Reliability of Safety-Critical Systems
5.1 Reliability Quantification with RBDs

Mary Ann Lundteigen and Marvin Rausand
mary.a.lundteigen@ntnu.no &marvin.rausand@ntnu.no

RAMS Group
Department of Production and Quality Engineering
NTNU

(Version 1.1 per August 2015)

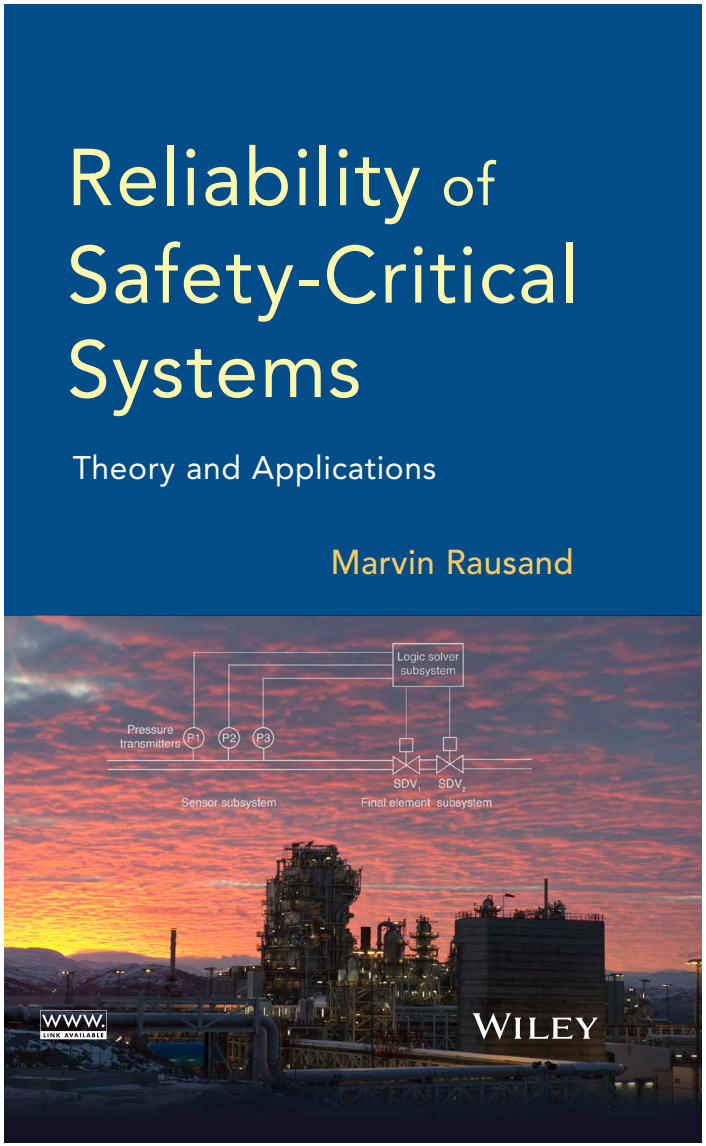
NTNU – Trondheim
Norwegian University of
Science and Technology

Slides related to the book

Reliability of Safety-Critical Systems
Theory and Applications

Wiley, 2014

Homepage of the book:
http://www.ntnu.edu/ross/books/sis



Purpose

The purpose of this slide series is to:

1. Briefly present the main properties of reliability block diagrams (RBDs)
2. Briefly present the main approach to developing structure functions
3. Present formulas for quantifying reliability based on structure functions, including:
4. Probality of failure
5. Mean time to failure (MTTF)

Application of RBDs

☞ RBD: A diagram that gives the relationship between component states and the success or failure of a specified system function.

An RBD:

- Has a single stating point (a) and end point (b)
- Use rectagles or squares to represent each task (or function) carried out by the system items
- Use lines and structuring into series or parallel structure, or a combination of these to illustrate the logical relationship between the functions

RBD applied to SIF

A safety instrumented function (SIF) may be represented by an RBD by:

- A single stating point (a) and end point (b)
- Rectagles or squares corresponding to the function of each subsystem, or a further breakdown of the subsystem items.
- Series or parallel structure, or a combination of these to illustrate the logical relationship between the subfunctions

☞ Parallel structure (or system): A system that is functioning if at least one of its n items is functioning.

☞ Series structure (or system): A system that is functioning if and only if *all* of its n items are functioning.

RBD example

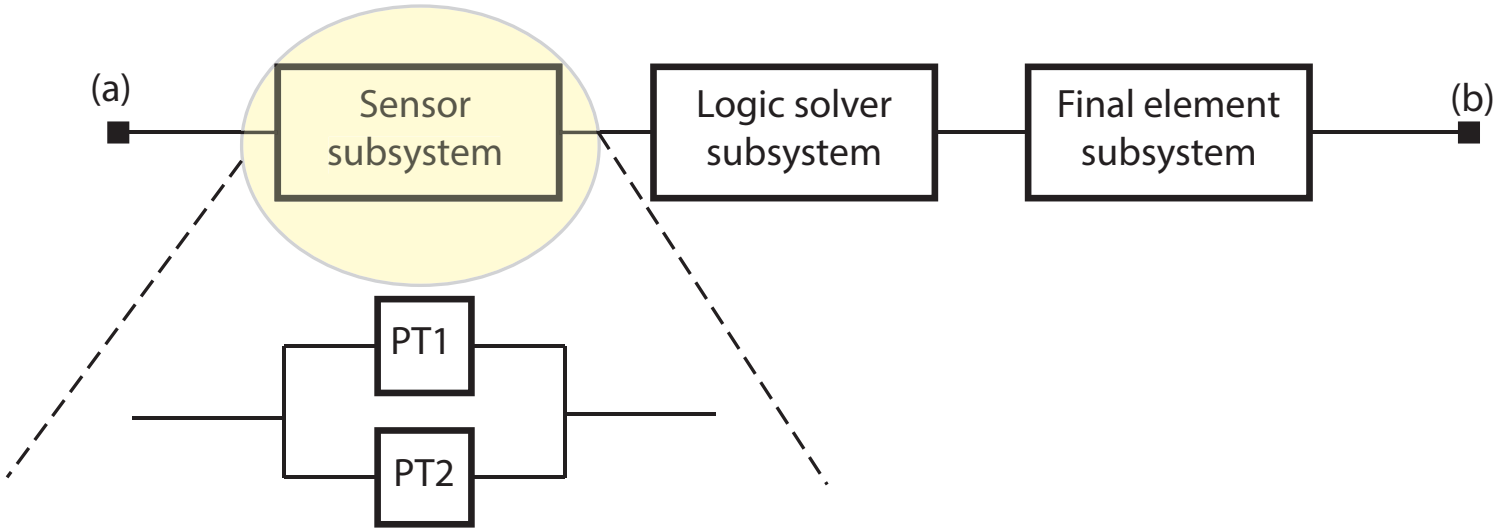


Figure: A SIF modelled with RBD

Each subsystems may be broken down to the item level. This is illustrated for the sensor subsystem above, where two pressure transmitters (PTs) are included in a parallel structure.

Item state versus system state

State of items:

- Each item in a RBD has two possible states: *functioning* or *failed*.
- The state of an item i can be represented by a state variable, x_i, where:

$$x_i = \begin{cases} 1 & \text{if item } i \text{ is functioning} \\ 0 & \text{otherwise} \end{cases}$$

- $\mathbf{x} = (x_1, x_2, ..., x_n)$ is called the state vector.

State of system:

- The state of the system can be described by the binary function $\phi(\mathbf{x})$, also called the *structure function*:

$$\phi(\mathbf{x}) = \phi(x_1, x_2, ..., x_n)$$

$$\phi(\mathbf{x}) = \begin{cases} 1 & \text{if the system is functioning} \\ 0 & \text{otherwise} \end{cases}$$

Structure function of series and parallel stuctures

The structure function of a series structure is:

$$\phi(\mathbf{x}) = x_1 \cdot x_2 \cdots x_n = \prod_{i=1}^{n} x_i$$

The structure function of a parallell structure is:

$$\phi(\mathbf{x}) = 1 - (1 - x_1)(1 - x_2) \cdots (1 - x_n) = 1 - \prod_{i=1}^{n} (1 - x_i)$$

Structure function of *koon* structures

A special case is the *koon*, which is functioning if (at least) k out of n items are functioning. This means that the structure function becomes:

$$\phi(\mathbf{x}) = \begin{cases} 1 & \text{if } \sum_{i=1}^{n} x_i \geq k \\ 0 & \text{otherwise} \end{cases}$$

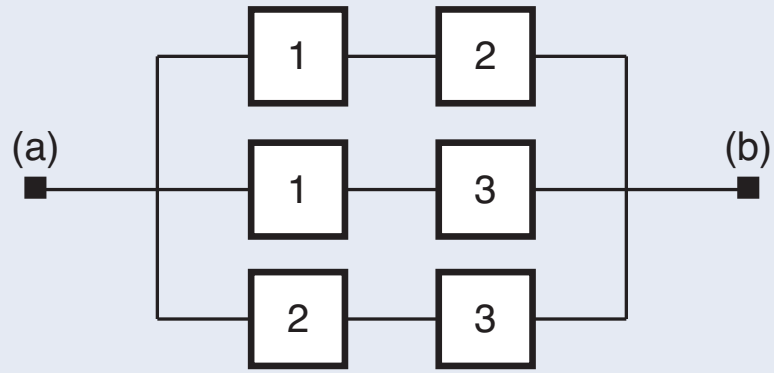
The most easy way to set up the structure function for a system with i different items is to *first* determine the minimal path sets and then use the fact thatthe system is functioning if the items of at least one path set is functioning (or alternatively, determine the minimal cut sets, and use the fact that the system fails if the items contained in one or more of the cut sets fail).

Minimal path sets

☞ Minimal path set: A minimal path is a set of items that if functioning secures that the system is functioning. A path set is said to be minimal if it cannot be reduced without loosing its status as a path set.

Example

Path sets are: {1,2}, {1,3}, {2,3}, and {1,2,3}. The three first ones are minimal.

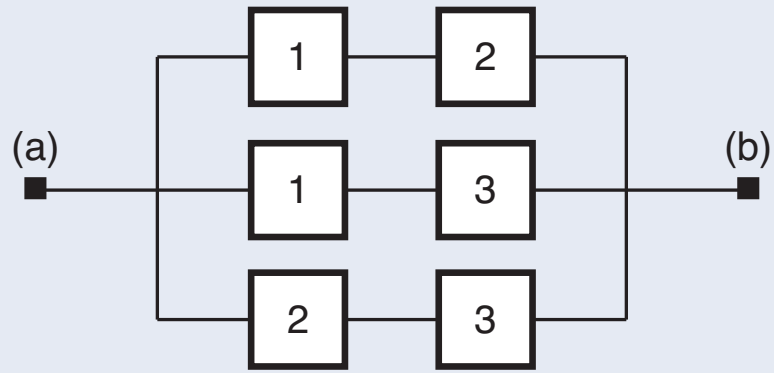


Minimal cut sets

☞ Minimal cut set: A minimal cut is a set of items that by failing secures that the system fails. A cut set is said to be minimal if it cannot be reduced without losing its status as a path set.

Example

Cut sets are: {1,2}, {1,3}, {2,3}, and {1,2,3}. The three first ones are minimal. Note that in this particular case, the minimal cut sets become identical to the minimal path sets.

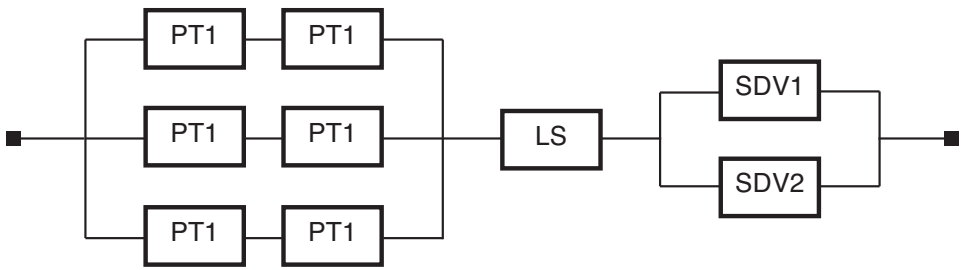


Structure function of a SIF

Consider a SIF with a sensor subsystem with 2oo3 voted pressure transmitters (PTs), one logic solver (LS), and two 1oo2 voted shutdown valves (SDVs).

The structure function is:

$$\begin{aligned}\phi(\mathbf{x}) &= (x_{\text{PT1}}x_{\text{PT2}} + x_{\text{PT1}}x_{\text{PT3}} + x_{\text{PT2}}x_{\text{PT3}} - 2x_{\text{PT1}}x_{\text{PT2}}x_{\text{PT3}}) \cdot x_{\text{LS}} \\ &\cdot (x_{\text{SDV1}} + x_{\text{SDV2}} - x_{\text{SDV1}}x_{\text{SDV2}})\end{aligned}$$



Note: Error in figure for PTs (to be updated)

From structure function to reliability function

In the structure function, the state variable x_i is a deterministic quantity (functioning *or* failed).

In system reliability analyses, we consider the state variables as *random* and dependent on time, denoted x_i instead of $X_i(t)$.

The randomness makes it of interest to determine the *probability* of being in a specific state, functioning or failed:

$$\begin{aligned} \Pr(X_i(t) = 1) &= \Pr(T > t) = p_i(t) \\ \Pr(X_i(t) = 0) &= \Pr(T < t) = 1 - \Pr(T > t) = 1 - p_i(t) \end{aligned}$$

The reliability function at item level

We often refer to $p_i(t)$ as:

- The survival function $R_i(t)$ for item i, if the item is *non-repairable*, and
- The availability function $A_i(t)$ for item i, if the item is *repairable* (i.e., repaired upon failure)

Example

The survival function for an item where we assume exponential time to failure is:

$$R_i(t) = e^{-\lambda_i t}$$

where λ_i is the constant failure rate of item i and t is the time at which the survival probability is calculated.

The reliability function, $p_s(t)$, at system level

For non-repairable systems, the reliability functions ($p_s(t)$) are:

System	**Reliability function** $p_s(t)$
Series structure	$\prod_{i=1}^{n} p_i(t)$
Parallel structure	$1 - \prod_{i=1}^{n}(1 - p_i(t))$
koon structure (identical items)	$\sum_{j=k}^{n} \binom{n}{j} p(t)^j (1 - p(t))^{n-j}$

Note that the *koon* here constitutes identical components $p_1(t), p_2(t) \cdots p_n(t)$ are equal and equal to $p(t)$.

The reliability function, $R_s(t)$, at system level

For non-repairable systems, assuming expontially distributed time to failure, we get:

System	**Reliability function** $R_s(t)$
Series structure	$\prod_{i=1}^{n} e^{-\lambda_i t} = e^{-(\sum_{i=1}^{n} \lambda_i)t}$
Parallel structure	$1 - \prod_{i=1}^{n}(1 - e^{-\lambda_i t})$
koon structure (identical items)	$\sum_{j=k}^{n} \binom{n}{j} e^{-j\lambda_i t}(1 - e^{-\lambda_i t})^{n-j}$

Mean time to failure (MTTF)

For non-repairable systems, we may calculate the MTTF at the item level and at the system level.

Item level:

$$MTTF = \int_{t=0}^{\infty} R_i(t)\,dt$$

System level:

$$MTTF = \int_{t=0}^{\infty} R_s(t)\,dt$$

Example

A series of two components has MTTF equal:

$$MTTF = \int_{t=0}^{\infty} e^{-(\lambda_1+\lambda_2)t}\,dt = \frac{1}{\lambda_1+\lambda_2}$$

A 2oo4 system

Consider a subsystem of four identical components in a 2oo4 voted structure. The component type has a constant failure rate λ.

The survival function becomes:

$$\begin{aligned} R_s(t) &= \sum_{j=2}^{4} \binom{4}{j} e^{-j\lambda t}(1-e^{-\lambda t})^{4-j} \\ &= 6e^{-2\lambda t} - 8e^{-3\lambda t} + 3e^{-4\lambda t} \end{aligned}$$

MTTF becomes:

$$MTTF = \frac{6}{2\lambda} - \frac{8}{3\lambda} + \frac{3}{4\lambda} = \frac{13}{12\lambda}$$

Repairable systems

For repairable systems, we replace each survival probabilities $p_i(t)$ by its availability $A_i(t)$.

Often, we work with average availabilities (A_i) rather than the time dependent availabilities, and more specifically average unavailabilities ($\bar{A}_i$).

- Consider a series system of two components, with failure rates λ_1 and λ_2, respectively:

$$\begin{aligned} \bar{A}_1 &= \Pr(\text{Comp 1 fails first} | \text{an item has failed}) = \Pr(T_2 > T_1) \\ &= \frac{\lambda_1}{\lambda_1 + \lambda_2} \end{aligned}$$

- The same can be set up for Component 2 ($\bar{A}_2$).

Repairable systems

Each time the component fails, it has a mean downtime MDT_i, $i = 1..2$. If the system goes down it is either down due to component 1 or component 2:

$$MDT_S = \frac{\lambda_1}{\lambda_1 + \lambda_2} MDT_1 + \frac{\lambda_2}{\lambda_1 + \lambda_2} MDT_2$$

The average unavailability of the system, $\overline{A}_{avg}$, is therefore:

$$\overline{A}_{avg} = (\lambda_1 + \lambda_2) \cdot MDT_S$$

For parallel systems it is not so straight forward due to the average of products being not equal to the product of averages.