Software Architecture documentation

Project information

Project: IPB

ECU: tbd

Production series: 2023

Abstract

This document is based on the

*Leitfaden zur Erstellung der Software Architektur Dokumentation*

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Rev. | Date | Author | Change Description |
| 00 | 02.06.2020 | M. Pisarek | First Release |
| 01 | 30.11.2020 | M. Pisarek | update |
| 02 | 01.02.2021 | M. Pisarek | Changes added due to concept change |
| 03 | 23.04.2021 | M. Pisarek | Changes added due to new design |
|  |  |  |  |

# Content

[1. Content 3](#_Toc63320957)

[2. Terms and Abbreviations 4](#_Toc63320958)

[2.1 Terms 4](#_Toc63320959)

[2.2 Abbreviations 4](#_Toc63320960)

[3. General information 5](#_Toc63320961)

[3.1 Technical Conditions 5](#_Toc63320962)

[3.2 Special requirements 5](#_Toc63320963)

[3.2.1 SW Release plan 5](#_Toc63320964)

[4. Concept view 6](#_Toc63320965)

[4.1 Overview 6](#_Toc63320966)

[4.2 Project takeover 6](#_Toc63320967)

[4.3 New concept / technology 6](#_Toc63320968)

[4.4 Critical architecture requirements 6](#_Toc63320969)

[4.5 Safety relevant aspects 7](#_Toc63320970)

[4.6 Security relevant aspects 9](#_Toc63320971)

[4.7 System interfaces 9](#_Toc63320972)

[4.8 Network System behavior 9](#_Toc63320973)

[4.9 Flexray 9](#_Toc63320974)

[4.10 Software updates 9](#_Toc63320975)

[4.11 Fail handling 9](#_Toc63320976)

[4.12 Special Modes 9](#_Toc63320977)

[5. Infrastructure overview 10](#_Toc63320978)

[5.1 Hardware components overview 10](#_Toc63320979)

[5.2 MCU description 12](#_Toc63320980)

[5.3 Peripheries 12](#_Toc63320981)

[5.4 Memory usage till SOP 14](#_Toc63320983)

[5.5 Hardware backup strategy 14](#_Toc63320984)

[5.6 Development tool chain 16](#_Toc63320985)

[5.7 Protection of not allowed Flash access 16](#_Toc63320986)

[5.8 WDG 16](#_Toc63320987)

[6. Logic view 17](#_Toc63320988)

[6.1 Layermodel of SWC 17](#_Toc63320989)

[6.2 Description if Software components 18](#_Toc63320990)

[6.3 Organisation 18](#_Toc63320992)

[6.4 Dataflow 18](#_Toc63320993)

[6.5 Safety Software-Architecture 18](#_Toc63320994)

[6.5 Security Software-Architecture 18](#_Toc63320994)

[7. Data view 19](#_Toc63320995)

[7.1 ROM Memory Map 19](#_Toc63320996)

[7.2 RAM Memory Map 19](#_Toc63320997)

[7.3 Variants 19](#_Toc63320998)

[7.4 Data location and content 19](#_Toc63320999)

[7.5 RAM mirror 19](#_Toc63321001)

[7.6 Reset protected data 19](#_Toc63321002)

[8. Process view 20](#_Toc63321003)

[8.1 OS 20](#_Toc63321004)

[8.2 Runnable 20](#_Toc63321005)

[8.3 Tasks 20](#_Toc63321006)

[8.4 ISRs 20](#_Toc63321007)

[8.5 OS-Hooks 20](#_Toc63321008)

# Terms and Abbreviations

## Terms

This document uses the requirement engineering terms shall and should. Shall is a mandatory requirement. Should is a recommendation.

## Abbreviations

|  |  |
| --- | --- |
| **Description** | **Acronym, Abbreviation or Mnemonic** |
| PFC | Power factor correction |
| BBC | Buck Boost Control |
| HVDC | High Voltage DC |
| LVDC | Low Voltage DC |
| DSP | Digital Signal Processor |

# General information

## Technical Conditions

**Terminal Connection**

* T30/T31

**CAN**

* Hybrid CAN-FD
* Debug CAN-FD

**OS**

* Os (SC3), Vector

**Planned Controller**

TC364/ TMS280049/ TC213

**TC364:** Flash 4MB / RAM 576kB

**TMS280049:** Flash 256kB / RAM 100kB

**TC213:** Flash 1MB / RAM 96kB

**FBL:**

COM: Vector, Version: 4.3

Other: Own development, Delta Energy Systems GmbH

## Special requirements

Maximal FUSI: ASIL D

Security: KS/SOK/FDS/SOD

OBD Relevant: Yes

PNC: No

Diagnostic class: DK3

### SW Release plan

|  |  |
| --- | --- |
| Release | Date |
| [D100](https://jiraext.deltaww.com/browse/PIPB/fixforversion/107312) | 11.11.2021 |
| [D060](https://jiraext.deltaww.com/browse/PIPB/fixforversion/107311) | 23.09.2021 |
| [D050](https://jiraext.deltaww.com/browse/PIPB/fixforversion/107310) | 12.08.2021 |
| [D040](https://jiraext.deltaww.com/browse/PIPB/fixforversion/102004) | 17.06.2021 |

# Concept view

## **Overview**



## **Project takeover**

* HVDC digital control model
  + Takeover form C2 HW Product

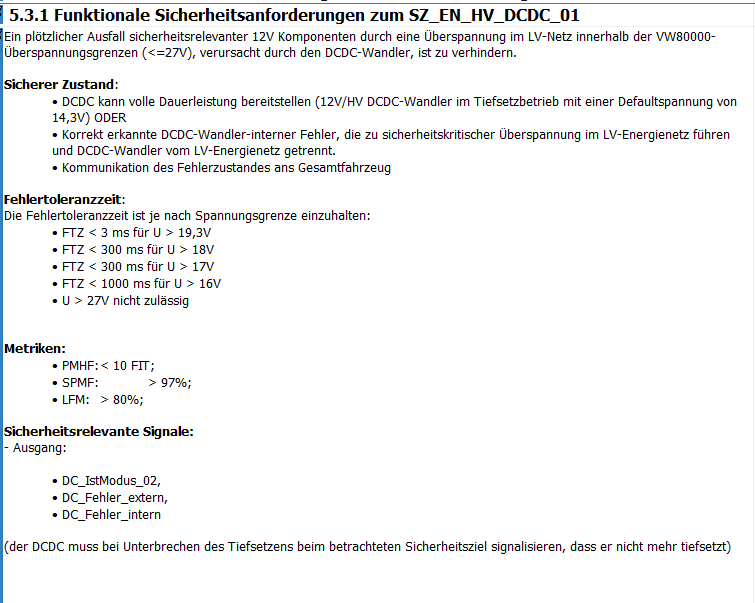
## **New concept / technology**

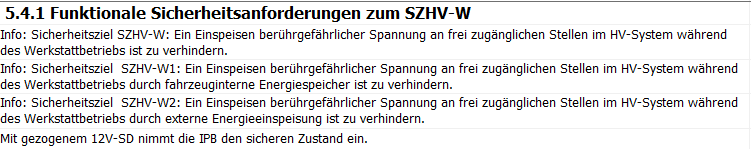
* Project with ASIL - D

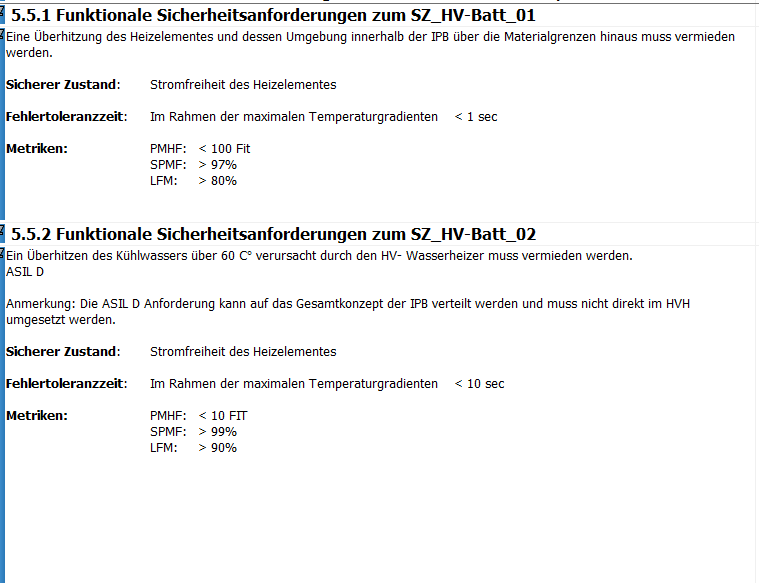
## Critical architecture requirements

* Security, ORU

## Safety relevant aspects







## Security relevant aspects

FDS, KS, Secure Boot, SFD needs to be integrated

## System interfaces

* Vector CANoe/ CANape
* PITT / ODIS
* vFlash
* Debug interfaces:
  + XCP
* Debugger
  + iSystems
  + PLS UDE

## Network System behavior

* KL30
  + Supply by KL30
* Wake Signals: CAN
* Awake signals: CAN
* PNC: No
* BAP: No
* DK: 3
* OBD Relevant: Primary
* FUSA relevant CAN Messages:

|  |  |
| --- | --- |
| ORU\_01 | 0x1A555548 |
| ORU\_Control\_D\_01 | 0x16A95595 |

* Ethernet: No

## Flexray

NA

## Software updates

Updates via CANFD

RnD: WinIdea ( iSystems ) or PLS UDE

## Fail handling

FTT: 30ms

COM stays in FBL if the flashing was not successful, via HW and DSP Control the HW will be locked.

## Special Modes

* Production mode
* Transport mode

# Infrastructure overview

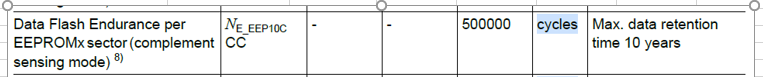
## Hardware components overview





## MCU description

**Taskfrequency:**

* 5ms/10ms/20ms/100ms
* Safety-Features: Lockstep, ECC
* Flash: TC364: 4MB
* 
* RAM: 576kB
* EEPROM: 128kB ( Dataflash )
* CPUs: 3
  + COM/PFC
  + HVDC
  + DCDC
* Security
  + MD-5, SHA-1 or SHA-224/SHA-256 function
* Interrupt controller
  + Tbd
* MPU
  + Tbd
* HW-Stackcheck
  + Tbd
* Addressroom
  + tbd

## Peripheries

**Which kind of:**

DSP

**Which function:**

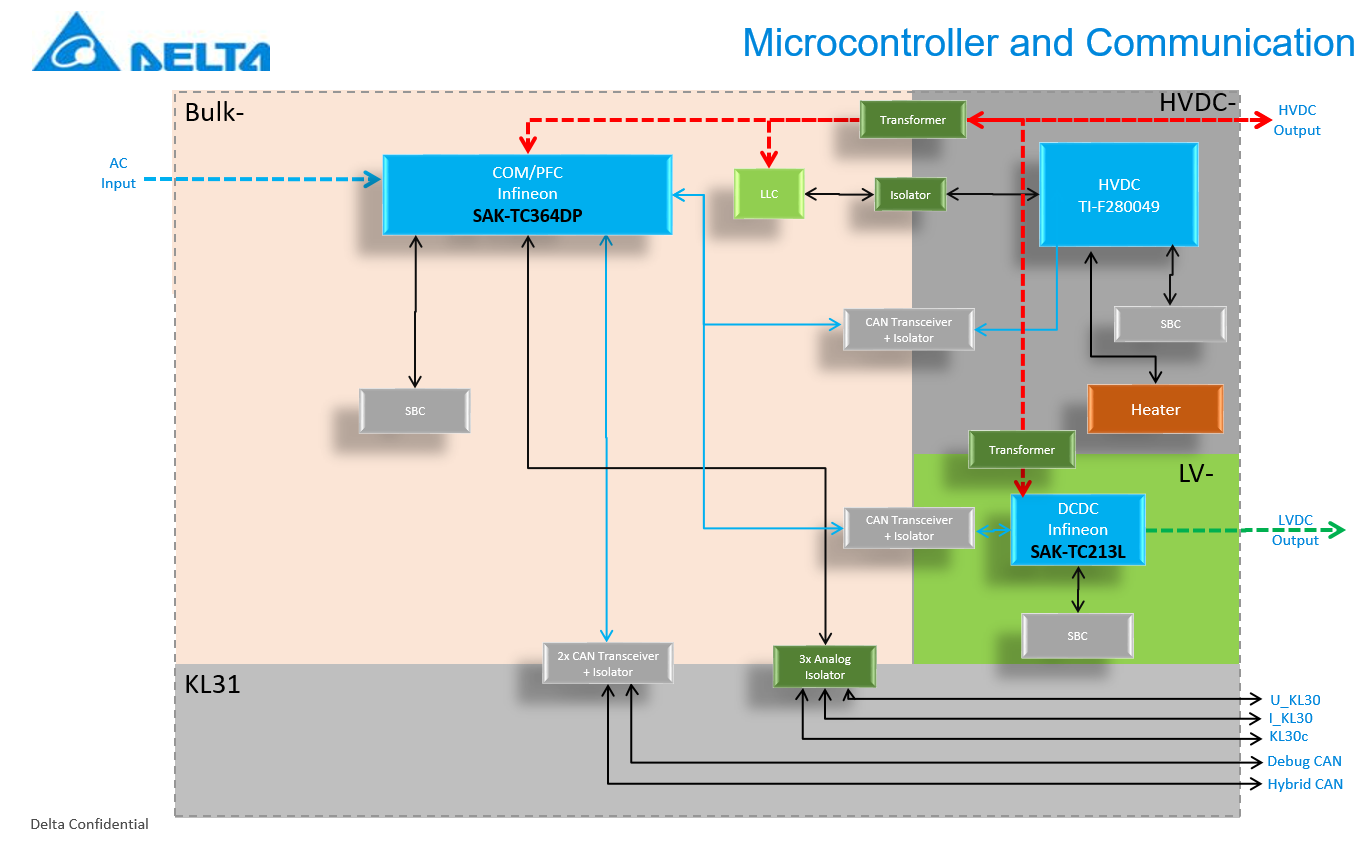
* SixSwitch PFC
* HVDC
* DCDC
* All have diagnostic
* All have FBL
* Only via HSK enable/disable

**ASIL:**

* D

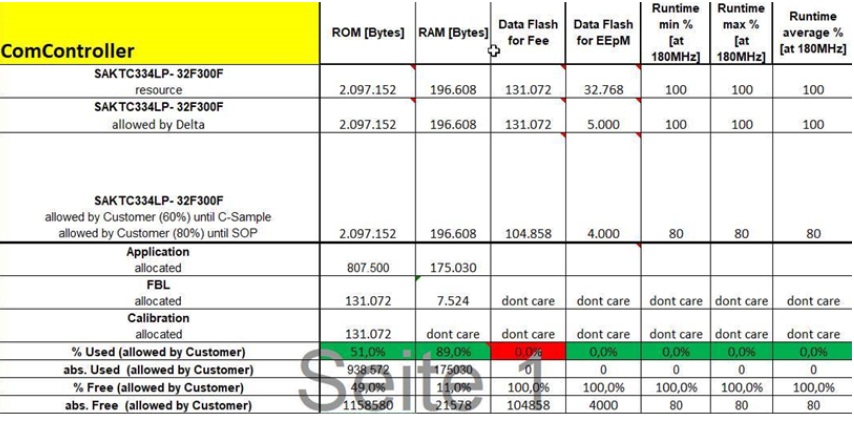
**Which interaction:**

* Internal CAN ( 500k CAN 2.0B )



## Memory usage till SOP

Based on the TC334, TC364 has more memory

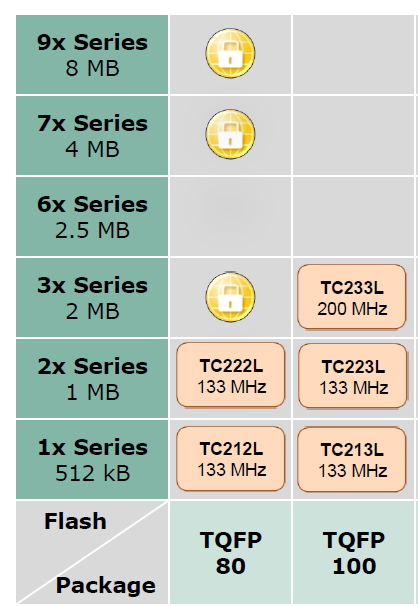


## Hardware backup strategy

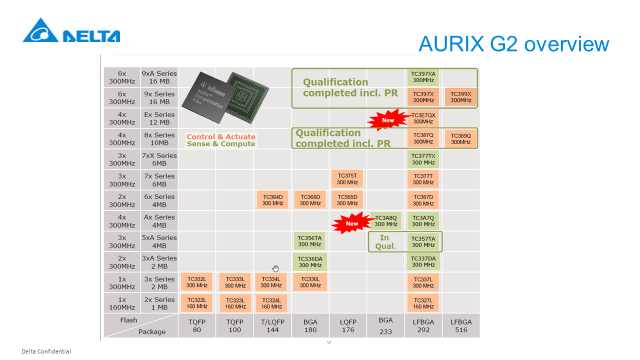
Current usage:

* + TC364
  + TMS280049
  + TC213

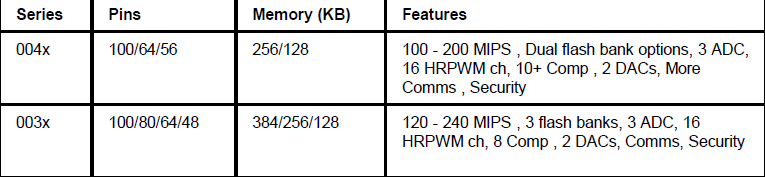
Backups for TC213



* Backups for TC364/TC367



* Backup for TMS280049



## Development tool chain

* Compiler HITEX: Version: HIGHTEC V4661 ( AURIX GEN1 )
* Compiler HITEX: Version: HIGHTEC V9920 ( AURIX GEN2 )
* Compiler Texas Instruments: Version ti-cgt-c2000\_20.2.1.LT

## Protection of not allowed Flash access

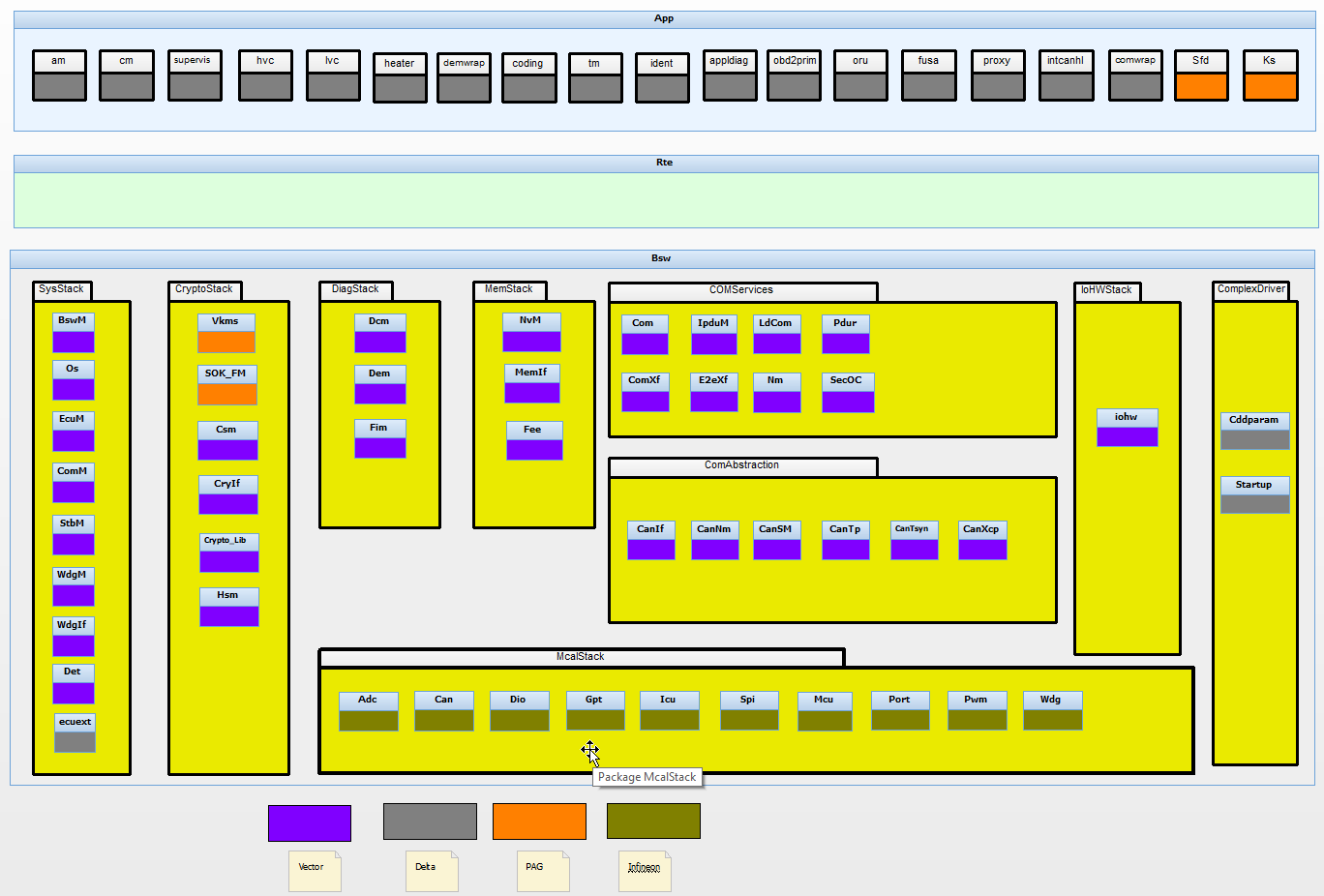
* Flash driver only in FBL
* Secure Boot

## WDG

* SBC: TLF35585 ( COM / DCDC )
* WDG: TPS3850H33QDRC ( HVDC )

# Logic view

## Layermodel of SWC



HVC: OBC Application ( PFC / HVDC )

LVC: DCDC Application

Heater: Heater Application

Appldiag: UDS Service layer

Demwrpp: Wrapper for the DEM

Coding: NVRAM

OVC: KL30, KL30c handling

Ts: Derating( OBC/DCDC/Heater )

## Description if Software components

# 

## Organisation

PM/OBC/HVDC

* + Soest, Germany

DCDC

* + Shanghai, China.

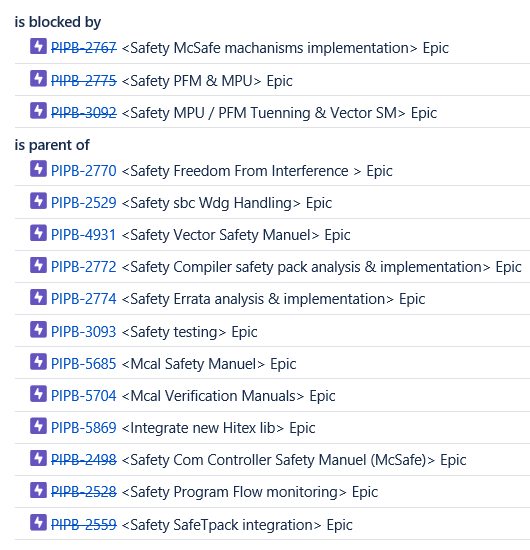
## Dataflow

All safety relevant data flow and interfaces are captured in the document IPB\_SW\_Com\_SDD.docx under chapter 6.16 Functional Safety Paths

## Safety Software Architecture

Complete software architecture and the split between ASIL and QM software parts are described in IPB\_SW\_Com\_SDD.docx under chapter 6.11 & 6.12. It also describes all safety mechanisms we employ to reach ASIL B safety level in software.

Additional Safety Measures Implemented in the microcontroller



## Security Software Architecture

## 

# Data view

## ROM Memory Map

ROM is divide into two parts Data Flash and Program Flash.

Data Flash or NvM layout with all the NvM blocks and there sizes are present in the following file IPB\_SW\_Com\_MemoryMap\_NvM.xlsx

For safety relevant NVM data we have an special checksum which will be written by the operator the SW will check if the checksum matches and only then will the safety component use the data if not the data is consider unsafe and a DTC will be logged.

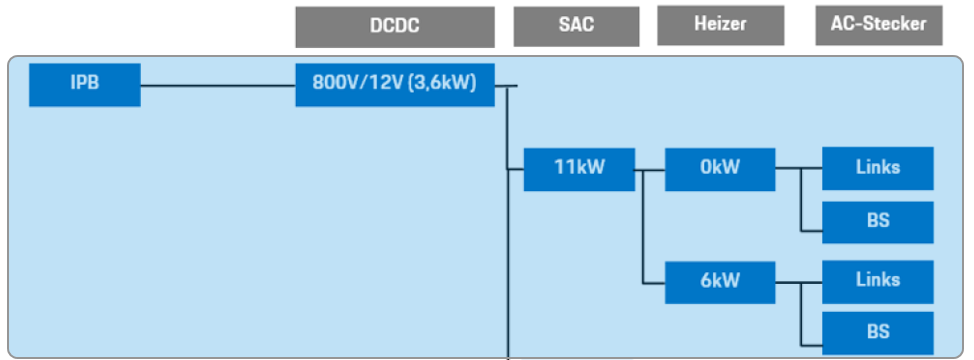
Program Flash with all the sections and there sizes are present in the following file IPB\_SW\_Com\_MemoryMap\_FLASH.xlsx

## RAM Memory Map

RAM with all the sections and there sizes are present in the following file IPB\_SW\_Com\_MemoryMap\_RAM.xlsx

Also, you will see the QM and ASIL RAM areas in this documents. MPU will protect against a wrong access between safety and non safety components.

## Variants



## Data location and content

## RAM mirror

Tbd

## Reset protected data

Defined in the IPB\_SW\_Com\_MemoryMap\_RAM.xlsx section in RAM layout

# Process view

## OS

SC: 3

ECC: 1

## Runnable

Please check the IPB\_SW\_TDS\_RunnableTaskMapping\_v1.0 to get all needed detailes.The relevant tab is **Core0 Tasks**

## Tasks

Please check the IPB\_SW\_TDS\_RunnableTaskMapping\_v1.0 to get all needed detailes.The relevant tab is **Core0 Tasks and Task Priorities**

## ISRs

Please check the IPB\_SW\_TDS\_RunnableTaskMapping\_v1.0 to get all needed detailes.The relevant tab is **ISR&Exceptions**

## OS-Hooks

Please check the IPB\_SW\_TDS\_RunnableTaskMapping\_v1.0 to get all needed detailes.The relevant tab is **Hooks**