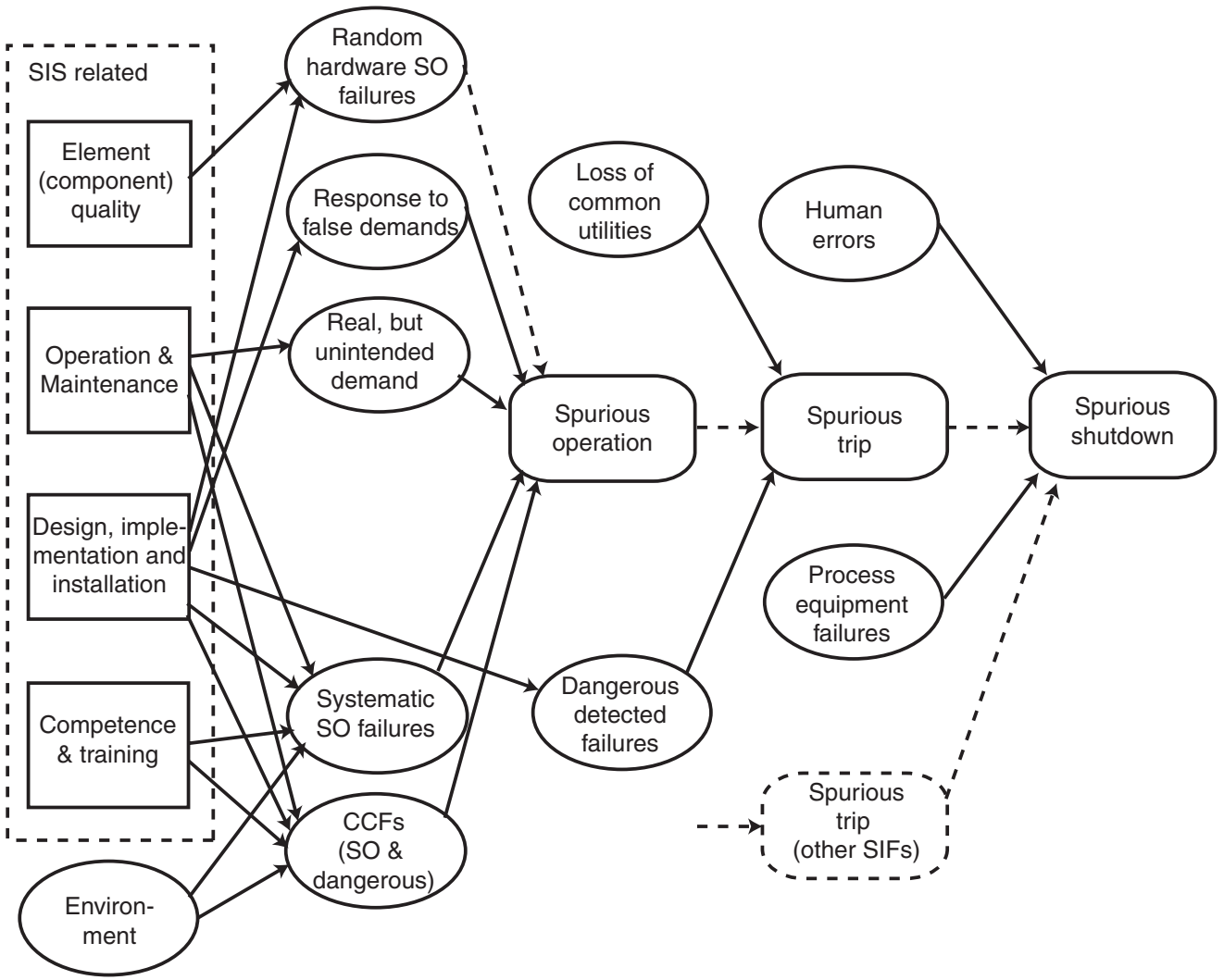
- Spurious operation:
  - A spurious operation is an activation of a SIS element without the presence of a specified process demand.
- Spurious trip:
  - A spurious trip is activation of one or more SIS elements such that the SIS performs a SIF without the presence of a specified process demand SIS element without the presence of a specified process demand.
- Spurious shutdown:
  - A spurious shutdown is is a partial or full process shutdown without the presence of a specified process demand.

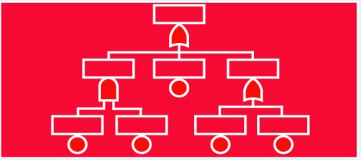


Spurious activation causes

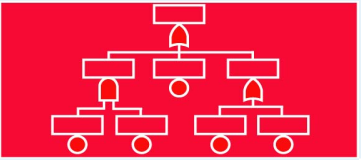


Spurious activation causes

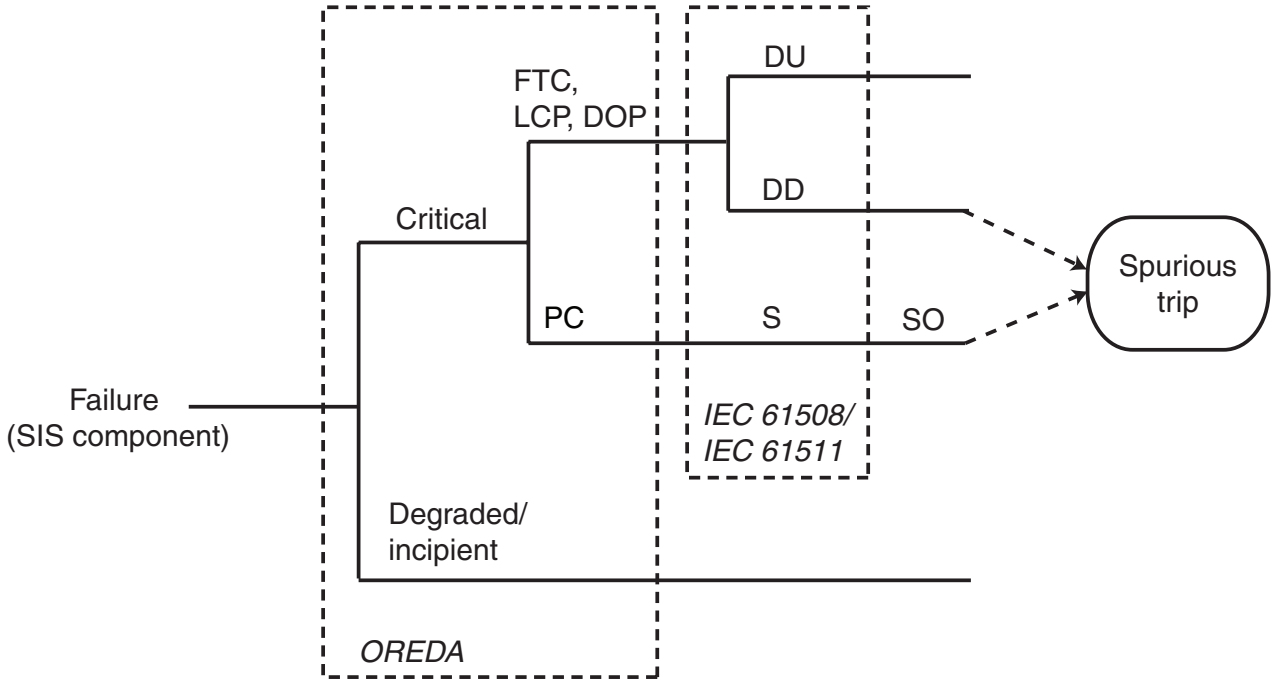


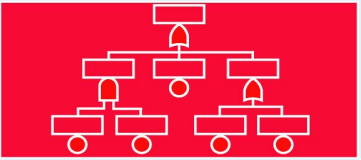


Failure modes and allocation

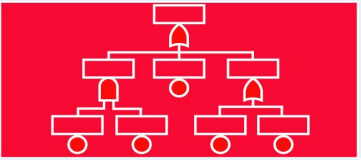


Failure modes and allocation of failure rates



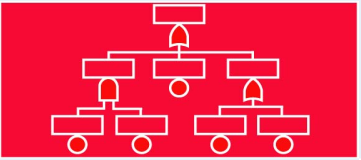


Assessment of spurious trip rate



Calculating the spurious trip rate

- The spurious trip rate may have three separate contributions
  - $\mathrm{STR} = \mathrm{STR}_{\text{Int. failures}} + \mathrm{STR}_{\text{False demands}} + \mathrm{STR}_{\mathrm{DD}}$
- In the following, these contributions are referred to as STR_1, STR_2 and STR_3.



Calculating the spurious trip rate

Contribution from internal component failures:

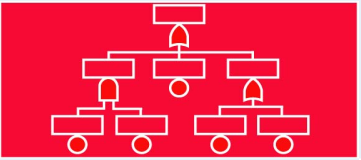
- STR_1:
  - 1oon (calculated for each component j):

$$\begin{aligned} \mathrm{STR}_{1,j} &= n(1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j} + \beta_j^{\mathrm{SO}}\lambda_{\mathrm{SO},j} \\ &= n\lambda_{\mathrm{SO},j} - (n-1)\beta_j^{\mathrm{SO}}\lambda_{\mathrm{SO},j} \end{aligned}$$

  - koon (also calculated for each component j):

$$\begin{aligned} \mathrm{STR}_{1,j}^{koon} &= n(1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j}\Pr(M \geq k-1) + \beta_j^{\mathrm{SO}}\lambda_{\mathrm{SO},j} \\ &\approx n(1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j}\left[\sum_{m=k-1}^{n-1}\binom{n-1}{m}p^m(1-p)^{n-1-m}\right] \\ &+ \beta_j^{\mathrm{SO}}\lambda_{\mathrm{SO},j} \end{aligned}$$

where $p = (1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j}\mathrm{MDT}_j$ and β_j^{SO} is the fraction of CCFs leading to spurious operation



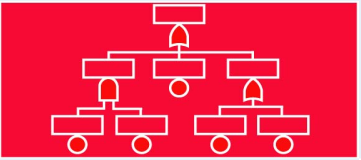
Calculating the spurious trip rate

Contribution from false demands:

- Two types of false demands:
  - Demands that are mistakenly treated by the SIS sensors as real demands (denoted λ_{F})
  - Demands that are real, but unintended (denoted λ_{SF})
- The contribution from false demands may therefore be expressed as:

$$\mathrm{STR}_{2,j} = (\lambda_{\mathrm{F}} + \lambda_{\mathrm{SF}})(1 - \mathrm{PFD})$$

where PFD is the (average) probability of failure on demand



Calculating the spurious trip rate

Contribution from dangerous detected failures (if such philosophy is implemented):

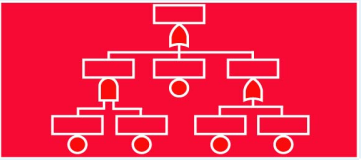
- STR_3:
  - 1oon (calculated for each component j):

$$\mathrm{STR}_{3,j} = \beta_j^{\mathrm{DD}} \lambda_{\mathrm{DD},j}$$

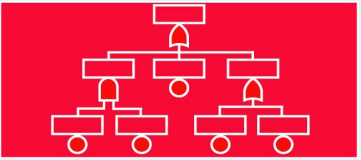
  - koon (also calculated for each component j):

$$\begin{aligned} \mathrm{STR}_{3,j}^{koon} &= n(1-\beta_j^{\mathrm{DD}})\lambda_{\mathrm{DD},j} \Pr\left(M^* \geq n-k\right) + \beta_j^{\mathrm{DD}} \lambda_{\mathrm{DD},j} \\ &\approx n(1-\beta_j^{\mathrm{DD}})\lambda_{\mathrm{DD},j} \left[\sum_{m=n-k}^{n-1} \binom{n-1}{m} p^m (1-p)^{n-1-m} \right] \\ &+ \beta_j^{\mathrm{DD}} \lambda_{\mathrm{DD},j} \end{aligned}$$

where $p = (1-\beta_j^{\mathrm{DD}})\lambda_{\mathrm{DD},j}\mathrm{MDT}_j^*$.

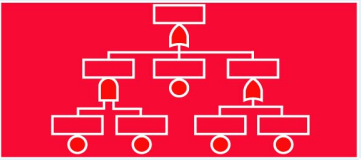


Comparing different formulas



Comparing different formulas

Configurations	New	PDS	ISA
1oo1	$\lambda_{SO} + \lambda_{DD}$	λ_{SO}	$\lambda_S + \lambda_{DD}$
1oo2	$(2 - \beta^{SO})\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$2\lambda_{SO}$	$2(\lambda_S + \lambda_{DD}) + \beta^{D}(\lambda_S + \lambda_{DD})$
2oo3	$\beta^{SO}\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$2.4\beta^{D}\lambda_{SO}$	$\beta^{D}(\lambda_S + \lambda_{DD})$
2oo4	$\beta^{SO}\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$4\beta^{D}\lambda_{SO}$	$\beta^{D}(\lambda_S + \lambda_{DD})$



Discussion and conclusions

- Different formulas give quite similar results
- The differences are due to:
  - The PDS approach only considers SO-failures and not DD failures
  - ISA applies the same approach to DD failures as for SO failures
  - The PDS approach used a calibration factor for M>1
  - The ISA and PDS approach do not distinguish between β_{SO} and β_{DD}