life.augmented

Functional Safety in Electronic Systems: Principles and Applications

Alessandro Bastoni

Functional Safety Expert

STMicroelectronics

Lesson #1

General introduction on safety including HARA

Summary:

- **General concepts: risk, safety functions, Hzard and Risk Analysis, risk reduction**
- **Safety standards**
- **Faults, failures, HRF vs systematic**

life.augmented

Why Functional Safety is important in everyday life

Protects human life and health by preventing accidents and hazardous failures

Reduces risk of property damage and environmental harm caused by system malfunctions

Ensures reliable operation of critical systems in vehicles, medical devices, and industrial equipment

Builds user trust in technology through consistent and safe performance

Minimizes downtime and costs associated with failures and recalls

Enables innovation by providing a safety framework for new technologies and automation

Some useful definitions

Hazardous event/hazard: an event which intrinsically have the capability to cause a harm (physical injury/death of people, or damage to things)

Risk: is associated to a hazard, and it combines the possibility of occurrence of harm and the resulting consequences (how much severe the harm is)

Tolerable/acceptable risk: risk which can be reasonably considered is accepted in a certain context or situation. It clearly depends on the current system of values adopted in the society

Safety: the absence of risks that are considered unacceptable.

E/E/PE acronym: Electrical/electronic/programmable electronic

What is Functional safety (IEC61508 definition)

It is a part of the overall safety (Overall safety >> functional safety; contribute to achieve tolerable risk)

Depends on the correct functioning of the control system (in our case, the E/EE/PE)

It may depend on additional measures capable to reduce the risk

About “risk” concept

The risk concept is usually based on three parameters:

Severity: how many people will be involved, and how (injuries/death…)

Exposure: how often we’re running the given risk

Controllability: is there a chance for involved people to control in some way the effect of the system failure

The three parameters are combined in a kind of cross-matrix to derive resulting risk.

life.augmented

The airbag “paradox”

One impressive example of risk classification is given by the well-know car airbag. In airbags we have two separate safety functions: a) Firing: to fire the airbag when it is needed (car accident) and b) Safing: do not fire the airbag when it is not needed (no car accident).

Parameter	Firing failure (airbag not fired when car has an accident)	Safing failure (airbag fire when no car accident)	Comparison
Severity	Medium: only the driver will be affected	High: loosing the control of your car (consequence of unexpected firing) you can involve pedestrians or other car’s drivers	Safing > Firing
Exposure	Low! When actually you have an accident so one/two time in your life, hopefully ☺	High! Any time you drive your car, even in the parking	Safing >> Firing
Controllability	None	Low or none	Safing = Firing

Conclusion: risk associated to Safing failure is higher than Firing case. That was not obvious too.

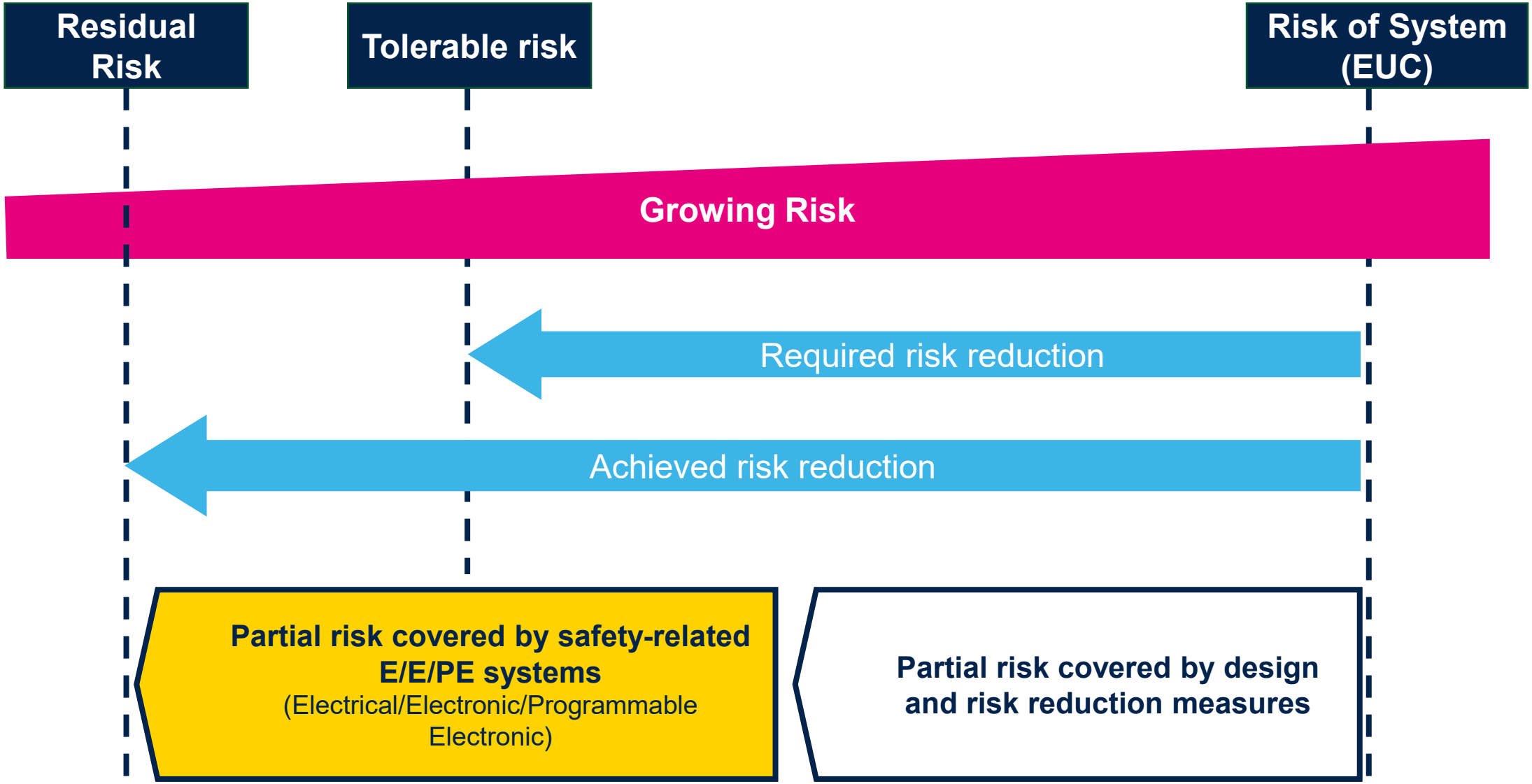
life.augmented

About “risk” concept

- We are not speaking about “risk elimination” (impossible!) but “risk mitigation” so avoiding unacceptable risks

- The concept of “tolerable risk” is in continuous evolution:
  - Once a new technology became widely diffused, people expectation for absence of correlated risk tends to increase (see for instance civil aviation)
  - Market/sector dependency, correlated to general public perception (e.g. space missions are reasonably believed to be more dangerous then commercial flights) and also legal approach (see for instance car market where the probability of high-cost class actions pushes for increased safety)

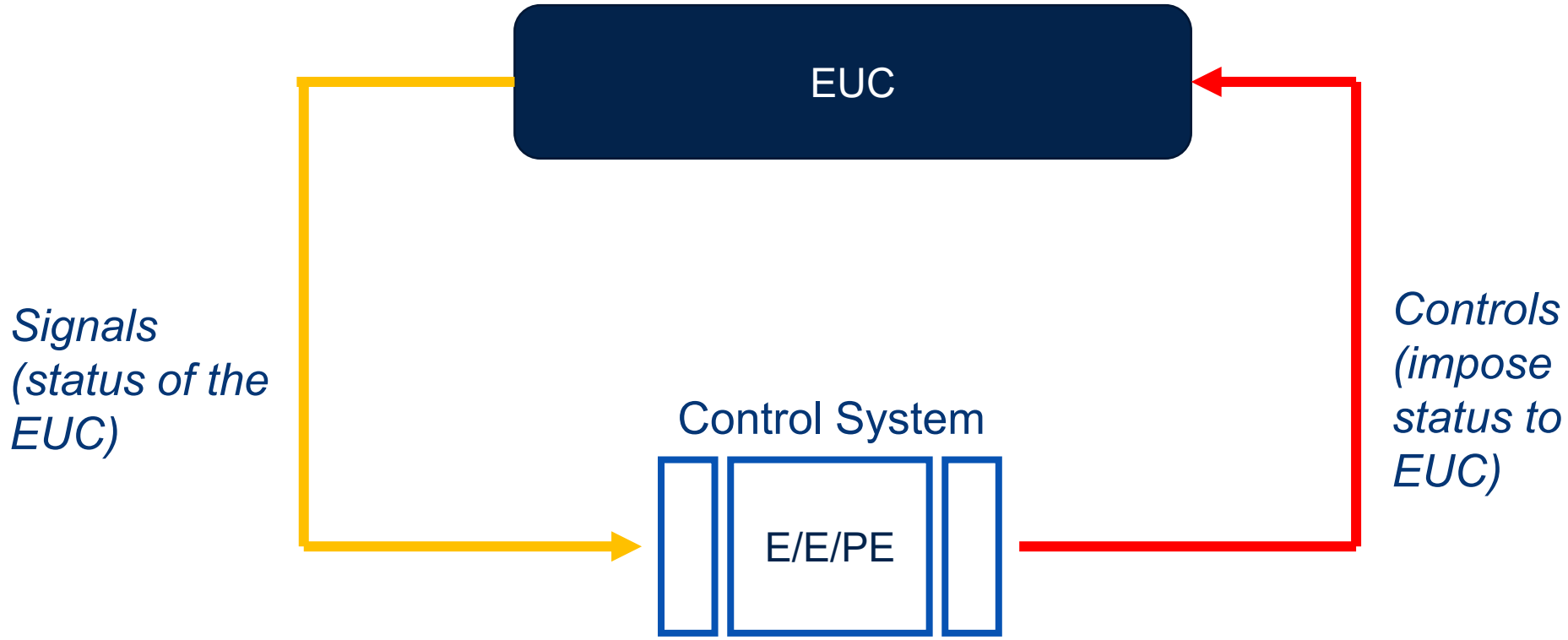
Risk Reduction



life.augmented

The EUC/control system dualism

IEC61508 is based on the concept that the final system (“the plant”) can be described as dual structure: controlled system (EUC, Equipment Under Control) / control system (i.e. kind of feedback control scheme).



The protagonist: the safety function

Safety function: function implemented by an E/EE/PE safety-related system (potentially also with the participation of additional measures to reduce the risk), that is

- intended to achieve or maintain the safety (so, no unacceptable risks) for the EUC,
- defined in dependency to a specific hazardous event

Examples of safety functions:

- *Functions required to be executed as positive action to avoid hazard (e.g. stopping the motor of a robot arm)*
- *Functions preventing actions being taken (e.g. preventing to open a door when a train is moving)*

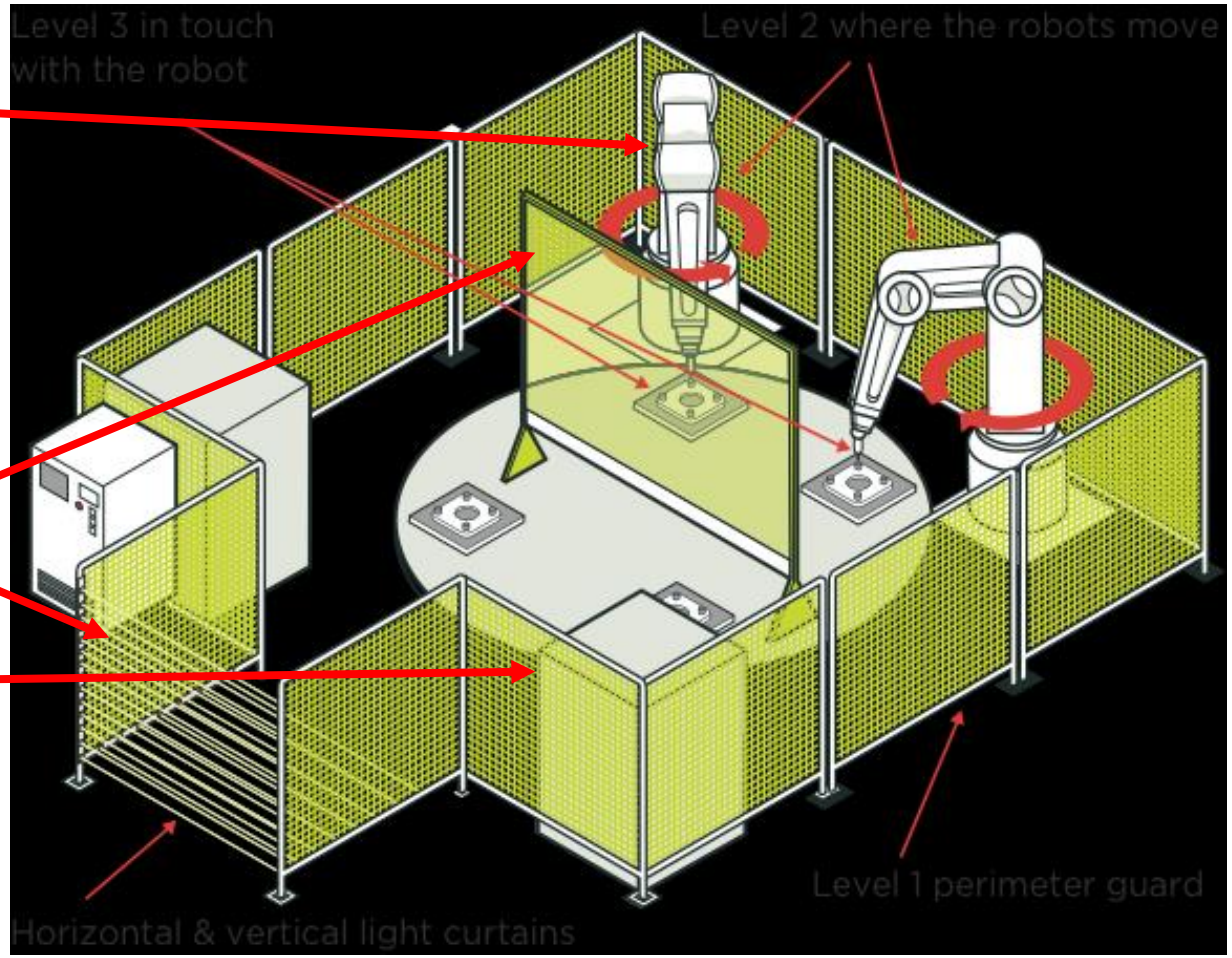
Mapping example – robot arm cage

part of the overall safety

EUC and the EUC control system

that depends on the correct functioning of the E/E/PE safety-related systems

risk reduction measures.



life.augmented

Hazard and Risk Analysis

Hazard and Risk Analysis is the process aimed to derive the target “safety integrity level” (i.e. “how much safety we need to add to the system”) according to the evaluation of several factors like exposure to the hazard, severity of the consequences, controllability and/or possibility to avoid the hazard.

Safety standards provides only guidance and not mandatory procedure. E.g., risk graph approach.

HARA example – ISO26262

Severity (S)	Exposure (E)	Controllability (C)	ASIL Outcome
S3	E4	C3	ASIL D
S3	E4	C2	ASIL C
S3	E4	C1	ASIL B
S3	E3	C3	ASIL C
S3	E3	C2	ASIL B
S3	E3	C1	ASIL A
S2	E4	C3	ASIL C
S2	E4	C2	ASIL B
S2	E4	C1	ASIL A
S1	Any	Any	QM

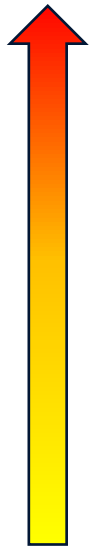
Severity (S) — Examples range from S0 (no injuries) to S3 (life-threatening injuries or fatality).

Exposure (E) — Ranges from E0 (incredible) to E4 (high probability).

Controllability (C) — Ranges from C0 (controllable in general) to C3 (difficult to control)

How to measure safety: Safety Integrity Levels

Safety integrity: it is a way to measure of the probability that a E/E/PE safety-related system performs in correct way a specified safety functions under, under specific conditions and time. Accordingly, there are Safety Integrity Levels (SIL)



SIL 4 (Nuclear plant, railways)

SIL 3 (Motor control, heavy industry)

SIL 2 (Industrial robot, small machinery, medical)

SIL 1 (E-bike, small appliances)

Similar “levels” appears in other safety standards (ASIL A->D in ISO26262, PL a->e in IEC13849, etc…)

life.augmented

Safety standards ecosystem

IEC 61508-4

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

IEC61508 is the meta-standard

Each “legacy” safety standard defined his proprietary:

- Scope of application (refined)
- Risk evaluation criteria (tuned on application)
- Safety integrity levels

General concepts and definitions are generally inherited from IEC61508.

life.augmented

Safety standards: Prescriptive vs. Risk-Based Approach

Feature	Risk-Based	Prescriptive
Approach	Risk-based Safety lifecycle	Fixed, based on detailed requirements
Application	Broad industrial safety-related systems	Specific products lines
Risk Assessment	Central and mandatory	Minimal or none
Safety Lifecycle	Defined and enforced	Often not defined
Verification	Formal verification & validation	Prescribed tests
Flexibility	High	Low
Certification Focus	Functional safety & Safety Integrity Level achievement	Product compliance

Risk-based: IEC 61508 and all its derivatives, ISO 13849

Prescriptive: IEC 60730/60335, UL 1998

life.augmented

Faults and Failures

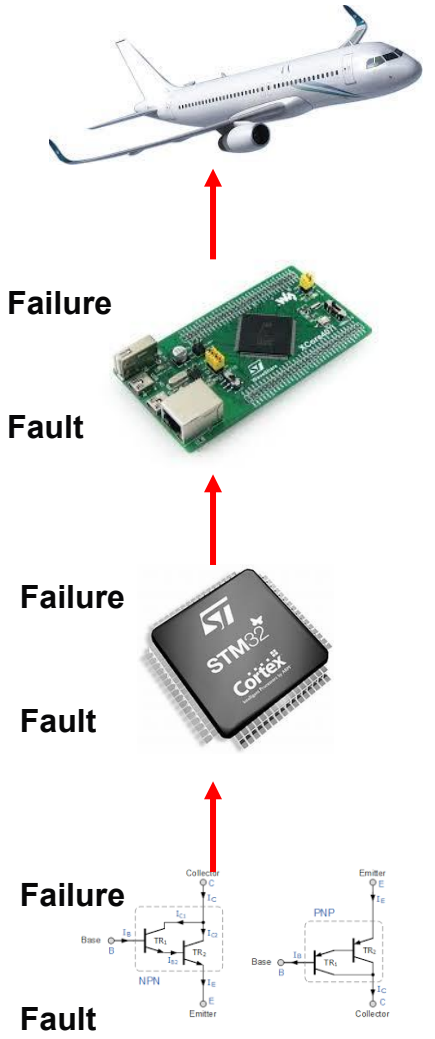
Fault: abnormal condition that may cause a reduction/loss of capability in a functional unit to execute a specific required function

Failure: termination of the ability of a functional unit to provide a required function/operation in any different way than as required

Definition is generic so include any kind of fault and failures.

Faults are the cause of failures.

Fault ⟶ Failure



Failures propagate from lower to upper layers in “modular” systems.

Why we focus on failures

Faults are always the root cause. BUT if they do not cause a failure, no risk is associated.

Faults “emerge”, are observed only through the caused failures.

A single fault can be source for multiple failures.

Safety **depends on the correct functioning of the E/E/PE safety-related systems**

and to possible other risk reduction measures.

We focus on failure as they are the termination of the system capability to execute a function, and therefore potentially to prevent that safety is achieved

Harm is caused by a wrong or missing functioning of the system – therefore, caused by failure(s) and not by fault(s).

The Functional Safety crossroad

random hardware failure: failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

systematic failure: failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

WARNING: this key concept is source of continuous misleading

life.augmented

Two kind of failures: RHF vs Systematic

Random Hardware Failures: the system is physically damaged (in permanent or transient way) leading to the failure of the expected functionality

- Based on probability analysis (unpredictable)
- Mainly quantitative (numbers!)
- Countermeasures based on fault detection and control

Systematic Failures: the system is wrongly designed and so under certain combination of external/internal conditions, or inputs, it will deviate from expected functionality (“bugs”)

- Based on process/method analysis (deterministic)
- Mainly qualitative (guidance)
- Countermeasures based on fault avoidance (process quality)

What is (NOT) safety

Functional Safety is NOT security

Safety: deals with failures on devices/software (system not working due to a fault)

Security: deals with intentional breaches/hacks on devices/hardware (system information and/or control are violated by an external attacker)

(Note: usually functional safety take into account as potential hazard a reasonably foreseeable misuse by the end user, and not voluntarily misuse).

Functional Safety is NOT reliability

Safety deals with the capability of a system to detect abnormal situations and to reach a specific safe state. Reliability deals on lifetime duration of systems perfectly working (all nonworking systems are considered the same – no mitigation/detection concepts exists, just redundancy if the case)

English wording: no misunderstandings (?)

… we will extensively use English wording in this training because, unfortunately, other European language are a bit misleading:

Sécurité
Sicurezza

Safety: deals with failures on devices/software (system not working due to a fault)

Security: deals with breaches/hacks on devices/hardware (system information is violated by external attacker)

Furthermore, despite IEC61508 has been published in English and French, English wording are well-known among industrial and safety community, so this last one allows major audience/understanding for documents..

… but still among English wording some misalignment still exist…

life.augmented

Hardware Random Failures theory

Summary:

- **Faults and failures (random hardware)**
- **Failure rate**
- **Faults classification**
- **Safety metrics: absolute and relative**

Hardware random failures: FAULT MODELS

For semiconductors components, two main falt model exists:

- Permanent faults
- Transient faults

Permanent faults

- The fault is irreversible (e.g. transistor broke, memory cell definitely open or short)
- Sources: aging, temperature stress

Transient faults

- The fault is not permanent (it can be a bit flip in a register, or a glitch in logic)
- Bit flips (aka known as “soft errors) can be corrected (or erased e.g. refresh for a FF)
- Sources: EMI, package radiation (alpha particles) , Sun radiation (neutron particles)

Permanent faults

Safety standards like IEC 61508 or ISO 26262 detail the minimum set of permanent faults to be considered (mainly as a “guidance”_:

- Stuck at 0/1
- Open circuit
- Short circuit
- Bridging
- High impendence
- Drift
- Oscillation

Note: they can be deen as “failures” with underlying faults generating them – depends on the abstraction level selected!

Transient faults

Also for trandsient faults .safety standards like IEC 61508 or ISO 26262 detail the minimum set of faults to be considered (mainly as a “guidance”_:

- Bit flips on registers
- Bit flips on volatile memory cells (RAM)
- Glitches on busses/connections/inputs

How to establish faults/failures

Given a certain component or technology, questions arise on how to establish a reasonable list of potential faults and resulting failures. Some main patterns are possible:

- Usually, each safety standard lists the minimum set of faults/failures to be analyzed according to the target safety integrity level (the higher the integrity , the larger will be the set of faults/failures)
- Collateral documentation listing potential faults/failures, see for instance reference NASA document [R1]. (search for “failure mode” for discrete and analog components)
- State-of-the-art tools for safety analysis (e.g. FMEDA tools) usually provide hands-on list of faults/failures for each given type of component.

How to deal with random failures

Random failures must be mitigated. Two ways are possible

- Fault avoidance
- Fault detection

Fault avoidance

- The probability of failure is decreased, for instance by redundancy of two independent functions. Best approach for mission-critical application and to increase availability. Concept associated Hardware Fault Tolerance (HFT)

Fault detection

- The system includes new, additional diagnostic functions devoted to detect failures. They are usually called safety mechanisms
- Once a failure is detected, a correction can be done (e.g. see ECC), or (if not possible) the system is informed of the failure, and safety is achieved by other means (system is driven in safe state)

life.augmented

How to deal with random failures - examples

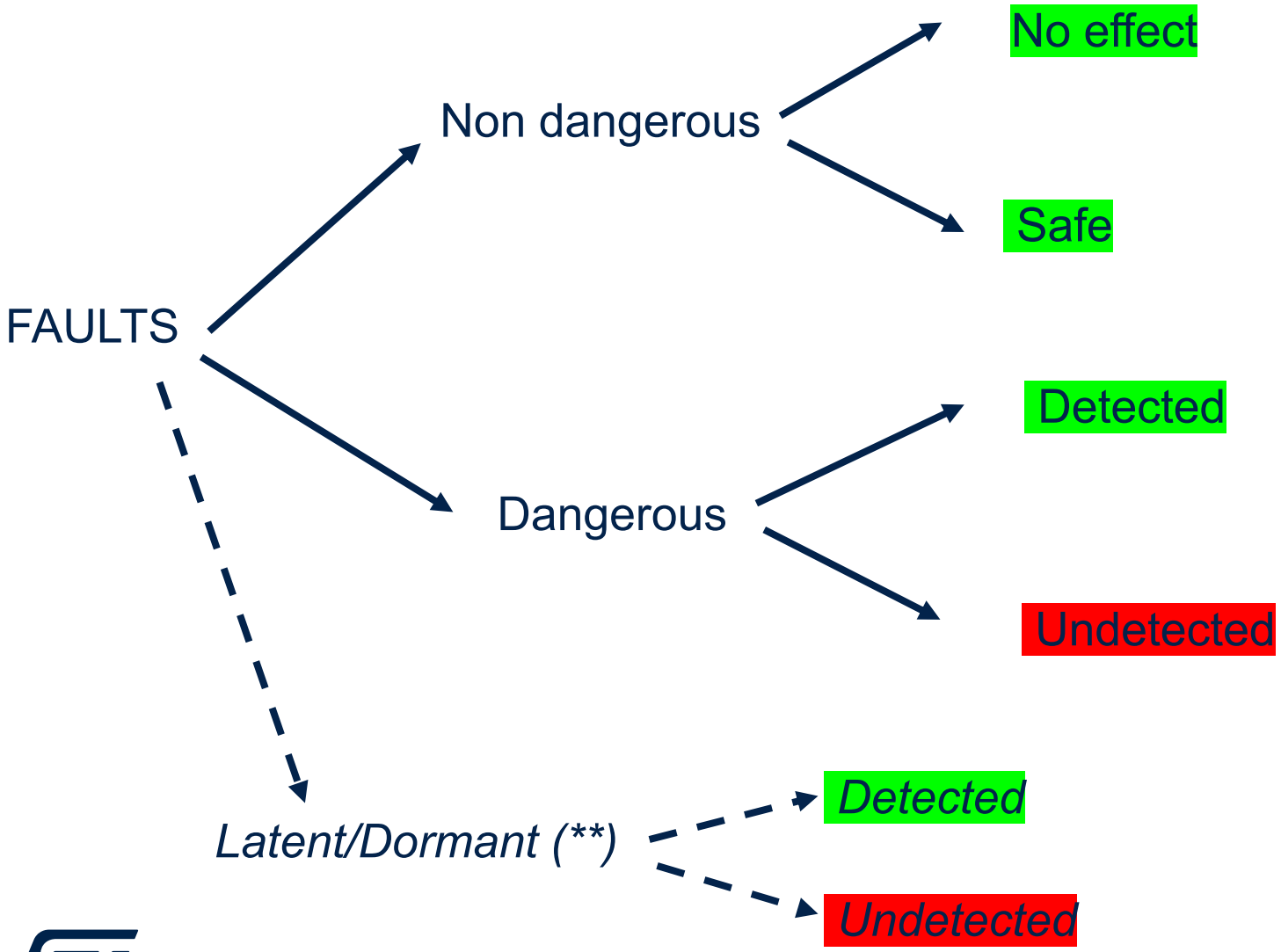
Fault avoidance example:

Register lock by key: Write access to configuration registers are protected by a key (software sequence of commands to be respected to unlock). Avoids faults related top unintended writes on the registers

Fault detection example:

Parity: a parity bit is added to each word (multiple schemes are possible), enabling single bit error discovery when data are read (computed parity bit doesn’t match with the stored one). Detects single bit flips faults.

Faults (*) classification



(*) Note: this terminology can be applied to failures as well

(**) defined only on some safety standard

Faults classification (definitions)

Faults/failures can be classified as:

No effect/no part/ non safety related: affecting hardware not involved in the implementation of the safety function

Safe: fault/failure driving (or helping to maintain) the system to a safe state (where safety is achieved)

Dangerous: able to interfere with the safety function

Detected: a fault/failure for which its presence is revealed by a safety mechanism(s)

Undetected: the vice-versa of previous

Latent/dormant: a fault which cannot directly interfere with the safety function, but which can do that in presence of another one.

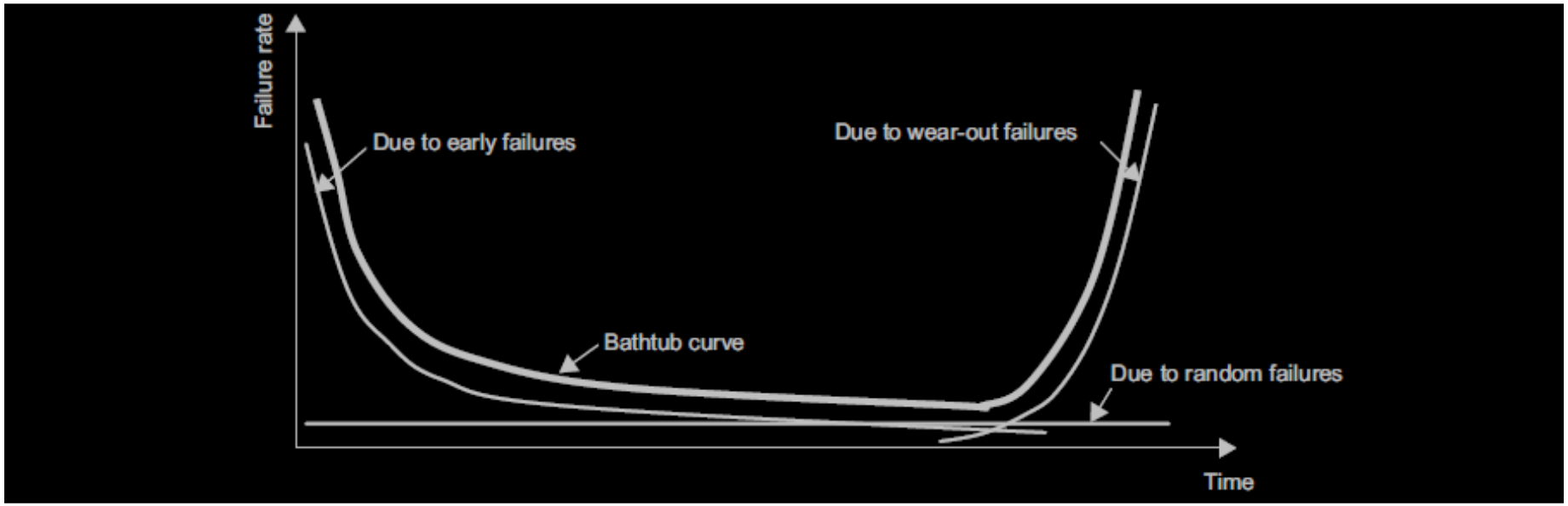
Note: general definitions, a mix between IEC 61508 and ISO 26262 definitions

Semiconductors failures

Early Failures: in the production process, semiconductor devices may contain defects due to the presence of tiny particles, as well as variations in manufacturing equipment and variations in dimensions. This fact is known as the initial defect density.

Random Failures: Failures resulting from production defects will attenuate with time.

Wear-out Failures: semiconductors fail when they reach the limits of their basic durability. This period is called the region of wear-out Wear-out failures differ with differences in the stresses applied to the device while it is being used.



life.augmented

Discrete components

Discrete components tend to show a constant failure rate (resistors, inductors, ceramic capacitors), while few specific exhibit a mild bathtub curve (electrolytic capacitors).

PCB connections and mechanical connectors show a constant failure rate with a wear-out increase phase, mainly depending on aging and mechanical stress cycles.

Relay often show a bathtub-like curve with noticeable wear-out phase due to aging and commutations cycles/electric load.

CONCLUSION: during the reasonable operating life of an electronic system, all failures can be considered to be in their constant value phase.

Failure rate

failure rate: reliability parameter (λ(t)) of a single components or system (entity) such that λ(t).dt is the probability of failure of this entity within [t, t+dt] under the assumption that it has not failed during [0, t].

Failure rate λ is therefore a probability divided by time (important!)

It is measured in FIT(s); 1 FIT is equivalent to 1 failure per 10E+9 hours

The failure rate of a series of components/systems is the sum of the failure rates of each of them. The failure rate of redundant (parallel) systems is generally non constant.

About base failure rates

“Base failure rate” for a given semiconductor component is the failure rate associated to an individual, specific subset of the component itself: for example, portion of the silicon area, transistor, memory bits etc

Base failure rate is a controversial argument as different methods (e.g accelerated tests and/or mathematical models) with different confidence levels exists in the industry. Main potential issue is to combine data coming from a different source in the system FMEDA

- For permanent failures, the most popular data sources are
  - IEC62380 (and its equivalent model in ISO26262-11)
  - SN29500-2:2010 Siemens norm (currently a bit outdated but still widely used)
- For transient failures, strong dependency on IC technology, package (LA vs ULA), altitude, shielding. Data are usually coming from irradiation tests or ITRS tables

Safety Metrics – absolute vs relative

Absolute metrics

λ expressed in FITs (1 failure over 1 billion hours)

They stroingly depends on assumptions on operating conditions *temperature, cycles)

They provide a measure of the probability of failure over time

Relative metrics

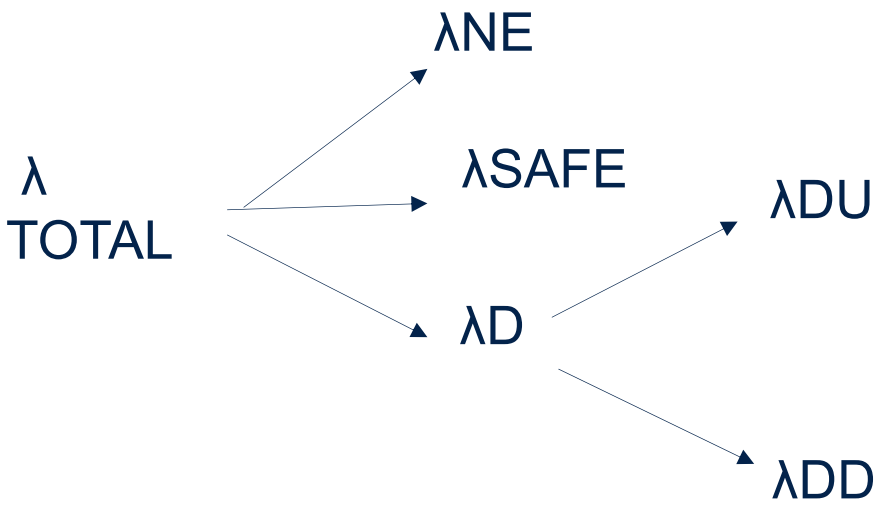
Expressed in percentages from 0% to 100%

They are the ration between homogeneous terms (λs) so they are only architectural dependent

They express a numerical evaluation on the overall combination of fault tolerance, safety mechanisms and mitigation measures.

About Safety Metrics – IEC 61508

Absolute metrics, λ expressed in FITs (1 failure over 1 billion hours)



Relative metrics
(percentages from 0% to 100%)

Diagnostic Coverage

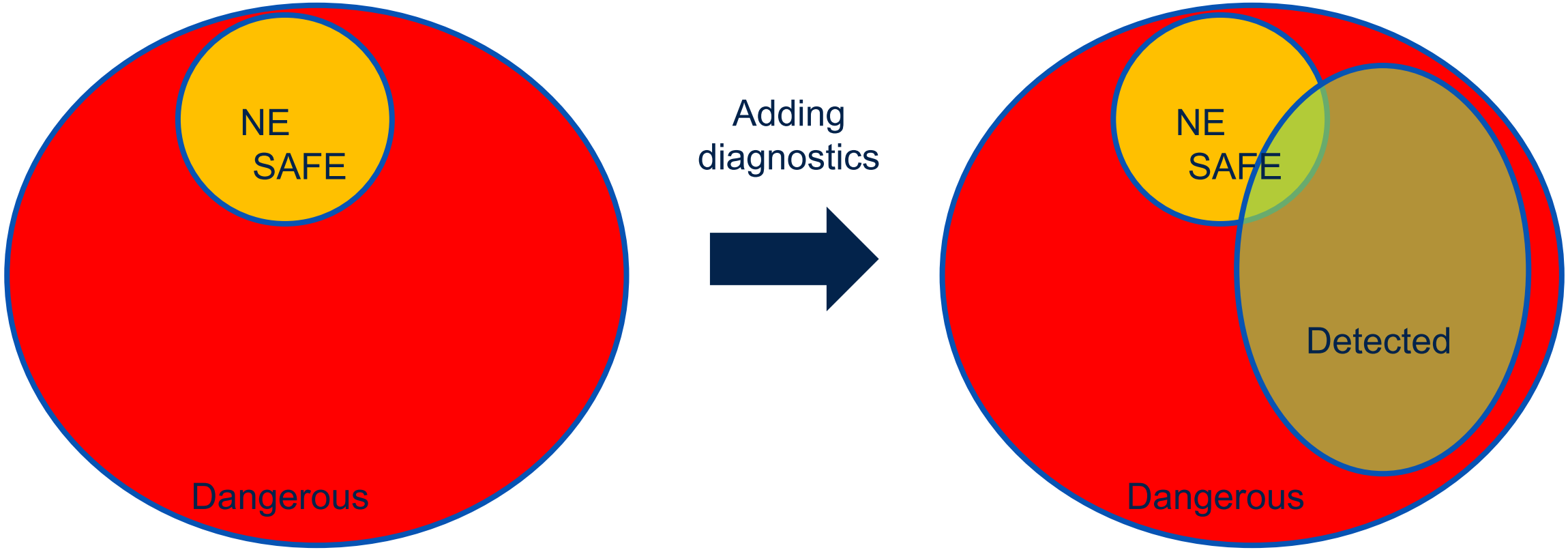
$$DC = \frac{\sum \lambda DD}{\sum \lambda D}$$

Safe Failure Fraction

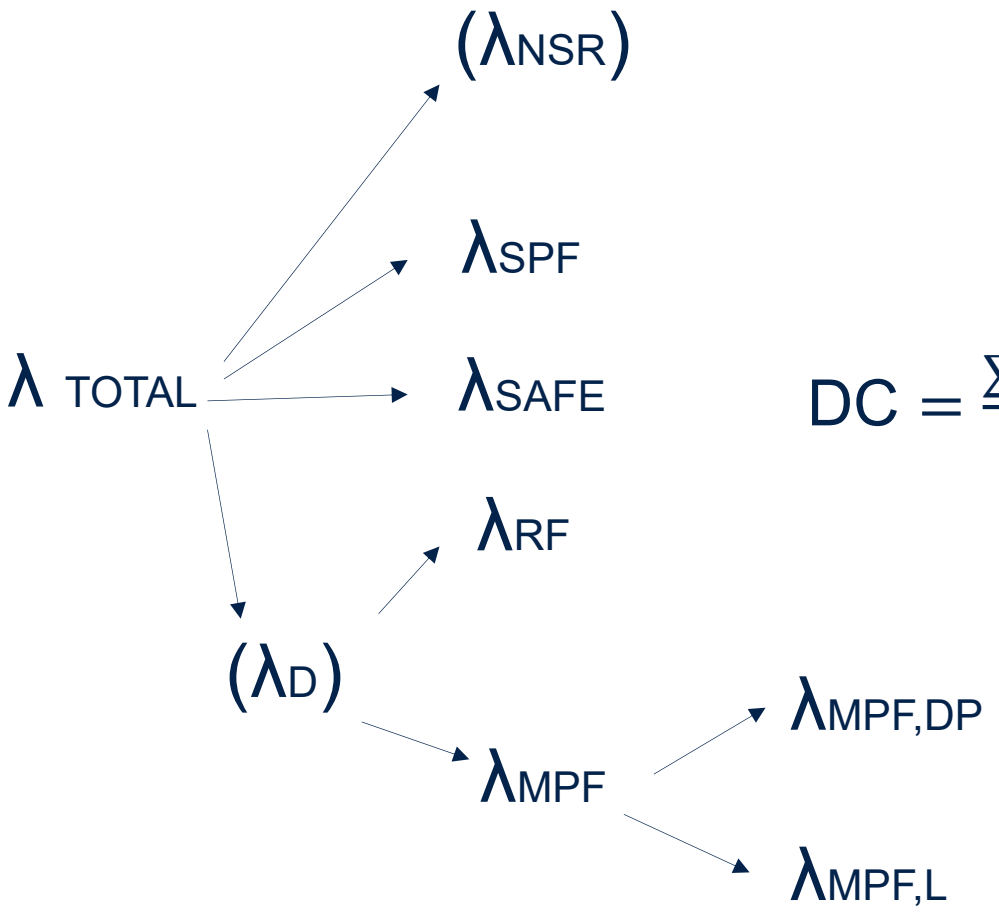
$$SFF = \frac{\sum \lambda DD + \sum \lambda SAFE}{\sum \lambda DD + \sum \lambda DU + \sum \lambda SAFE}$$

life.augmented

Faults detection



About Safety Metrics – ISO 26262



$$DC = \frac{\sum \lambda DD}{\sum \lambda D}$$

Single Point Fault metric

$$SPFm = \frac{\sum \lambda MPF + \sum \lambda SAFE}{\sum \lambda MPF + \sum \lambda SPF + \sum \lambda RF + \sum \lambda SAFE}$$

Latent Fault metric

$$LFm = \frac{\sum \lambda MPFdp + \sum \lambda SAFE}{\sum \lambda D - \sum \lambda SPF - \sum \lambda RF}$$

Note: ISO 26262 fault classification is quite specific because of its explicit classification for dual faults

life.augmented

Relative Safety metrics - targets

IEC 61508-2 relative metrics targets (*)

SFF	HFT = 0	HFT = 1	HFT = 2
< 60%	Not allowed	SIL 1	SIL 2
60% - 90%	SIL 1	SIL 2	SIL 3
90% - 99%	SIL 2	SIL 3	SIL 4
>99%	SIL 3	SIL 4	SIL 4

(*) For a Type B element

SFF is the reference

ISO 26262 relative metrics targets

SPFm	
90% - 97%	ASIL B
97% - 99%	ASIL C
>99%	ASIL D

LFm	ASIL
60% - 80%	ASIL B
80% - 99%	ASIL C
>90%	ASIL D

life.augmented

Absolute Safety metrics - targets

SIL	Average frequency of dangerous failure (for HD/CM)
SIL 1	1E3 FIT< PFH < 1E4 FITs
SIL 2	100 FIT< PFH < 1000 FITs
SIL 3	10 FIT< PFH < 100 FITs
SIL 4	1 FIT< PFH < 10 FITs

IEC 61508-2 relative metrics targets

ASIL	PMHF Probabilistic Metric for random Hardware Failures
ASIL B	PMFH < 100 FITs
ASIL C	PMFH < 100 FITs
ASIL D	PMFH < 10 FITs

ISO 26262 absolute metrics targets

Note: PHF/PMHF computation is linked to λDU/λRF values. Details will be provided in the lesson related to safety architectures

life.augmented

How many faults in the system?

In principle, 1 to N faults can affect in the same time the system. If faults are independent, the propability of multiple faults is low and anyway depends on the time.

Each safety standard provide explicit guidance to the minimum number of *simultaneous* faults to be considered in the analysis of the system:

IEC 61508 ask for single faults, nut ask to “consider” multipe, faults scenarios

ISO 26262 ask for single faults + a second fault just on the diagnostics (latent) N>2 is out of scope

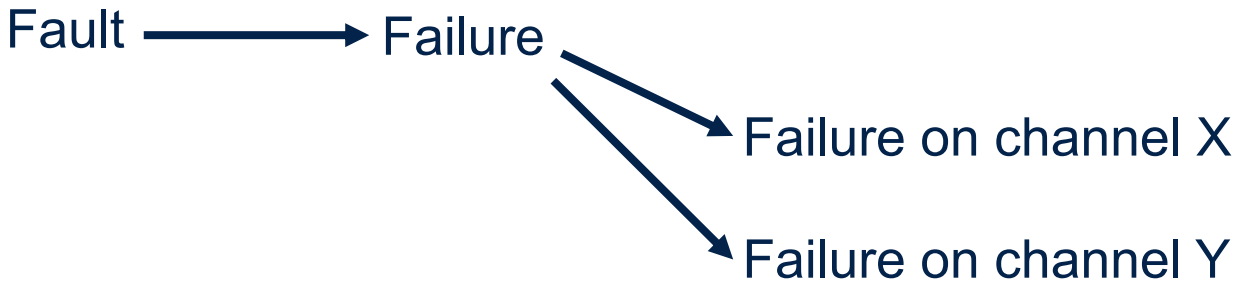
ISO 13849 requires only one fault except for specific PL/architexcture where HFT=1 is required

Non-independent failures

Dependent failure: .failures caused by non-independent events i.e. P(A and B) > P(A) × P(B).

Common cause failure: failure causing multiple concurrent failures in a multichannel system

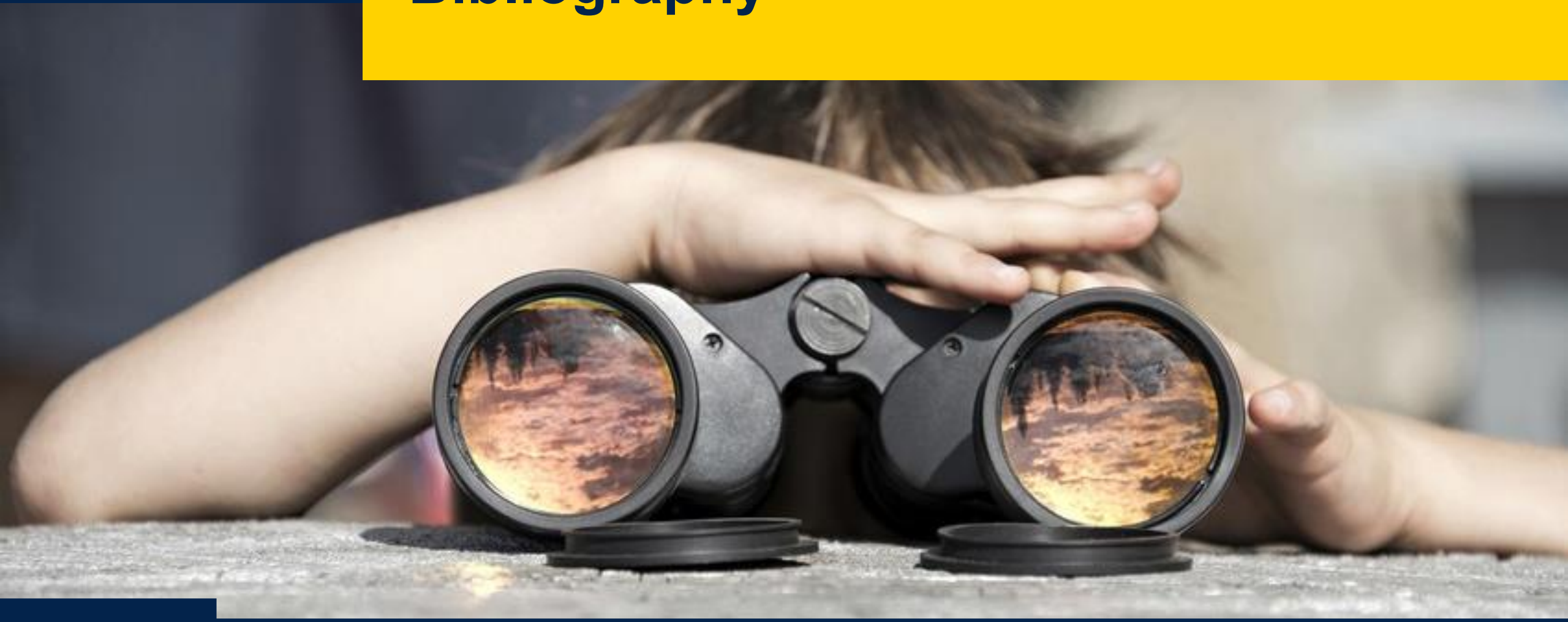
(example: failures of the common supply for a multichannel system)



Related problems

- They cannot be included in “standard” DC, λ computations
- They potentially undermine fault tolerance of the system

Bibliography



life.augmented

Reference documents

[R1]: Microelectronics Reliability:Physics-of-Failure Based Modeling and Lifetime Evaluation - Jet Propulsion LaboratoryCalifornia Institute of Technology Pasadena, California

[R2]: : Semiconductor Reliability Handbook – Renesas Electronics, Rev.2.50 Jan. 2017

Thank you

life.augmented