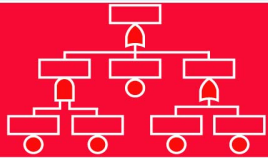

CCFs - Definitions, models and defenses

Mary Ann Lundteigen

Department of Production and Quality Engineering
Norwegian University of Science and Technology

mary.a.lundteigen@ntnu.no



Overview

[Content](#)

[Background](#)

[Modeling approach](#)

[CCF parameters](#)

[Defenses](#)

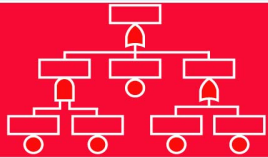
[New procedure](#)

[Practical example](#)

[Summing up](#)

[Learnt anything?](#)

Overview



Overview of presentation

Overview

Content

Background

Modeling approach

CCF parameters

Defenses

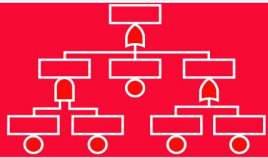
New procedure

Practical example

Summing up

Learnt anything?

1. Background
 - What is the context?
 - What are common cause failures (CCFs)?
 - Why are they important?
2. How should CCFs be taken into account in reliability modeling?
 - (a) Methods
 - (b) Practical examples
3. How may we defend against CCFs?
 - (a) Methods
 - (b) Practical examples
4. Discussion & conclusions
5. Did you learn anything?



Overview

Background

Context

CCF threats

Previous events

Definitions

Attributes

Examples

Clarification

Modeling approach

CCF parameters

Defenses

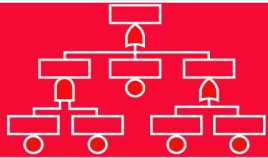
New procedure

Practical example

Summing up

Learnt anything?

Background



What is the context?

Overview

Background

Context

CCF threats

Previous events

Definitions

Attributes

Examples

Clarification

Modeling approach

CCF parameters

Defenses

New procedure

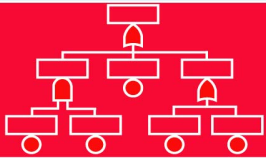
Practical example

Summing up

Learnt anything?

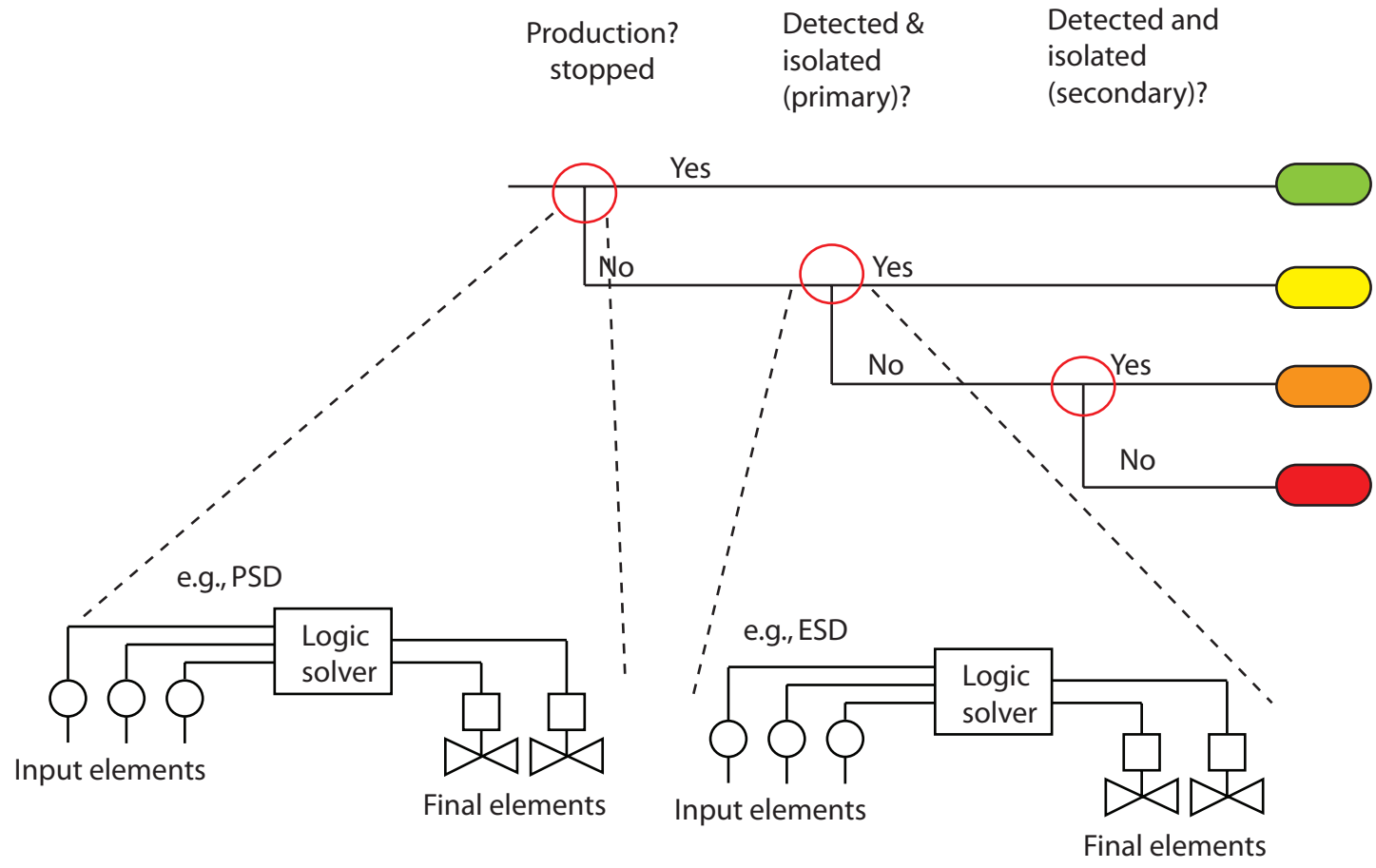
Our focus is on *safety instrumented systems* (SIS):

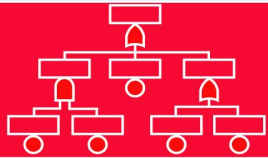
- The SIS is used to implement several *safety instrumented functions* (SIFs)
- The SIFs may represent *independent safety barriers*
- More than one SIS may exist
- Redundancy is often used to reduce vulnerability to (single) failures
- Independence between redundant components or between safety barriers is a key issue
- The SIS is often a passive system: Many failures are only revealed during a function test or upon a real demand



What is the context?

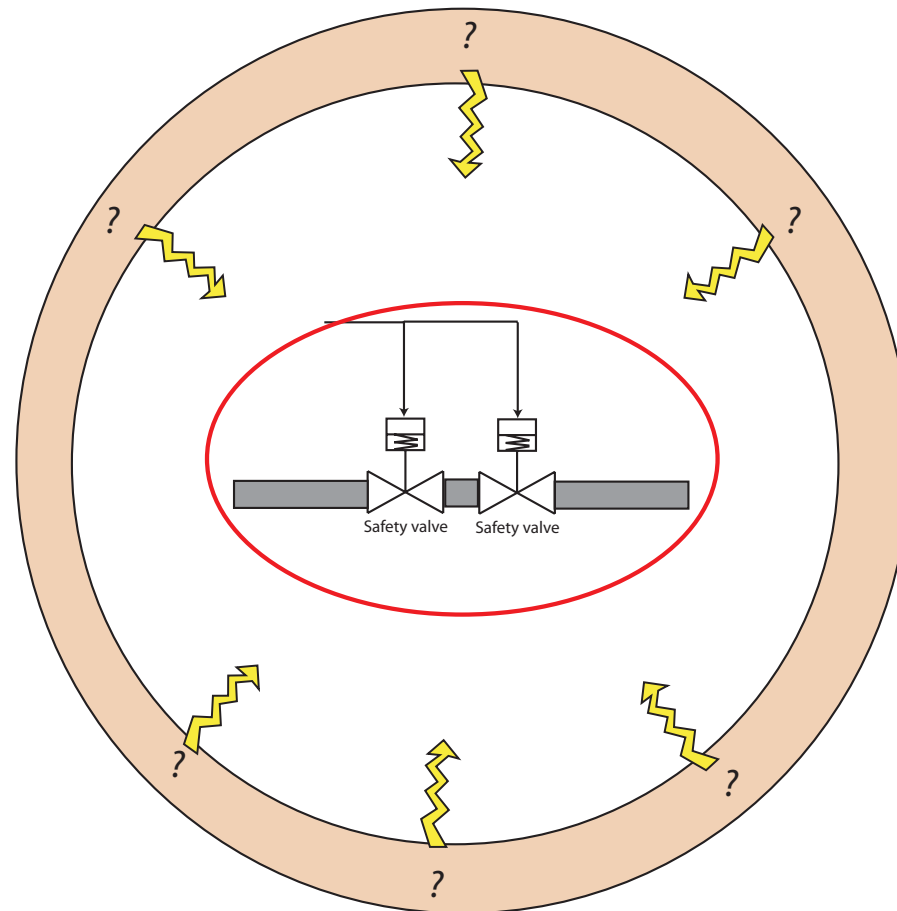
- Overview
- Background
- Context**
- CCF threats
- Previous events
- Definitions
- Attributes
- Examples
- Clarification
- Modeling approach
- CCF parameters
- Defenses
- New procedure
- Practical example
- Summing up
- Learnt anything?





What is a common cause failure (CCF)?

A CCF involves failure of two or more components, and may cause the safety function(s) to fail...



[Overview](#)

[Background](#)

[Context](#)

CCF threats

[Previous events](#)

[Definitions](#)

[Attributes](#)

[Examples](#)

[Clarification](#)

[Modeling approach](#)

[CCF parameters](#)

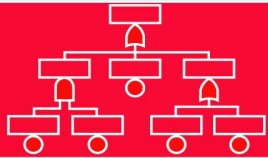
[Defenses](#)

[New procedure](#)

[Practical example](#)

[Summing up](#)

[Learnt anything?](#)



Why are CCFs important?

Overview

Background

Context

CCF threats

Previous events

Definitions

Attributes

Examples

Clarification

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Summing up

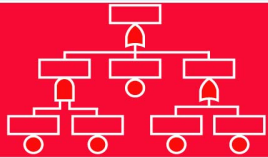
Learnt anything?

Previous accidents that have been caused by CCFs:

- Piper Alpha fire (oil and gas installation)
- Browns Ferry reactor fire (human error (using candle light) /cables to redundant systems located together)
- Three Mile Island (reactor): Failure of several feed water valves (design error?/ same type of valves?)

Luckily, many CCFs are discovered before they are able to cause large accidents...

- The most severe accidents may be when several safety barriers are affected



Definitions and basic concepts

Overview

Background

Context

CCF threats

Previous events

Definitions

Attributes

Examples

Clarification

Modeling approach

CCF parameters

Defenses

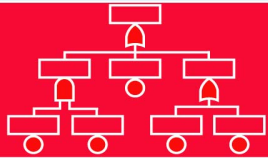
New procedure

Practical example

Summing up

Learnt anything?

- Several definitions exists
- A CCF may be defined as:
 1. The CCF event comprises multiple (complete) failures of two or more redundant components or two or more SIFs due to a shared cause
 2. The multiple failures occur within the same inspection or function test interval*), and
 3. The CCF event leads to failure of a single SIF or loss of several SIFs**).
- *) One may choose to omit this aspect if it is an important dependency (ref: PDS-CCF report).
- **) We are normally only considering *dangerous* failures. But we may have a “safe” CCFs as well.



Definitions and basic concepts

Overview

Background

Context

CCF threats

Previous events

Definitions

Attributes

Examples

Clarification

Modeling approach

CCF parameters

Defenses

New procedure

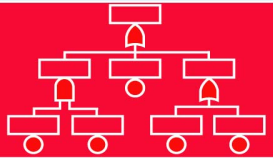
Practical example

Summing up

Learnt anything?

Mathematically we may define express CCFs through the β -factor:

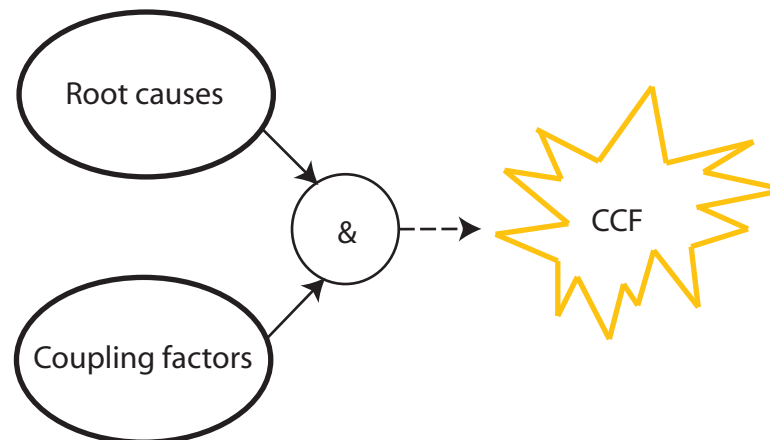
$$\begin{aligned}\beta &= \Pr(\text{CCF} | \text{a dangerous failure has occurred}), \text{ alternatively;} \\ &= \text{the fraction of CCFs to the total number} \\ &\quad \text{of dangerous failures}\end{aligned}$$

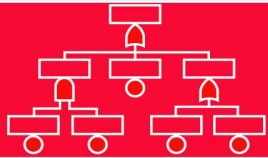


Main attributes of CCF causes

- Overview
- Background
- Context
- CCF threats
- Previous events
- Definitions
- Attributes**
- Examples
- Clarification
- Modeling approach
- CCF parameters
- Defenses
- New procedure
- Practical example
- Summing up
- Learnt anything?

- A shared cause exists
- The shared cause comprises two elements; a root cause and a coupling factor
 - Root cause; Why did the component fail? (*linked to the component*)
 - Coupling factor: Why were several components affected? (*linked to the link among several components*)





Main attributes of CCF causes

Overview

Background

Context

CCF threats

Previous events

Definitions

Attributes

Examples

Clarification

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Summing up

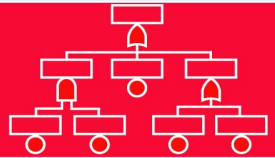
Learnt anything?

Root cause:

- Most basic cause of component failure that, if corrected, would prevent recurrence of this and similar causes

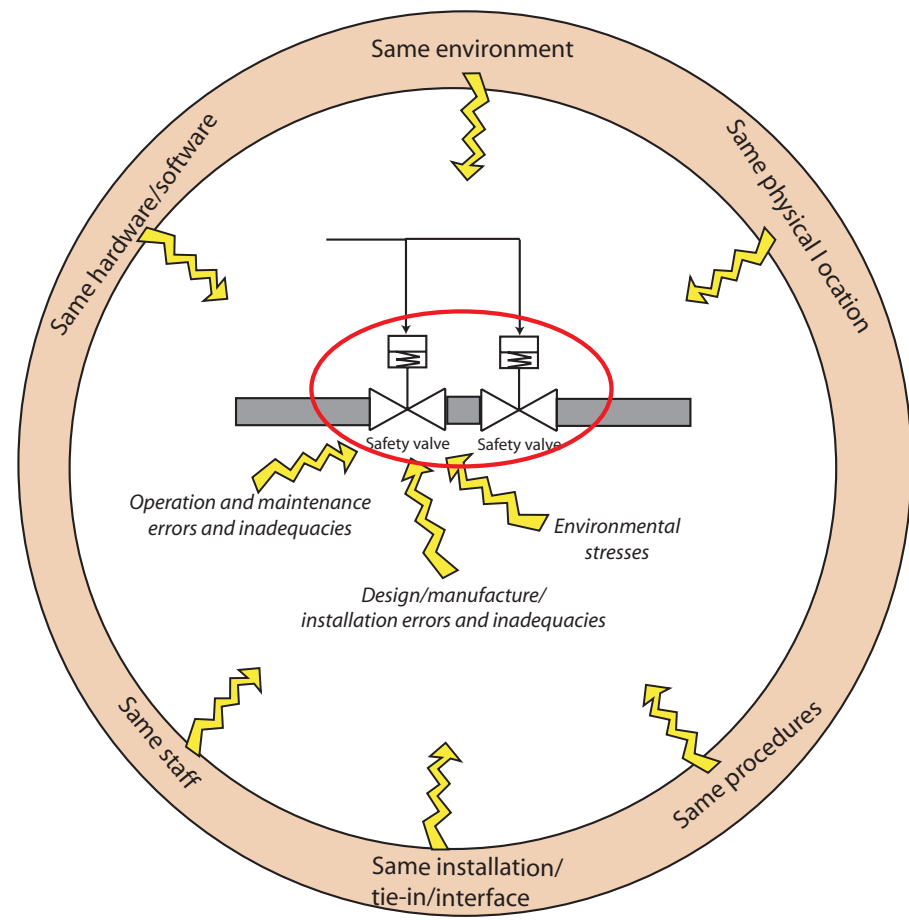
Coupling factor:

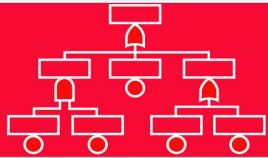
- Property that makes multiple components susceptible to the same root cause



Root causes versus coupling factors

- [Overview](#)
- [Background](#)
- [Context](#)
- [CCF threats](#)
- [Previous events](#)
- [Definitions](#)
- [Attributes](#)**
- [Examples](#)
- [Clarification](#)
- [Modeling approach](#)
- [CCF parameters](#)
- [Defenses](#)
- [New procedure](#)
- [Practical example](#)
- [Summing up](#)
- [Learnt anything?](#)





Typical root causes

Overview

Background

Context

CCF threats

Previous events

Definitions

Attributes

Examples

Clarification

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Summing up

Learnt anything?

We may distinguish between *pre-operational causes* and *operational causes*:

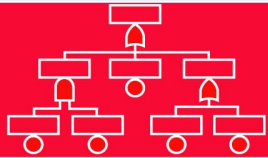
➤ Pre-operational causes:

➡ Design, manufacturing, construction, installation and commissioning errors

➤ Operational causes:

1. Operation and maintenance related: Inadequate maintenance and operation procedures, execution, competence and scheduling, or
2. Environmental related: Internal or external stress/exposure outside the design envelope

The typical root cause is *systematic* of nature. This means that the failure cause may only be corrected upon a modification to the design, implementation, manufacturing process, installation, commissioning, testing, operation, maintenance, documentation and so on.



Typical coupling factors

Overview

Background

Context

CCF threats

Previous events

Definitions

Attributes

Examples

Clarification

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Summing up

Learnt anything?

To look for coupling factors is the same as to look for similarities....

Hardware related:

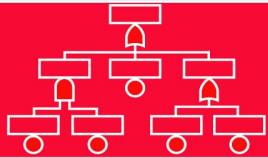
- Same/similar design principles, design procedure and practices, hardware, software

Operation related:

- Same/similar operation/maintenance/test schedule, procedures, staff

Environment related:

- Same/similar internal or external environment



Practical examples

Overview

Background

Context

CCF threats

Previous events

Definitions

Attributes

Examples

Clarification

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Summing up

Learnt anything?

- *Two level transmitters in a 1oo2 configuration are not able to raise an alarm upon high level due to a shared cause:*

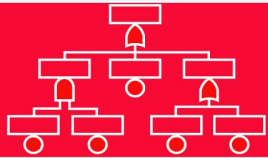
Root cause: e.g. a calibration error (causing the transmitters never to reach the trip set point, regardless of level)

Coupling factor: e.g using the same calibration procedure

- *Two pressure transmitters in a 2oo3 configuration are not able to detect a high pressure due to a shared cause:*

Root cause: e.g. plugged sensor lines (freezing or installation)

Coupling factor: e.g hooked up to the same heading (sensor lines), same type of installation/choice of dimensions/environment



Practical examples (continued)

Overview

Background

Context

CCF threats

Previous events

Definitions

Attributes

Examples

Clarification

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

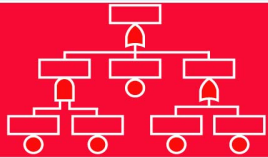
Summing up

Learnt anything?

- *Several gas detectors located in the same area are not able to detect a gas leakage due to a shared cause*

Root cause: e.g wrong location, inadequate detection principle (point versus line)

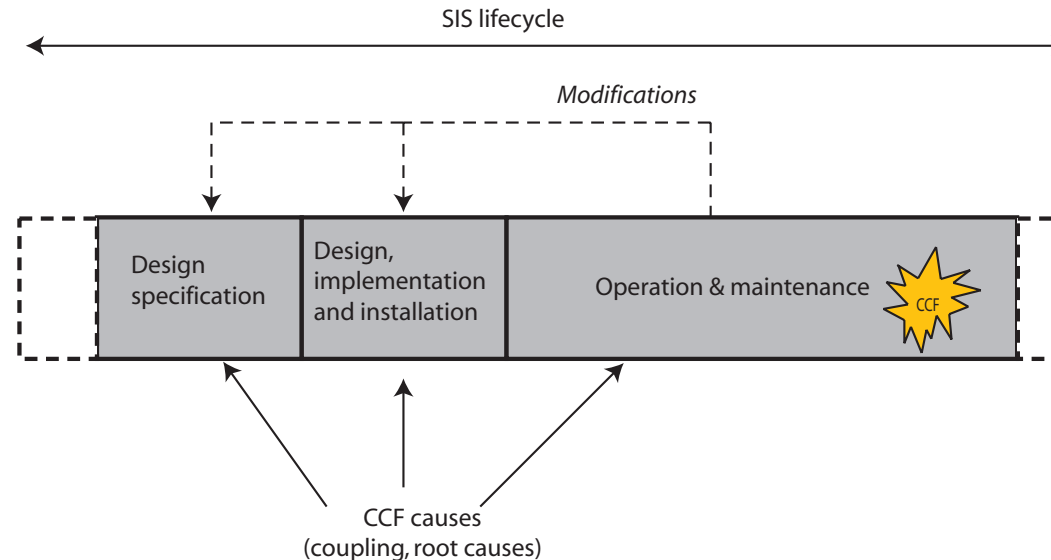
Coupling factor: e.g same design, same (too long) distance from the potential gas leakage points

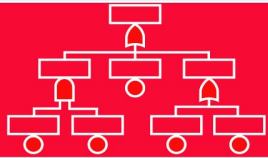


CCFs versus CCF causes

- Overview
- Background
- Context
- CCF threats
- Previous events
- Definitions
- Attributes
- Examples
- Clarification**
- Modeling approach
- CCF parameters
- Defenses
- New procedure
- Practical example
- Summing up
- Learnt anything?

- A CCF is an *event* occurring in the *operational phase*
- *CCF causes* may be introduced at any stage of the SIS life cycle
- CCF causes may be latent, and lead to a CCFs under certain conditions in th operational phase
- Discussion issue: Is a specification error a CCF cause?





Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

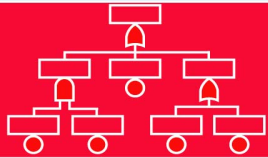
New procedure

Practical example

Summing up

Learnt anything?

Modeling approach



Why do we need to take CCFs into account

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

New procedure

Practical example

Summing up

Learnt anything?

1. CCFs dominate the unreliability

- When we have redundant components, the contribution from independent failures to the (average) Probability of failure on demand (PFD) is (usually) very small:

$$\Rightarrow \text{PFD}_{1002} = \frac{(\lambda\tau)^2}{3}$$

$$\Rightarrow \text{PFD}_{1003} = \frac{(\lambda\tau)^3}{4}$$

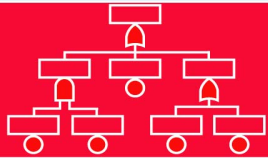
$$\Rightarrow \text{PFD}_{2003} = (\lambda\tau)^2$$

- A CCF may take down all components simultaneously (with a frequency of $\beta \cdot \lambda$), regardless of how much redundancy that has been implemented:

$$\Rightarrow \text{PFD}_{\text{CCF}} = \frac{(\beta\lambda\tau)}{2}$$

2. Authorities and mandatory standards require that CCFs are taken into account when estimating the SIS reliability:

- See e.g., IEC 61508, IEC 61511 and guideline OLF070 (www.olf.no) which all are referenced by the Norwegian Petroleum Authority.



Overall modeling approach

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

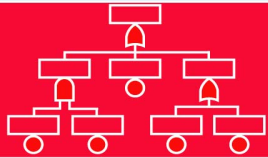
New procedure

Practical example

Summing up

Learnt anything?

1. Development of system logic models
2. Identification of *common cause component groups*
3. Update the system logic model with CCFs, by either (or both):
 - (a) Explicit modeling
 - (b) Implicit modeling
4. Determine the CCF reliability parameters



Two main modeling approaches

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

New procedure

Practical example

Summing up

Learnt anything?

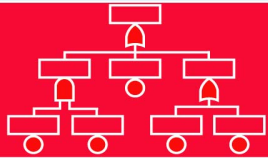
There are two main approaches:

Explicit:

- The CCF cause is rather evident and may be included in the reliability model as a separate basic event or functional block

Implicit:

- The failure causes are more complex, and are included in the reliability model on a “higher level”.



How to perform explicit modeling

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

New procedure

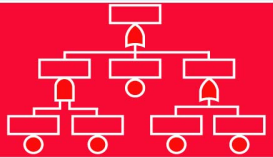
Practical example

Summing up

Learnt anything?

Explicit failure causes may be:

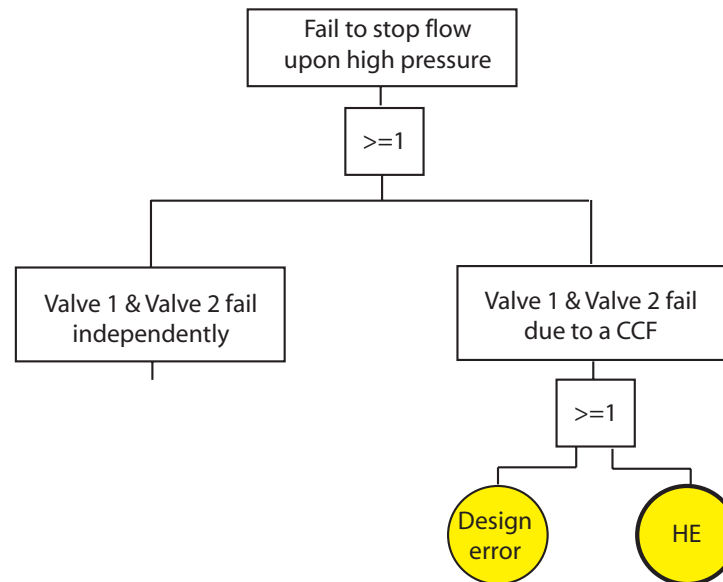
- Human errors
- Utility failures (e.g., electricity, hydraulic supply, pneumatic supply, cooling, heating, etc)
- Environmental events (e.g., earthquakes, lightning, etc)



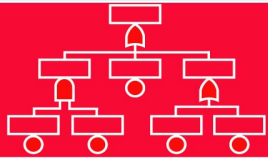
How to perform explicit modeling (continued)

- [Overview](#)
- [Background](#)
- [Modeling approach](#)
- [Why?](#)
- [Steps](#)
- [Approaches](#)
- [Explicit](#)**
- [Implicit](#)
- [CCF parameters](#)
- [Defenses](#)
- [New procedure](#)
- [Practical example](#)
- [Summing up](#)
- [Learnt anything?](#)

One alternative may be to use the fault trees:



- Pros: Failure causes more precisely modeled
- Cons: One basic event per root cause, often difficult to find data for each one.



How to perform implicit modeling

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

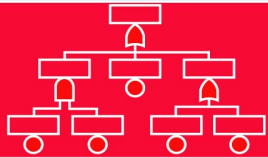
New procedure

Practical example

Summing up

Learnt anything?

- Implicit modeling is often used when the CCF cause is more complex or compounded (residual causes);
- In this situation, explicit modeling may result in overwhelming models
- For example:
 - Two valves may fail simultaneously due to improper maintenance, which may comprise several elements (human errors, incomplete procedures, lack of proper training etc)



How to perform implicit modeling

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

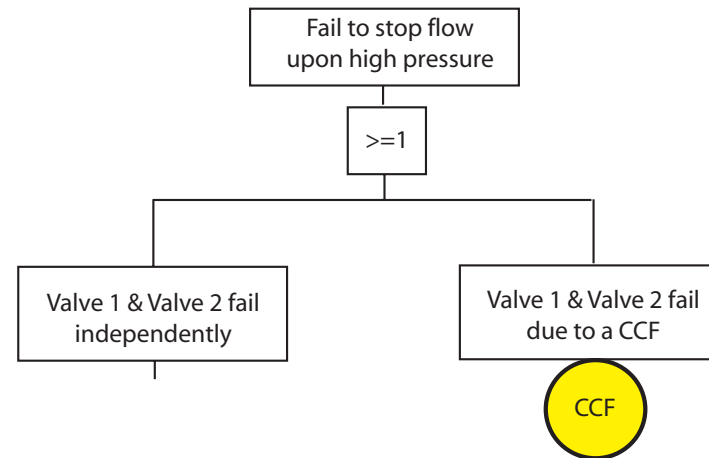
New procedure

Practical example

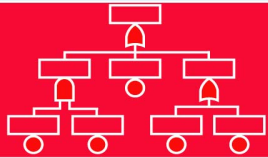
Summing up

Learnt anything?

One alternative may be to use the fault trees:



- Pros: Simplifies the modeling
- Cons: It is not so straight forward to determine the CCF “parameter”. So we need some models...



How to perform implicit modeling

[Overview](#)

[Background](#)

[Modeling approach](#)

[Why?](#)

[Steps](#)

[Approaches](#)

[Explicit](#)

[Implicit](#)

[CCF parameters](#)

[Defenses](#)

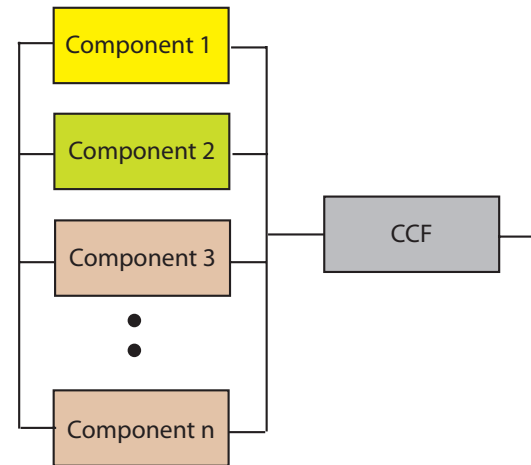
[New procedure](#)

[Practical example](#)

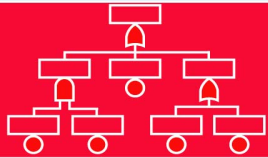
[Summing up](#)

[Learnt anything?](#)

Another alternative is to use reliability block diagrams:



This approach also applies to explicit modeling.



Several implicit modeling approaches exist

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

New procedure

Practical example

Summing up

Learnt anything?

Several approaches exist for implicit modeling:

➤ Non-shock models:

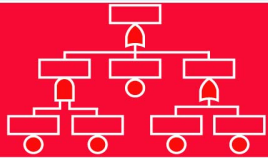
- Basic parameter model
- Beta factor (BF) model *
- Alpha factor model
- Square root model
- Multiple Greek Letter (MGL)model
- Multiple beta-factor (MBF) model *
- C-factor model

➤ Shock-models:

- Binomial failure rate model (BFR)

Note:

- The implicit modeling approaches are also referred to as “parametric models”.
- *) These models are discussed further in the following



Non-shock versus shock models

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

New procedure

Practical example

Summing up

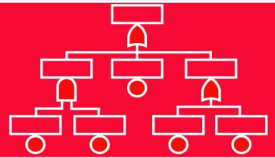
Learnt anything?

➤ Shock models:

- ➡ The contribution from CCFs is *added* to the random failure rate (λ) and is modelled as a product of:
 - ➔ The frequency of shocks (*failure process*)
 - ➔ The conditional probability of failure given a shock
- ➡ The shock models allows combinations of multiple failures

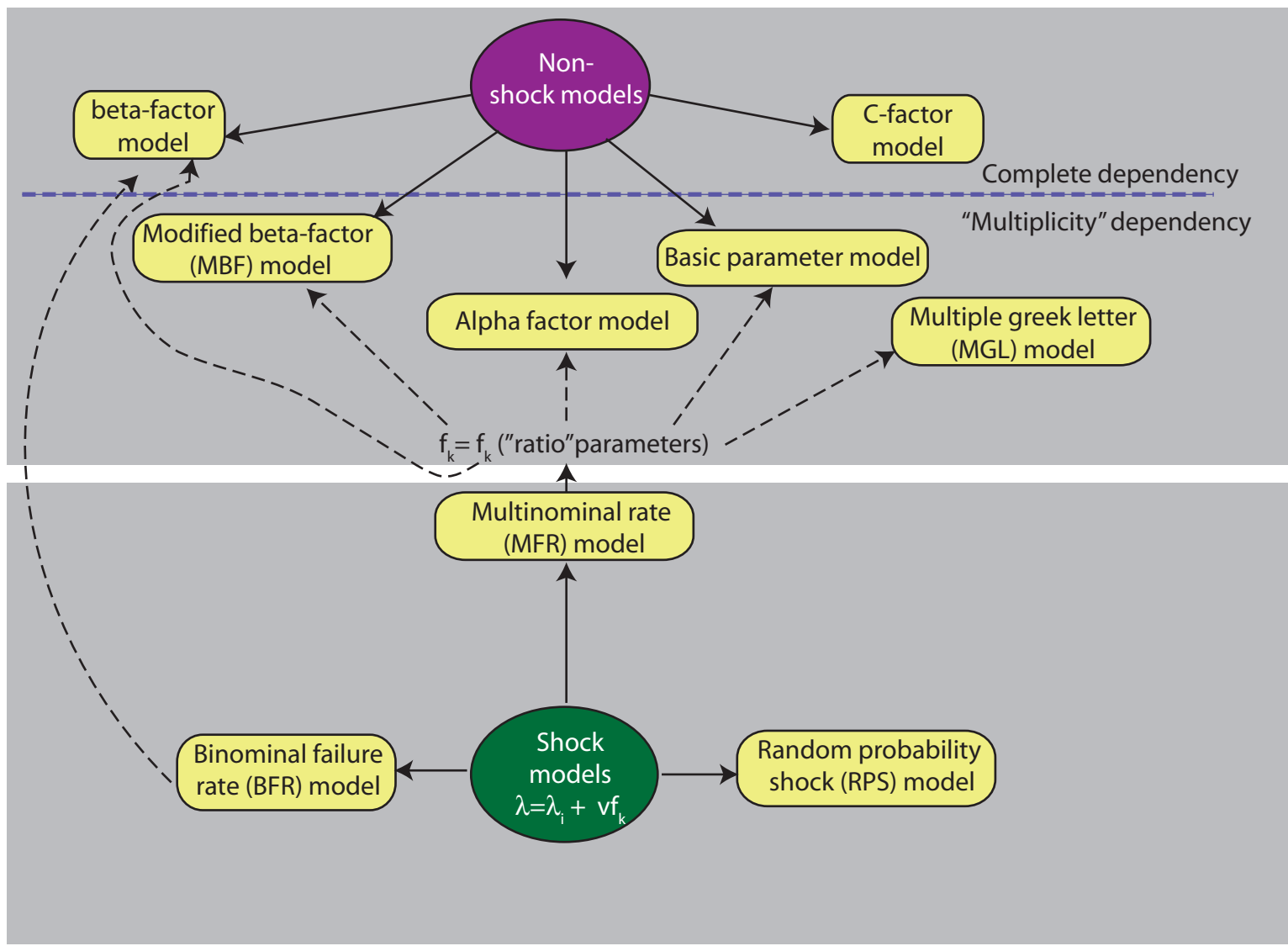
➤ Non-shock models:

- ➡ The contribution from CCFs is derived from probability/fraction estimates of having $k=2,3,\dots,n$ failures

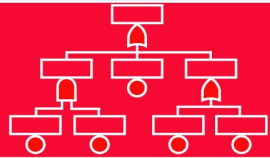


Non-shock versus shock models

- Overview
- Background
- Modeling approach
- Why?
- Steps
- Approaches
- Explicit
- Implicit**
- CCF parameters
- Defenses
- New procedure
- Practical example
- Summing up
- Learnt anything?

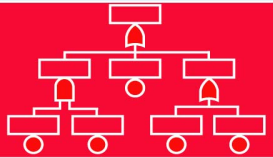


Short version comparison of (some) implicit models



- Overview
- Background
- Modeling approach
- Why?
- Steps
- Approaches
- Explicit
- Implicit**
- CCF parameters
- Defenses
- New procedure
- Practical example
- Summing up
- Learnt anything?

Model	Characteristics
Basic parameter model	The events $Q_k^{(m)}$ are <i>mutually exclusive</i> - which is seldom the case
Beta factor model	CCF events and single failure events are <i>independent</i> Introduces a β -factor β is a fraction of the total (dangerous) failure rate If a CCF event occur, then <i>all</i> components fail simultaneously
MGL model	Extension of the beta-factor model Introduces γ and δ to capture events where not all components fail simultaneously
MBF model	Extension of the beta-factor model Introduces β_k and C_{k00n} to capture events where not all components fail simultaneously
C-factor model	Introduces a C-factor which is similar to the beta-factor model However; the C-factor is a fraction of the independent failure rate



The beta-factor model

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

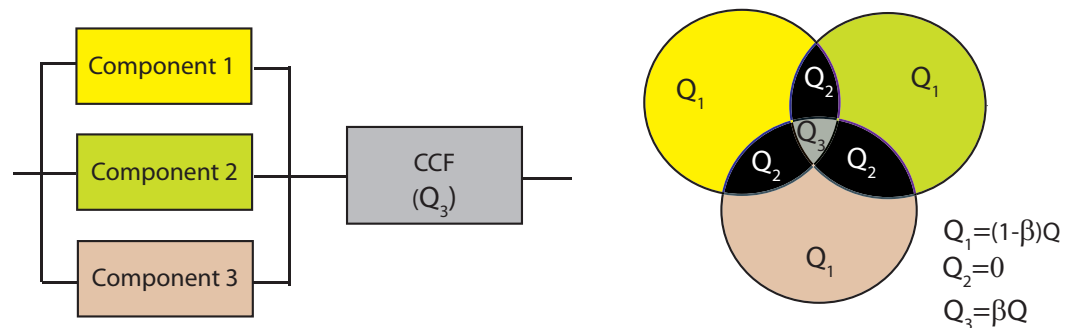
New procedure

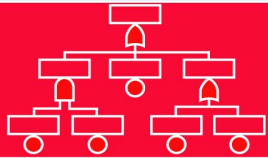
Practical example

Summing up

Learnt anything?

- Failure rate is allocated to an independent part and a dependent part:
 - ➡ $\lambda = (1 - \beta)\lambda + \beta \cdot \lambda$
- Here, it is always assumed simultaneous failure of all redundant components.





The beta-factor (BF) model

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

New procedure

Practical example

Summing up

Learnt anything?

The PFD may, for a 2oo3 configuration, be estimated in (at least) two ways (does only consider DU-failures, not DD):

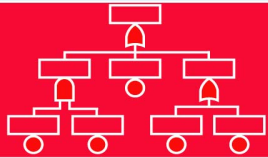
- Alternative I:

$$\text{PFD} = [(1 - \beta)\lambda\tau]^2 + \frac{\beta\lambda\tau}{2}$$

- Alternative II (IEC 61508-6):

$$\begin{aligned}\text{PFD} &= 3 \cdot [(1 - \beta)\lambda] \cdot t_{\text{CE}} \cdot 2 \cdot [(1 - \beta)\lambda] \cdot t_{\text{GE}} \\ &+ \beta\lambda \cdot t_{\text{CE}} \\ &= 6[(1 - \beta)\lambda]^2 t_{\text{CE}} t_{\text{GE}} + \beta\lambda \cdot t_{\text{CE}}\end{aligned}$$

- Downtime per channel: $t_{\text{CE}} = \frac{\tau}{2} + \text{MTTR}$
- Downtime of two parallel channels: $t_{\text{GE}} = \frac{\tau}{3} + \text{MTTR}$



The modified beta-factor (MBF) model

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

New procedure

Practical example

Summing up

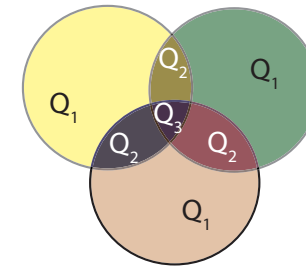
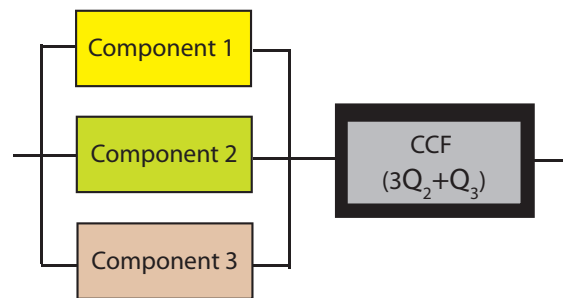
Learnt anything?

- Independent and dependent part “modified”
- New β_k parameters are introduced in addition to the β -factor. For a configuration of three redundant components (note: In this example, we have omitted the contribution from independent failures):

➤ $\beta_2 = \Pr(\text{3rd component fails} \mid \text{Component 1 and 2 have already failed})$

➤ $\text{PFD}_{\text{koon}} = C_{\text{koon}} \cdot \beta \cdot \text{PFD}$

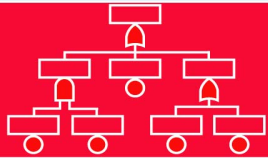
- The β_2 is used to “calibrate” the correction factor C_{koon} :



$$Q_1 = Q - [2(1-\beta_2)\beta Q + \beta_2\beta Q] = [1 - (2-\beta_2)\beta]Q$$

$$Q_2 = (1-\beta_2)\beta Q$$

$$Q_3 = \beta_2\beta Q$$



The MBF model applied for a 2oo3 configuration

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

New procedure

Practical example

Summing up

Learnt anything?

The SIF fails if two or more component fail (tolerates *one* component failure):

➤ $\text{PFD}_{2oo3,CCF} = f_{2,3} + f_{3,3}$

➤ where

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

⇒ $f_{3,3} = \beta_2\beta \cdot Q$

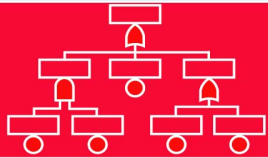
⇒ $f_{2,3} + f_{3,3} = (3 - 2\beta_2)\beta \cdot Q$

➤ which means that:

⇒ $C_{2oo3} = (3 - 2\beta_2)$

⇒ $\text{PFD}_{2oo3,CCF} = (3 - 2\beta_2)\beta Q$

➤ Note: Here we have only considered CCFs. We may still want to show the independent part (as we did with the beta-factor model).



The multiple greek letter (MGL) model

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

New procedure

Practical example

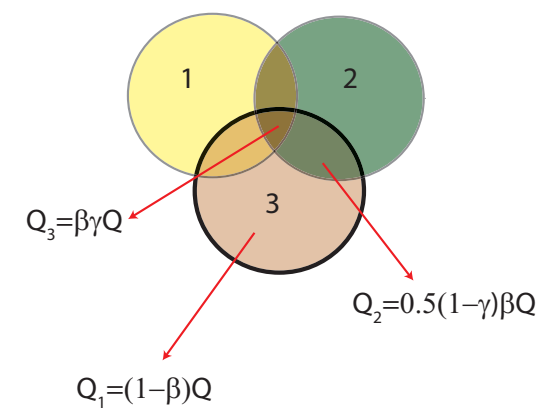
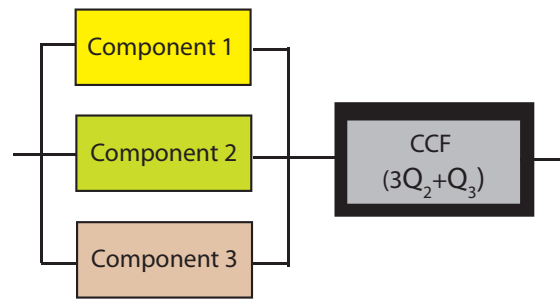
Summing up

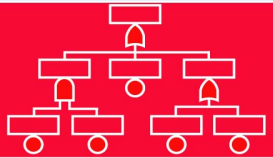
Learnt anything?

- Also an extension of the beta-factor model.
- As with the MBF model, the MGL also introduces additional parameters (γ and δ) to cater for the various CCF combinations
- The parameters used are defined as:
 - ➡ $\beta = \Pr(\text{A failure} \mid \text{the failure cause is shared by } \textit{at least one additional} \text{ component})$
 - ➔ Which is the same as the fraction of double and triple failures to the total number of failures (if three components are involved)
 - ➡ $\gamma = \Pr(\text{A failure} \mid \text{the failure cause is shared by } \textit{at least two additional} \text{ components})$
 - ➔ Which is the same as the fraction of triple failures to the total number of failures (if three components are involved)

The multiple greek letter (MGL) model

- Overview
- Background
- Modeling approach
- Why?
- Steps
- Approaches
- Explicit
- Implicit**
- CCF parameters
- Defenses
- New procedure
- Practical example
- Summing up
- Learnt anything?





Confused? MBF versus MGL model (2oo3 configuration)

Overview

Background

Modeling approach

Why?

Steps

Approaches

Explicit

Implicit

CCF parameters

Defenses

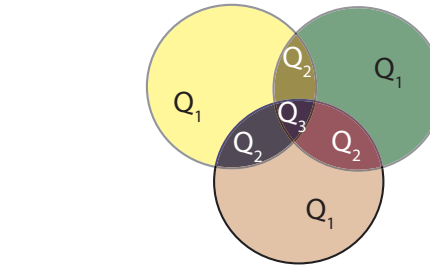
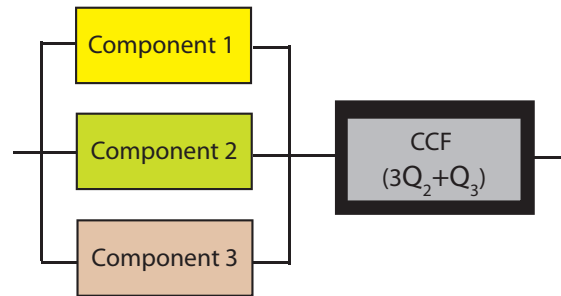
New procedure

Practical example

Summing up

Learnt anything?

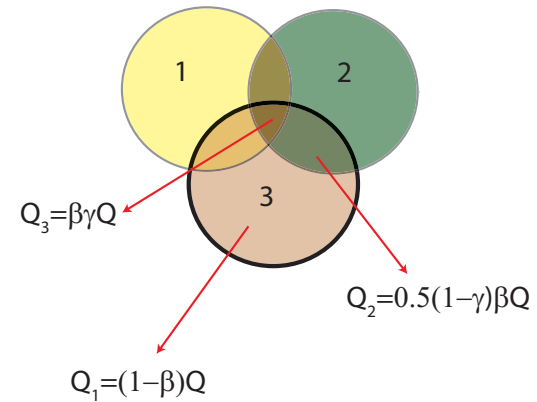
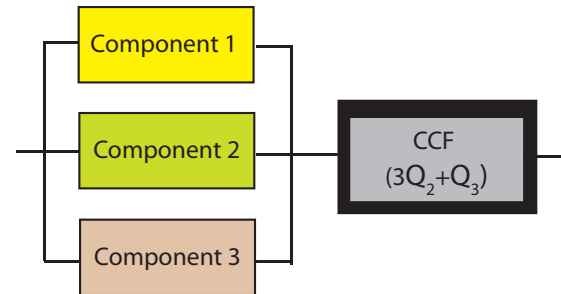
I am....:

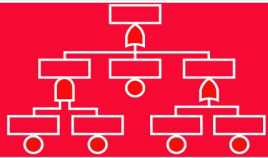


$$Q_1 = Q - [2(1-\beta_2)\beta Q + \beta_2\beta Q] = [1 - (2-\beta_2)\beta]Q$$

$$Q_2 = (1-\beta_2)\beta Q$$

$$Q_3 = \beta_2\beta Q$$





Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

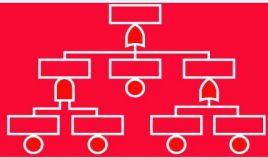
New procedure

Practical example

Summing up

Learnt anything?

CCF parameters



Determine an (initial) value of β

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

New procedure

Practical example

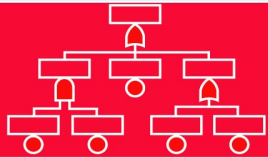
Summing up

Learnt anything?

In the design phase, it is necessary to select β for each common cause component group in order to perform the reliability calculations. Here several approaches may be applied:

1. **Expert judgments:** See the OLF 070 guideline or the PDS data handbook *)
2. **Checklists:** Alternatives will be presented in more details*)
3. **Models:** Using e.g., influence diagrams
4. **Using historical data:** Analyzing historical failure reports or databases (like e.g. OREDA) and determine how many failures that may be CCFs for different type of components

*)Now we are talking about the β -factor in the standard BF model and the MBF model.



Using expert judgments

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

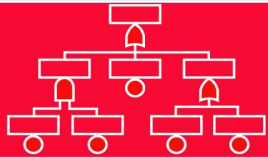
New procedure

Practical example

Summing up

Learnt anything?

- Expert judgment provides “generic” β -factors
- This means that they are based on the experts *belief*
- Data may be collected through e.g. work shops where experts are gathered to discuss and agree upon “representative” values.
- Pros: Easy to apply
- Cons: Does not consider plant specific conditions



Using checklists

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

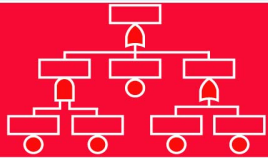
New procedure

Practical example

Summing up

Learnt anything?

- Several alternative checklists exist
 - IEC 61508-6*
 - Humphrey*
 - Partial beta-factor model
 - Betapluss (commercial product)
 - Pros: Requires some more work to apply
 - Cons: Provides more plant specific values
- *) We will look closer at these ones in lecture



The checklist in IEC 61508-6

[Overview](#)

[Background](#)

[Modeling approach](#)

[CCF parameters](#)

[Approaches](#)

[Experts](#)

[Checklists](#)

[Models](#)

[Events](#)

[Updating](#)

[Defenses](#)

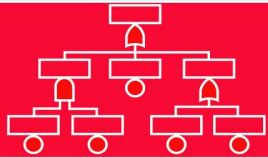
[New procedure](#)

[Practical example](#)

[Summing up](#)

[Learnt anything?](#)

- This is a rather comprehensive checklist (nearly 40 questions) (view excel sheet)
- Logic solvers and field equipments are assessed separately
- For all questions given the answer “yes”; The corresponding X values and Y values are summed up.
- A table is provided to determine the corresponding β for the $\sum(X_i + Y_i)$
- Provides a β -factor between 0.5% and 5% (logic solvers) and 1% and 10% for final elements/sensors.



Checklist in the IEC 61508-6

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

New procedure

Practical example

Summing up

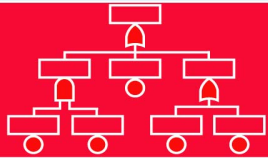
Learnt anything?

Pros:

- Provides a plant (or design) specific β :

Cons:

- Many of the questions are ambiguous or difficult to answer by even SIS designers, e.g.,:
 - *Are all devices/components conservatively rated (for example, by a factor of 2 or more)?*
 - *Does the system diagnostic tests report failures to the level of a replaceable module?*
- Several questions ask for practices that are not common for SIS design at least in the oil and gas industry, e.g.,:
 - *Do the channels employ different electrical technologies for example, one electronic or programmable electronic and the other relay?*
 - *Are separate test method and people used for each channel during commissioning?*



Checklist in the IEC 61508-6 (example)

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

New procedure

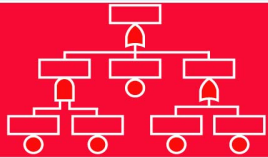
Practical example

Summing up

Learnt anything?

A single improvement is usually not sufficient to improve the β factor, so what ever you do you get a “1” or a “2”...

- Each question ($X_i + Y_i$) provides usually between 1 and 3 points.
- Example:
 - ➡ If I have have obtained 58 points for my logic solver (corresponding to a β -factor of 2%, and I would like to improve it to 1%, I would need to make 4 to 12 improvements.
 - ➡ This means that - single improvements (normally) does not have any effect on the β - factor



Checklist by Humphreys

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

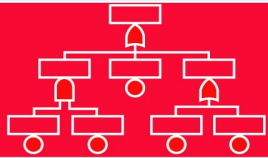
New procedure

Practical example

Summing up

Learnt anything?

- Less comprehensive (and perhaps easier to use) checklist than IEC 61508-6 (show excel sheet)
- Some guidance to each checklist question is provided in the article by R.A. Humphreys (1987)
- Provides a β -factor between 0.1% and 30%
 - *...the latter is perhaps a too high value nowadays, on the other hand; if the worst scores applies, then the design may not deserve any better...*
- The “average design” gives a $\beta \approx 5\%$ which is a little higher than the average value obtained by IEC 61508-6 for a similar SIS design
- Pros: Easier to use, more sensitive to single improvements
- Cons: Perhaps is the scaling up to 30% is too conservative?



Partial beta factor model (Johnston, B.D. (1987))

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

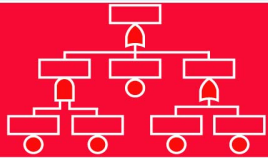
New procedure

Practical example

Summing up

Learnt anything?

- Less comprehensive checklist than IEC 61508-6 (show excel sheet)
- A so called “Perturbation” analysis
- The values assigned each questions are multiplied
- The result after multiplication is not evident: $\lambda\beta$ or β)



Partial beta factor model (continued)

[Overview](#)

[Background](#)

[Modeling approach](#)

[CCF parameters](#)

[Approaches](#)

[Experts](#)

[Checklists](#)

[Models](#)

[Events](#)

[Updating](#)

[Defenses](#)

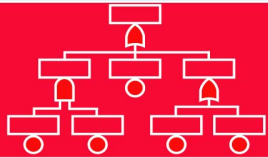
[New procedure](#)

[Practical example](#)

[Summing up](#)

[Learnt anything?](#)

- Unclear how the author defines the failure rate (failures per hour or failures per years)
- If failure rate is given as failures per hour (using 1E-6):
 - ➡ Provides an incorrect range of β values: 10 for a typical SIS design and 100 as the reference
- If failure rate is gives as failures per year (8.8E-3):
 - ➡ Provides a β values: 0.10 (10%) as reference and 4% for a typical SIS design
 - ➡ This looks ok, but if we look at some extremes (all low or all high) the range of β is from 1E-17 to 15.
 - ➡ So it is still something strange about the method...



Unified partial model (Brand P.V (AEA report 1996), Zitrou/Bedford (2003, 2004))

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

New procedure

Practical example

Summing up

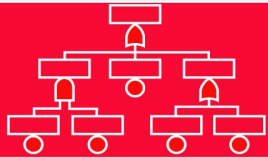
Learnt anything?

- Developed for the British nuclear power industry
- Based on the beta factor model
- The β is estimated as follows:

$$\Rightarrow \beta = \frac{s_1(x_{1i}) + \dots + s_8(x_{1i})}{d}$$

⇒ $d > 0$ is a scaling factor

Unified partial model - extension (Zitrou/Bedford (2003, 2004))



Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

New procedure

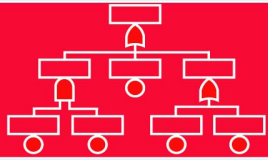
Practical example

Summing up

Learnt anything?

- Argue that the UPM model fails to take existing interactions among defenses into account
 - ➡ e.g., If we have performed a very good analysis in the design process, we may not gain so much (additional) improvements by investing in more diversity.
 - ➡ The reason is that most of the failure causes typically avoided by having diversity, are already detected during the analysis and removed.
- The authors suggest using *influence diagrams* in combination with *functional interactions table* to determine *conditional scores*

Analyzing historical events and thereby find a β



Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

New procedure

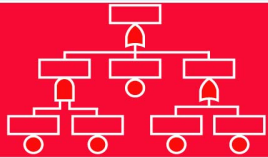
Practical example

Summing up

Learnt anything?

➤ Data sources:

- Few data sources available
- To a large extent they are from the nuclear industry
 - ➔ ICDE data base (ICDE = International Common Cause Failure Data Exchange)
 - ➔ SKI data reports (SKI = Statens Kernkraft Inspektion)
- The oil and gas industry does not collect CCFs. However, they may in the future, due to the recommendations in the new version of ISO 14224 (on data collection and exchange)



The β may be updated to reflect plant specific conditions

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

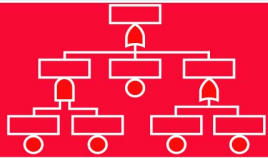
New procedure

Practical example

Summing up

Learnt anything?

- In the operational phase, one may want to update (e.g. to take credit for improvements) the β parameter (for each group of components)
- Some approaches have been suggested:
 - The PDS approach
 - Use checklists (that were previously presented) and see if any improvements leads to an improvement in the β
 - Count events and insert into a *β -estimator equation*



The PDS approach

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

New procedure

Practical example

Summing up

Learnt anything?

There are also two alternative approaches presented in the PDS method:

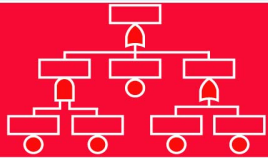
➤ The “simple” approach: Correcting the β by k_β

$$\Rightarrow \beta^* = k_\beta \cdot \beta$$

➤ The “extended” method: Adding another correction factor k_S

$$\Rightarrow \beta^{**} = k_S \cdot k_\beta \cdot \beta$$

*) Will be discussed in more detail during lecture



Using the checklists

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

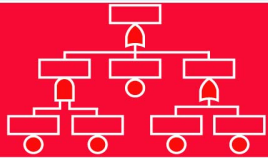
New procedure

Practical example

Summing up

Learnt anything?

Here we refer back to the previous mentioned methods



Counting events and using β -estimator equations

[Overview](#)

[Background](#)

[Modeling approach](#)

[CCF parameters](#)

[Approaches](#)

[Experts](#)

[Checklists](#)

[Models](#)

[Events](#)

[Updating](#)

[Defenses](#)

[New procedure](#)

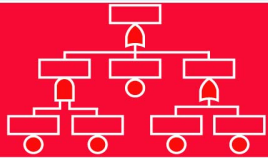
[Practical example](#)

[Summing up](#)

[Learnt anything?](#)

Here, we may choose a “rough” approach or a “comprehensive” approach

- The rough approach:
- The (rather) comprehensive approach:
- The even more comprehensive approach:



Using estimators - the rough approach

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

New procedure

Practical example

Summing up

Learnt anything?

➤ The rough approach:

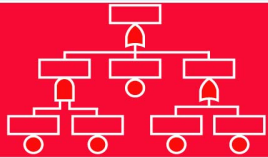
$$\Rightarrow \hat{\beta} = \frac{\text{The number of CCF events for a group of similar/same equipment}}{\text{All (dangerous) failures recorded for the same equipment}}$$

➤ Example:

➤ We observe one CCF in a period of 1 year for (safety critical) level transmitters. In the same period we observed 5 other dangerous failures. We have all together 20 level transmitters at the installation.

➤ Then $\hat{\beta} = \frac{1}{5} = 20\%$

➤ Is this a very polite result? Note that the number of components observed and the observation time is irrelevant here...



Using estimators - the rather comprehensive approach

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

New procedure

Practical example

Summing up

Learnt anything?

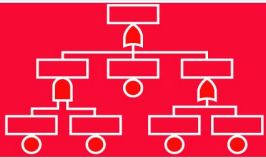
- The (rather) comprehensive approach:

$$\Rightarrow \hat{\beta} = \frac{\sum_{j=2}^n j \cdot X_{j,n}}{\sum_{j=1}^n j \cdot X_{j,n}}$$

- Example: *5 events involving one channel, 1 event involving two channels, 0 events involving three channels*

$$\Rightarrow \hat{\beta} = \frac{2 \cdot 1 + 3 \cdot 0}{1 \cdot 5 + 2 \cdot 1 + 3 \cdot 0} = 28\%$$

- Is this result better? Also here, the result is independent of the number of components observed and the observation time.



Using estimators - the comprehensive approach

Overview

Background

Modeling approach

CCF parameters

Approaches

Experts

Checklists

Models

Events

Updating

Defenses

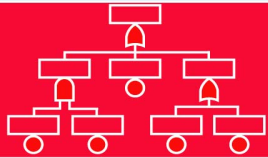
New procedure

Practical example

Summing up

Learnt anything?

- The even more comprehensive approach:
 - Using Bayesian method with prior and posterior distribution:
 1. We may estimate a $\lambda_{c,init} = \beta_{init} \cdot \lambda_{BE}$
 2. Then we may update the $\lambda_{c,init}$ which we may refer to as $\hat{\lambda}_c = \frac{\alpha+x}{\delta+t}$
 3. And find how $\hat{\lambda}_c$ has changed relative to the initial value
 4. And eventually allocate the increase or decrease to the β
 - One may also apply a more *sophisticated* updating of the $X_{j,n}$ based on impact vectors and hypothesis (see articles by Mosleh for more information)



The more comprehensive approach (example)

[Overview](#)

[Background](#)

[Modeling approach](#)

[CCF parameters](#)

[Approaches](#)

[Experts](#)

[Checklists](#)

[Models](#)

[Events](#)

[Updating](#)

[Defenses](#)

[New procedure](#)

[Practical example](#)

[Summing up](#)

[Learnt anything?](#)

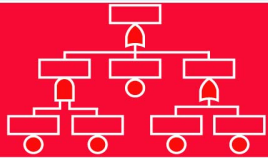
- Example: Make a calculation with $\lambda_{c,init} = 0.6E-6$ and $\beta_{init} = 0.1$. We assume that we observe one failure over an observation period of one year (or 8760 hours). Here we must, in addition to the observation time, also consider the number of components observed (which we assume is 20).

- We then get:

$$\Rightarrow \hat{\lambda}_c = \frac{0.6+1}{10^6+8760 \cdot 20} = 1.4 \cdot 10^{-6}$$

$$\Rightarrow \hat{\beta} = \beta_{init} \cdot \frac{\hat{\lambda}_c}{\lambda_{c,init}} = 0.22 \text{ (or 22\%)}$$

- Here $\frac{\hat{\lambda}_c}{\lambda_{c,init}}$ is used as a "correction factor"
- Perhaps a more polite result?



Overview

Background

Modeling approach

CCF parameters

Defenses

Approaches

Avoiding

Revealing

Improving

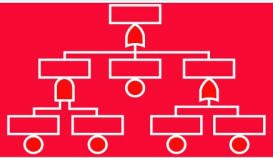
New procedure

Practical example

Summing up

Learnt anything?

Defenses



How may we defend against CCFs?

Overview

Background

Modeling approach

CCF parameters

Defenses

Approaches

Avoiding

Revealing

Improving

New procedure

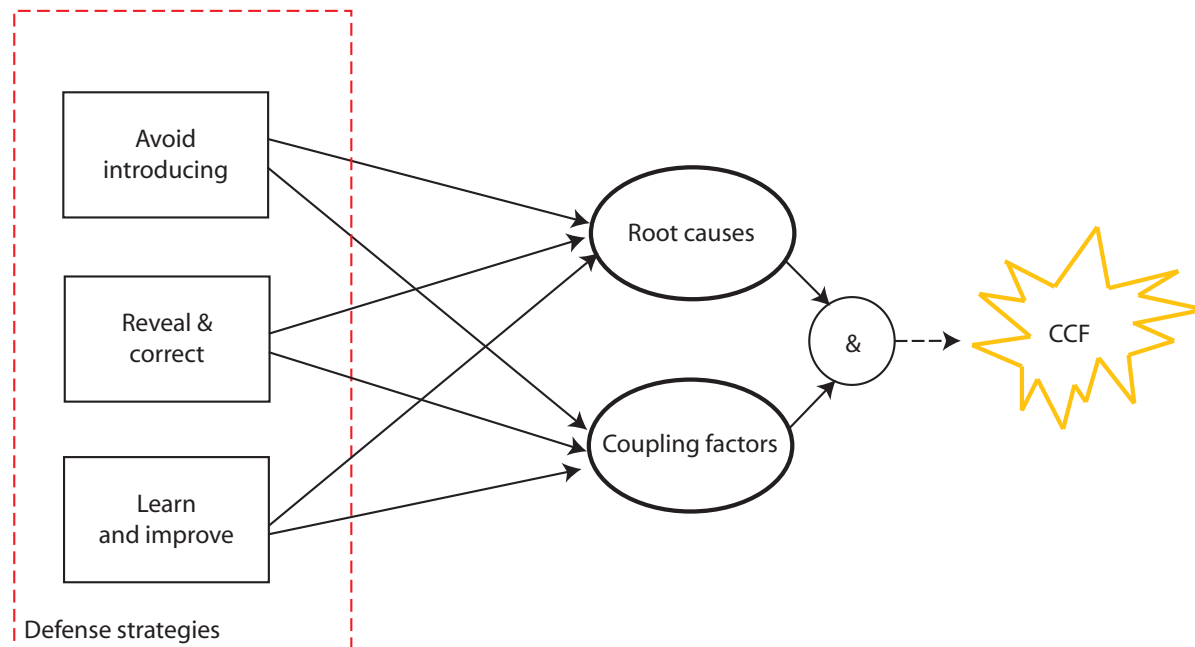
Practical example

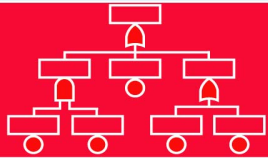
Summing up

Learnt anything?

Three main approaches:

1. **Avoid** introducing CCFs (proactive)
2. **Reveal and correct** CCFs (corrective)
3. **Learn and improve** (proactive)





Avoid introducing prior to operation

[Overview](#)

[Background](#)

[Modeling approach](#)

[CCF parameters](#)

[Defenses](#)

[Approaches](#)

[Avoiding](#)

[Revealing](#)

[Improving](#)

[New procedure](#)

[Practical example](#)

[Summing up](#)

[Learnt anything?](#)

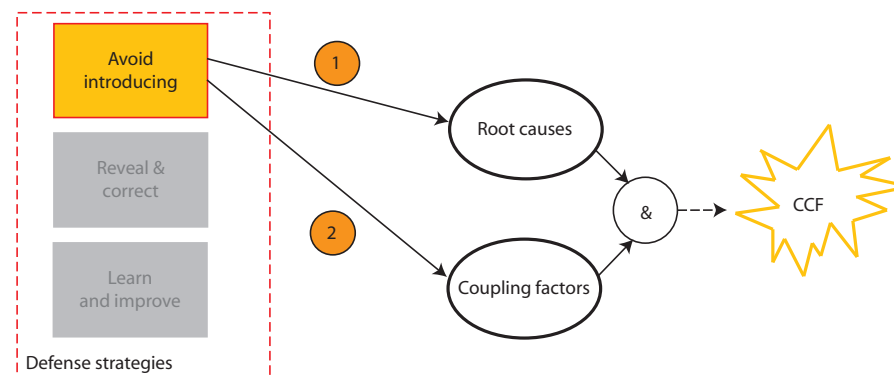
The best approach is perhaps to avoid introducing them...

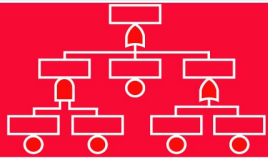
1. Avoid introducing root causes:

- e.g., Quality assurance, reviews, checklists, FMECA, HAZOP, training and competence, adequate tools and aids, and selection of "proven in use" or fit for purpose technology

2. Avoid introducing coupling factors in:

- Physical design (physical or functional separation/protection of redundant components and systems or using diverse technology)
- Work processes (using e.g. different staff for installation and testing, and different staff for implementation of different systems)





Avoid introducing in operation

Overview

Background

Modeling approach

CCF parameters

Defenses

Approaches

Avoiding

Revealing

Improving

New procedure

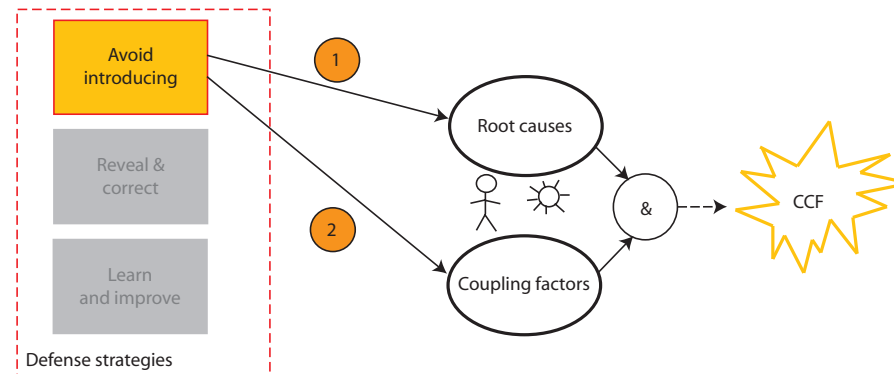
Practical example

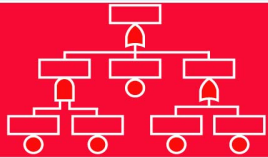
Summing up

Learnt anything?

In the operational phase, the SIS design is “set”. So here, the main focus is to avoid failures from:

- ‘Operation and maintenance activities (“Human exposure”)
- Environmental exposure





Avoid introducing in operation

Overview

Background

Modeling approach

CCF parameters

Defenses

Approaches

Avoiding

Revealing

Improving

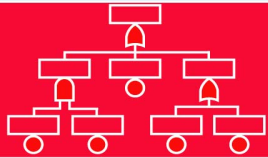
New procedure

Practical example

Summing up

Learnt anything?

1. Avoid introducing root causes:
 - e.g., Ensure unambiguous procedures, adequate preparation and restoration, adequate training and competence, appropriate tools, unambiguous responsibility
2. Avoid introducing coupling factors by:
 - Reducing coupling in work activities, for example use different function test procedures for similar components belonging to different SIS (e.g. PSD and ESD)
 - Having different schedule for function testing and inspection of similar components in different SIS
 - Ensure that also minor modifications to SIS are checked for potentially *new* couplings
 - Verify that environmental and operational conditions remain within the specified limits



Reveal and correct prior to operation

Overview

Background

Modeling approach

CCF parameters

Defenses

Approaches

Avoiding

Revealing

Improving

New procedure

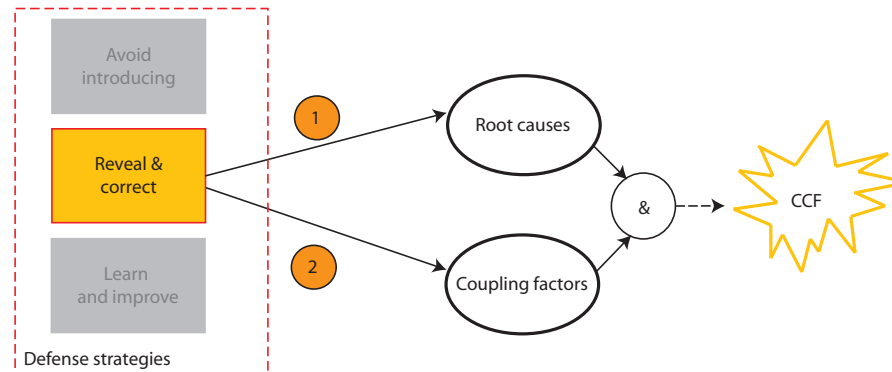
Practical example

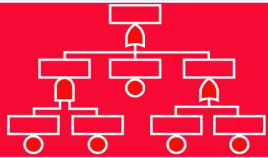
Summing up

Learnt anything?

Defenses relevant for root causes (1) as well as coupling factors (2):

- Consider CCFs during design reviews, FMECA, HAZOP, audits
- Perform tests in several stages (unit tests, integration tests, site tests) and inspections
- Implement tracking and follow-up systems (to follow-up any findings)



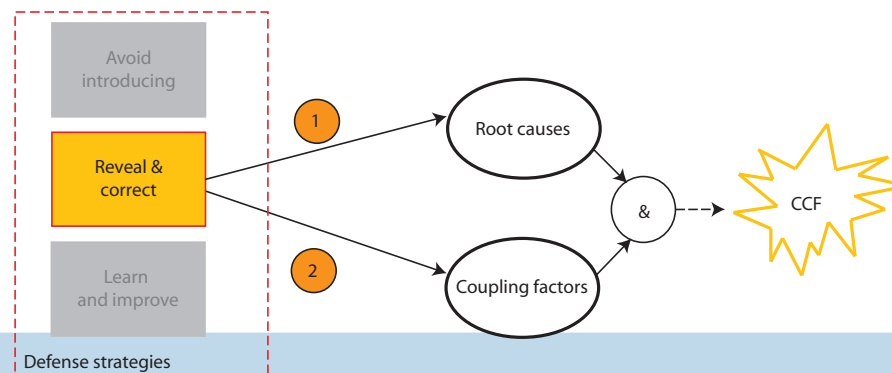


Reveal and correct in operation

- Overview
- Background
- Modeling approach
- CCF parameters
- Defenses
- Approaches
- Avoiding
- Revealing**
- Improving
- New procedure
- Practical example
- Summing up
- Learnt anything?

Defenses relevant for root causes (1) as well as coupling factors (2):

- Monitor and verify (by automatic means or by inspections) environmental and operational conditions
- Address potential CCF causes and coupling factors in relevant function test, inspection and repair procedures
- Review failure records to identify CCF events, and analyse root causes and coupling factors as basis for selecting appropriate measures that may prevent similar failures in the future
- Ensure that all failures revealed are followed up and corrected
- Ensure adequate experience transfer between different plants/installations, crews etc on CCF events



“Learn and improve”

Overview

Background

Modeling approach

CCF parameters

Defenses

Approaches

Avoiding

Revealing

Improving

New procedure

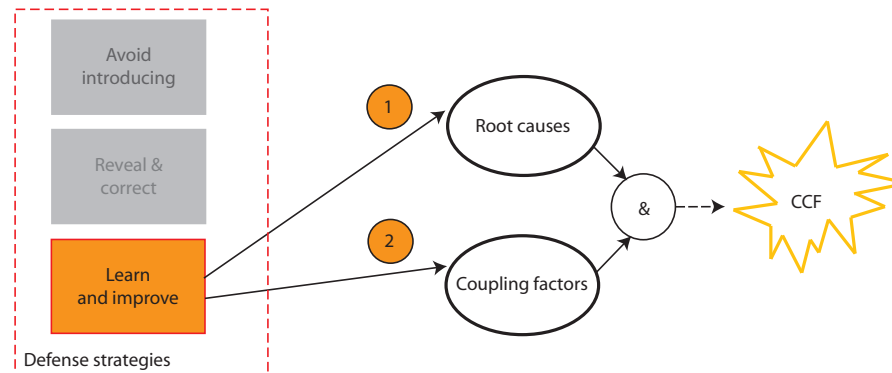
Practical example

Summing up

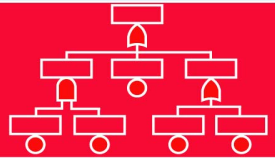
Learnt anything?

Some examples are:

- Validate procedures and practices:
 - ➡ Are they adequate and unambiguous? Are also restoration and preparation sufficiently addressed?
- Increase awareness to CCF causes:
 - ➡ Have CCFs and CCF causes been discussed with relevant plant personnel and personnel responsible for follow-up of SIS?

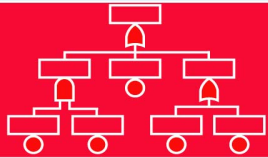


“Learn and improve” (continued)



- Overview
- Background
- Modeling approach
- CCF parameters
- Defenses
- Approaches
- Avoiding
- Revealing
- Improving**
- New procedure
- Practical example
- Summing up
- Learnt anything?

- Record failure history properly:
 - ➡ Do the failure reports provide necessary information to identify CCF events and CCF causes?
- Verify that implemented defenses are efficient:
 - ➡ Is it possible to monitor the effect of defenses (quantitatively or qualitatively)?
- Ensure feedback on CCF to new projects/modification projects
 - ➡ Do the plant or company have in place a system for experience transfer of CCF events (internally and with relevant vendors and suppliers)?



Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

Further

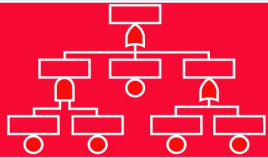
improvements

Practical example

Summing up

Learnt anything?

New procedure



Implemented defenses through function testing

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

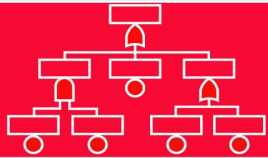
Further improvements

Practical example

Summing up

Learnt anything?

- Based on an article by Lundteigen and Rausand (accepted for the Journal of Loss Prevention in the Process industries)
- Suggests an overall approach to defend against CCFs during function testing and follow-up
- Cover the main ways of defending against CCFs:
 - Avoid introducing CCFs *during function testing, execution and restoration* (proactive)
 - Reveal and correct CCFs *by improved failure reporting* (corrective)
 - Learn and improve *by improved follow-up and validation* (proactive)



Implemented defenses through function testing

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

Further
improvements

Practical example

Summing up

Learnt anything?

The new procedure builds on:

- Previous publications and reports
- Own experience (previous, and in interaction with the industry)

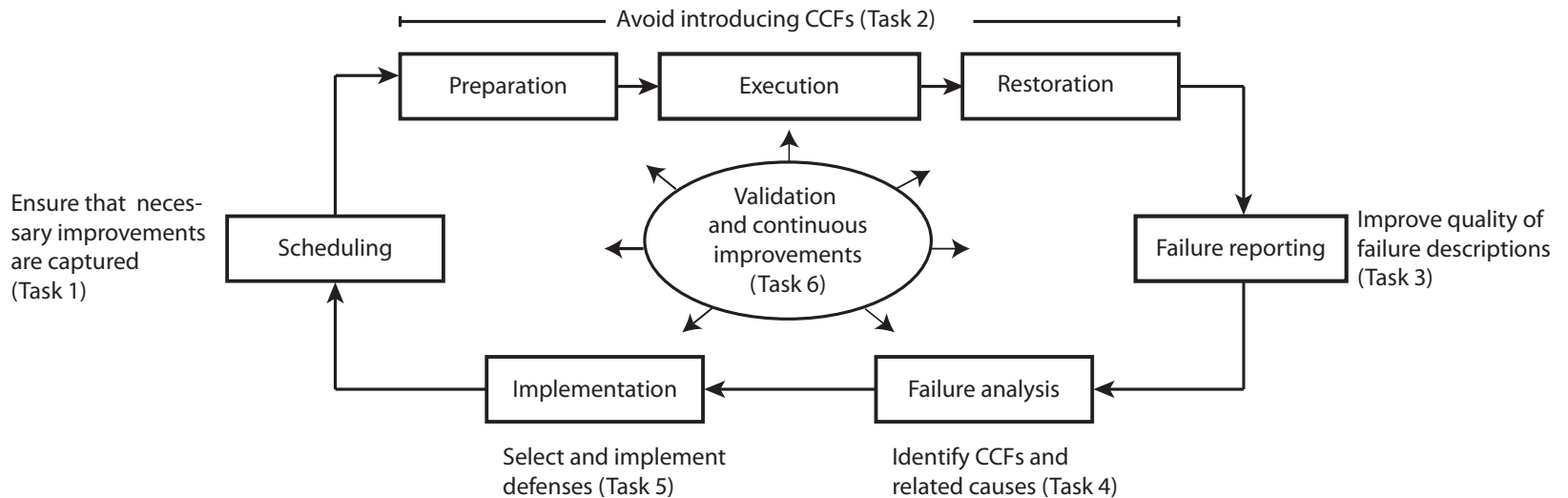
Main elements:

- Influence diagrams
- Checklists*)
- Cause-defense matrices
- Operational sequence diagrams (task analysis)

*) Yes/no questions, where *no* indicate a deviation

Implemented defenses through function testing

The procedure comprises 6 tasks



[Overview](#)

[Background](#)

[Modeling approach](#)

[CCF parameters](#)

[Defenses](#)

[New procedure](#)

Scope

[Task1](#)

[Task2](#)

[Task3](#)

[Task4](#)

[Task5](#)

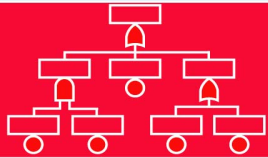
[Task6](#)

[Further improvements](#)

[Practical example](#)

[Summing up](#)

[Learnt anything?](#)



Task1: Capturing improvements before scheduling

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

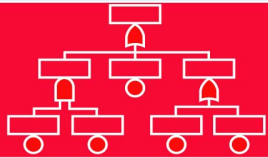
Further
improvements

Practical example

Summing up

Learnt anything?

- “Ensure that any corrections and improvements to the procedure are captured before scheduling”
- Which means that the improvements are not complete unless they are adopted into the next scheduled work procedure



Task2: Avoid introducing CCFs during preparation, execution and restoration

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

Further improvements

Practical example

Summing up

Learnt anything?

“Experience shows that inadequate preparation, execution and restoration is an important source of CCFs”

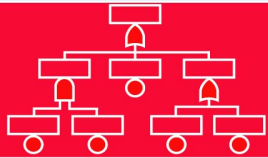
➤ The new procedure suggest new checklist questions, like e.g.,:

➤ Preparation:

- ➔ Have potential human errors during execution and restoration been identified and discussed?
- ➔ Are the calibration tools calibrated?

➤ Execution:

- ➔ Are the components operated within the specified environmental and operating conditions?
- ➔ Are the components protected against damage from nearby activities?



Task2: Avoid introducing CCFs during preparation, execution and restoration (continued)

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

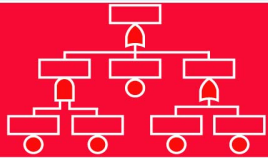
Further
improvements

Practical example

Summing up

Learnt anything?

- Continued:
 - Restoration:
 - ➔ Has the physical restoration been verified (by e.g. a colleague)?
 - ➔ Are any remaining inhibits, overrides or bypasses logged, and compensating measures identified and implemented?
- The questions may be adopted into the function test procedure or the JSA/SJA procedure



Task3: Improve the quality of failure reporting

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

Further
improvements

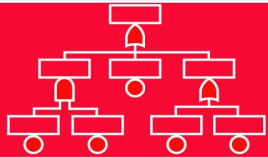
Practical example

Summing up

Learnt anything?

“Currently, maintenance systems do not allow directly recording of CCFs”

- Recognizes that free-text descriptions are essential for being able to reveal CCFs (and classify them correctly)
- Suggests a set of questions that should be answered, e.g.,:
 - How was the failure discovered or observed (Incidental, by diagnostics, during function testing...)?
 - Has the component been overexposed (operational or by environmental stresses), and if so, what may be the related causes?
- The questions should be straight forward and easy to answer by technicians



Task4: Identify CCFs through failure analysis

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

Further
improvements

Practical example

Summing up

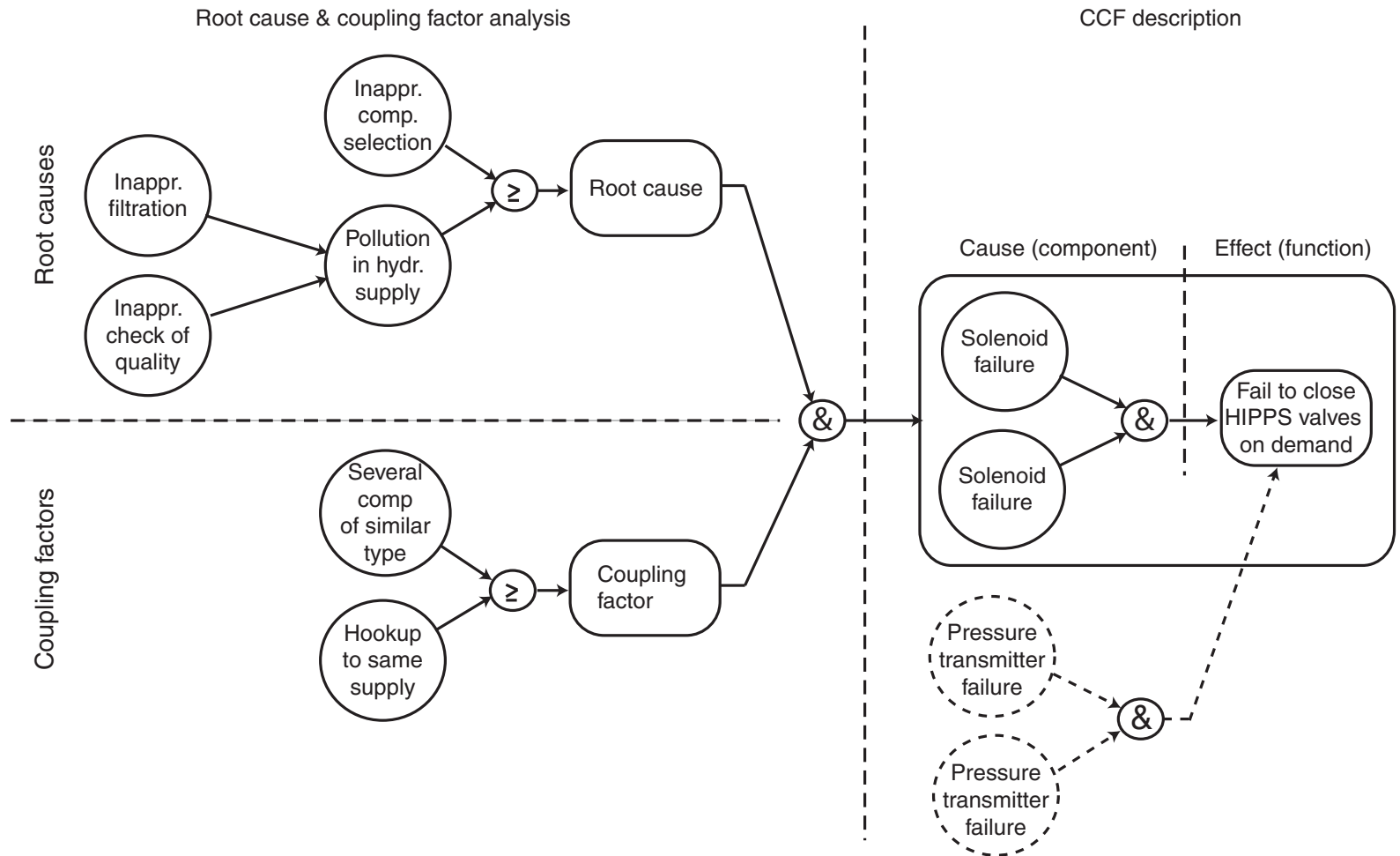
Learnt anything?

“Failure classification is often inadequate to capture CCFs”

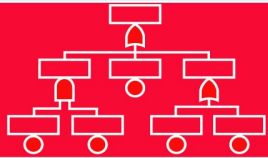
- Utilize the free-text descriptions to identify CCFs
 1. Review notifications/failure reports on relevant equipment. Also verify the initial classification.
 2. Perform an initial screening (grouping) of relevant notifications with respect to CCFs:
 - (a) That have similar design
 - (b) That share failure causes
 - (c) Than have been discovered within the same test or inspection interval (distinguish CCFs and *single* systematic failures)
 - (d) The failure causes are not random (\approx independent)
 3. Perform a root cause and coupling factor analysis by using *influence diagrams*
 4. List the root causes and coupling factors in a *cause-defense matrix*

Task4: Example: Influence diagram

- [Overview](#)
- [Background](#)
- [Modeling approach](#)
- [CCF parameters](#)
- [Defenses](#)
- [New procedure](#)
- [Scope](#)
- [Task1](#)
- [Task2](#)
- [Task3](#)
- [Task4](#)
- [Task5](#)
- [Task6](#)
- [Further improvements](#)
- [Practical example](#)
- [Summing up](#)
- [Learnt anything?](#)



Task4: Example: Cause-defense matrix



Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

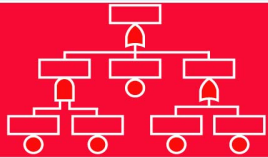
Further improvements

Practical example

Summing up

Learnt anything?

CCF	Root Cause	Coupling Factor	Defense alternatives	R	C	Impact (H/L)	Cost (H/M/L)
Failure of ESD valves	Solenoid stuck due to pollution in hydraulic supply	Same design	Hook-up to same hydraulic supply				



Task5: Suggest and implement defenses

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

Further
improvements

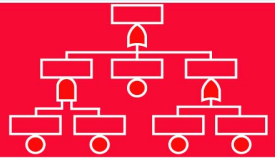
Practical example

Summing up

Learnt anything?

1. Continue filling out the cause-defense matrix
2. Assisted by a checklist of typical defenses associated with:
 - Administrative control
 - Documentation
 - Procedures
 - Monitoring and surveillance
 - Physical barriers
 - Hardware or software modifications of SIS

Task4: Example: Updating the cause-defense matrix



Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

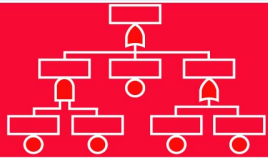
Further improvements

Practical example

Summing up

Learnt anything?

CCF	Root Cause	Coupling Factor	Defense alternatives	R	C	Impact (H/L)	Cost (H/M/L)
Failure of ESD valves	Solenoid stuck due to pollution in hydraulic supply	Same design	Implement regular quality check of hydraulics	✓	✓	M	L
		Hook-up to same hydraulic supply	Installing filters in hydraulic supply	✓		H	M
			Replacing existing solenoids with new and more robust ones				



Validation and continuous improvements

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

Further
improvements

Practical example

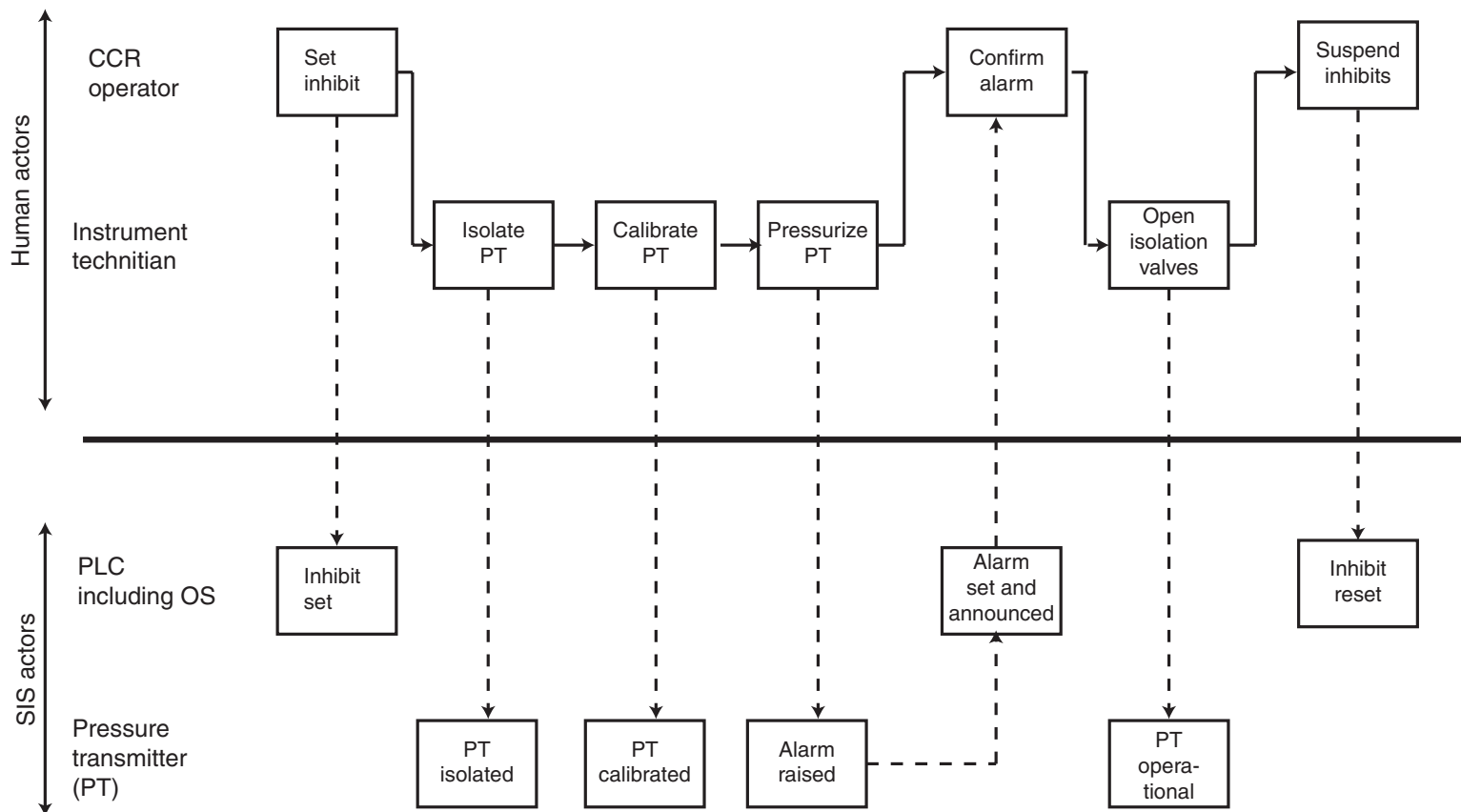
Summing up

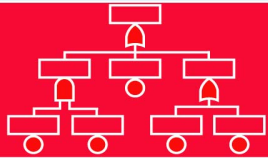
Learnt anything?

1. Task analysis using operational sequence diagrams
2. Validation checklist (focusing on procedures and work processes)
3. The intention is to perform such type of validation e.g. every five years (may focus on one or two SIFs per year)

Example: Operational sequence diagram

- Overview
- Background
- Modeling approach
- CCF parameters
- Defenses
- New procedure
- Scope
- Task1
- Task2
- Task3
- Task4
- Task5
- Task6**
- Further improvements
- Practical example
- Summing up
- Learnt anything?





Example: Validation questions

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

Further
improvements

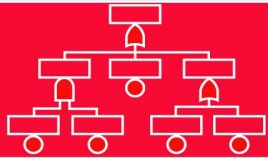
Practical example

Summing up

Learnt anything?

A few examples:

- Are all disciplines involved in SIS testing, inspection, maintenance and follow-up familiar with the concept of CCFs?
- Are the test limitations known?
- Are dangerous undetected failure modes known and sufficiently catered for in the function test or inspection procedures?



Further improvements

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Scope

Task1

Task2

Task3

Task4

Task5

Task6

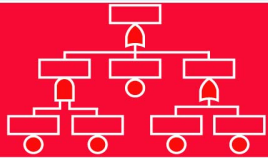
**Further
improvements**

Practical example

Summing up

Learnt anything?

- Quantify CCFs
- Assess implemented defenses and update e.g. the β -factor



Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Basis

Task1

Task2

Task3

Task4

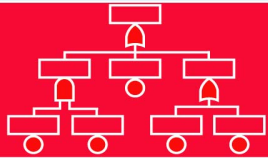
Task5

Task6

Summing up

Learnt anything?

Practical example



Using the new procedure

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Basis

Task1

Task2

Task3

Task4

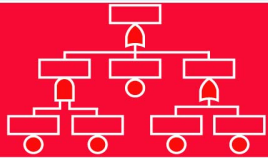
Task5

Task6

Summing up

Learnt anything?

- Assume that we want to apply the new procedure to improve the defense against CCFs associated with level transmitters



Example: Task 1 - Verify scheduling

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Basis

Task1

Task2

Task3

Task4

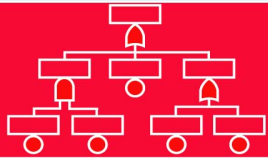
Task5

Task6

Summing up

Learnt anything?

- We verify that any improvements or suggestions (e.g. from previous assessments or registered notifications) are incorporated in the prevailing procedure
- The first time, one would here include the checklist questions (task 2) for preparation, execution and restoration into the test procedure for level transmitters.



Example: Task 2 - Avoid introducing during preparation, execution and restoration

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Basis

Task1

Task2

Task3

Task4

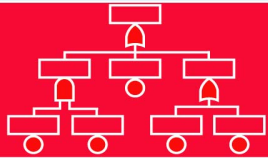
Task5

Task6

Summing up

Learnt anything?

- We assume that the level transmitters are tested once every year
- The offshore technicians apply the preparation (x1), execution and restoration questions
- Benefit: The likelihood of introducing new CCFs are minimized because the work is better prepared and the restoration re-verified and communicated.



Example: Task 3 - Failure reporting

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Basis

Task1

Task2

Task3

Task4

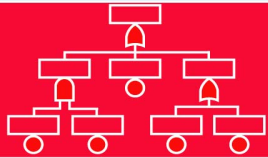
Task5

Task6

Summing up

Learnt anything?

- We assume that *four dangerous failures* have been found during function testing
- By answering the questions, we ensure that the technicians knowledge about the failures are properly recorded:
- The following information may be read out of the questions answered (we assume that the same answers apply to all events):
 - ▮ The failures were discovered during a function test
 - ▮ The failure cause seems to be inadequate calibration of the transmitters
 - ▮ If a real demand (too high level) had occurred, the level transmitters would not have been able to detect the event
 - ▮ It does not seem to be anything unusual about the test approach or operating conditions that could have influenced the failure cause
 - ▮ To their immediate knowledge, such a failure has not occurred at this installation before
- Benefit: Answering the questions does not take that much extra time, compared to the time needed to find out more about the failures after wards...



Example: Task 4 - Identify CCFs

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Basis

Task1

Task2

Task3

Task4

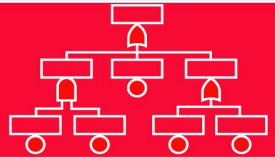
Task5

Task6

Summing up

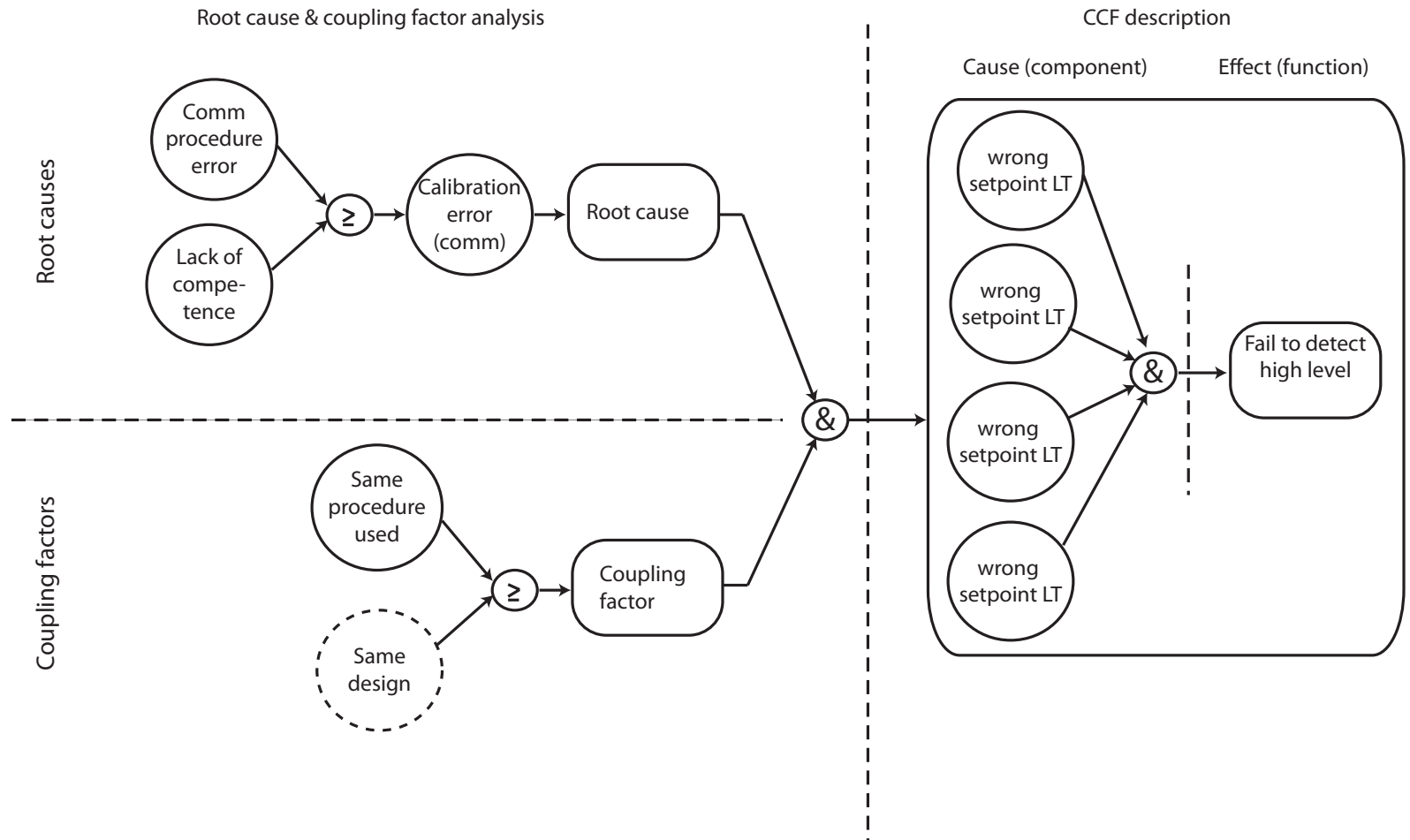
Learnt anything?

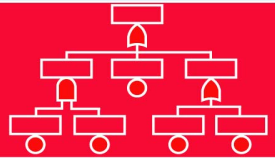
1. The failure notifications are reviewed and found ok (with respect to free text descriptions and classification)
2. The initial screening shows that we have four failure events where the:
 - Same type of level transmitter is involved
 - The cause of failure is shared by all four events
 - The failures have been discovered at the end of the same function test interval
 - The failure causes are systematic (and not random)
3. A root and coupling factor analysis shows that the failure cause may be traced back to incomplete commissioning
4. The failure causes are listed in a cause-defense matrix



Example: Influence diagram

- [Overview](#)
- [Background](#)
- [Modeling approach](#)
- [CCF parameters](#)
- [Defenses](#)
- [New procedure](#)
- [Practical example](#)
- [Basis](#)
- [Task1](#)
- [Task2](#)
- [Task3](#)
- [Task4](#)**
- [Task5](#)
- [Task6](#)
- [Summing up](#)
- [Learnt anything?](#)



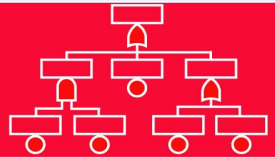


Example: Cause-defense matrix

- Overview
- Background
- Modeling approach
- CCF parameters
- Defenses
- New procedure
- Practical example
- Basis
- Task1
- Task2
- Task3
- Task4**
- Task5
- Task6
- Summing up
- Learnt anything?

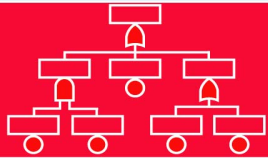
CCF	Root Cause	Coupling Factor	Defense alternatives	R	C	Impact (H/L)	Cost (H/M/L)
Failure of level transmitters	Level transmitter has wrong set point due to inadequate execution of commissioning	Same type	Same commissioning procedure				

Example: Task 5 - Select and implement defenses



- Overview
- Background
- Modeling approach
- CCF parameters
- Defenses
- New procedure
- Practical example
- Basis
- Task1
- Task2
- Task3
- Task4
- Task5**
- Task6
- Summing up
- Learnt anything?

CCF	Root Cause	Coupling Factor	Defense alternatives	R	C	Impact (H/L)	Cost (H/M/L)
Failure of level transmitters	Level transmitter has wrong set point due to inadequate execution of commissioning	Same type	Review meetings dedicated to commissioning procedures	✓			
		Same commissioning procedure	Additional quality control of set points by other staff (commissioning) Monitoring?	✓	✓		



Example: Task6 - validation and improvements

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Basis

Task1

Task2

Task3

Task4

Task5

Task6

Summing up

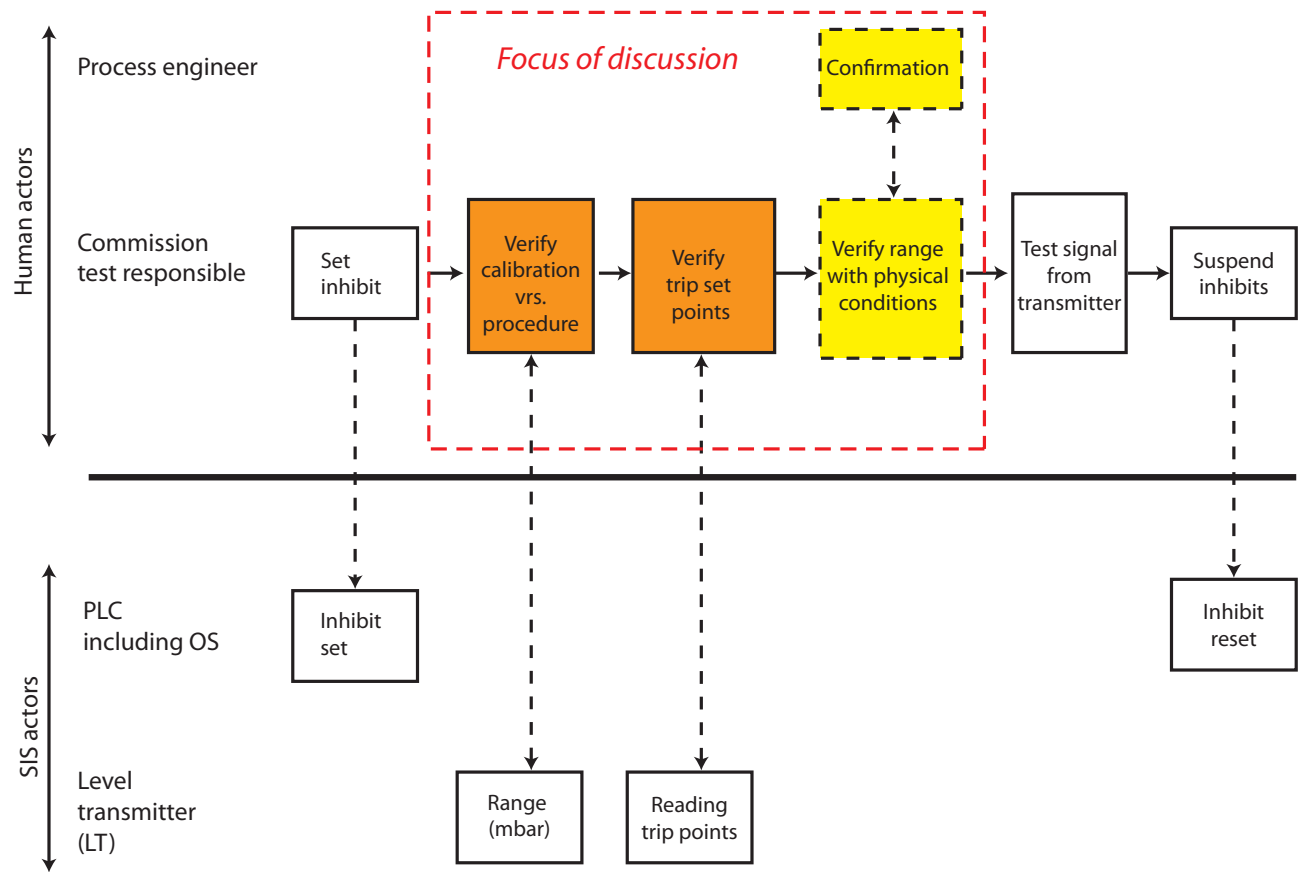
Learnt anything?

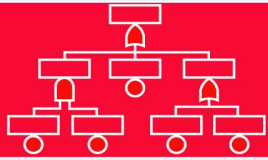
- Relevant validation question (which in this case would get a “no”):
 - ➡ Are procedure deficiencies (in this case not the function test procedure, but the commissioning procedure) communicated to the responsible persons and followed-up?

- Task analysis:
 - ➡ In this case it may be relevant to assess the commissioning work processes rather than the function test work processes

Example: Operational sequence diagram

- Overview
- Background
- Modeling approach
- CCF parameters
- Defenses
- New procedure
- Practical example
- Basis
- Task1
- Task2
- Task3
- Task4
- Task5
- Task6**
- Summing up
- Learnt anything?





Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

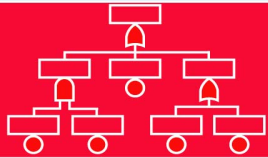
Practical example

Summing up

Conclusions

Learnt anything?

Summing up



Discussion and conclusions

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

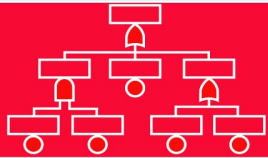
Practical example

Summing up

Conclusions

Learnt anything?

- A CCF involves failure of two or more components
- A CCF is characterized by root causes and coupling factors
- We may incorporate the effect of CCFs through explicit or implicit modelling
- Several implicit models exist
- The CCF parameters (e.g. β) may be determined by using checklists
- It is important to implement defenses against CCFs



Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

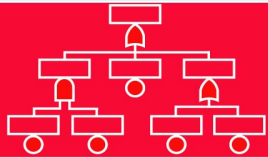
Practical example

Summing up

Learnt anything?

Evaluation

Learnt anything?



Feedback on lecture

Overview

Background

Modeling approach

CCF parameters

Defenses

New procedure

Practical example

Summing up

Learnt anything?

Evaluation

- Do you have any comments or feedback?