MCU as a SEooC

Journey into the integration of a MCU Safety Manual on a E/E Automotive ECU Design

24° Workshop on Automotive Systems and Software

Automotive SPIN Italia, 2026/05/21

META ELECTRONICS

DISCLAIMER: Integration of a SEooC involves receiving from supplier confidential/restricted WP under NDA. What is presented here is for technically trained staff and for informational/learning purposes, it does not intend to disclose any restricted content.

About us

Luca Pistoni

Functional Design, FuSa and CybSec Manager
CySec Specialilst (TÜV Rheinland) # 736/22 – Automotive

luca.pistoni@metasystemcorporation.com

Stefano Prati

Functional Safety Expert
TÜV SÜD FSCP (FuSa), UL-CASP (SOTIF)

stefano.prati@metasystemcorporation.com

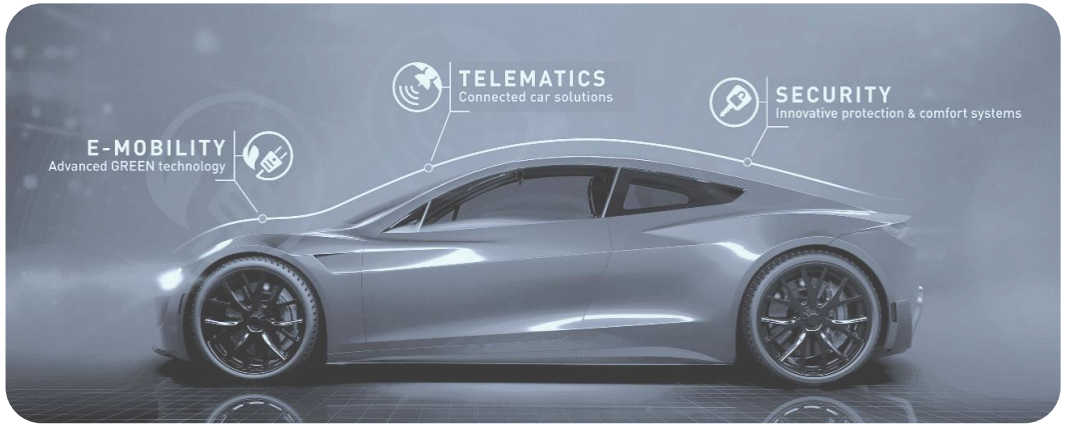
About Us

Meta Electronics continues and strengthens the long-standing experience of **Meta System**, pursuing a path of excellence in the research, development, and production of advanced electronic solutions for telematics, the safety and security sector, and automotive power systems.

The **Research and Development team** designs and manufactures highly technological and innovative products, supported by an in-house state-of-the-art testing laboratory capable of validating devices in compliance with the most stringent standards and specifications of the Automotive sector.

With the establishment of **Meta Electronics**, the company makes available engineering solutions based on its extensive know-how, offering clients and partners the services of the **Project & Product Development Department** and the **Test & Validation Center**, with the aim of reducing time-to-market and ensuring high value-added engineering solutions.

PRODUCTS



SERVICES

Plan of the presentation

Project
- Motivation
- Challenges
- Digression: *SEooC*

Tool
- Solution
- Digression: *Rules of the road*
- Structure
- Data exchange
- Workflow

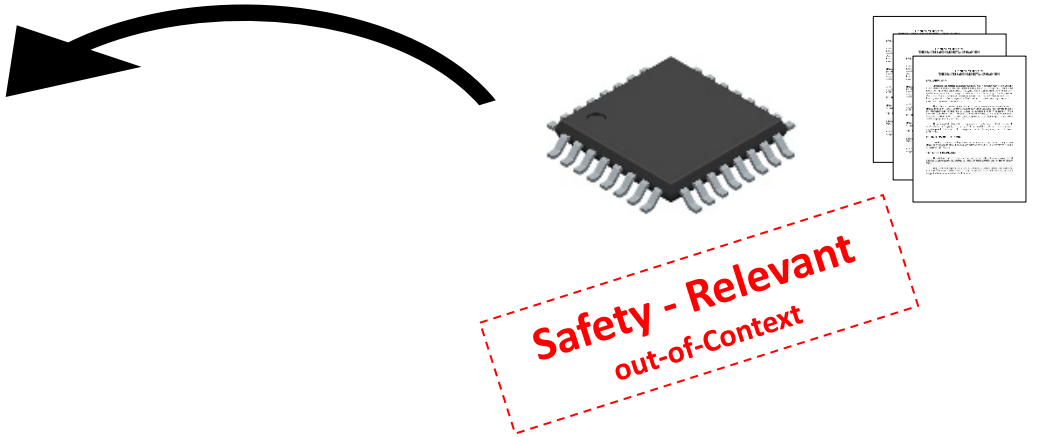
FuSa Process
- Convention
- Hierarchy
- Compliance effort 1…3

Conclusion
- Pros / Cons
- Future work / Discussion
- Q/A

Project

Motivation - **Project**

- Automotive Ev On-Board-Charger 11/22kW ASIL B Project
- Integrate 32bit MCU as a SEooC
- Comply with AoU and safety concept from Safety Manual
- Argument appropriate choices to:
  Assessor, Customer, Safety Case…and design team



Implement OBC SR functions assigned to MCU and tailor to ASIL B

- Master **understanding** of Safety Manual document
  Infer the underlying safety concept, and x-traceability of MCU safety measures to peripherals
- Identify the implied **workflow** for integration effort
- Collect and demonstrate proper **diligence** in the execution
  Motivate choices on the variety of details of the MCU safety architecture
- Have a valid **dashboard** for technical discussion and understanding
  Possibility to extract necessary/minimal information for the audience
  Interface with external supporting experts
- Use existing / **simple** tools,
  with easy configuration and data exchange capability
  supporting the learning curve
- Flexible instrument to be adapted for **future** projects

Digression: *SEooC* - **Project** ●●●

- Integration of a complex (MCU) **COTS** into a Safety Relevant project is guided by ISO 26262-10 Clause 9 (Informative), such component not tailored for a specific item is named **SEooC**.

- SEooC MCU is usually delivered with
  - **Certificate** compliance to the Standard by external body
  - Statement on Systematic and HW Metrics **Capability**
  - Safety **Manual** / AoU
  - Configurable **FMEDA**

- Safety manual typically presents AoU for concepts for ASIL D compliance, tailoring on what is necessary for lower ASIL is not always easy to do.

Tool

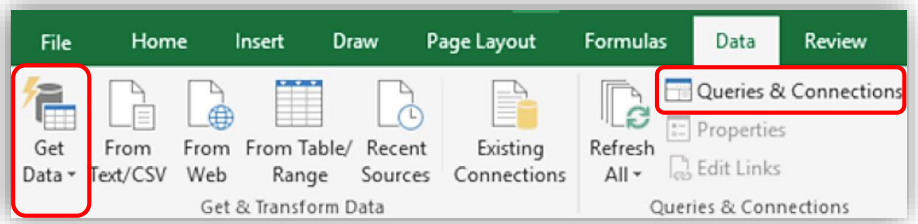
Solution - **Tool** ○○○○●

- A well-constrained **hierarchy** of excel workbooks
- Arrangement with traced and documented static data sync
- Workbooks principles:
  - ✓ Contain a basic a **model** that restates the strategies, peripherals, and safety mechanisms of the safety manual.
  - ✓ Distinguish Safety Manual **recommendations** from our design **decisions**
  - ✓ Record the **tailoring**, justifications, applicability for the component under development
  - ✓ **No duplicates** for information and models

Digression: *Rules of the road* - **Tool** ○○○●●

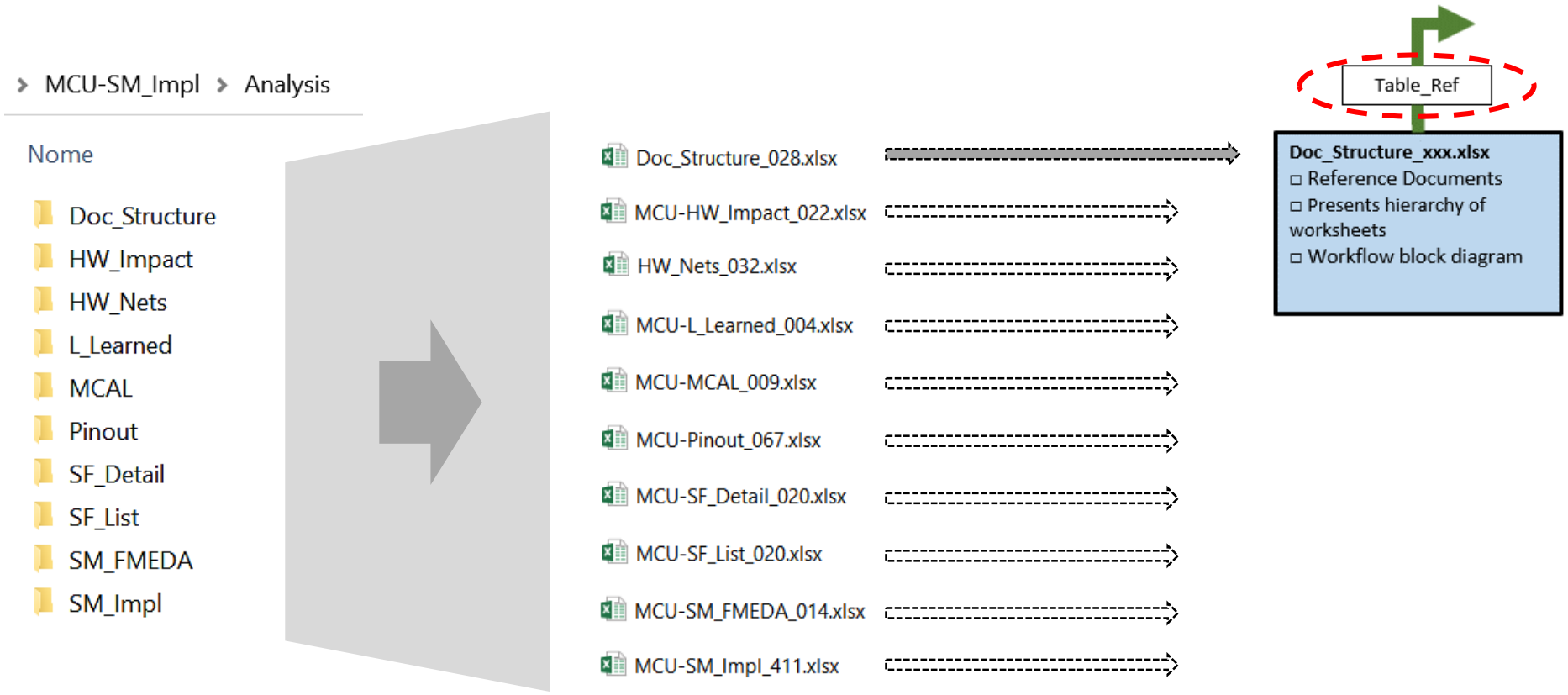
Friends

- (Excel) Table – (dataset on an adjacent range)
- Information exchange via imported Tables from other workbooks in the hierarchy
- Manual update of imported table (no self update)
- Tables contain metadata for traceability
- Import/exports Tables managed on a dedicated worksheet
- Document the overall project tree of workbooks

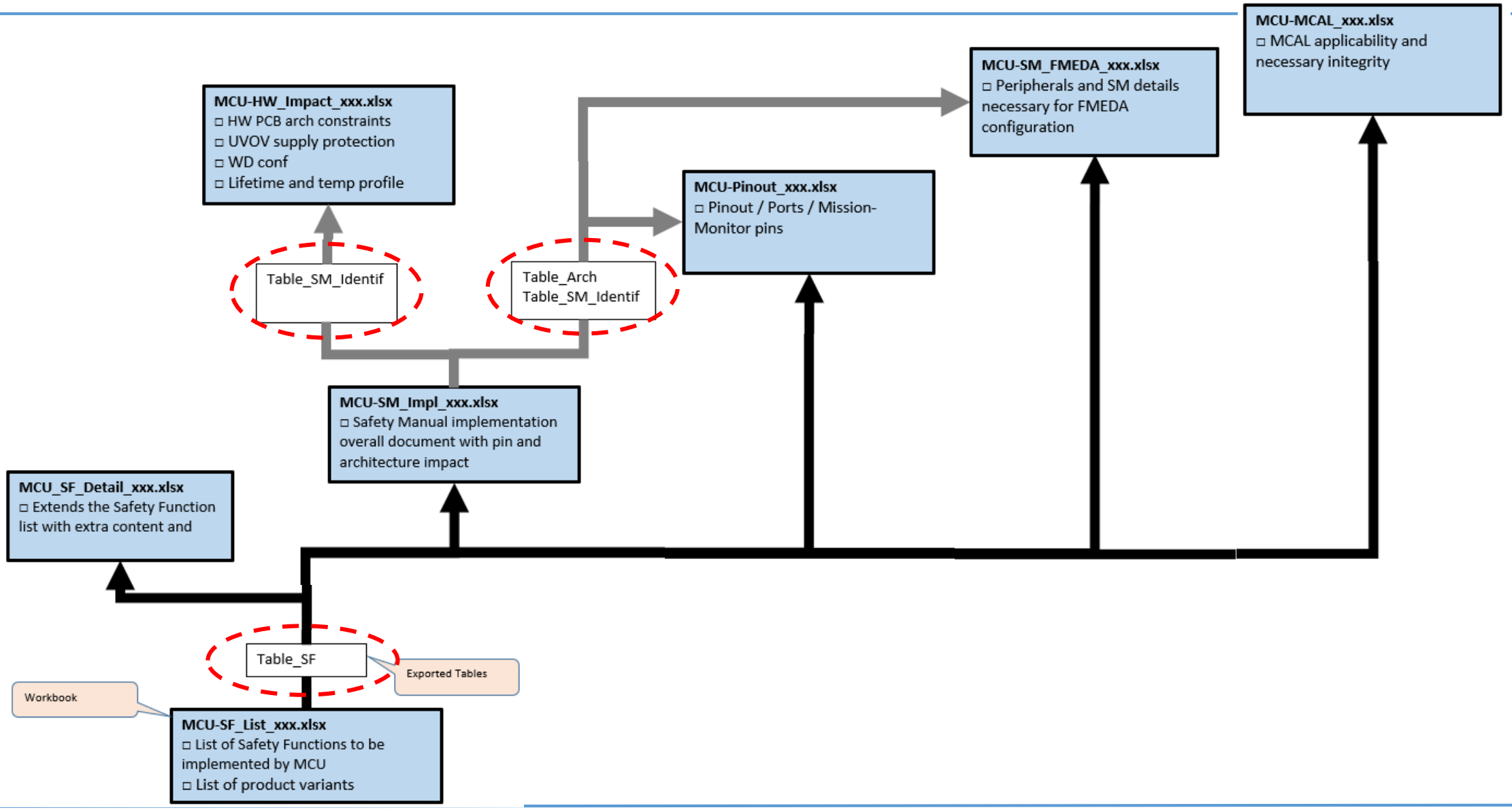


Foes

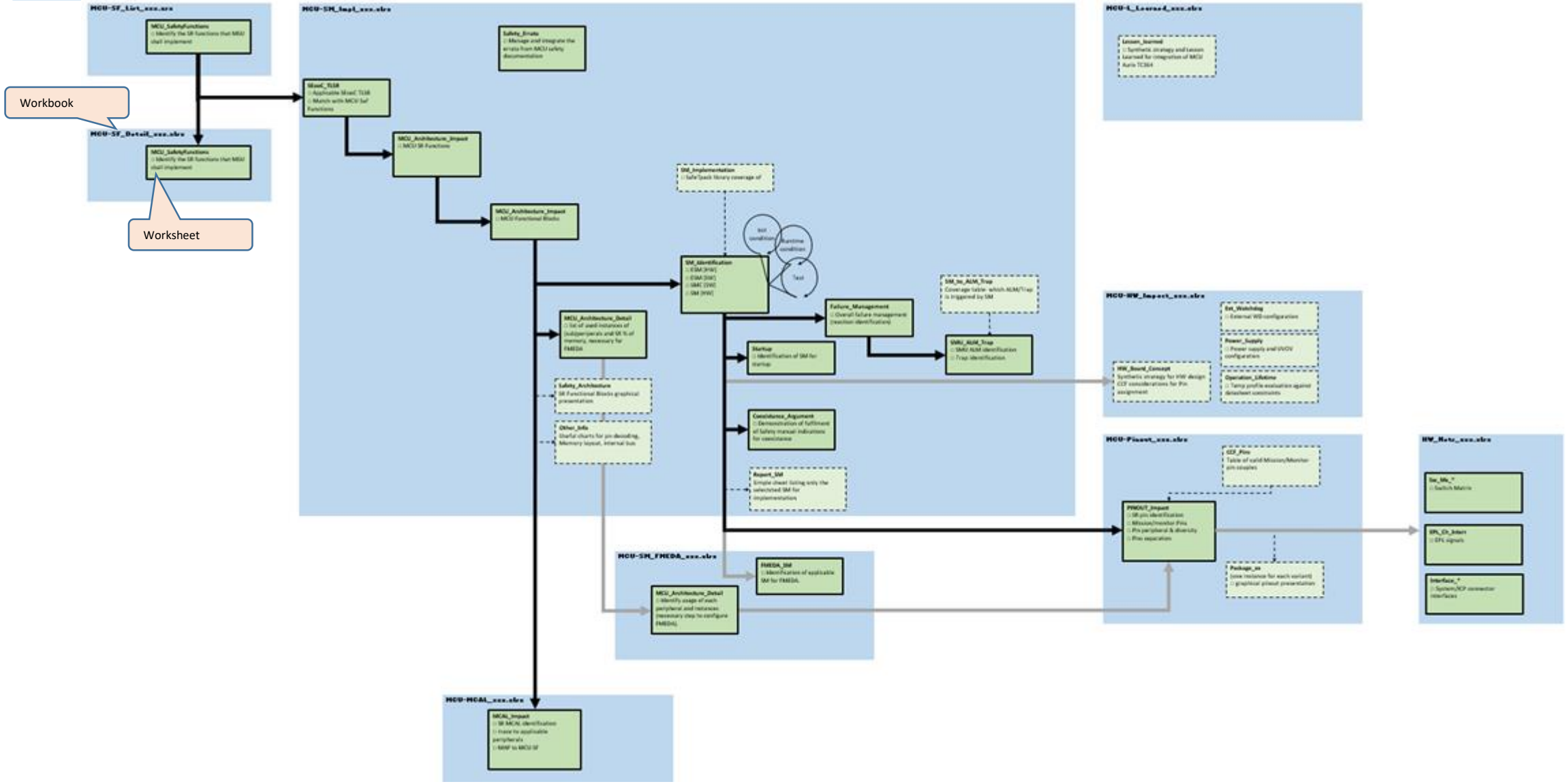
- Merged cells
- VBA (kills undo-redo)
- External references/paths in cells/names
- Hidden columns/rows
- Long unmanageable formulas


MCU-SM_Impl
Analysis
Nome
Doc_Structure
HW_Impact
HW_Nets
L_Learned
MCAL
Pinout
SF_Detail
SF_List
SM_FMEDA
SM_Impl
Doc_Structure_028.xlsx
MCU-HW_Impact_022.xlsx
HW_Nets_032.xlsx
MCU-L_Learned_004.xlsx
MCU-MCAL_009.xlsx
MCU-Pinout_067.xlsx
MCU-SF_Detail_020.xlsx
MCU-SF_List_020.xlsx
MCU-SM_FMEDA_014.xlsx
MCU-SM_Impl_411.xlsx
Table_Ref
Doc_Structure_xxx.xlsx
□ Reference Documents
□ Presents hierarchy of worksheets
□ Workflow block diagram

Data exchange - **Tool** ○●●●●



Workflow - **Tool ●●●●●**



FuSa Process

Convention - **FuSa Process** ○○○○●

OBC component (In-Context)

- OBC SR functions

MCU (COTS / Out-Of-Context)

- TLSR
- SR Functions
- HW Functional blocks “FB”

Hierarchy - **FuSa Process** ○○○●●

Safety Manual TOC distribution misguides the integration effort

It presents first:

MCU Architecture, **HW Functional blocks "FB"** (safety features), and their monitoring concept

Only later:

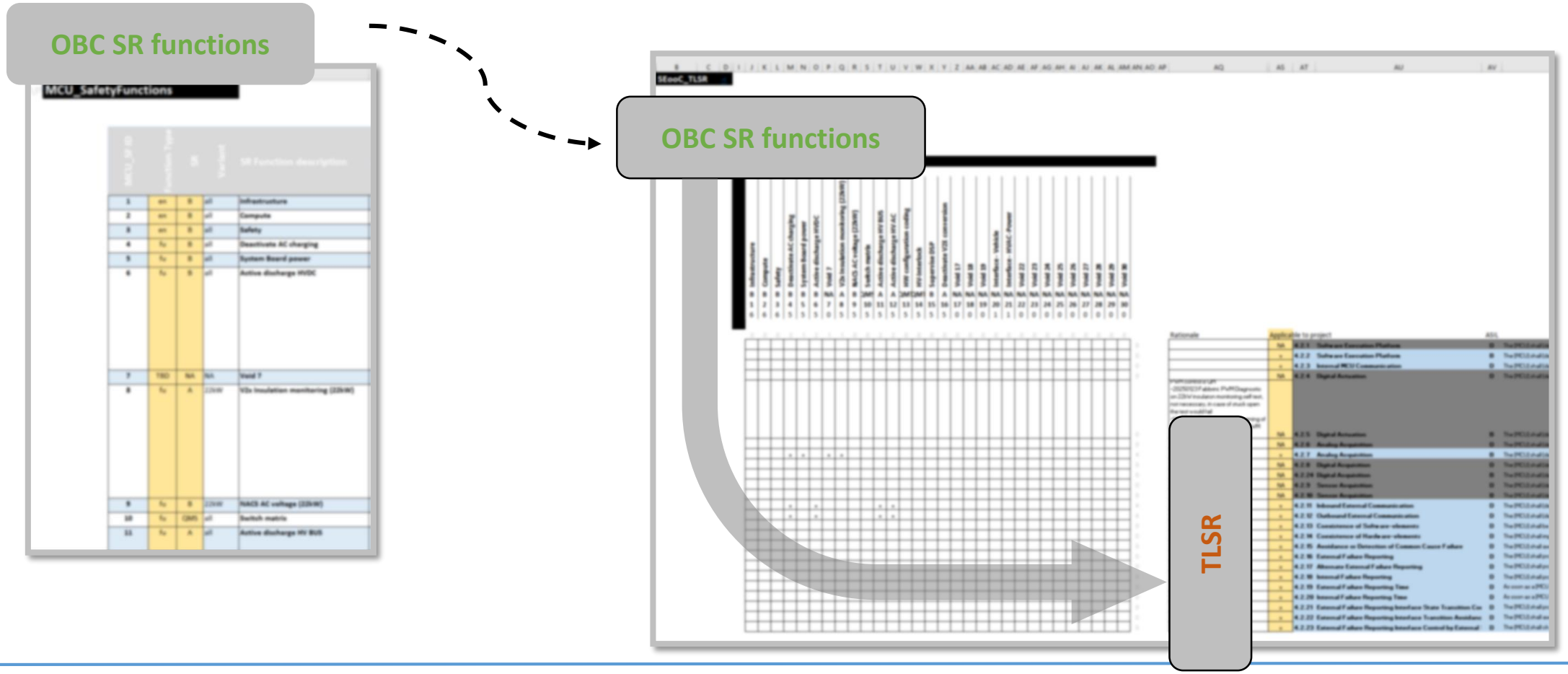
Safety Related Functions, with no structured presentation on **Top-Level Safety Requirements "TLSR"** of the SEooC

A rational evaluation should be the other way around: Function/Requirements → Structure.
In a complex design, first shall come a top-down **Functional Analysis**, and it shall be traced to the **Top-Level Safety Requirements TLSR** exposed by SEooC design from the vendor.
Such traceability is also necessary in terms of 26262-10 compliance.

→The Safety Case itself of the MCU properly presents Top-Level Safety Requirement TLSR
→The Safety Manual then traces them to → SR Functions → FB Functional blocks

Compliance effort - **FuSa Process** ○○●●●

This is indeed how we proceeded in our integration and demonstration of compliance:
1) Identify **OBC SR functions** that the MCU shall implement for the OBC component
2) Chose the necessary **TLSR**



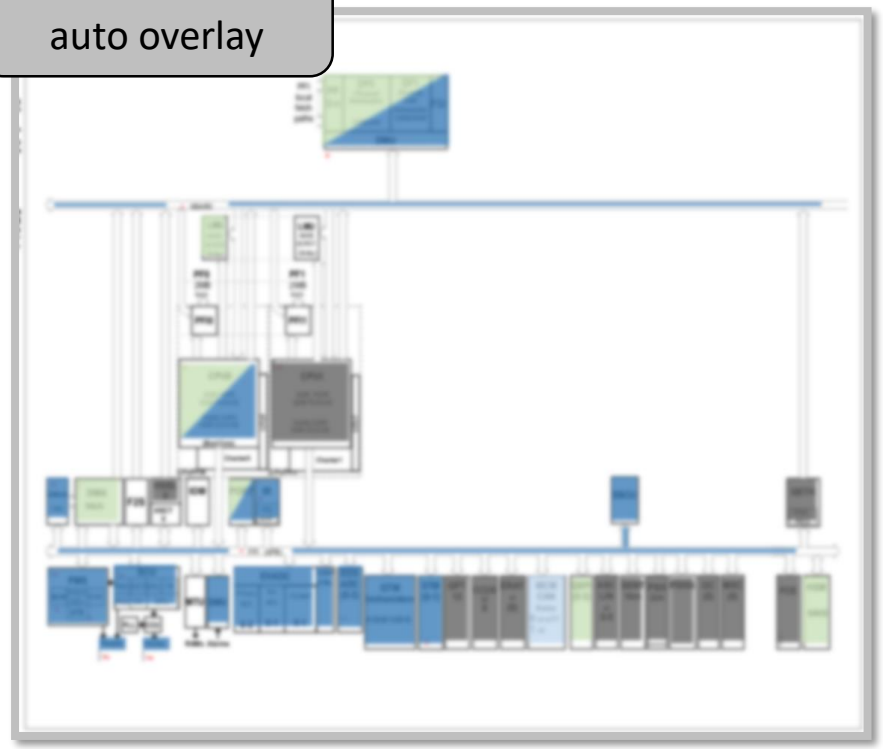
Compliance effort - **FuSa Process** ○●●●●

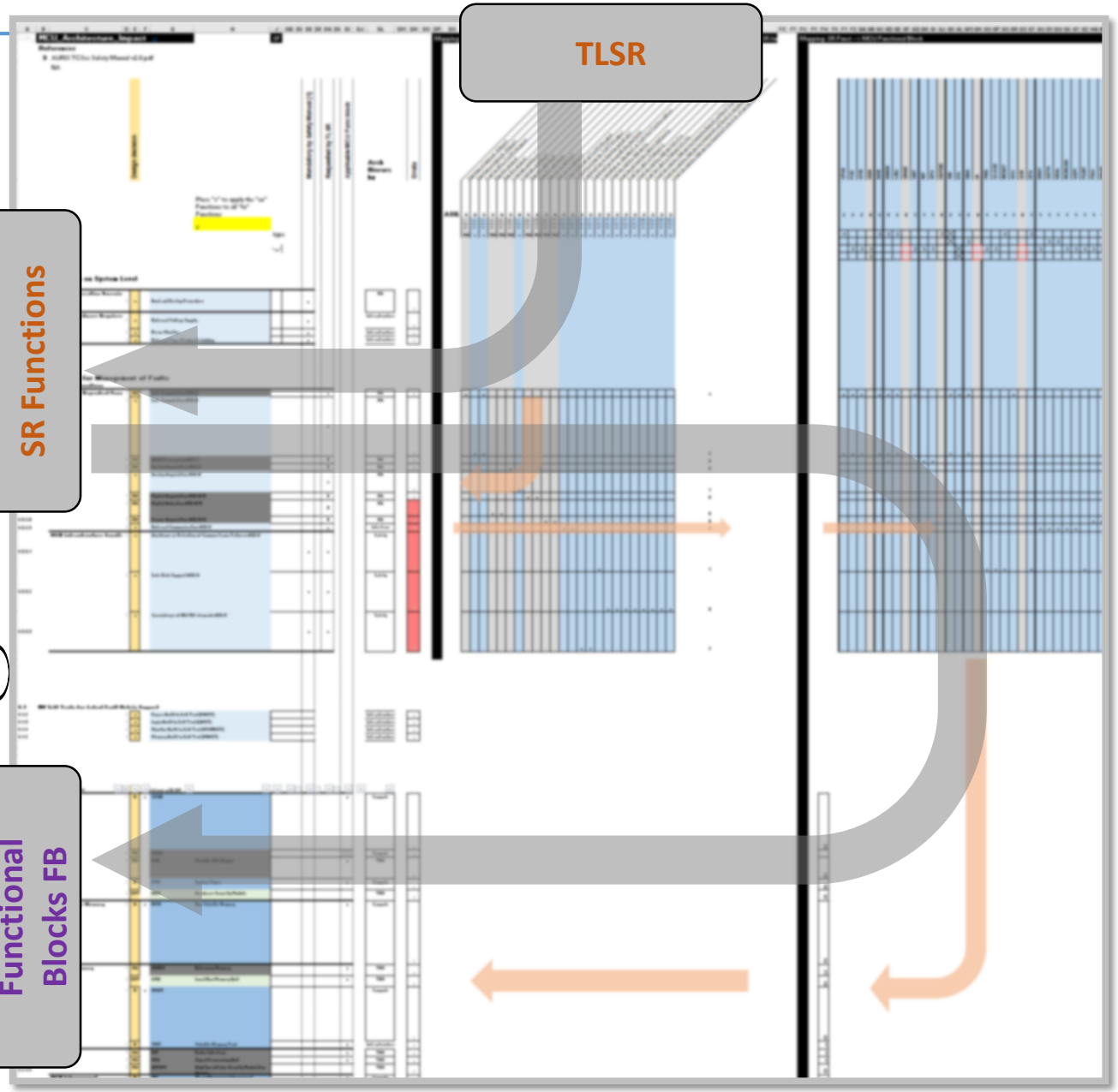
Given the **TLSR**

3) Identify mapping to **SR Functions** (Appl. & Infrastr.)

4) pick necessary **FB**

FB Architecture auto overlay



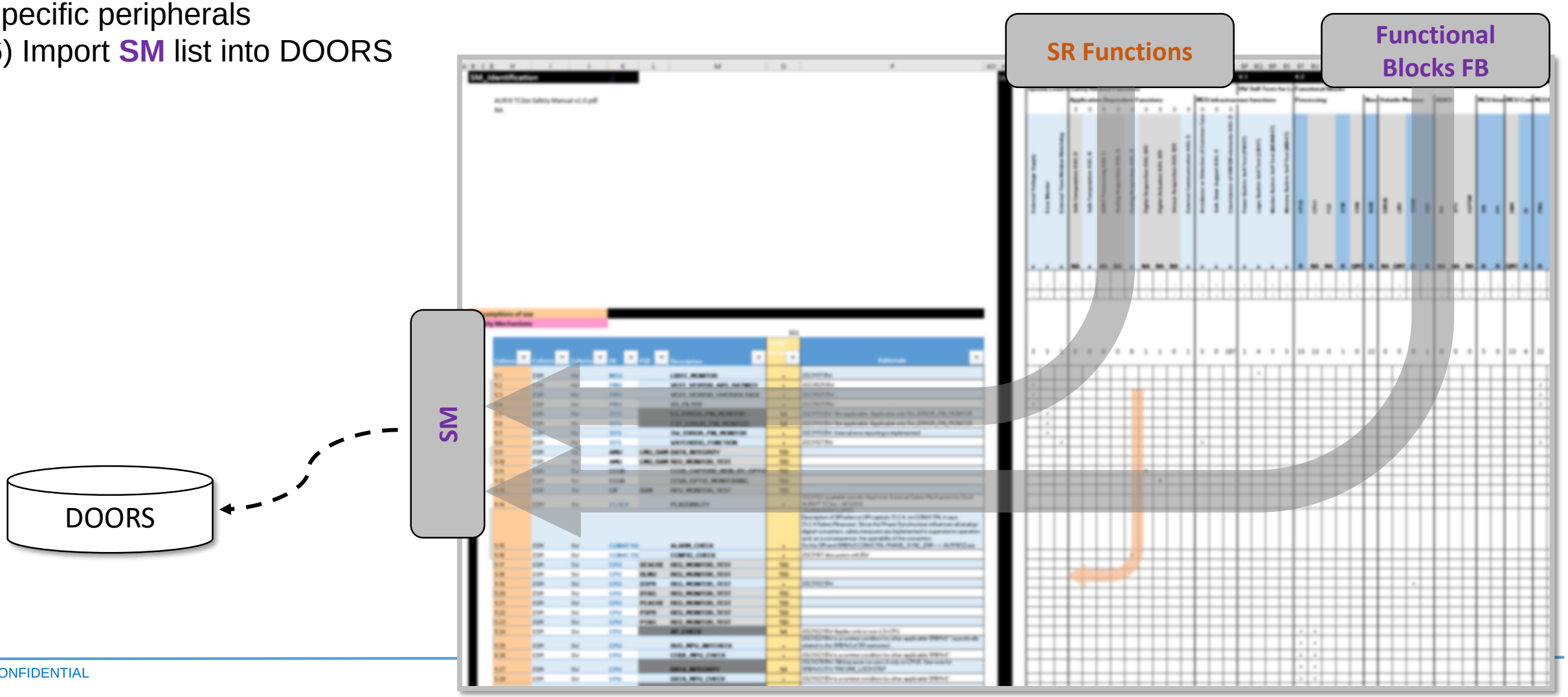


Compliance effort - **FuSa Process** ●●●●●

Given **SR** Functions, **FB**

5) select monitoring use cases **FUC** → pick necessary **SM** and specific peripherals

6) Import **SM** list into DOORS



Conclusion

Pros / Cons - **Conclusion** ○○●

Pros

- Tool with no cost, on every desktop
- Easy configuration/export
- Simple, flexible
- (self) Explainable, no hidden stuff
- Anybody can do it, no rocket-science

Cons

- Can’t constrain user actions (in a maintainable way)
- Single user access (per Workbook)
- Data and model are together
- Data integrity among Workbooks requires strict approach on modifications
- Traceability←→Impact have very limited scalability/dimensionality
- This is not a real model (*à la* MBSE)

Future work / Discussion - **Conclusion** ○●●

- The value of this experience was to create with a simple tool a **model of our understanding** of the safety manual, and along the way collect rationales and decisions...

  Extending / enhancing would mean:
  Rewrite into SysML project, for a MBSE workflow.

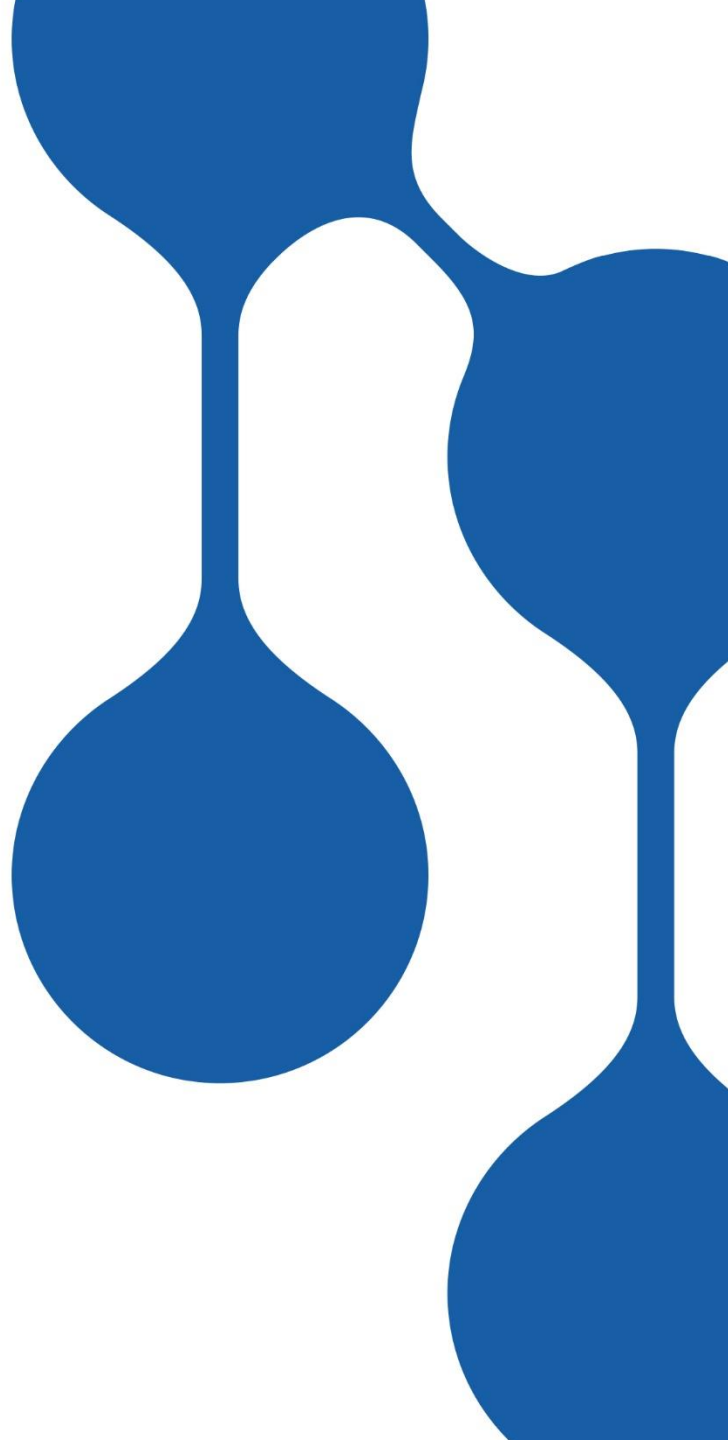
- Availability of ReqIF safety manual, is just a minor help, content is still provided as **prose**. Suppliers should prepare a **model** of the MCU for the purpose of the integration...

  No extra information as compared to Manuals, just a model equivalent to what is described in (safety) documentation…
  (like HW IO buffers IBIS model or Simulink behavioral models)

Q/A - **Conclusion** ●●●

Questions?

Thank you for your attention



META ELECTRONICS

Meta Electronics s.r.l. – Via T. Galimberti 9, 42124 Reggio Emilia (Italy)