Chapter 1
Introduction

Marvin Rausand
marvin.rausand@ntnu.no

RAMS Group
Department of Production and Quality Engineering
NTNU

(Version 0.1)

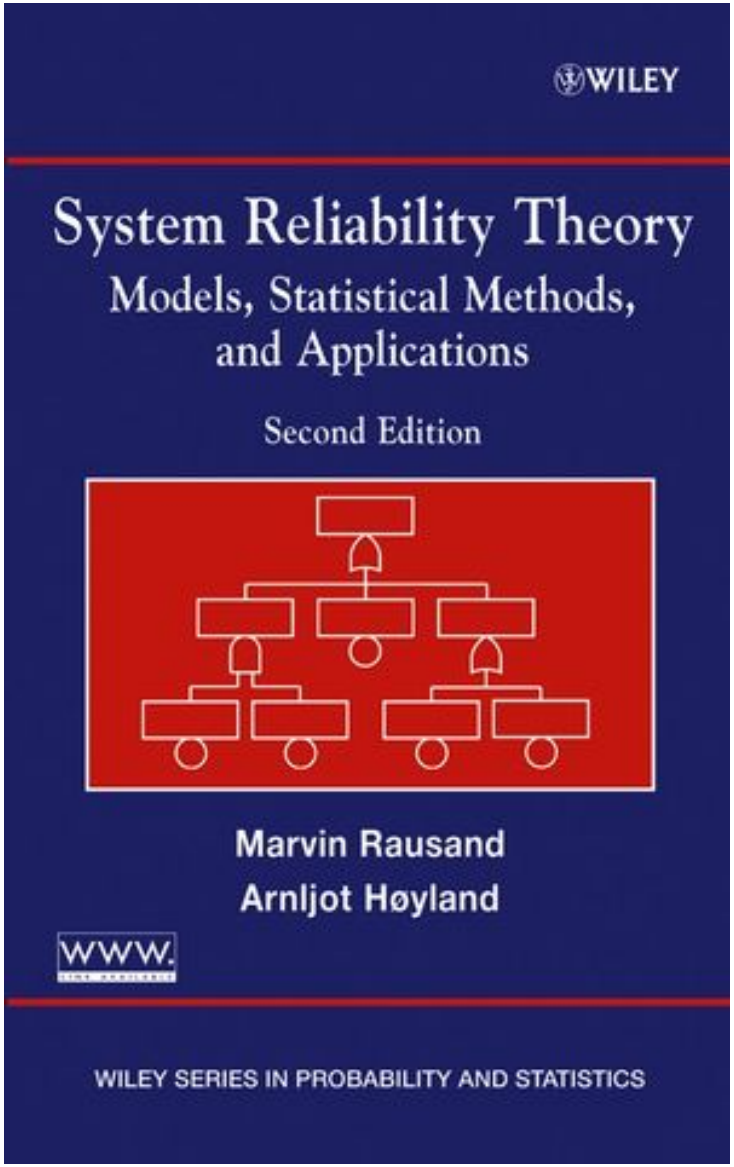
NTNU – Trondheim
Norwegian University of
Science and Technology

Slides related to the book

System Reliability Theory
Models, Statistical Methods, and Applications

Wiley, 2004

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



Brief history

1930's:	Statistical methods for quality control of industrial products (Shewhart, Dodge and Romig)
	Determination of air crash probability
1940's	Analysis of German V1 missiles (Robert Lusser)
1950's	Failure modes and effects analysis (FMEA)
	Reliability growth (AGREE)
1960's	Analysis of intercontinental ballistic missiles
	Space research programs
	Fault tree analysis (Minuteman missile)
	New textbooks in reliability (e.g., Barlow and Proschan)
1970's	Reactor Safety Study (WASH-1400)
	Offshore activities (e.g., in Norway and the U.K.)
	Reliability centered maintenance (e.g., Nowlan and Heap)
1990's	Integration of RAMS into product and process design

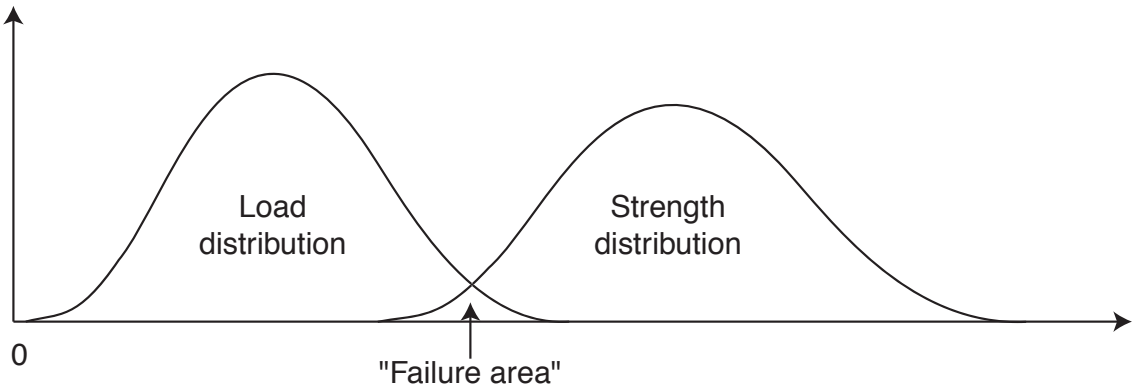
Different approaches

- Hardware reliability – with two different approaches:
  - Structural reliability
    - Also called the *physical* approach
    - Based on the assessment of loads and stresses
    - Mainly applicable to structural elements
  - Systems reliability
    - Also called the *actuarial* approach
    - Based on the study of the time-to-failure of single components
    - Mainly applicable to components and systems
- Software reliability
- Human reliability

Structural reliability

Basic idea

A structural element has the strength S and is exposed to a load L both of which are random variables.



The element will fail when $S < L$.

The *reliability* of the item is defined as:

$$R = \Pr(S > L)$$

Single load application

$$R = \Pr(S > L) = \int_0^\infty \Pr(S > l)\, f_L(l)\, dl$$
$$= \int_0^\infty \left(\int_l^\infty f_S(s) \right) f_L(l)\, dl$$

or

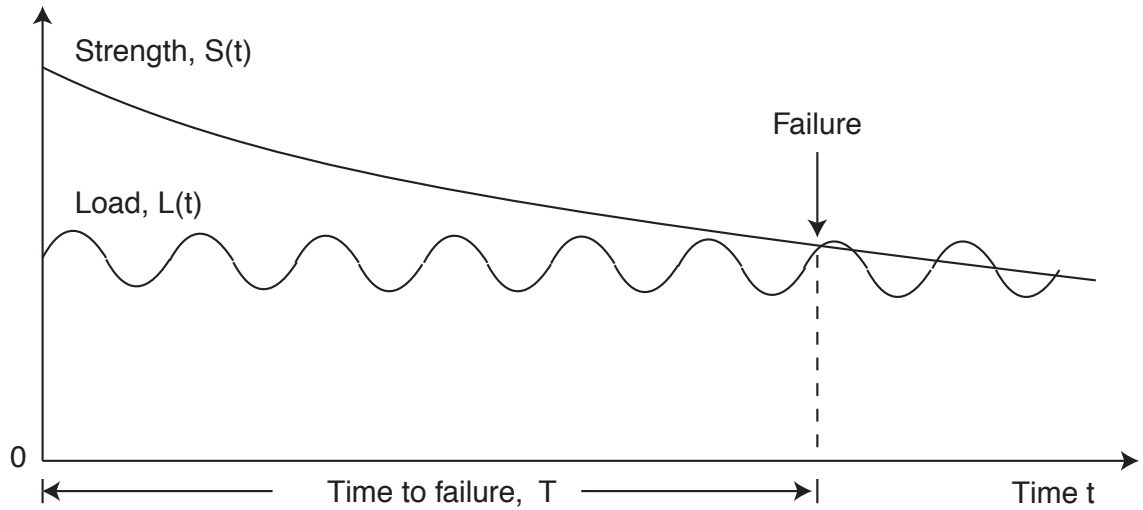
$$R = \Pr(L < S) = \int_0^\infty \Pr(L < s)\, f_S(s)\, ds$$
$$= \int_0^\infty F_L(s)\, f_S(s)\, ds$$

There are a lot of approaches to solve these integrals.

Structural reliability

Time dependent

In practice, both the strength S and the load L vary with the time t.



The time to failure T is

$$T = \min\{t; S(t) < L(t)\}$$

and the reliability $R(t)$ may now be defined as

$$R(t) = \Pr(T > t)$$

Structural reliability

Challenges

- The strength is multi-dimensional and must be expressed as a vector $\mathbf{S}$
- The load is multi-dimensional and must be expressed as a vector $\mathbf{L}$
- The strength and the load may be dependent random vectors.
- The strength at time t is generally depending on the load history $\mathcal{H}_t$ up to time t

Safety factor

Many elements are designed with a safety factor, which is sometimes defined as

$$\text{SF} = \frac{\text{Strength of the element}}{\text{Load placed on the element}} = \frac{S}{L}$$

or, perhaps as

$$\text{SF} = \frac{E(S)}{E(L)} = \frac{\mu_S}{\mu_L}$$

or even

$$\text{SF} = \frac{\text{mode}(S)}{\text{mode}(L)}$$

Safety margin

The safety margin is the "normalized" difference between the strength and the load on the element

$$\mathrm{SM} = \frac{\mu_\mathrm{S} - \mu_\mathrm{L}}{\sqrt{\sigma_\mathrm{S}^2 + \sigma_\mathrm{L}^2}}$$

Loading roughness

The loading roughness of an element is defined as

$$\mathrm{LR} = \frac{\sigma_\mathrm{L}}{\sqrt{\sigma_\mathrm{S}^2 + \sigma_\mathrm{L}^2}}$$

Actuarial approach

The time to failure T is considered as a random variable with a probability distribution $F(t)$, with parameters that are estimated based on field data.

The distribution may be decided based on physical interpretation of the properties of the distribution, e.g., by studying the failure rate function.

This is the topic of the current book/course.

Reliability

☞ Reliability: The ability of an item:

- to perform a *required function*,
- under given environmental and operational *conditions*, and
- for a stated *period of time*

[IEC 60050-191]

Quality

☞ Quality: The totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs [ISO 8402]

Maintainability

☞ Maintainability (1): The probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval, when the maintenance is performed under stated conditions and using stated procedures and resources. [IEC 60050-191]

☞ Maintainability (2): The measure of the ability of an item to be retained in or restored to specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. [MIL-STD21C]

Maintenance

☞ Maintenance: The combination of all technical and administrative actions, including supervision actions, intended to retain an item in, or restore it to, a state in which it can perform a required function. [IEC 60050-191]

- Maintenance can be corrective or preventive
- Maintenance should not be mixed with the related concept *maintainability*

Availability – 1

☞ Availability: The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided

[IEC 60050-191]

- Note 1: This ability depends on the combined aspects of the reliability performance, the maintainability performance and the maintenance support performance.
- Note 2: Required external resources, other than maintenance resources do not affect the availability performance of the item.

Availability – 2

The *availability* of an item at time t

$$A(t) = \Pr(\text{item is functioning at time } t)$$

The *average availability* (under certain conditions)

$$A_{\text{avg}} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

where

$$\text{MTTF} = \text{Mean time to failure}$$
$$\text{MTTR} = \text{Mean time to repair}$$

Safety

☞ Safety (1): Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property.

[MIL-STD-882D]

☞ Safety (2): The expectation that a system does not, under defined conditions, lead to a state in which human life is endangered. [DEF-STAN 00-56]

☞ Safety (3): A state where the risk has been reduced to a level that is as low as reasonably practicable (ALARP) and where the remaining risk is generally accepted. [Preferred definition]

Security

☞ Security: Dependability with respect to prevention of deliberate hostile actions.

- Security is often used in relation to information and computer systems. In this context, security may be defined as "dependability with respect to prevention of unauthorized access to and/or handling of information" [Laprie 1992].
- The security of critical infrastructures is thoroughly discussed in CCIP (1997)

Dependability

☞ Dependability (1): The collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance [IEC 60300]

☞ Dependability (2): A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission. (Item state during a mission includes the combined effects of the mission-related system R&M parameters but excludes non-mission time).

[MIL-STD 721C]

Reliability measures

- Mean time to failure (MTTF)
- Number of failures per time unit (*failure rate*)
- The probability that the item does not fail in a time interval $(0, t]$ (*survival probability*)
- The probability that the item is able to function at time t (*availability at time t*)

Important standards

- IEC 60050-191 Dependability and quality of service (the most important terminology standard)
- IEC 60300 Dependability management (a series of important standards)
- IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems (the standard for safety-instrumented systems)

Application areas

- Reliability engineering (i.e., the design and development of reliable systems)
- Verification of reliability and quality
- Production assurance
- Warranty assessment
- Risk analysis
- Barrier assessment
- Maintenance planning and optimization
- Environmental assessment

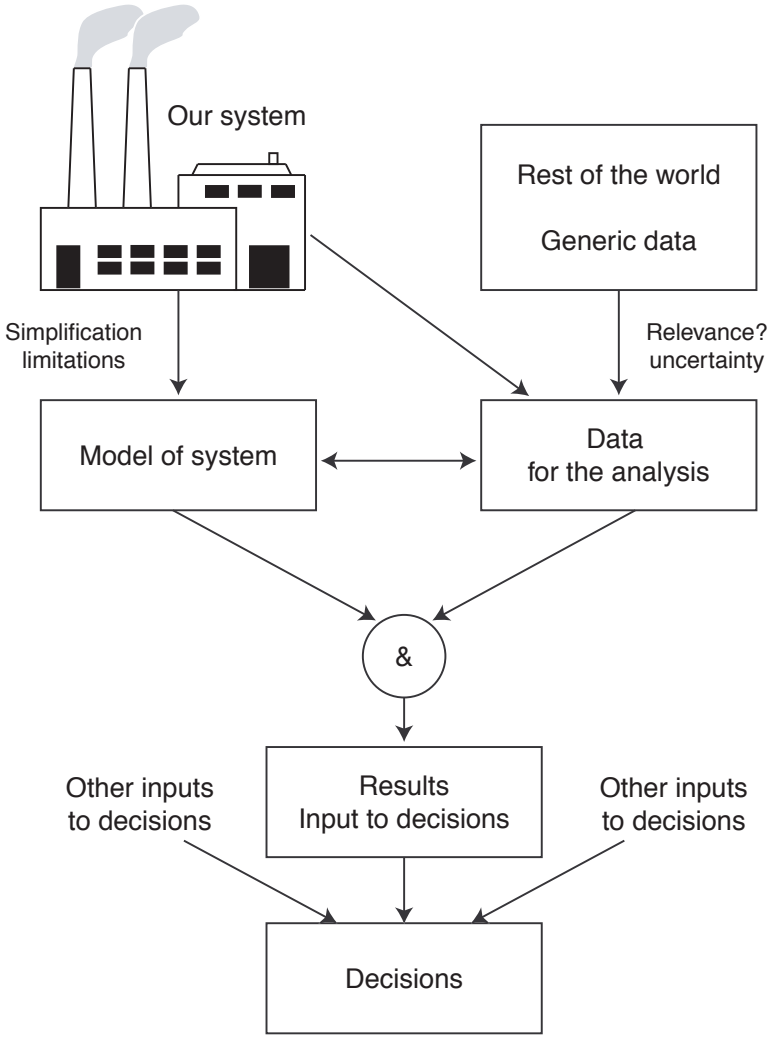
Models and uncertainties – 1

"…no model is absolutely correct. In particular situations, however, some models are more useful than others"

G. E. P. Box

- The model should be sufficiently simple to be handled by available mathematical and statistical methods
- The model should be sufficiently "realistic" such that the deducted results are of practical use.

Models and uncertainties – 2



RAMS activities in program phases – 1

- Feasibility phase
  - Definition of the system mission
  - RAMS requirements definition
- Design phase
  - Technical specifications
  - Reliability allocation
  - Hazard identification
  - Assessment of design options
- Development phase
  - Design validation
  - Reliability testing
  - Reliability growth

RAMS activities in program phases – 2

- Manufacturing phase
  - Product realization tasks
  - Assurance of RAMS performance
- Operations phase
  - Ensure that the RAMS objectives are reached
  - Data collection and analysis
- Dismantling phase