Chapter 12.
Spurious Operation and Spurious Trips

Mary Ann Lundteigen Marvin Rausand

RAMS Group
Department of Mechanical and Industrial Engineering
NTNU

(Version 0.1)

NTNU – Trondheim
Norwegian University of
Science and Technology

Learning Objectives

The main learning objectives associated with these slides are to:

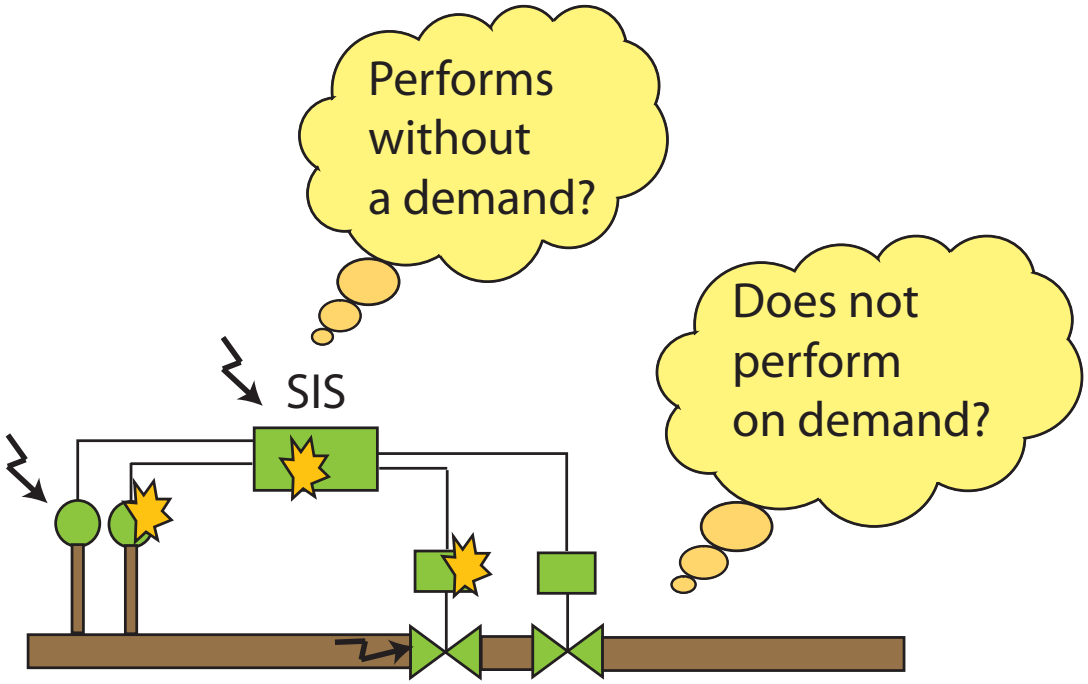
1. Introduce and discuss key concepts related to spurious activation
2. Explain some of the spurious activation causes
3. Explain different approaches for calculating the spurious trip rate

The main content of the slides builds on chapter 12 in the textbook. In addition, the following literature has been used:

- *Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas*by M.A. Lundteigen and M. Rausand, published in *Reliability Engineering & System Safety*.

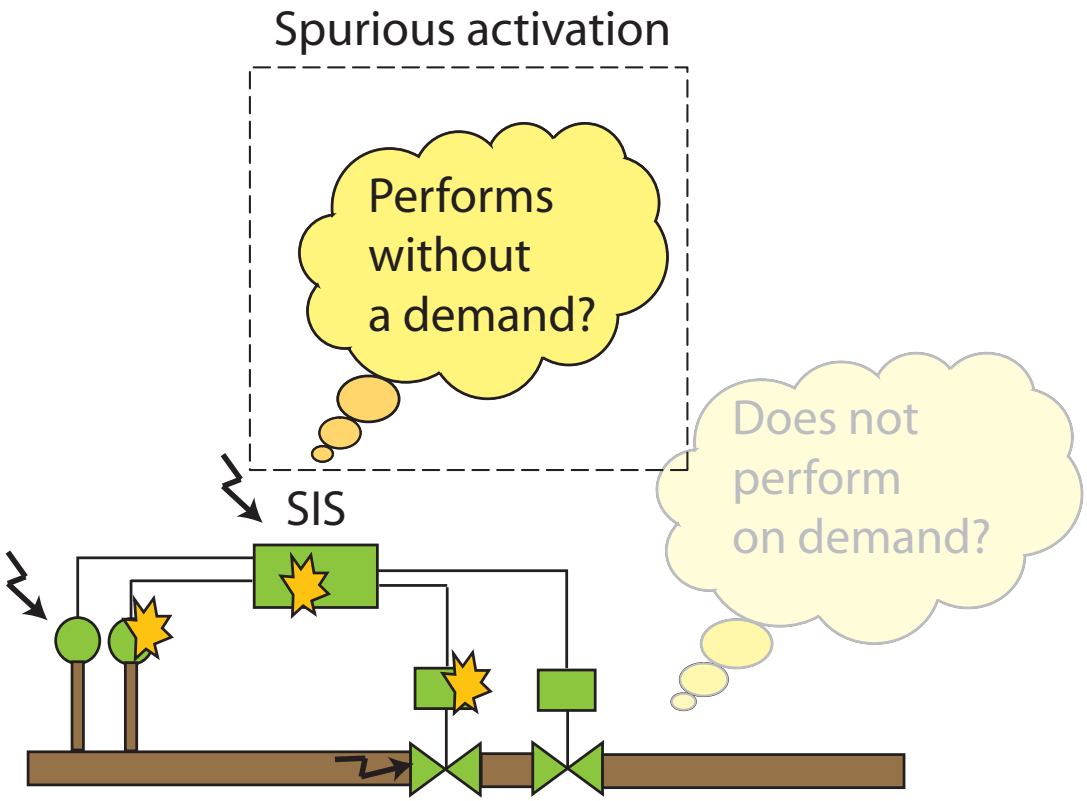
Motivation: SIS related failures

Two main types of SIS related failures:



Motivation: Spurious activation failure

A spurious activation is an activation of a SIF without the presence of a demand.



Motivation: Do we need to worry?

A spurious activation of a SIS will normally result in the safe state of the equipment under control (EUC). Yet, spurious activations may be undesired because of:

- Creating unnecessary production losses
- Generating “false alarms”, which again may result in the loss of confidence to the SIS
- Increased risk of hazardous events following a spurious activation, such as during start-up
- Excessive stresses on components and systems during shutdown and start-up

A spurious activation may even create an hazardous event. For example a false deployment of an airbag while driving, or spurious closure of a valve on the outlet of a production separator.

What does the standards require or suggest?

- IEC 61508 considers spurious activations as safe failures, and that they result in the safe state of the EUC
- IEC 61511 requires that the spurious activation rate is estimated and considered when selecting SIS design (but does not say in what way)
- OREDA considers spurious activation as critical failures, due to it's impact on the production availability
- ISO TR 12489, a recommended practice for reliability analysis in the petroleum sector, calls for a balance (and analysis to confirm this) between safety and production. Spurious activations is given considerable attention in this recommended practice document.
- ISA TR84.00.02.x on methods to use for reliability analysis in the process industry suggest that spurious trip rates are considered along with measures for safety unavailability.

Names of spurious activations

Spurious activation is not the only term used for non-intended (not-demanded) activation of a function:

- Spurious trip
- Spurious operation
- Spurious stop
- Nuisance trip
- False trip
- False activation
- Premature closure

...and perhaps many more.

Existing terms and definitions

IEC 61508: Spurious activation is mentioned in the definition of a safe failure.

☞ Safe failure: Failure of an element and/or a subsystem that plays a part in implementing the safety function that:

(a) results in the spurious operation of the safety function to put the EUC (or parts thereof) into a safe state or maintain a safe state; or

(b) incereases the probability of a spurious operation of the safety function to put the EUC (or parts thereof) into a safe state or maintain a safe state.

(IEC 61508-4, para. 3.6.8)

Existing terms 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 TR 12489 (2013) - has introduced several terms of relevance for spurious activation:
  - *Spurious failure is a failure triggering an action in an untimely manner*
  - *Critical safe failure (of a safety system), due to safe failure(s) of its component(s), triggering the safety action and leading to a spurious safety action.*
  - *Spurious activation (of a safety function) is an untimely demand of a safety function when it is not needed.*
  - *Spurious safety action (of a safety system) is the result of a spurious activation of a safety function*

What attributes apply to spurious activations?

- Non-intended, unexpected, and unrequested demand
- May involve the SIF or a SIF element
- May result in the safe state of the EUC

It may be feasible to distinguish a spurious activation at the element level, the subsystem level, and the EUC level, as the causes and effects may be different for the three.

Refined definitions

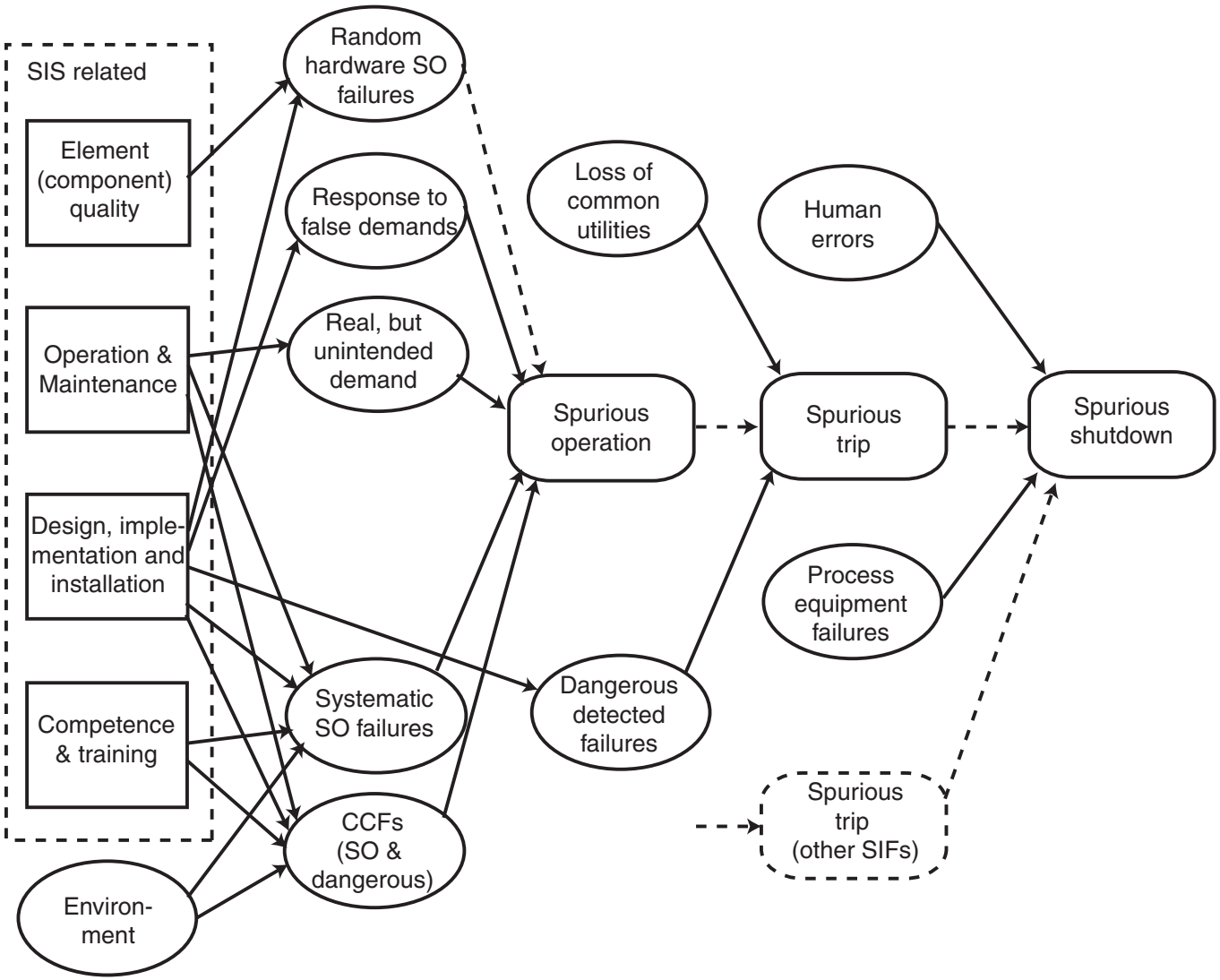
☞ Spurious operation: A spurious operation is an activation of a SIS element without the presence of a specified process demand.

☞ 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.

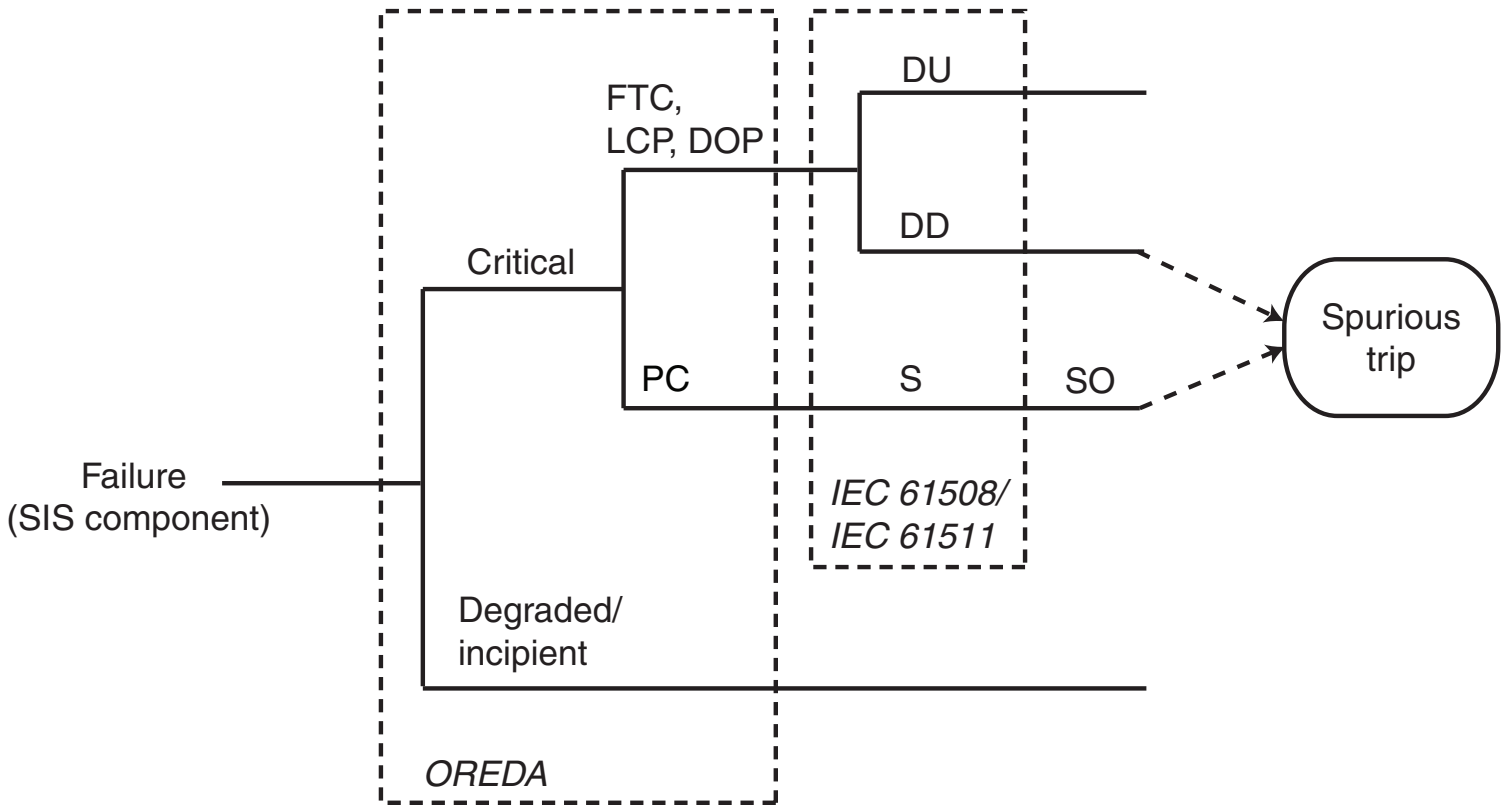
☞ Spurious shutdown: A spurious shutdown is a partial or full process shutdown without the presence of a specified process demand.

Lundteigen and Rausand (2008)

Spurious operation → trip → shutdown

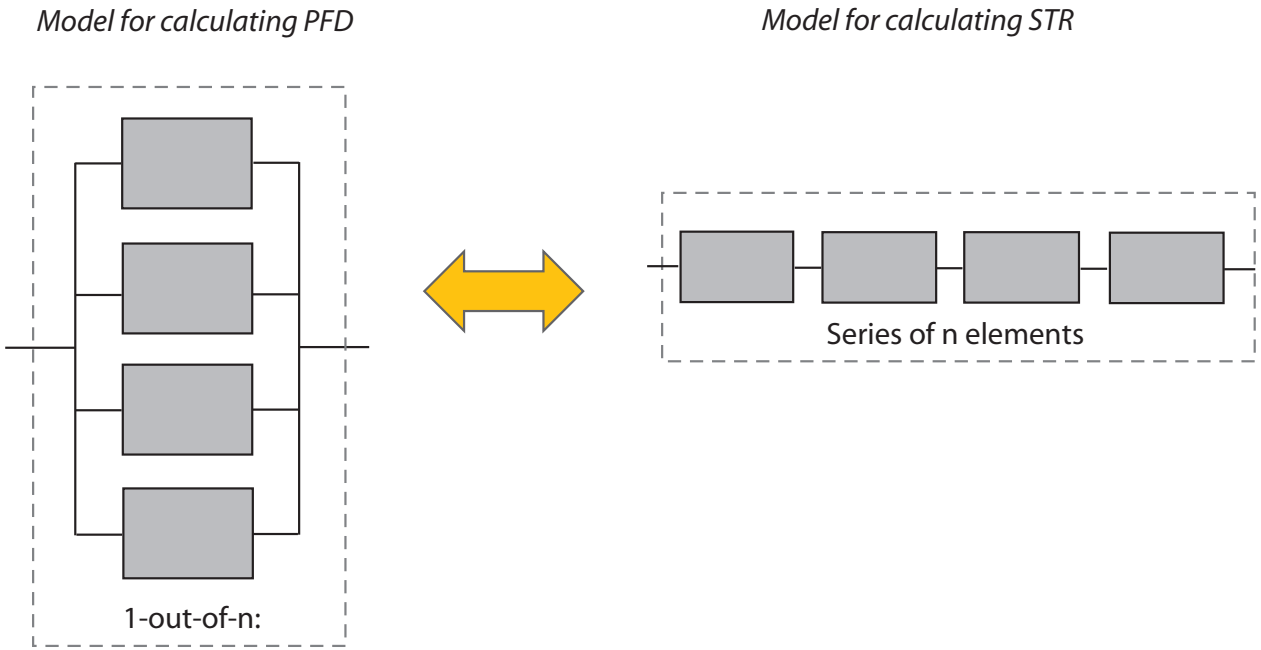


Spurious trip and failure classifications



Implications for reliability model

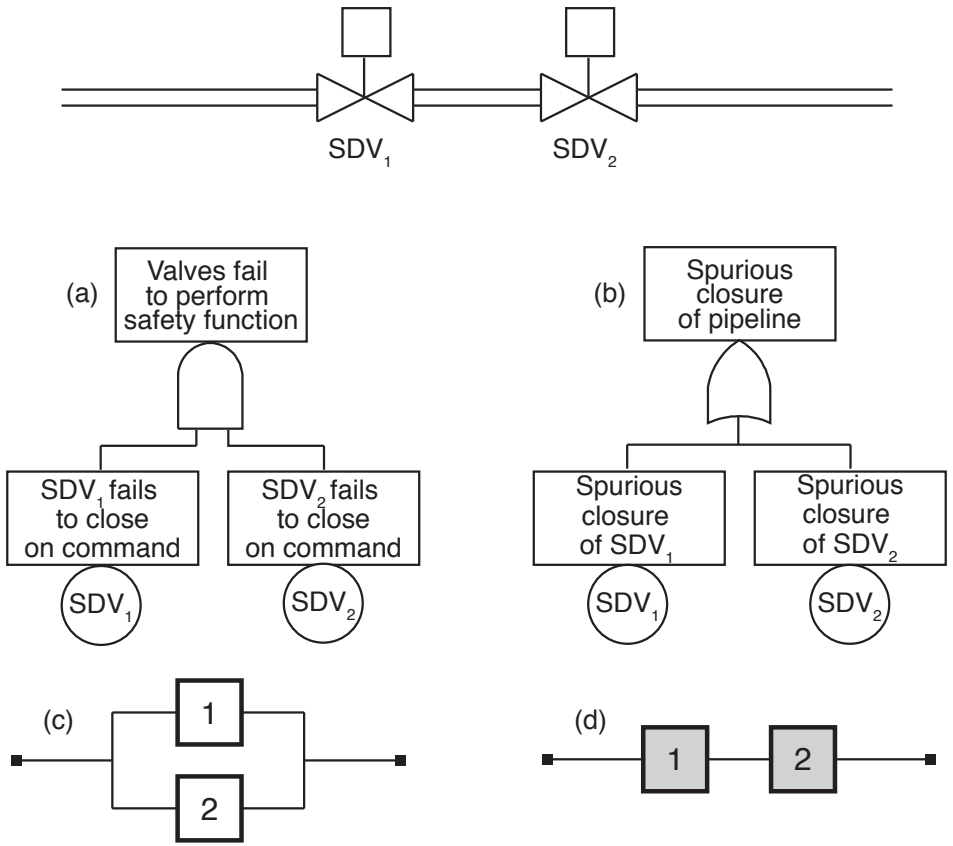
A 1oon parallel structure in a RBD may be converted to a series structure of n elements:



This indicates that the more safe, the more prone to spurious activations.

Modeling for spurious trip

From the textbook:



Fault tolerance

The hardware fault tolerance (with respect to dangerous failures) of a *koon* system is n-k. The corresponding HFT with respect to spurious trips, here denoted HFT_S is (n-(n-k+1)) = k-1.

	Voting					
Fault tolerance	1oo2	1oo3	2oo3	1oo4	2oo4	3oo4
HFT	1	2	1	3	2	1
HFT_S	0	0	1	0	1	2

Spurious trips and spurious trip rate

We often assume that the number of spurious trips follows a homogenous poisson process with the rate STR_{tot} of the SIF (assuming that the repair times of the spurious trip failures are negligble compared to the mean time between spurious trips)

- Assume that the number of failures occuring in the time interval t is $\mathrm{N}_{ST}(t)$
- The probability that $\mathrm{N}_{ST}(t) = n$ is:

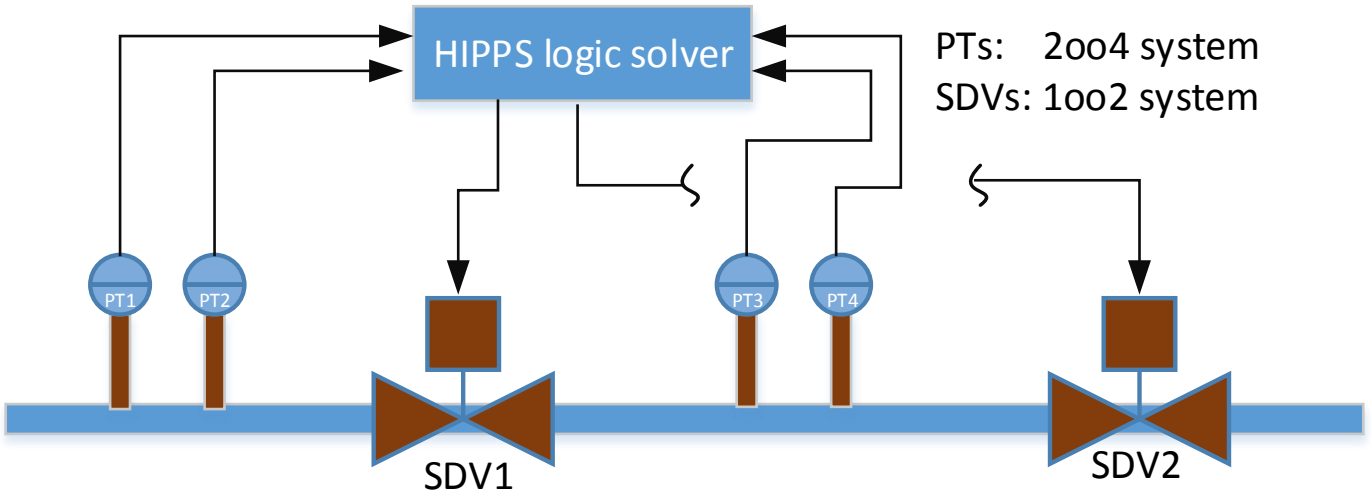
$$\Pr(N_{ST}(t) = n) = \frac{(STR_{tot} \cdot t)^n}{n!} e^{-STR_{tot} \cdot t}$$

The mean number of spurious trips in the time period t is:

$$E[N_{ST}(t)] = STR_{tot} \cdot t$$

But how can we find STR_{tot}?

The spurious trip rate of the SIF is the sum of the spurious trip rates of the subsystems.



$$STR_{tot} = STR_{PTs} + STR_{LS} + STR_{SDVs}$$

And how can we find STR of the subsystems

The STR of each subsystem (IE, LS, and FE), in the textbook called STR_G is determined separately for each subsystem. STR_G is calculated as the sum of the following three contributors:

- Spurious operation (SO) failures, denoted STR_{IF}
- False demands, denoted STR_{FD}
- Dangerous detected failures (if one or more DD failure results in a transition to the safe state), denoted STR_{DD}

where IF means internal (SO) failure, FD means false demands, and DD means dangerous detected failures.

Failure rates associated with STR_{IF} and STR_{DD}

STR_{IF} is calculated on the basis of:

- Independent SO failures, $(1 - \beta^{SO})\lambda_{SO}$, where β^{SO} is the fraction of SO failures that are common cause failures.
- Common cause failures, denoted $\beta^{SO}\lambda_{SO}$

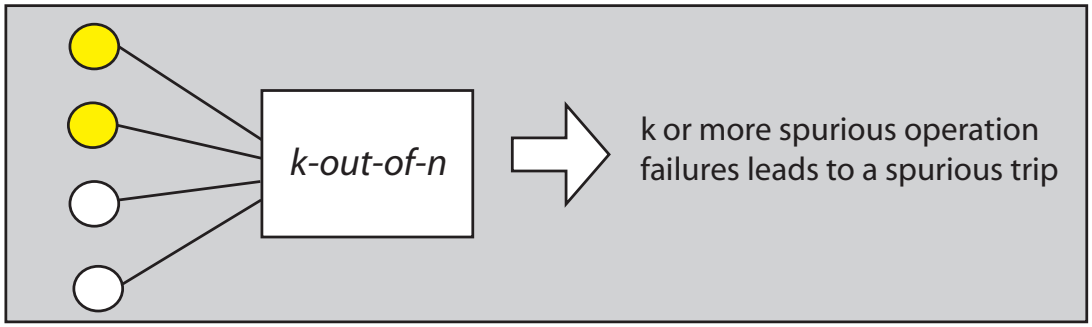
STR_{DD} is calculated on the basis of:

- Independent DD failures, $(1 - \beta^{DD})\lambda_{DD}$, where β^{DD} is the fraction of DD failures that are common cause failures.
- Common cause failures, denoted $\beta^{DD}\lambda_{DD}$

Mean downtime of DD failures is MDT^* and mean downtime of a SO failure is MDT.

Approach for including SO failures, STR_{IF}

Step 1: First consider that any of the n elements may fail:



Step 2: Calculate the spurious trip rate with respect to spurious operation (SO) failures:

(a): The first element fails with a spurious operation rate $n \cdot \lambda_{SO}$.

(b) Probability that at least (k-1) out of the (n-1) elements have spurious operation failures may follow the binomial distribution, with

(i) (n-1) experiments

(ii) Two possible outcomes: spurious operation or spurious operation of the element

(iii) Each outcome have the same probabilities (p or [1-p]), where

$$p = Pr(T < MDT) = 1 - e^{-[(1-\beta^{SO})\lambda_{SO} \cdot MDT]} \approx (1-\beta^{SO})\lambda_{SO} \cdot MDT$$

This means that the probability that at least k-1 out of the (n-1) remaining elements are:

$$Pr(M \geq k-1) = \sum_{m=k-1}^{n-1} \binom{n-1}{m} p^m (1-p)^{n-1-m}$$

(c) Spurious trip rate is then $n \cdot \lambda_{SO} \cdot Pr(M \geq k-1)$

Contribution from spurious operation failures, STR_{IF}

Consider a 1oo$n$ voted group of independent and identical channels.

- Any SO failure of a channel gives a spurious trip of the voted group. The spurious trip rate due to internal failures of a 1oo$n$ configuration of channels is therefore

This means that:

$$STR_{G,IF} = n\lambda_{SO}$$

Contribution from spurious operation failures, STR_{IF}

Consider a *koon* voted group, with k≥ 2, with respect to internal failures is

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

where $p = (1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}}\mathrm{MTTR}_{\mathrm{SO}}$. As p usually is a very small number, $1-p \approx 1$, and the STR can be approximated by

$$\begin{aligned}
\mathrm{STR}_{\mathrm{G,IF}}^{(koon)} &\approx n(1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}} \left[\sum_{m=k-1}^{n-1} \binom{n-1}{m} p^m\right] + \beta_{\mathrm{SO}}\lambda_{\mathrm{SO}} \\
&\approx n(1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}} \left[\sum_{m=k-1}^{n-1} \binom{n-1}{m} ((1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}}\mathrm{MTTR}_{\mathrm{SO}}{}^m\right] \\
&\quad + \beta_{\mathrm{SO}}\lambda_{\mathrm{SO}}
\end{aligned}$$

Contribution from spurious operation failures, STR_{IF}

Because p is a very small number, $p^{m+1} \ll p^m$ for all $m \geq 1$. This means that the sum can be approximated by the first addend, such that

$$\begin{aligned}\mathrm{STR}_{\mathrm{G,IF}}^{(koon)} &\approx n(1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}}\binom{n-1}{k-1}[(1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}}\mathrm{MTTR}_{\mathrm{SO}}]^{k-1} \\ &\quad + \beta_{\mathrm{SO}}\lambda_{\mathrm{SO}} \\ &= n\binom{n-1}{k-1}[(1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}}]^{k}\,\mathrm{MTTR}_{\mathrm{SO}}^{k-1} + \beta_{\mathrm{SO}}\lambda_{\mathrm{SO}}\end{aligned}$$

Note that this formula for k=1i s 1oo$n$ is $\mathrm{STR}_{\mathrm{G,IF}} = n\lambda_{\mathrm{SO}}$.

Example

Consider a 2oo3 system. In this case the formula for internal failures becomes:

$$\begin{aligned}\mathrm{STR}_{\mathrm{G,IF}}^{(2oo3)} &= 3\binom{2}{1}\left[(1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}}\right]^2 \mathrm{MTTR}_{\mathrm{SO}}^1 + \beta_{\mathrm{SO}}\lambda_{\mathrm{SO}} \\ &= 6(1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}}^2 \mathrm{MTTR}_{\mathrm{SO}} + \beta_{\mathrm{SO}}\lambda_{\mathrm{SO}}\end{aligned}$$

For comparison, consider a 1oo3 system. In this case, we get:

$$\mathrm{STR}_{\mathrm{G,IF}}^{(1oo3)} = 3\lambda_{\mathrm{SO}}$$

If we erranously used the formula for $k$oo$n$ we would have gotten:

$$\begin{aligned}\mathrm{STR}_{\mathrm{G,IF}}^{(1oo3)} &= 3\binom{2}{0}\left[(1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}}\right]^1 \mathrm{MTTR}_{\mathrm{SO}}^0 + \beta_{\mathrm{SO}}\lambda_{\mathrm{SO}} \\ &= 3(1-\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}} + \beta_{\mathrm{SO}}\lambda_{\mathrm{SO}} = (3-2\beta_{\mathrm{SO}})\lambda_{\mathrm{SO}}\end{aligned}$$

which is slightly odd result (indicating that CCFs reduces the spurious trip rate...)

Contribution from false demands, STR_{FD}

False demands may be one out of the following two types:

- Type (a): Demands that are mistakenly treated by the SIS as real demand (e.g., reflection of sun taken to be a fire)
- Type (b): Demands that are real, but unintended (e.g., flame from welding activity)

$$STR_{FD} = (\lambda_{FDa} + \lambda_{FDb})(1 - PFD_{avg})$$

PDF_{avg} is usually so small that $1 - PFD_{avg} \approx 1$ and can be omitted, such that

$$STR_{FD} \approx (\lambda_{FDa} + \lambda_{FDb})$$

Contribution from DD failures, STR_{DD}

A binomial situation is also assumed here for (n-1) trials. It is when (n-k) trials of out of the (n-1) has a DD failure, that we assume an automatic transition to the safe state.

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

where $p^* = (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\mathrm{MTTR}$. We make the same assumptions as for $\mathrm{STR}_{\mathrm{G,IF}}$, and get that $\mathrm{STR}_{\mathrm{G,DD}}$ is approximately

$$\mathrm{STR}_{\mathrm{G,DD}}^{(koon)} \approx n\binom{n-1}{n-k}\left[(1-\beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\right]^{n-k+1} \mathrm{MTTR}^{n-k} + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}$$

Example

Consider a 2oo3 system. In this case the formula for internal failures becomes:

$$\begin{aligned} \mathrm{STR}_{\mathrm{G,DD}}^{(2oo3)} &\approx 3\binom{2}{1}\left[(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\right]^2 \mathrm{MTTR}^1 + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}} \\ &= 6\left[(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\right]^2 \mathrm{MTTR}^1 + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}} \end{aligned}$$

For comparison, consider a 1oo3 system. In this case, we get:

$$\begin{aligned} \mathrm{STR}_{\mathrm{G,DD}}^{(1oo3)} &\approx 3\binom{2}{2}\left[(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\right]^3 \mathrm{MTTR}^2 + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}} \\ &= 3\left[(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\right]^3 \mathrm{MTTR}^2 + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}} \end{aligned}$$

For $noon$ we should use $\mathrm{STR}_{\mathrm{G,DD}}^{(noo)} = n\lambda_{\mathrm{DD}}$.

Regarding the common cause failures

When calculating the STR, we include two different β's:

- β_{SO}: Fraction of SO failures that are CCFs
- β_{DD}: Fraction of DD failures that are CCFs (may be determined by checklists in IEC 61508-6 (check))

IEC 61508-6 has a checklist that may be used to determine β_D, however, it should be noted that this checklist may not be suited for determining β_{SO} because the (shared) failure causes may be different.

Example: Shutdown valve

A stuck valve actuator may lead to a "fail to close" failure mode, but the same failure cause is not applicable for premature closure.

Comparing different analytical formulas

The following table shows a selection of formula results for SO and DD failures.

Configurations	SIS book	PDS method	ISA/TR 84.00.02-part 4
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	$\beta^{SO}\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$C_{2oo3}\beta^D\lambda_{SO}$	$\beta^D(\lambda_S + \lambda_{DD})$
2oo4	$\beta^{SO}\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$C_{3oo4}\beta^D\lambda_{SO}$	$\beta^D(\lambda_S + \lambda_{DD})$

$C_{2oo3} = 2.0$ and $C_{3oo4} = 2.8$. The referenced sources may be visited for more details.

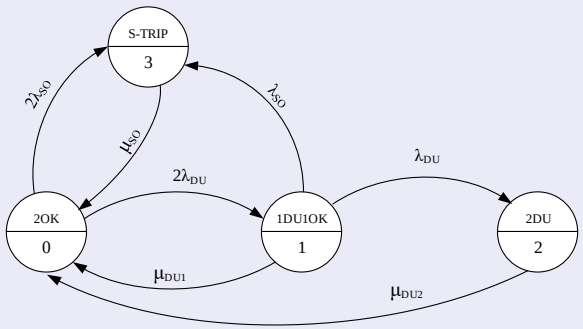
Using Markov Approach to find spurious trip rate

The spurious trip rate using Markov may be found by:

$$STR_{tot} = \sum_{j \in F_{ST}} P_i \lambda_{ij}$$

where F_{ST} denotes the failure state space for spurious trips, and $j \neq i$.

Example: Consider the Markov model below



In this case, STR_{tot} becomes:

$$STR_{tot} = P_0 \cdot 2\lambda_{SO} + P_1 \cdot \lambda_{SO}$$

It may be remarked that this model did not include the contribution from DD failures and false demands.

Discussion and conclusions

- Three types of spurious activations have been introduced; spurious operation (of an element), spurious trip (of a SIF), and spurious shutdown (of the process)
- When calculating the spurious trip rate of a SIF, it may be necessary to include more than the spurious operation failures
- A $koon$ system with respect to carrying out the safety function is a $(n-k+1)oon$ system with respect to avoiding spurious trips.
- Analytical formulas have been suggested, as well as the Markov approach