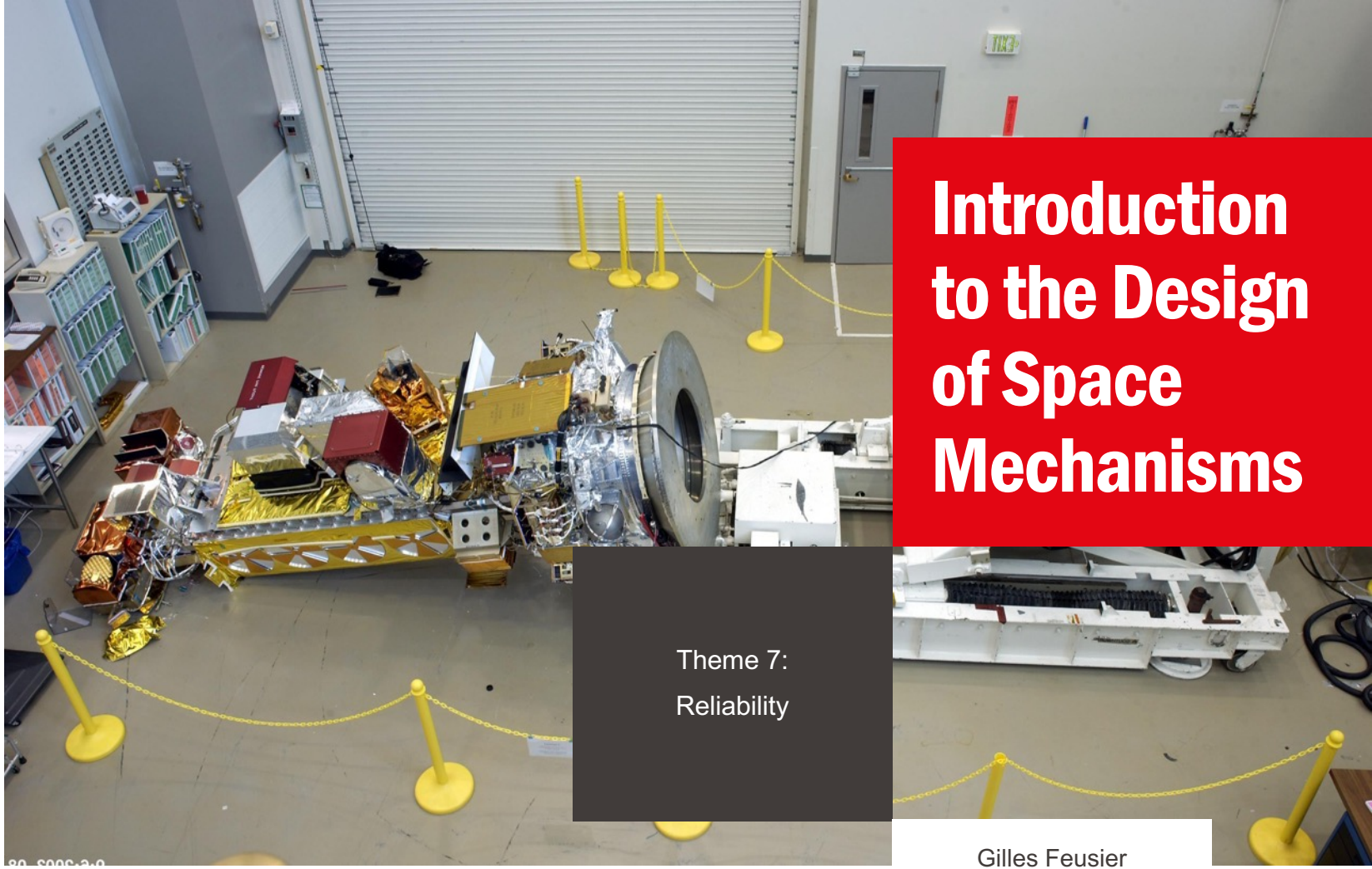


Introduction to the Design of Space Mechanisms

Theme 7:

Reliability

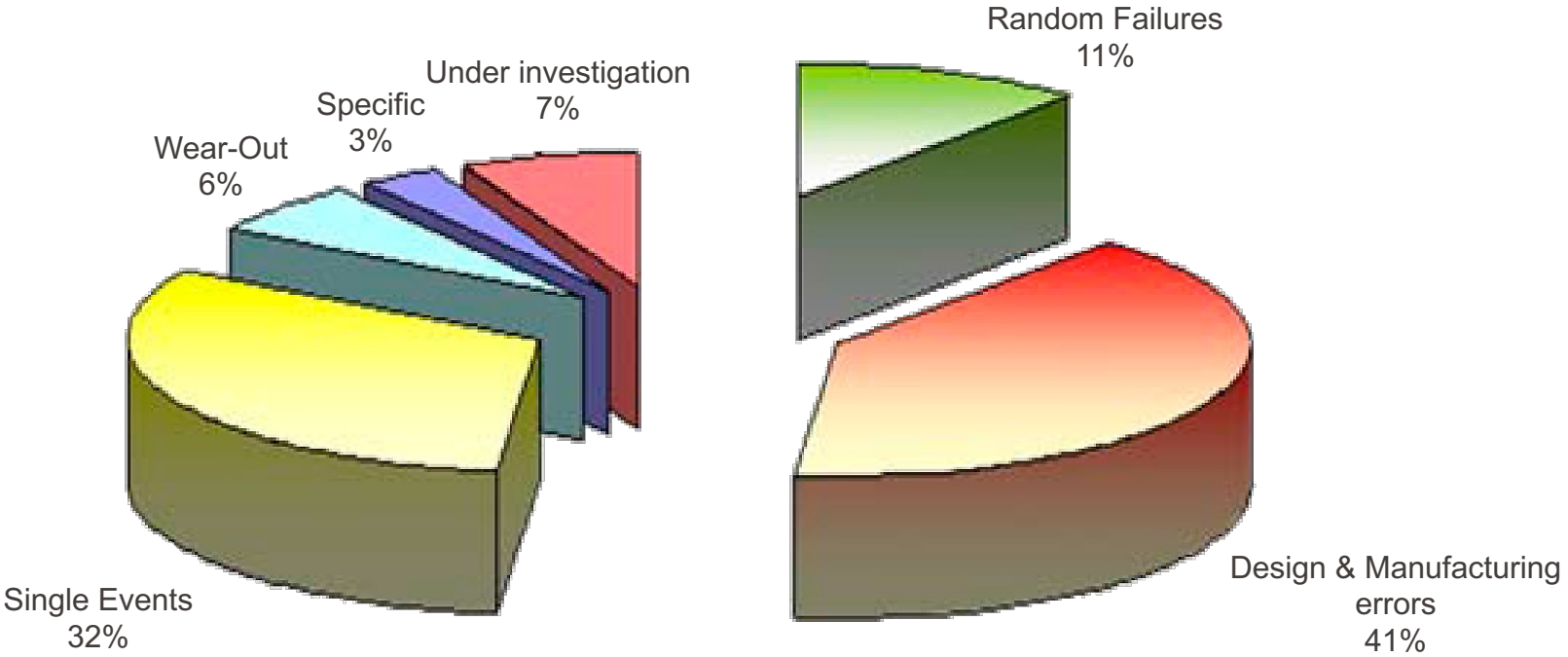
Gilles Feusier

Reliability

- Goal
  - To ensure the performances during the whole mechanism lifetime
  - To give at system level the risks associated with the use of the mechanism
    - Top-down: down to the lowest level
  - To ensure safety
    - Of human life (in particular for manned missions)
    - Of environment (before, during and after operational life)
    - Of material (on board and ground equipment, properties)
  - But also
    - To ensure the mastering of the mechanism production means
    - To ensure the delivery time and the cost
    - To produce comprehensive and complete documentation

Failure Repartition

In-orbit feedback: Anomaly types repartition



Source: ESA White Paper “Effective Reliability Prediction for Space Applications”, ESA-TECQQD-WP-0969, 2016
RAMS (Reliability, Availability, Maintainability and Safety) In-Orbit Data Exploitation (RIDE) Anomaly Root Cause Repartition (ESA GSTP activity)

Reliability

- Systematic management and control approach
  - Quality assurance
    - Quality system (QA): *ECSS-Q-ST-20C Rev.2*
    - Product assurance (PA): *ECSS-Q-ST-20C Rev.2*
  - Management (organization, planning, documentation configuration …): *ECSS-M-ST-10C Rev.1*
  - Risk management
    - How to control and manage risks: *ECSS-M-ST-80C*
    - Dependability (reliability, availability, maintainability): *ECSS-Q-ST-30C Rev.1*
    - Safety management: *ECSS-Q-ST-40C Rev.1*
- Systematic design and analysis approach
  - Control and organization of the full system, the mechanism being one part of the system: System Engineering: *ECSS-E-ST-10C Rev.1*
  - Control of the materials, mechanical parts and processes: *ECSS-Q-ST-70C Rev.2*
  - Structural design methods: *ECSS-E-ST-32C Rev. 1*
- Standards
  - Reliability Prediction of Electronic Equipment *MIL-HDBK-217F (obsolete)*
- Handbooks and Guides
  - Components data sources and their use *ECSS-Q-HB-30-08A*
  - Reliability Methodology for Electronic Systems *FIDES Guide 2009, Edition A*
  - Handbook of Reliability Prediction Procedures for Mechanical Equipment *NSWC-11, May 2011*
  - Nonelectronic Parts Reliability Data Publication *NPRD-2016*

Note: this is a non-exhaustive list of base documents, which are relevant, but more detailed references may be required to cover all the aspects of reliability

Reliability

- Systematic use of design rules
  - General analysis of the design (documents will evolve during the whole project)
    - Risk analysis (functions, hazards)
    - Analysis of the Single Points of Failure (SPF)
    - Critical item control (generates development actions for each critical element)
    - Failure Modes, Effects and Criticality Analysis (FMECA)
- Structural analysis
  - Evaluation of the maximum stresses and deformations, analysis of the vibration modes
  - Thermal analysis
  - Specific analysis in function of the requirements (radiations, aging, wear, fatigue, outgassing, lubrification …)
- Verification/Validation
  - Compliance to the requirements
  - Traceability (justifications, changes, decisions, …)

Technology Readiness Level

http://tiny.cc/EE580TRL

© ESA/ATG medialab

TRL 9 — Flight proven

TRL 8 — Flight qualified

TRL 7 — Model demonstration for operational environment

TRL 6 — Models (full scale) demonstration in relevant environment

TRL 5 — Breadboards (reduced scale) verification in relevant environment

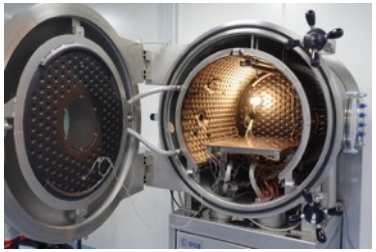
TRL 4 — Functional verification

TRL 3 — Proof-of-concept

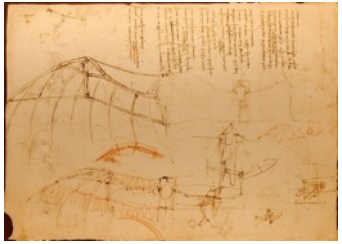
TRL 2 — Application formulated

TRL 1 — Basic principle

Source: ESA



© Akron NV



© L. Da Vinci

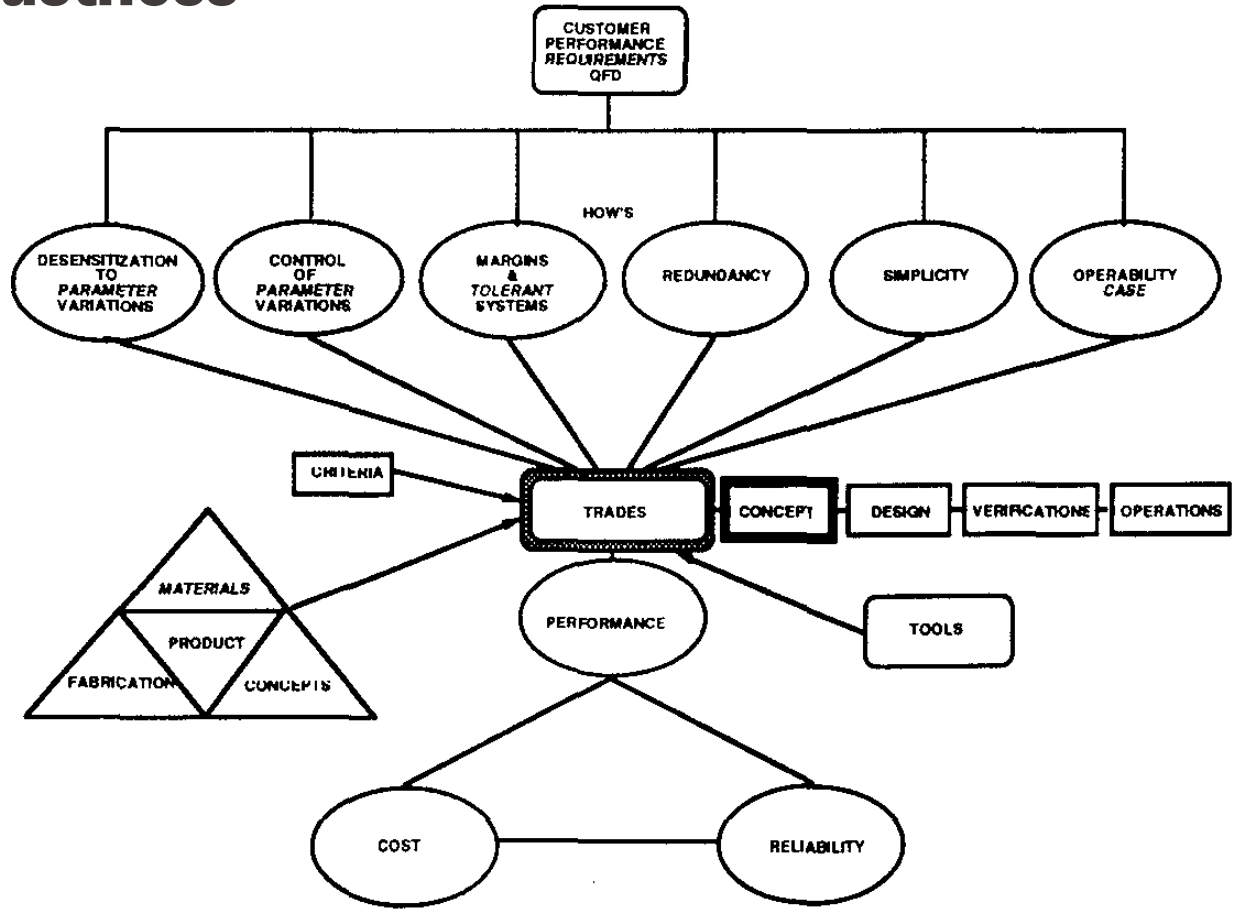
Cf. ECSS-E-AS-11C/ISO 16290
and
ECSS-E-HB-11A “Technology readiness level (TRL) guidelines”

Robustness

- Ability to perform under a variety of circumstances; ability to deliver desired functions in spite of changes in the environment, uses, or internal variations that are either built-in or emergent (Prof. O. de Weck, MIT)

- Space systems may spend significant time operating in degraded or off-nominal states
  - Yet current early-stage design focuses on improving performance in the nominal or most-likely state.
  - Future ultra long endurance vehicles require more attention to robustness in off-nominal states

Robustness



Source: Robert Ryan “Robustness”, AIANAHS/ASEE Aerospace Design Conference (1993), AIM-93-0974

Creation of the Reliability Data Package

- Input data
  - Requirements
  - Definition Data Package (or, at the project starts: preliminary concept)
- Creation of the Failure Mode Effects and Criticality Analysis (FMECA)
  - Describe the function of the mechanism
    - Schemes and words
    - Description and enumeration of the redundant parts
    - Functional fault tree
    - Enumeration of the base rules specific to the project reliability
  - List the **failure modes** for each function or part of the mechanism
  - Search for the possible causes of each failure mode
  - Search for the effects of each failure mode
  - Give values for the Severity (SN), the Probability (PN) and the Criticality (CN)

Example of FMECA (Function)

ECSS-Q-ST-30-02C
6 March 2009

Failure Modes Effects and Criticality Analysis (FMECA)

Product:	System:	Subsystem:	Equipment:

Ident. number	Item/ block	Function	Failure mode	Failure cause	Mission phase/ Op. mode	Failure effects a. Local effects b. End effects	Severity classification	Failure detection method/ observable symptoms	Compensating provisions	Severity Number SN	Probability and PN	Criticality Number CN	Recommendations	Remarks
								…		1-4	X 1-4	1-16		

Ball-bearing flange screw

Maintain ball-bearing pre-load

Screw breakage

- Vibrations
- Thermal cycles
- …

- Ground transportation
- Testing
- Launch
- In-orbit
- Specific in-orbit phases

Local:
- Loss of preload

End effects:
- Loss of pointing accuracy
- Early wear out

- Catastrophic
- Critical
- Major
- Minor or Negligible

Source: ECSS-Q-ST-30-02C Failure modes, effects (and criticality) analysis (FMEA/FMECA), Figure C-1

Example of FMECA (Process)

ECSS-Q-ST-30-02C
6 March 2009

Process Failure Modes, Effects and Criticality Analysis (FMECA)

Analysed process:				System:			Subsystem:				Equipment:
Ident. number	Item	Description	Failure mode/ Failure cause	Failure effects: a) safety b) product c) process d) programmatic e) others	Detection means	Existing preventive or compensatory provisions	Severity SN	Occurrence PN	Detection DN	Criticality CN	Recommendations and remarks

Source: ECSS-Q-ST-30-02C Failure modes, effects (and criticality) analysis (FMEA/FMECA), Figure F-1

Creation of the Reliability Data Package

- SN: Severity Number
- PN: Probability Number
- (DN: Detectability Number)
- CN: Criticality Number

$$CN = SN \cdot PN \cdot (DN)$$

Severity level	Severity category	SN
1	Catastrophic	4
2	Critical	3
3	Major	2
4	Negligible	1

Level	Limits	PN
Probable	P > 1E-1	4
Occasional	1E-3 < P ≤ 1E-1	3
Remote	1E-5 < P ≤ 1E-3	2
Extremely remote	P ≤ 1E-5	1

Source: ECSS-Q-ST-30-02C
Failure modes, effects (and criticality) analysis (FMEA/FMECA)

Creation of the Reliability Data Package

- Severity of consequences

Severity category	Severity number (SN)	Description of consequences (failure effects)	
		Dependability effects (as specified in ECSS-Q-ST-30)	Safety effects (as specified in ECSS-Q-ST-40)
Catastrophic	4	Failure propagation (refer to 4.2c)	Loss of life, life-threatening or permanently disabling injury or occupational illness.
			Loss of an interfacing manned flight system.
			Severe detrimental environmental effects.
			Loss of launch site facilities.
			Loss of system.
Critical	3	Loss of mission	Temporarily disabling but not life-threatening injury, or temporary occupational illness.
			Major detrimental environmental effects.
			Major damage to public or private properties.
			Major damage to interfacing flight systems.
			Major damage to ground facilities.
Major	2	Major mission degradation	
Minor or Negligible	1	Minor mission degradation or any other effect	

Source: ECSS-Q-ST-30-02C Failure modes, effects (and criticality) analysis (FMEA/FMECA)

Creation of the Reliability Data Package

How to define the criticality analysis parameters? **SEVERITY**

- ***SN*** (depends on the system level, on the type of mission …)
  - Negligible — Negligible impact on the function
    Example: loss of a telemetry sensor (if not required for the function)
  - Major — Jeopardize a local function
    Example: loss of a SADM slipring power line
  - Critical — Jeopardize an upper level function, without risk of propagation
    Example: significant electrical noise of the slipring
  - Catastrophic — Jeopardize the mission
    Example: blocking of the SADM rotation

Creation of the Reliability Data Package

How to define the criticality analysis parameters? **PROBABILITY**

- ***PN*** (examples)
  - Extremely Remote — Not much chance this will become problem
  - Remote — Risk like this may turn into a problem once in awhile
  - Occasional — There is an even chance this may turn into a problem
  - Probable — Everything points to this becoming a problem

Criticality Matrix

Source: ECSS-Q-ST-30-02C
Failure modes, effects (and criticality) analysis (FMEA/FMECA)

Severity category	SNs	Probability level			
		10^{-5}	10^{-3}	10^{-1}	1
		PNs			
		1	2	3	4
catastrophic	4	4	8	12	16
critical	3	3	6	9	12
major	2	2	4	6	8
negligible	1	1	2	3	4

- An item shall be considered a critical item if:
  1. a failure mode has failure consequences classified as catastrophic, or
  2. a failure mode is classified as CN greater or equal to 6 […]

Reliability prediction

- Main purposes:
  - to establish whether a design meets/exceeds the system reliability requirement.
  - to focus attention on weak parts/problem areas in the design.
  - to assess the impact of design changes on system reliability.
  - to compare competing designs or design alternatives.
  - to determine the number and type of spare units for repairable systems.
  - to support the system availability, repair, maintenance and lifecycle cost assessment.

Source: ESA White Paper “Effective Reliability Prediction for Space Applications”, ESA-TECQQD-WP-0969, 2016

Reliability modelling

- End-to-end process, composed of the following steps
  - **Specification** of reliability requirement at system level
  - **Allocation** of reliability requirements to lower levels (down to unit level)
  - **Verification** of reliability specifications with reliability prediction at component level using handbook sources and supplier data (e.g. board level) followed by modelling at higher levels with reliability block diagrams (RBD) or simulation techniques (Monte Carlo, Markov, Bayesian networks, …)
  - Potentially reliability predictions can be **updated** with test and or in-orbit data

Source: ESA White Paper “Effective Reliability Prediction for Space Applications”, ESA-TECQQD-WP-0969, 2016

Reliability

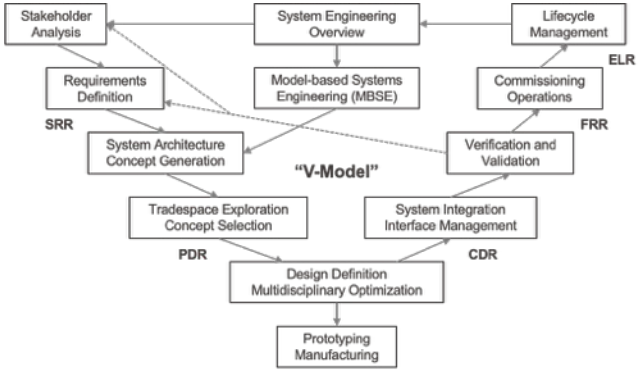
- Systematic Test Plan, Test Philosophy (which models, sub-systems …)
  - Development tests (breadboard models **BBM**)
    - Verification of the function at component level
      E.g. operation of a component in thermal vacuum, functional verification of a non-qualified component, unknown properties of materials, …
  - Functional tests of **EM** (Engineering Model)
    - Search of the operational limits (maybe destructive)
  - Qualification tests of **QM** (Qualification Model)
    - The level of the qualification tests is in general more severe than the level of the acceptance tests applied to the FM
  - Acceptance tests of **FM** (Flight Model)
    - Verify the workmanship, the proper built.

Reliability

- Creation of a complete documentation (shall be up-to-date!)
  (following list gives key documents, but is not exhaustive)
  - Requirements
    - Mechanism
    - Components
    - Tests and verifications
    - …
  - Design description
  - Interface Control Document (ICD)
  - Declared Material List (DML) and Declared Process List (DPL)
  - Mechanical and structural analysis
  - Manufacturing, Assembly, Integration and Verification Plan (MAIV)
  - Procedures (tests, manufacturing, assembly, material treatments, …)
  - Configuration Item Data List (CIDL)
  - As-Built Configuration Data List (ABCL)
  - Reports (tests, qualifications, specific analysis, …)
  - Delivery Data Package (DDP)

Reliability ⟷ Systems Engineering

- Development follow-up processes:
- Documentation, design, industrial organization, sub-contractor control performed during the reviews:
  - Preliminary Design Review (PDR)
  - Critical Design Review (CDR)
  - Test Readiness Review (TRR)
  - Delivery Review Board (DRB)
  - Material Review Board (MRB)
  - Quality Audit



Based on: Olivier de Weck, Fundamentals of Systems Engineering (2020)

- Specific reviews
  - **Internal**: internal design discussions, brainstorming, organization, management and planning meeting, procurement meeting
  - **Progress meeting** (with customer)
  - **Follow-up of the suppliers**
    - Technical reviews, progress meetings, delivery reviews, MRB
    - Quality Audit

Reliability at system level

Project	Directorate (purpose)	Specified Lifetime	Satellite Reliability Specification	Reference
Cryosat 2	Earth Observation (investigation of Ice Polar Regions)	3.5 years including commissioning and validation.	The success probability of 70% or better is required for nominal performance for the overall mission time.	CS-RS-ESA-SY-0006 (SRD)
GOCE	Earth Observation (gravity field)	20 months	No quantitative reliability specification (A reliability target was derived from an availability requirement by the prime)	GO-RS-ESA-SY-0002 (SRD)
Mars Express	Science (investigation of Mars)	1610 days (extended)	No quantitative reliability specification	MEX-EST-RS-2003
Meteosat Second Generation	Earth Observation, (weather)	7 years	The specified reliability figure is 0.68 for a 7 years in orbit mission.	MSG.ASC.SA.SY>0075
Meteosat Third Generation (MTG)	Earth Observation (weather)	8.5 years following a maximum on-ground storage of 10 years	• **SA-REL-010**: Regarding the FCI mission, the reliability of the MTG-I satellite shall be higher than 0.75 at the end of the satellite specified lifetime. • **SA-REL-020**: Regarding the LI mission, the reliability of the MTG-I satellite shall be higher than 0.75 at the end of the satellite specified lifetime.	MTG.ESA.SA.RS.0062 (SRD)
			...	
Rosetta	Science (investigation of a comet)	3888 days	The reliability target for the Rosetta avionics is given equal to 0.93 for a mission duration of 11 years (3888 days).	RO.DSS.RS.2001
Sentinel 1	Earth Observation	7 years after a maximum on-ground storage of 10 years.	• **PAS-004** :The Platform shall provide the nominal required support to the Payload instrument with a probability better than 0.80 over the specified life, including the launch phase.	S1-RS-ESA-SY-0001 (SRD)
			...	

Source: ESA White Paper “Effective Reliability Prediction for Space Applications”, ESA-TECQQD-WP-0969, 2016

Failure Probability

A single mechanism: no statistic

Manufacturing and testing of many identical mechanisms

→ Failure statistic is possible

Failure Probability

- Principle of analysis of the failures
  - **Test** of the functional parts of a mechanism
    - To get **statistical data about the components** (after testing many identical or similar systems)
      - Example: ball-bearings, connectors, solders, electronic components …
      - Difficulty: to get meaningful test data in similar use conditions as for the considered application (cf. e.g. ECSS-Q-HB-30-08A)
    - To get **statistical data about meaningful characteristics of the materials** (ultimate strength, yield strength, fatigue, …) in the same temperature ranges as for the considered application
    - To **test the "non-repeatable" characteristics**, outside of their theoretical performances (loads, temperature, lifetime, … including safety factors determined with respect to the nominal conditions of the considered application)
  - **Calculate the probability of failure** of the mechanism by associating the probabilities of failure of the individual parts according to defined schemes.
  - Difficult analysis: availability of meaningful data

Failure Probability

- **Failure probability *F(t)***
  - N systems tested in parallel
  - In a time range t_i-t_{i-1}, f_i systems failed

    The failure probability becomes $F(t_i) = \frac{\sum f_i}{N}$
  - Passage to the limit when t_i - t_{i-1} and $i \longrightarrow \infty$: $F(t) = \int_0^t f(\tau) d\tau$

    Where $f(\tau)$ is the **Probability Density Function** (**PDF**), i.e. the probability density of failure.
- **Reliability *R(t) = 1 – F(t)*** (1)
- $F(t)$ and $R(t)$ are the measurable functions. An auxiliary function ***Z(t)*** is defined: the **failure rate**.

$$Z(t) = \frac{dF(t)/dt}{R(t)} = \frac{F'(t)}{R(t)} = \frac{f(t)}{R(t)} \quad \Rightarrow \quad f(t) = Z(t) \cdot R(t) = Z(t) \cdot (1 - F(t)) \qquad (2)$$

Failure Probability

- With (1): $R(t) = 1 - F(t)$ ➡ $\frac{dR(t)}{dt} = R'(t) = -F'(t)$ (3)

- Consequently: $Z(t) = \frac{F'(t)}{R(t)} = -\frac{R'(t)}{R(t)} = -\frac{d[\ln(R(t)]}{dt}$ (4)

  By integrating (4): $R(t) = e^{-\int_0^t Z(x)dx}$ (5)

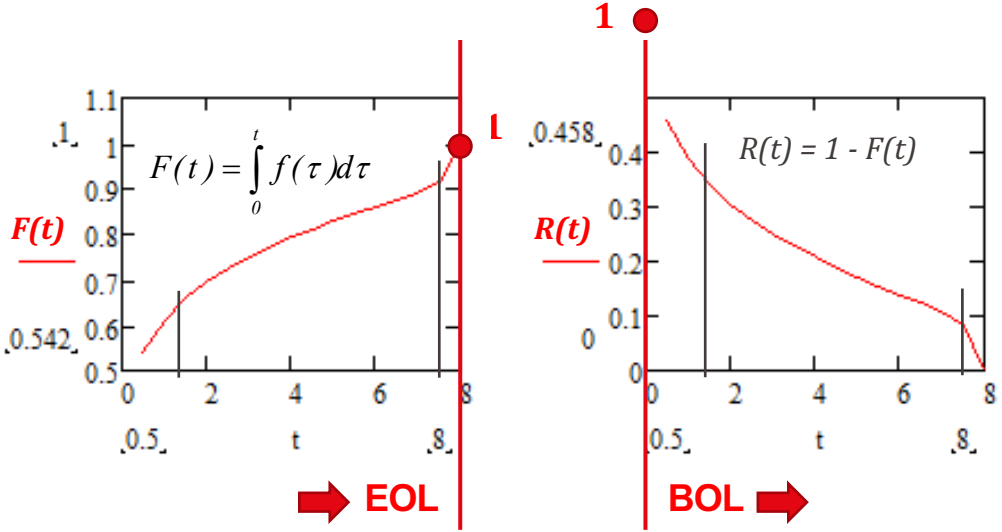
  With (2) here above: $f(t) = Z(t) \cdot e^{-\int_0^t Z(x)dx}$ (6)

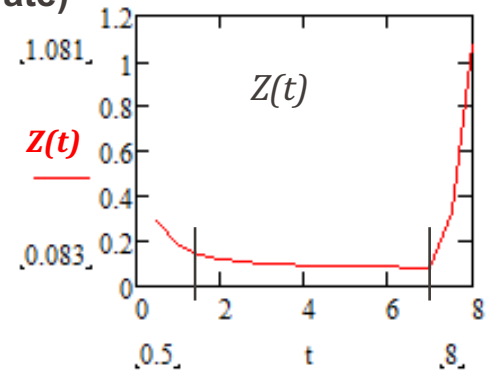
- In the case $\boldsymbol{Z(t) = \lambda = constant}$, (6) becomes (for $t > 0$): $\boldsymbol{f(t) = \lambda \cdot e^{-\lambda \cdot t}}$ (7)

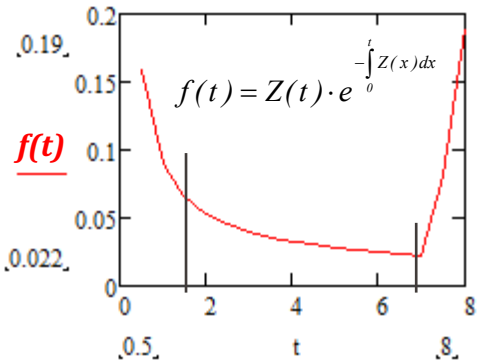
  And the reliability: $\boldsymbol{R(t)} = 1 - \int_0^t f(x)dx = \boldsymbol{e^{-\lambda \cdot t}}$ (8)

Failure Probability

- Characteristic shape of **Probability Density Function** (PDF, i.e. $f(t)$):
  - Typical bathtub curve shape of the function $Z(t)$ **(failure rate)**
  - The **Cumulative Distribution Function** (CDF) is **1**
    - At **end of life** (**EOL**) for the **Probability of failure** $F(t)$
    - At **beginning of life** (**BOL**) for the **Reliability** $R(t)$





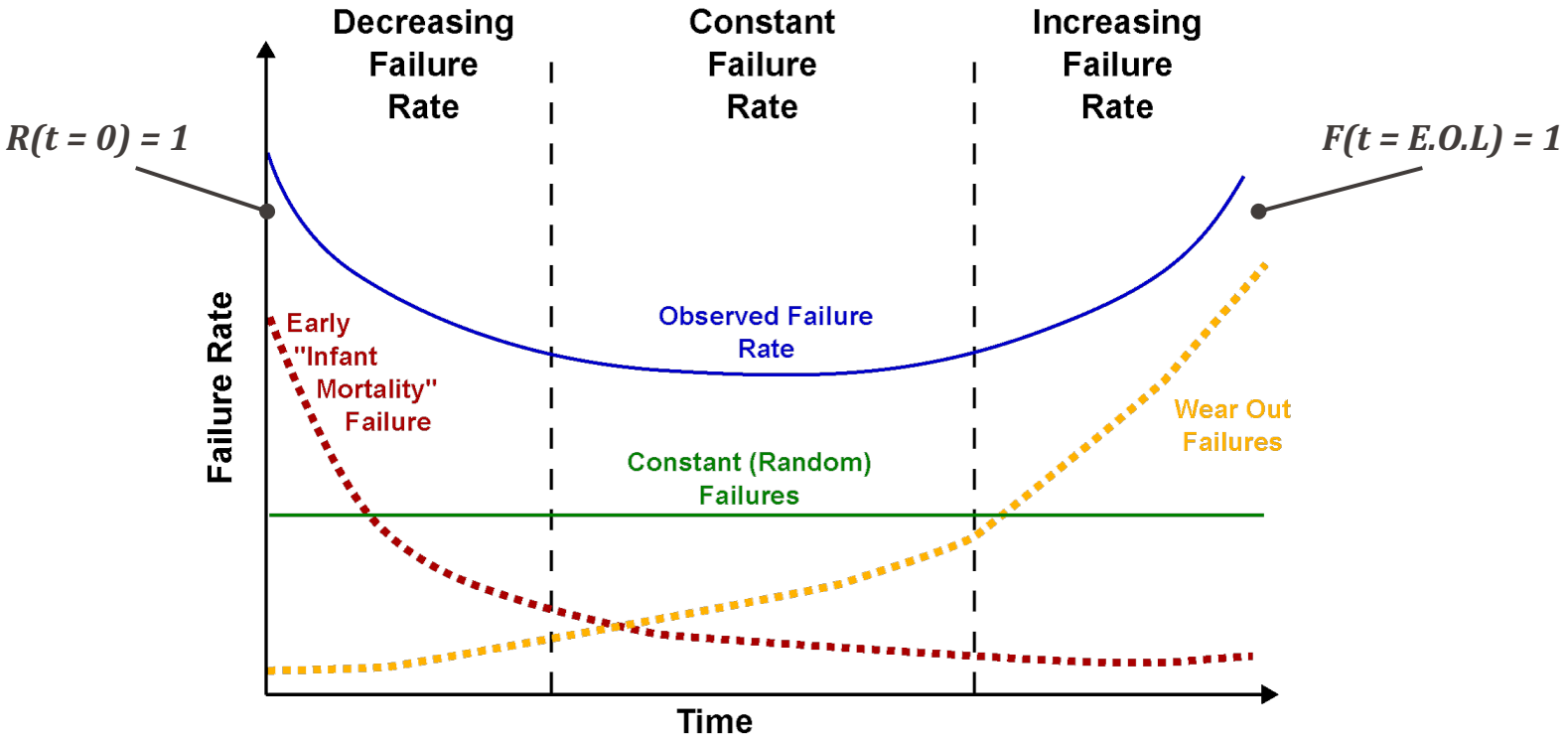


Failure Probability

- Typical lifetime behavior of a system
  - First phase**: running-in period** (early infant mortality failures)
    - Related to manufacturing and materials defects
    - High Failure Probability Density Function (PDF) at the beginning, then rapid decrease
  - Second phase: **random failures**
    - Various causes, related to design, to usage, …
    - Failure Probability Density Function (PDF) more or less constant
  - Third phase: **end of life** (wear out failures)
    - Mainly wear out of one or several components
    - Steep increase of the Failure Probability Density Function (often in relation with failure propagation effects)

Failure Probability

- Distribution of Weibull

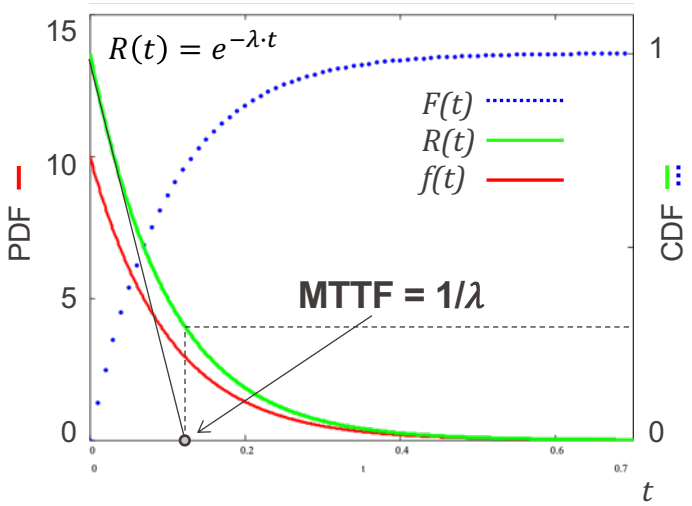


Source: ESA White Paper “Effective Reliability Prediction for Space Applications”, ESA-TECQQD-WP-0969, 2016

Failure rate

- When the **Probability Density Function is constant** with respect to the time, a constant failure rate λ is used
  - Units:
    - Number of failures / units of …xxx…
    - …xxx… can be hours, kilometers, revolutions, cycles, …
    - 10^{-9} failures / hour is named "**FIT**" and is very common in the evaluation of electronic components.

- **MTTF: Mean Time To Failure**
  - It is the **mean value of *f(t)*** $\left(f(t) = \lambda \cdot e^{-\lambda \cdot t} \right)$
  - It corresponds to the **survival of 36.8%** of the samples
  - Consequently **a system that shall have a lifetime of 15 years shall have a MTTF much larger than 15 years**



Failure rate

- Orders of magnitudes
  - Required reliability for a mechanism: 0.999
  - Lifetime: 15 years
  - **What shall be the failure rate of such a mechanism?**
- Solution: $R(15\ years) = 0.999 = e^{-\lambda \cdot (15 \cdot 365 \cdot 24)} = e^{-\lambda \cdot 131400}$
- Hence $\lambda = -\frac{\ln(0.999)}{1314000} = 7.6 \cdot 10^{-9}$ [Failures/h] = 7.6 FIT
- This is a usual value for a component, but a very low value at system level!
  - In the case of a required reliability of 0.9999, the failure rate would even be one order of magnitude lower!!
  - How to solve this issue?

Failure rate

- How to solve previous side issue (very low required failure rate)?

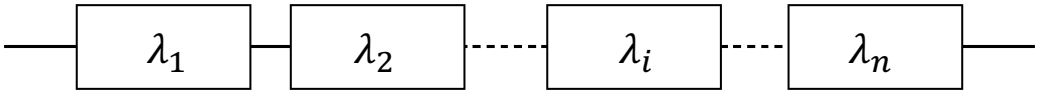
  - Introduce the effective operating time
    ➡ The effective operating time is limited
  - Example: 5'000 cycles of 0.2s lead to a total operating time, including a safety factor of 1.5, of 0.42h
    ➡ λ(0.42h, 0.9999) = 238'107 FIT

    This value is acceptable without too much concerns

    CAUTION: the non-operational status of the mechanism could lead to other failure modes that shall also be taken into account!

Reliability of Systems

- Systems in series



$$R_S = \prod_i^n R_i = \prod_i^n e^{-\lambda_i \cdot t} = e^{-\sum_i^n (\lambda_i) \cdot t}$$

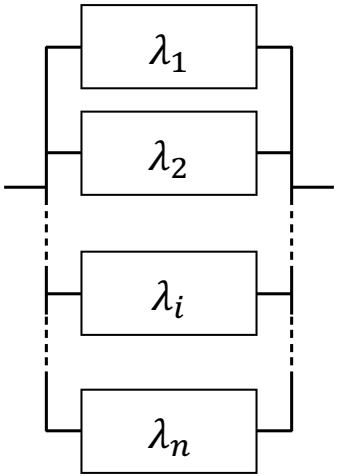
Reliability block diagrams (RBD)

$$\lambda_S = \sum_i^n \lambda_i$$

- Systems in parallel
  - Two cases
    - Cold redundancy: only one system operational at a time
    - Hot redundancy: all systems are operational during the whole lifetime

Reliability(cold redundancy) > Reliability(hot redundancy)

    - Systems in parallel: most of the time the reliability of n systems is calculated with the constrain that at least n - k systems shall work.



Reliability of Systems

- Common modes
  - The sub-systems are interacting
    - ➢ The failure rate depends on the number of failure of the system

  - Examples
    - Brushes or contacts in parallel
      - 4 brushes in parallel, 10 A ⟹ 2.5 A / brush
      - Failure of 1 brush ⟹ 3.3 A / brush : much higher current

    - Bolted system
      - Flange with 10’000 N axial load, held by 12 preloaded screws.
        Preload by screw: 800 N ⟹ 1’633 N / screw
      - Failure of 1 screw (e.g. untightened) ⟹ 1’709 N / screw

Extract of ECSS-E-ST-33-01C Rev.2: Mechanisms

4.2.5.2 Redundancy

a. During the design of the mechanism, **all single point failure** modes shall be identified.

b. All single points of failure should be **eliminated by redundant components**.

c. If single points of failure cannot be avoided, they **shall be justified** by the supplier and **approved** by the customer.

d. Redundancy concepts shall be agreed by the customer.

NOTE Redundancy concepts are selected to minimize the number of single points of failure and to conform to the reliability requirements.

e. Where a single point failure mode is identified and redundancy is not provided, **compliance with** the reliability, availability and maintainability requirements specified in **ECSS-Q-ST-30 shall be demonstrated**.

f. Unless redundancy is achieved by the provision of a complete redundant mechanism, active elements of mechanisms, such as sensors, motor windings, brushes, actuators, switches and electronics, shall be redundant.

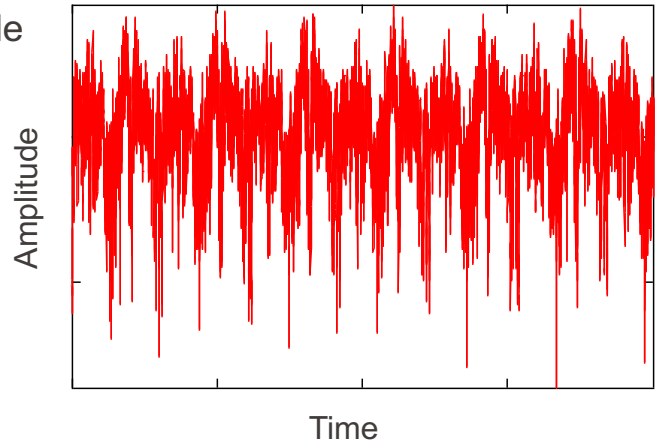
g. **Failure of one element or part** shall **not prevent** the other redundant element or part from **performing its intended function**, nor the mechanism from meeting its performance requirements specified in the specific mechanism specification.

NOTE High-reliability of a mechanism can be incorporated in a design by including component redundancy or high design margins. The aim is to deliver a design which is single failure tolerant.

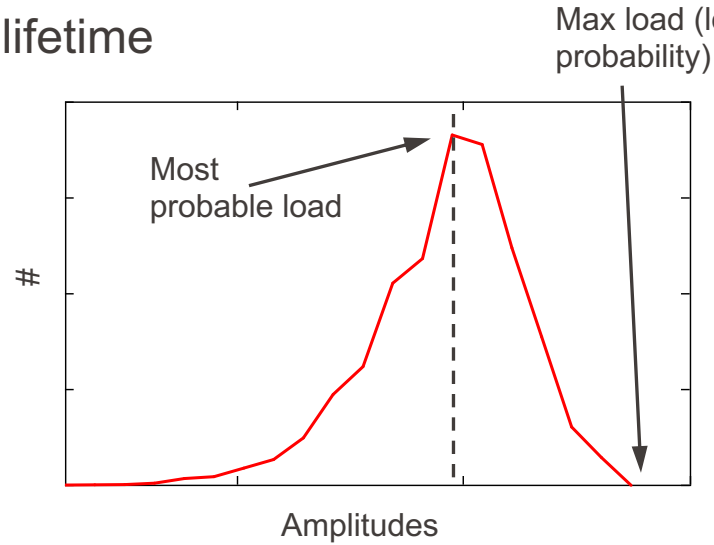
Reliability of structures

- Structures shall be sized with respect to:
  - Loads
  - Environmental constrains
  - Materials
- Loading cycles during the mechanism lifetime

Example



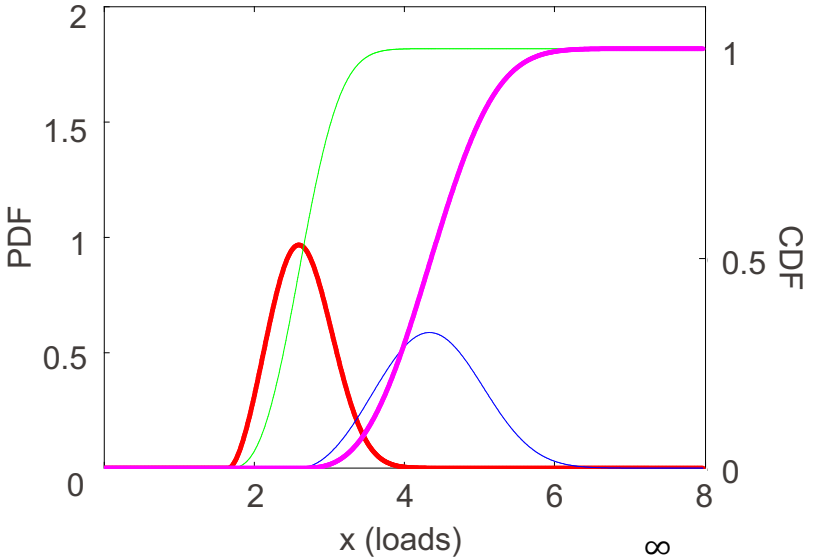
Load amplitude vs time (arbitrary units)



Histogram of the load amplitude

Reliability of structures

- Comparison of the loads (including time scattering) with the material strength
  - The characteristics of the material are also scattered!



$F_S(x)$: CDF of the loads

$F_L(x)$: CDF of the material allowable loads

$f_s(x)$: PDF of the loads

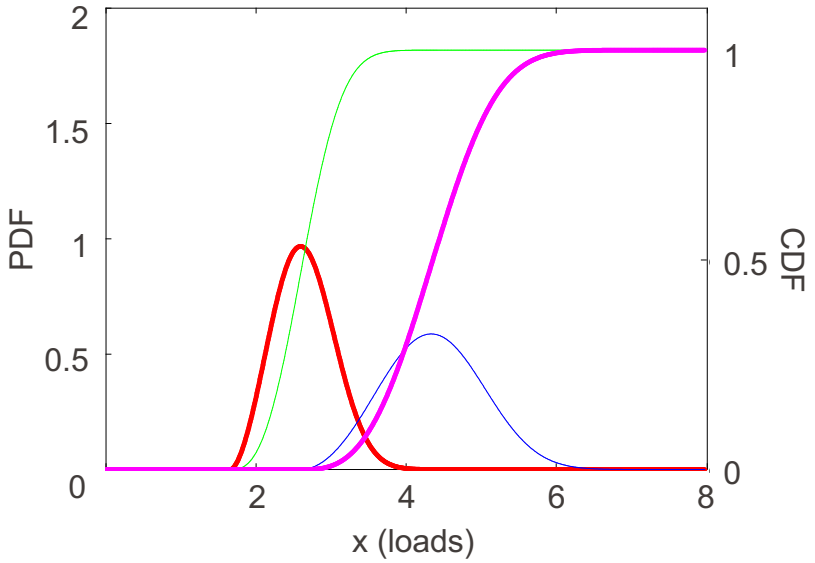
$f_l(x)$: PDF of the material allowable loads

Reminder
CDF: Cumulative Distribution Function
PDF : Probability Density Function

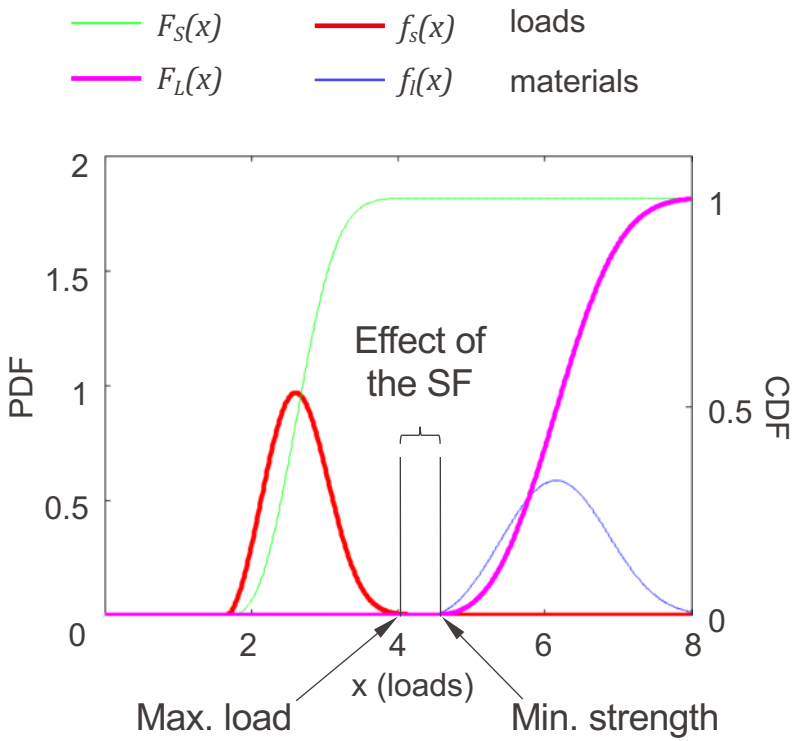
- Probability of failure: $P_D = \int_0^\infty f_s(x) \cdot F_L(x) \cdot dx$

Reliability of structures

- Effect of the Safety Factor (SF)



Overlapping of f_s and f_l:
High risk of failure!



No overlapping of f_s and f_l:
No risk (!) of failure for the used material

Reliability of structures

- Definitions
  - Safety Factor (SF)
    - Multiplication factor of the maximum load
    - Pre-defined for the design
    - Generally given by the requirements or the design rules
    - Used to reduce the risk of failure

      Example: Max. load: $L_{max} = 57\text{N}$

      Safety Factor: $SF = 1.25$

      Load that shall be taken into account for the design:

      $$\boldsymbol{L_{des} = SF \cdot L_{max}} = 71.25\text{N}$$

      Allowable material load: $L_{adm} = 93\text{N}$
  - Margin of Safety (MS)
    - Gives the margin related to the allowable material load: $\boldsymbol{MS = \frac{Allowable\ load}{Design\ load} - 1}$
    - With the previous example: $\boldsymbol{MS = \frac{L_{adm}}{L_{max} \cdot SF} - 1} = \frac{93\text{N}}{71.25\text{N}} - 1 = \boldsymbol{0.31 > 0}$

Reliability: Limitations

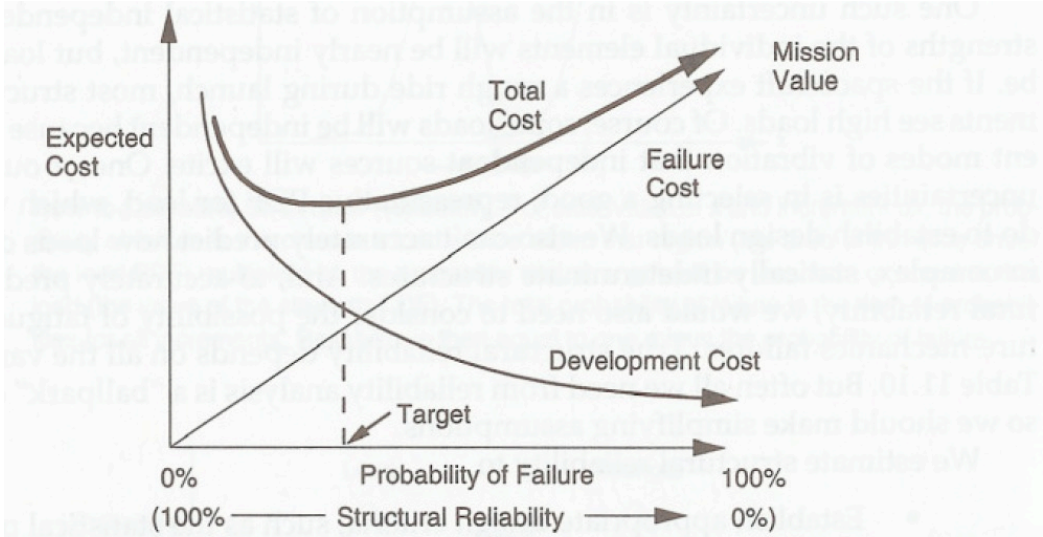
- In general assumes that components have an intrinsic constant failure rate.
- Predicted failure rate = sum of the predicted failure rates of all the components ⟹ worst-case (conservative) prediction.
- Lack of relevant experimental data for support.
- Most handbook based predictions do not account for physics or mechanics of failure nor systematic failures (over emphasis on temperature).
- MIL-HDBK-217, the most widely used prediction handbook is obsolete.

➡ Various initiative to improve: ESA roadmap, NASA , FIDES, HDBK-217Plus …

Reading: [7.1] ESA “Effective Reliability Prediction for Space Applications” White Paper, ESA-TECQQD-WP-0969, May 2016

Cost and Reliability

- Development cost optimization is difficult (impossible?) to achieve



Idealized Relationship between Reliability and Cost for a Hypothetical Space Mission. Total expected cost equals the sum of expected costs of development and failure. We've assumed here that it costs more to develop reliable structures, which is generally true.

Source: Th. P. Sarafin (ed.), "Spacecraft, Structures and Mechanisms", Wiley J. Larson, Managing ed., 2003, p. 348

Theme 7 Summary

- Goals of reliability processes:
  - Performances (lifetime), safety, risk management
  - Input to quantitative availability, maintainability and safety objectives and requirements
  - End-to-end process (specify, allocate, verify and update)
- Causes
  - Random
  - Design and manufacturing errors
  - Wear-Out
- Tools
  - FMECA (Failure Mode Effects and Criticality Analysis)
  - Data package, reviews, test philosophy (BBM, EM, QM, …)
  - Calculation of failure probability, of reliability (Probability Density Function, Cumulative Distribution Function, MTTF)
  - Bathtub curve
- Reliability of systems, of structures (Factor of Safety, Margin of Safety)
- Costs and limitations

Course Outline

- Theme 1 - Intro
- Theme 2 – Constrains
  - Shocks, vibrations
  - Vacuum (outgassing, heat exchanges …)
  - Radiations
  - Thermal …
- Theme 3 - Project Management and Systems Engineering
- Theme 4 - Materials
- Theme 5 - Structures
- Theme 6 - Components
  - Ball-bearings (configurations, lifetime, lubrication/tribology, …)
  - Actuators
  - Sensors, …
- 3D Printing
- Theme7 - Reliability

Exams

- June 27th, 30th and July 1st, according to list
  *(to be published on MOODLE, **check again before exam**)*
- Room ELE 111 *(**check again before exam**)*
- Duration: 20 minutes *(please be on time!)*
- One question randomly drawn
- No preparation
- Closed-book exam