life.augmented

Functional Safety in Electronic Systems: Principles and Applications

Alessandro Bastoni

Functional Safety Expert

STMicroelectronics

Lesson #7

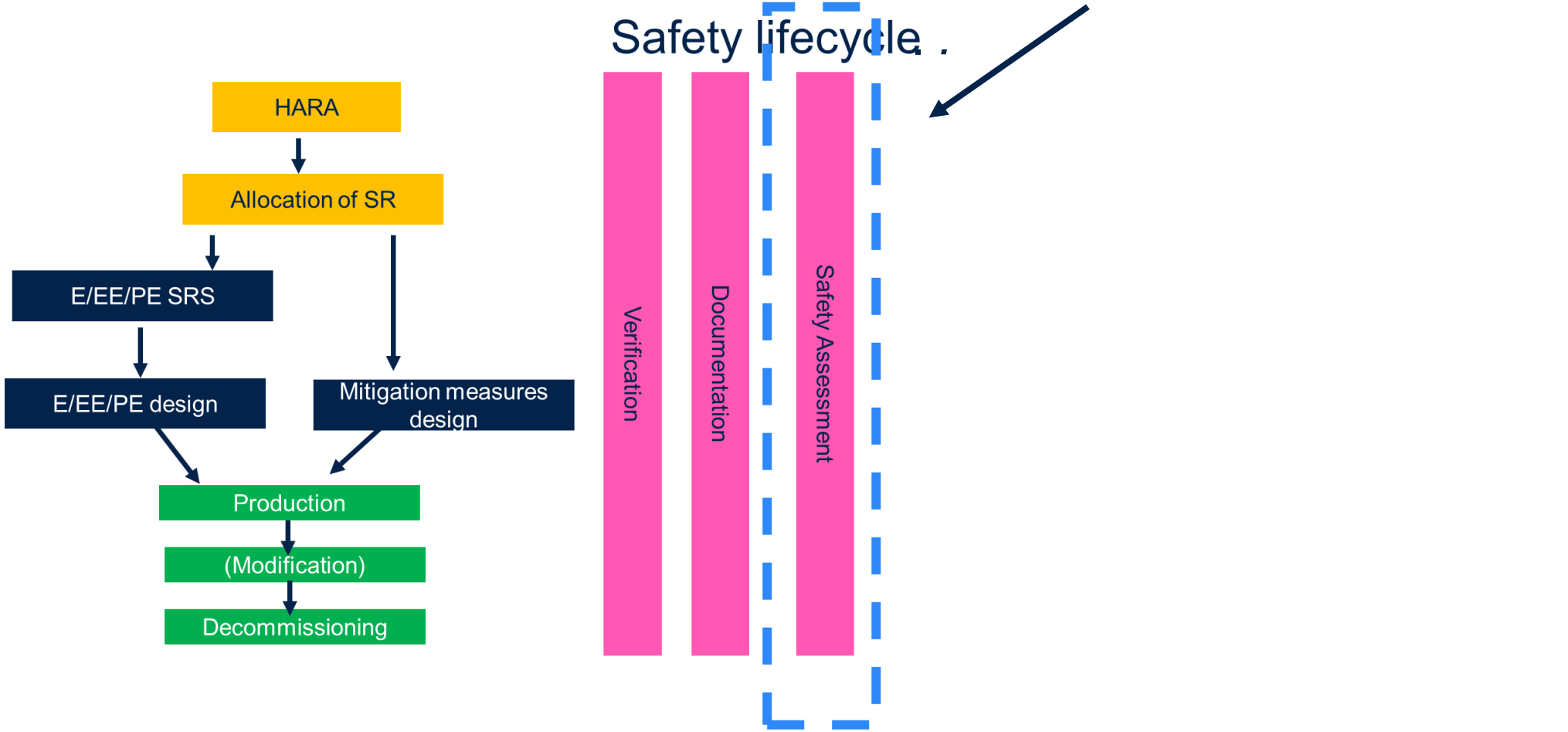
Miscellaneous in safety process

Summary:

- **Functional Safety Assessment, Independency**
- **Safety Case**
- **Certification process**

life.augmented

Recap on safety lifecycle



Functional Safety Assessment

What it is: IEC61508-4: 3.8.3: “investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems and/or other risk reduction measures”

Who will do it: the Assessor (person, persons or organization that performs the functional safety assessment in order to arrive at a judgement on the functional safety achieved by the E/E/PE safety-related systems and other risk reduction measures) required to be independent as per below table.

Minimum level of independence	Safety integrity level / Systematic capability			
	1	2	3	4
Independent person	Allowed	Allowed on consolidated and simple designs	Insufficient	Insufficient
Independent department		Allowed on novel/complex designs/technologies	Allowed on consolidated and simple designs	Insufficient
Independent organization			Allowed on novel/complex designs/technologies	Allowed

Independency

life.augmented

About independency

Independency criteria are specified in IEC61508-4, 3.8.11-13:

- independent person: person who is separate and distinct from the activities which take place during the specific activity, with not direct responsibility.
- independent department: department that is separate and distinct from the departments responsible for the activities
- independent organization: organization that is separate and distinct, by management and other resources, from the organizations responsible for the activities

When an independent organization is required, even for large organization like semiconductor manufacturers it is common to rely on Competent Bodies/Certification Agency (e.g. TÜEV, UL, etc.) – in that case the independency is clearly achieved and accepted. .

The Safety Case

The Safety Case is perfectly described in ISO26262:10, 5.3.1

The purpose of a safety case is to provide a clear, comprehensive and defensible argument, supported by evidence, that an item is free from unreasonable risk when operated in an intended context

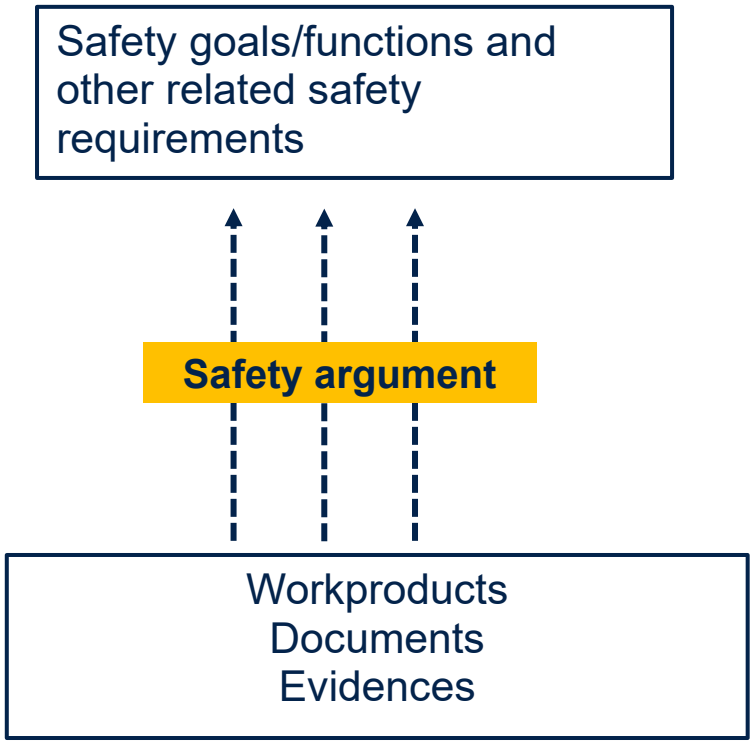
Principal elements:

the safety goals and related safety requirements

the collection of safety arguments (related to product or process)

the ISO 26262 series of standards work products (the evidence)

The description is applicable also for IEC61508 framework (where safety case isn't formally defined)



life.augmented

How to build a Safety Case

The perfect way to build a Safety Case is to follow the ISO26262 description with a formal implementation (in other words, by using formal languages e.g. Goal Structured Network).

The greatest benefit would be to link the description with the tool used to formally manage the requirements.

The approach is often found difficult, so in industry the tendence is to build the Safety Case by “narrative text“ (in the form of a Safety Report).

Narrative text could be confusing as there’s a risk to loose the boundaries between claims and related rationale. So, it’s recommended to formally keep the causal chain

Claims↔ Arguments ↔ Evidences

Note: the presence of a narrative text approach in third parties documentation (Safety Manuals, etc.) usually requires an additional effort to enable a more structured organization for the included requirements.

Certifications zoo in a nutshell

Certification: is one of the most ambiguous (and abused) wordings in functional safety, as it's used to describe multiple, different situations. Some examples:

- Pre-certified: software developed according to a certified V-model. The certification and related claims addresses the generic development flow followed by the organization, and the compliance of each specific software must be evaluated on the basis of the provided artifacts/documents
- Pre-certified: a T2 or T3 tool for which an off-line support tool analysis according to IEC61508-3m 7.4.4 has been executed and independently reviewed, but complex actions on end user side still exist
- Pre-certified: a hardware or software item formally certified vs specific claims, used as part of a whole solution integrating it (and not capable to magically extend the claims to the whole system)

.

The SIL certificate

The SIL certificate is a functional safety certification demonstrating that a product or process meets the IEC 61508 international standards.

It is issued by an independent third party to ensure compliance with IEC 61508-1 requirements for independence, especially for achieving the highest SIL levels 3 and 4, which mandate involvement from a separate division or independent body.

The certificate is self-supporting, providing all necessary information for integration into a safety system. Alongside the certified item's safety manual, it includes instructions for proper use to guarantee the declared SIL level is maintained

The certificate also contains a registered trademark with the identification ID of the certified product that must be affixed to the product to allow traceability and clear differentiation between SIL and non-SIL products. Certifixctes are usually stored I public-available database on the web.…

Different types of SIL certificate

Certificates can be issued in one of the following 3 types:

- **SIL type certificate**: valid for a whole type of product, the certification process is developed starting from the analysis of a prototype which, once certified, will be suitable to be mass-produced. The certificate is therefore valid for an unlimited number of products, when identical in every aspect to the validated prototype. The SIL type certificate has a duration that is defined by the certification body based on the complexity of the object (e..g limited in time, or subject to yearly confirmation). Example: safety Microcontrollers.
- **Single product SIL certificate**: limited to the device expressly covered by the certificate, this type is frequent for non-series production, custom, and project assemblies. The certificate expressly states the serial number or an unique identifier of the addressed product. Example: a factory.
- **Process SIL certificate**: states the compliance with the international standard IEC 61508 of the implementation process of one or more phases of the Safety Lifecycle/ Example: checking the compliance of processes and procedures with regulatory requirements.

Main information in a certificate

IDENTIFICATION OF THE CERTIFIED PRODUCT This isn't trivial. Always pay attention to what actually is the boundary of the certification (a single product? A line of products? etc.)

REFERENCE STANDARD This is the basis used for the certification, important for the understanding of the real scope (e.g. IEC61508:2010 ≠ IEC61508-3:2010)

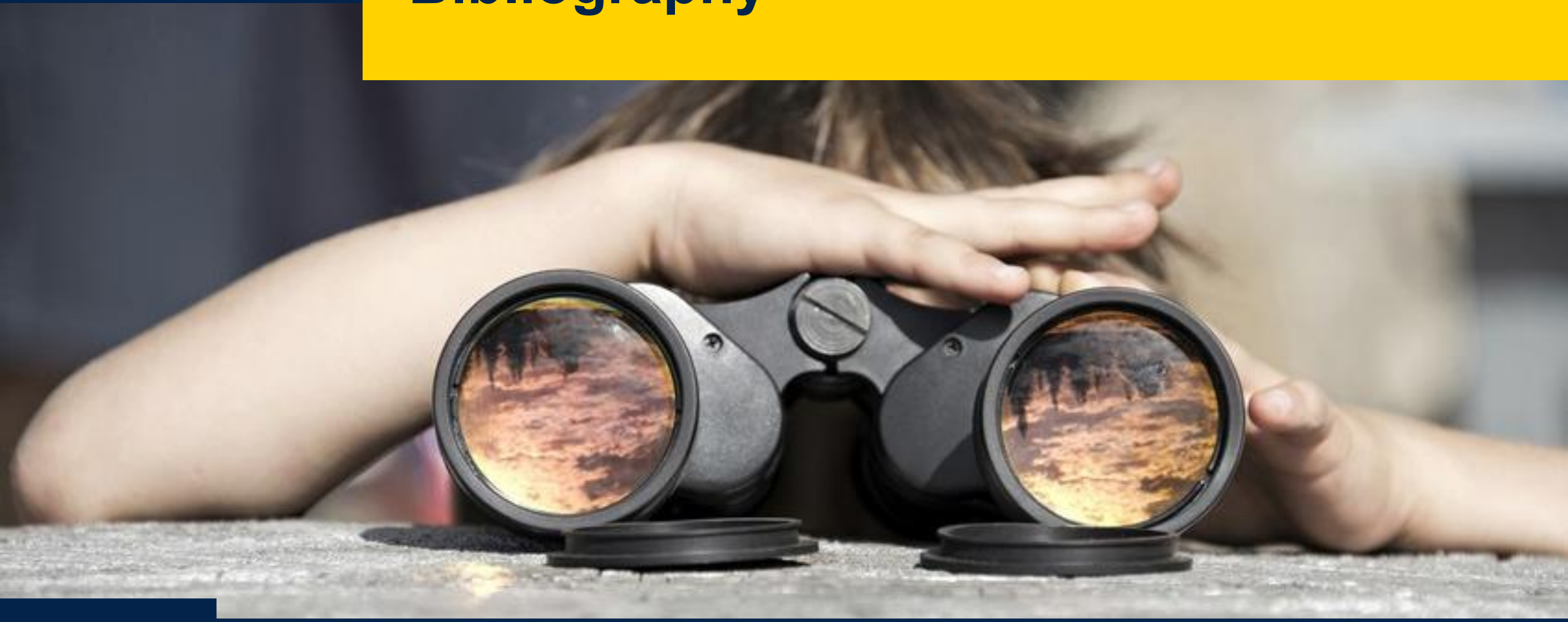
CLAIM The most important information. What is the actual claim done in the certificate? Pay attention to generic statements (e.g. "compliant to IEC 61508"… really all 7 parts???) with no clear boundaries on the achieved capability Always remember: HRF and SC have deterministic targets

ADDITIONAL INFORMATION Very different from one certificate to other. They can recommend complying with additional requirements included in a Safety Manual, or a Safety Report. Pay attention to sentences like „the Report is integral part of this certificate" – immediately inspect the Report in such a case

Backup slides

life.augmented

Bibliography



life.augmented

Reference documents 1/2

[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

[R3]: ExoMars 2016 - Schiaparelli Anomaly Inquiry (ESA) downloaded from https://exploration.esa.int/web/mars/-/59176-exomars-2016-schiaparelli-anomaly-inquiry

[R4]: Fault Tree Handbook with Aerospace Applications - NASA Office of Safety and Mission Assurance, V 1.1 , 2002

[R5]: open FTA software can be found on the wed, e.g. https://www.fault-tree-analysis.com/free-fault-tree-analysis-software, or check for OpenFTA download

Reference documents 2/2

[R6]:Safety Manual for TMS570LS31x and TMS570LS21x Hercules™ ARM®-Based Safety Critical Microcontrollers

[R7]: UM2331- STM32H7 singlecore series safety manual STMicroelectronics – from https://www.st.com/en/embedded-software/x-cube-stl.html#documentation

[R8]: Safety Manual for TPS65919-Q1 Power Management Unit (PMU)

Thank you

life.augmented