Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Risk Analysis of Highly-integrated Systems

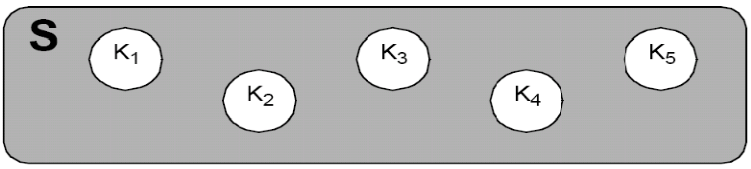
RA III: Systematic Failures

- **Categorization**
- **Modeling Approaches**

Independent Failures

Component Reliability and System Reliability

system S = {K_1, ... , K_n}, number of components: n



Conclusions if the system structure is known:
Reliability of K_1, ... , K_n $\Leftrightarrow$ **Reliability of S** (both directions)

Assumption:
Failures of the components are **stochastically independent**.

Dependent Failures

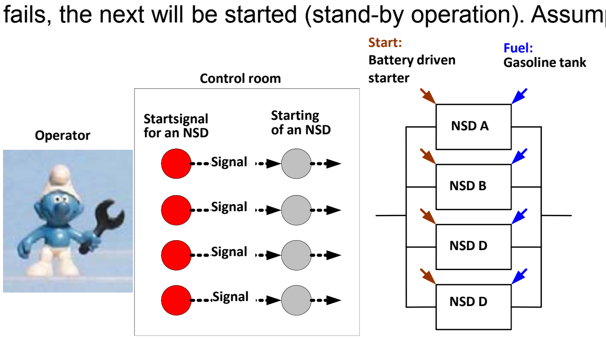
Present model assumptions:

All failures of a system are due to independent failures at components (‘elements’) level, i.e.:
• The failure of an element has no functional influence on other system elements
• The physical effects of failure of one element on other elements are marginal
• By adding (redundant) elements to the system, its failure probability can be reduced to a minimum

These assumptions contradict common experience!

Example of dependent failures: Emergency power supply

A data processing service centre of a major bank has a largely redundant emergency power supply. Four emergency power engines (NSD) are installed, one engine guarantees the operability of the centre for two days. If one engine fails, the next will be started (stand-by operation). Assumptions:



NSD are started by an operator in the control room.
Each NSD has its own control device.
Each NSD has its own starter, battery and tank.
All NSD are maintained and fuelled in one process.

Definitions

Dependent failure (DF)

•Event, of which the occurrence probability cannot be modelled as a product of single occurrence probabilities (mathematical), or

•Event, which is caused by any interdependent structures (multiple failure, technical)

CCF (common cause failure)

Description of a type of a dependent failure, at which a common single cause triggers several failures occurring (almost) simultaneously

CMF (common mode failure)

Description for a specific CCF, in which several (system-)units fail in the same way

CF (causal or cascade failures)

Description for spreading or interdependent failures

Common cause initiating events

Description for initiating events which can cause several events or event scenarios, e.g. area event such as earthquakes or flooding

• DF are only important in redundant (parallel) systems.

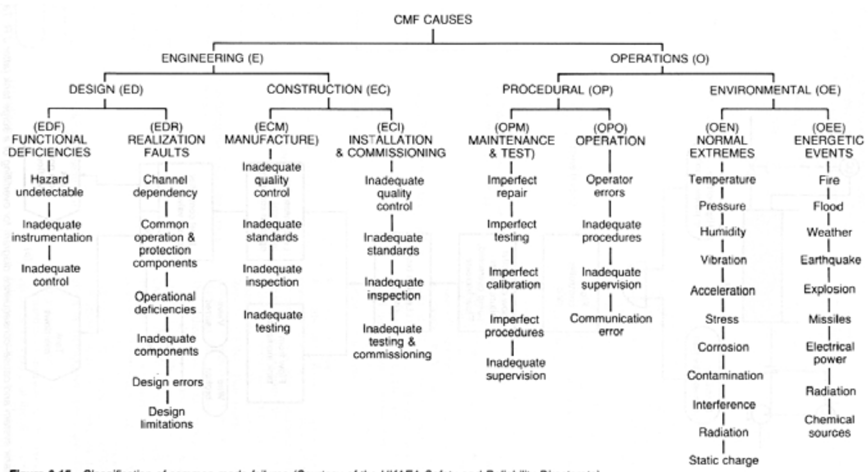


Figure 9.15 Classification of common mode failures (Courtesy of the UKAEA Safety and Reliability Directorate)

Transition to the Modeling of DF

Without consideration of existing DF

- incomplete description of technical systems
- too optimistic results of safety analysis for redundant systems

Problems:

- Lack of data for highly reliable systems, usually from limited operational experiences (normal operation state, functional testing)
- It is difficult to classify observed events into dependent and independent ones.

Required steps to consider DF:

- Identification of potential DF in a technical system.
- Qualitative and quantitative consideration of DF within a reasoned framework (model building).
- Possibility to prevent or to reduce the consequences of DF.

Modeling approaches: Methods considering DF

Explicit Methods:

- **Event specific models**
Consideration special consequences from earthquakes, fire, floods, broken pipes or leakage in the primary loop, etc.

- **Event tree and fault tree analysis**
Consideration of functional dependencies (units).

- **Models for the quantification of human actions**
Consideration of interdependencies between single human actions.

Examples are models in THERP (Technique for Human Rate Error Prediction).

Explicit methods comprise structural and functional dependencies, they are system-specific but they do not cover all safety-relevant dependent failures completely.

Implicit Methods (to consider residual dependent failures)

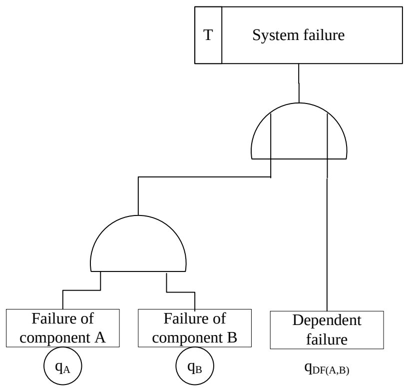
• Marshall-Olkin-Model, β-Factor-Model, MGL-Model (Multiple Greek Letter), BFR-Model (Binominal Failure Rate) et al.

General

• In principle, implicit methods can completely cover dependent failures, but great uncertainties arise because the data are based solely on the level of considered items (CMF).
• Rigorous application bears the danger of insufficient fault tree analyses, e.g. failure of notice or correctly value structural/functional dependencies.

Modelling:

Explicit method



Modeling (implicit method)

Marshall-Olkin-Model (fundamental modeling)

1. System modelling excluding DF

Example: '2 out of 3-system' with units A, B and C

- System failure, when two units fail: {A, B}, {A, C}, {B, C}
- Probability of system failure: $Q_s = q_a{\cdot}q_b + q_a{\cdot}q_c + q_b{\cdot}q_c - 2\, q_a{\cdot}q_b\, q_c$

Simplification and notation

- *All units failure probabilities are identical:* $q_a = q_b = q_c = Q_{k=1}$
  k (k = 1, 2, …, n): Number of involved units in the failure
- *Simplification:* $Pr(a \cup b) \approx Pr(a) + Pr(b)$

System failure probability of a '2 out of 3-system' excluding DF

$$Q_s = q_a{\cdot}q_b + q_a{\cdot}q_c + q_b{\cdot}q_c = 3{\cdot}\, Q_1^2$$

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

2. Inclusion of DF

Probabilities of failure combinations

- q_{AB}, q_{BC}, q_{AC}
- q_{ABC}

Assumption: equality of all units:

- $q_{AB} = q_{BC} = q_{AC} = \ldots = Q_{k=2}$
- $q_{ABC} = Q_{k=3}$

'2 out of 3-system'

- Probability of a DF including two units: $3{\cdot}Q_2$
- Combination of three (all) failures: $q_{ABC} = Q_3$.

3. System failure probability

System failure probability Q_s including DF:
$Q_s = \Sigma$Pr(independent failures) + ΣPr(dependent failures)

'2 out of 3-system'

$$Q_s = 3{\cdot}\, Q_1^2 + 3{\cdot}Q_2 + Q_3.$$

4. Failure probability of the units

Q_t is the total failure probability of an element in a group of redundant elements, inclusive of all dependencies. The interrelationship between Q_t and Q_k is asked for:

$$Q_t = \sum_{k=1}^{n} \binom{n-1}{k-1} \cdot Q_k$$

,

with binominal coefficient .

$$\binom{n-1}{k-1} \equiv \frac{(n-1)!}{(n-k)! \cdot (k-1)!}$$

Number of failure combinations of an element with (k-1) different elements in a group of (n-1) identical elements.

Group of 3 redundant elements

$$Q_t = \binom{3-1}{1-1} \cdot Q_1 + \binom{3-1}{2-1} \cdot Q_2 + \binom{3-1}{3-1} \cdot Q_3 = Q_1 + 2 \cdot Q_2 + Q_3$$

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Calculation of Q_k by using relative frequencies

$$Q_k = \frac{n_k}{\binom{n}{k}}$$

n_k: Number of failures with k involved elements and the binominal coefficient for the calculation of the combinations with k of n elements.

Annotation:
Ideally the different Q_k can be drawn directly from of observation data. Some models simplify the consideration of DF by making additional assumptions.

One of these models is the ***β*-factor-model**.

Simplifying assumptions

- Failures in a group of redundant elements are either independent or all of the *n* elements fail.
- With $k = 1$, $Q_{k=1}$ is the failure probability of independent failures
- With $k = n$, $Q_{k=n}$ is the failure probability for (totally) dependent failures
- All other failure combination are excluded by definition, so

$Q_k = 0$ for $n > k > 1$ (for other failure combinations)

For 'm out of n-system' it is generally

$$Q_t = Q_1 + Q_n.$$

Definition: β -factor

$$\beta = \frac{Q_n}{Q_1 + Q_n} = \frac{Q_n}{Q_t} \qquad \beta = \frac{Number\ of\ DF}{Number\ of\ all\ failures}$$

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

From this it follows directly

$$\beta \cdot Q_t = Q_{k=n}$$

$$\beta \cdot \left(Q_1 + Q_n\right) = Q_{k=n}$$

- With $Q_n = Q_t - Q_1$ follows

$$Q_{k=1} = Q_t\left(1 - \beta\right)$$

- Finally

$$Q_k = \begin{cases} \left(1-\beta\right)\cdot Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta \cdot Q_t & k = n \end{cases}$$

'2 out of 3-system'

System failure probability $Q_s = 3 \cdot Q_1^2 + 3 \cdot Q_2 + Q_3$

Changes in the β-factor-model to $Q_s = 3 \cdot \left(1-\beta\right)^2 \cdot Q_t^2 + \beta \cdot Q_t$

Discussion of the β-Factor-Model

β-Factor-Model:	
Advantages	**Disadvantages**
easy to apply	too conservative in the case of simultaneous failures of more than two units
β-Parameter can be determined relatively easily by operational experiences	Results are too conservative if there are more than two groups of redundancies (n>2)
	danger of too general application

Multiple-Greek-Letter-Model (MGL-Model)

Assumptions identical to the β-factor-model, but combinations of failures are possible

Parameter, Definitions	Example: Group of 3 Redundant Elements
Q_t: total failure probability of a unit	$Q_t = Q_1 + 2Q_2 + Q_3$
α = 1	α = 1
β: all *dependent* failure probabilities relating to Q_t	$\beta = \frac{2Q_2 + Q_3}{Q_t} = \frac{2Q_2 + Q_3}{Q_1 + 2Q_2 + Q_3}$
γ: *fraction* of DF probability of a unit, with *at least* 2 units failing	$\gamma = \frac{Q_3}{2Q_2 + Q_3}$

To consider the MGL-factors the equation for Q_t will be solved for Q_k (k = 1, 2, 3). The resulting terms will be replaced by the parameters β, γ, etc.

Example: Group of 3 Redundant Elements	given: $Q_t = Q_1 + 2Q_2 + Q_3$
$Q_1 = \frac{Q_t - (2Q_2 + Q_3)}{1} = Q_t - (\beta Q_t) = Q_t(1-\beta)$	$\beta = \frac{2Q_2 + Q_3}{Q_t} = \frac{2Q_2 + Q_3}{Q_1 + 2Q_2 + Q_3}$
$Q_2 = \frac{Q_t - (Q_1 + Q_3)}{2} = \frac{Q_t - [Q_t(1-\beta) + \gamma(2Q_2 + Q_3)]}{2}$ $= \frac{Q_t - [Q_t(1-\beta) + \gamma(\beta Q_t)]}{2} = \ldots = \frac{Q_t - \beta(1-\gamma)}{2}$	$\gamma = \frac{Q_3}{2Q_2 + Q_3}$
Q_3 ...	etc.

The results for a redundant group can be generalized by using the notation
$\Phi_1 = 1,\ \Phi_2 = \beta,\ \Phi_3 = \gamma,\ \ldots,\ \Phi_{m+1} = 0$

$$Q_k = \frac{1}{\binom{n-1}{k-1}} \cdot \left(\prod_{i=1}^{k} \Phi_i\right) \cdot (1 - \Phi_{k+1}) \cdot Q_t$$

Example: Redundant Group with 3 Elements

$Q_{k=1}$	$Q_{k=2}$	$Q_{k=3}$
$= \frac{1}{\binom{3-1}{1-1}} \cdot (\Phi_1) \cdot (1-\Phi_2) \cdot Q_t$	$= \frac{1}{\binom{3-1}{2-1}} \cdot (\Phi_1 \cdot \Phi_2) \cdot (1-\Phi_3) \cdot Q_t$	$= \frac{1}{\binom{3-1}{3-1}} \cdot (\Phi_1 \cdot \Phi_2 \cdot \Phi_3) \cdot (1-\Phi_4) \cdot Q_t$
$= 1 \cdot (1-\beta) \cdot Q_t$	$= \frac{1}{2} \cdot 1 \cdot \beta \cdot (1-\gamma) \cdot Q_t$	$= 1 \cdot \beta \cdot \gamma \cdot (1-0) \cdot Q_t$

Example: Substituting Q_k in the equation "System Failure Probability of a 2 out of 3 System Q_s with DF portion", $Q_s = 3 \cdot Q_1^2 + 3 \cdot Q_2 + Q_3$, equals

$$Q_s = 3(1-\beta)^2 Q_t^2 + \frac{3}{2}\beta(1-\gamma)Q_t + \beta\gamma Q_t$$

Supposing the MGL-factors are unknown, they can be determined via the respective Q_k (see above: parameters, definitions). The probabilites can be determined via

$$Q_k = \frac{n_k}{\binom{n}{k}}$$

.

Equating $\gamma = 1$ leads to the result of the β-factor-model. In general, the β-factor-model is a special case of the MGL-Model

Methodic uncertainties 1/2

Illustrating example: Nuclear Power Plant PSA Level 1; Core Damage Frequency

Plant model Fault Tree (CCF,HRA), Event Tree(physical phenomena)

- Adequacy of modeling approach: static approach vs. dynamic behavior; exclusion of certain failure types (e.g. human error of commission); system boundaries; unrealistic documents

Methodic uncertainties 2/2

- Quantification of the model
  - Data base: statistical basis
    - o Engineered judgment
    - o Generic
    - o Plant specific
  - Population, relevance, uncertainty bands (→ error propagation)
  - Assumptions: rare event approximation, „cut-offs", „binning" (→sensitivity studies)

- Completeness of accident scenarios (→ large number) and model validity (→check against experiments and experience)