Camera Base SW CompReqSpec

Projekt Interior Camera System ICS CompSpec (RM)

Gedruckt von Dohmeyer, Volker (059)

22. Dezember 2023, 11:12:19 MEZ

Konfiguration Interior Camera System ICS CompSpec (GC) WORK

Konfigurationstyp Globale Konfiguration

Komponente Interior Camera System ICS CompSpec (RM)

Inhaltsverzeichnis

1 Introduction

These component requirement specifications (German: KLH) describe the requirements for the provision of services within the framework of the development or series production of component parts, modules, software or components (all referred to as the "component" or the "scope of supply" in the following) by the supplier (referred to as the "contractor" in the following) to Mercedes-Benz AG or the specific subsidiary or corporate affiliate of Mercedes-Benz AG with whom the contractor has contractually agreed to provide components or a scope of supply (that party in the following referred to as the “client”).

For reasons of linguistic simplification for natural persons alone, these specifications are often used only in the masculine form. In terms of content, this refers to persons of any gender identity.

1.1 Document Landscape

Together with all other documents referenced here, these requirement specifications form the basis of the scope of supply to be provided by the contractor.

References to other documents are shown in square brackets, e.g [LHV 310 00x]. Documents referenced this way are to be found in the chapter "Other Applicable Documents" (see STM-867662). The download options using the DocMaster system are also described there.

1.1.1 Document Creation

This document was generated from a requirements management database. Maintenance and updating of this document are performed in this database.

In order to uniquely identify document contents, the database assigns identifiers (IDs). The following forms of the identifier can appear in the document depending on the formatting used:
- ID left, text right (requirement)
- ID under the text (requirement)
- ID in brackets after a heading

The requirements contained in this document may be acquired by the contractor as a database export.

1.1.2 Common Requirements

The document "Common Requirements Pertaining to the Component Requirement Specifications" [LHV 310 00x] contains requirements that are valid for all scopes of supply provided by the client.

In the case of deviations between the provisions of the requirement specifications and those in the Common Requirements [LHV 310 00x], the provisions described in the requirement specifications shall apply.

Chapters or requirements in [LHV 310 00x] are referenced not by chapter number but rather by the corresponding Requirement ID, e.g. "Scheduling in the Project" CRCS-3339913.

The Common Requirements are available in versions containing different scopes, for example with or without E/E requirements. In this case, the document numbers differ in the final digit (placeholder "x" in [LHV 310 00x]).
- LHV 310 001 = E/E + Software + Mechanical scopes
- LHV 310 002 = Software scopes only
- LHV 310 003 = Mechanical scopes only

- LHV 310 004 = Assembly scopes
The documents can be found in the DocMaster system using these document numbers.

Under CRCS-3339913, the Common Requirements contain major changes at the versions of the specification template. This overview has descriptive character, in order to facilitate orientation in the document. It does not relieve the contractor of a detailed examination of the requirements.

1.1.3 Logistics Component Requirements Specifications

With each sourcing scope, the contractor receives, via the "proSource" system, the logistics component requirement specifications (LOG-KLH), which also describe the logistics concept. The logistics concept will differ depending on the component part, the client plant, the form of delivery and the contractor's production and dispatch location. The contractor shall fulfill the requirements of the logistics component requirement specifications LOG-KLH).

1.1.4 Excerpt from the Process Master Plan for Suppliers

The document "Excerpt from the Process Master Plan for Suppliers" contains the most important skeleton schedule dates of the leading model series project for this scope of supply.

The contractor can obtain the "Excerpt from the Process Master Plan for Suppliers" via the "proSource" system.

1.1.5 Additional Documents in the Requirements Specifications

These requirement specifications and the other documents cited refer to various types of documents, including:
- Implementation regulations (AV)
- Function specifications (FV)
- Drawings
- External standards and company standards (MBN)
- Supply specifications (DBL)
- Legislation
- Other component-specific specification documents
These types of documents are referred to in the following as "Other Applicable Documents" (German: MGU) pertaining to the requirement specifications and to the other cited documents.

The documents referenced in the chapter "Other Applicable Documents" supplement the requirements described in the present document. The requirements set forth in these documents are hence likewise binding specifications for fulfilling the scope of supply and services.

If the present requirement specifications or the Common Requirements contain more stringent or less stringent specifications than are found in the Other Applicable Documents, the specifications contained in the requirement specifications and/or Common Requirements shall apply. No weakening of safety-relevant requirements or legal specifications is permitted.

If a company standard (German: MBN or DBL) is referenced by these requirement specification or by the Common Requirements Pertaining to Technical Component Requirement Specifications, the contractor shall check whether an approval of procurement source (German: BQF) exists for the referenced company standard. The indication of an approval of procurement source is documented on the cover sheet of the company standard. It shall be possible to retrieve the approval of procurement source under

document number "BQF ..." in DocMaster (example: MBN12345 -> BQF 12345). The restrictions applied by the approval of procurement source shall be complied with in the context of the contract.

An approval of procurement source is needed whenever the company standard makes specific requirements that can or may only be provided by one or more particular suppliers, that need to be verified by means of special tests, or that can only be satisfied by particular products (quoting a trade or brand name and their manufacturers).

contractor drawings with the associated 2D/3D data records are the intellectual property of the contractor who created them. The disclosure of external supplier drawings by the contractor to competitors of that contractor is only permitted with the written approval of the drawing owner (for example, in the context of supplier-bound parts).

The procurement of directed parts is, as with a BQF, only permitted through the contractor documented on the contractor drawings; otherwise, there is a risk of violating competition and intellectual property laws.

In the case of drawings prepared by the client, there are no specifications governing the contractor for procurement.

1.2 General Specifications

The contractor shall treat all information and documents pertaining to development as confidential.

If the cited documents do not define requirements or define these differently, and these requirements are required for the flawless and unimpeded function and quality of the scope of supply, then the contractor shall reveal this to the client in writing.

If, in the course of performance, the contractor wishes to deviate from the requirements described in the cited documents, the contractor shall require the written consent of the client.

If the contractor is familiar with quality- or reliability-enhancing or cost-reducing alternatives to the content of the cited documents, the contractor shall reveal these alternatives to the client in writing.

The contractor shall critically analyze the client's proposals and specifications and, if necessary, shall jointly develop improved solutions (shared responsibility).

The contractor shall ensure that the scope of supply meets all the requirements set forth in the requirement specifications. In particular, the contractor shall ensure that the planned tests and checks are suited to and sufficient for the development and delivery of a specification-compliant scope of supply, even in such cases where the type or number of tests and checks is proposed by the client. Should the contractor deem further tests and checks to be necessary, the contractor shall notify the client of this without delay and take appropriate action. Neither the performance of tests and checks by the contractor or client nor compliance with such tests and checks shall ever relieve the contractor of the obligation to fulfill the requirements of the requirement specifications. The contractor shall document fulfillment of the requirements in writing by means of test plans and reports.

The client is at all times authorized to demand changes and additions to the project description.

The contractor is obliged to propose to the client technical changes that the contractor deems necessary or practical. The contractor shall implement these changes after receiving the written approval of the client.

The contractor may reject changes or additions if these are deemed unreasonable, provided that notice of such rejection is immediately submitted to the client. The reasons for deeming them unreasonable shall be presented in writing.

To the extent that changes affect costs and/or deadlines, the contractor shall immediately upon receipt of the demand for changes or additions, or together with the contractor's proposal for changes, submit a cost estimate to the client with an itemized and justified listing of higher or lower costs as well as information on how deadlines may change. In such cases, the contractor shall not implement changes and additions until the parties to the contract have reached a written agreement. The written order to implement the changes may only be issued through the client's material supply process.

When designing the component, the contractor shall take all boundary conditions given by the overall vehicle into consideration. This refers in particular to space requirement investigations and associated tolerance considerations, assembly, feasibility of assembly, ease of servicing, visual matching with trim parts (inside and outside), environmental compatibility, country variants and the use of modular systems.

To meet the client's demand for functionality and quality at the lowest possible cost, the contractor should submit its own proposals, stating the risks and potential benefits.

The contractor shall select all component elements and suppliers in such a way that life cycle support is ensured for 15 years following the end of series production.

The client reserves the right to use the scope of supply in other vehicle/engine model series as well.

The contractor shall not make changes to the scope of supply that limit the use of the scope of supply in the vehicle/engine model series.

Changes made by contractors of parts to both the contractor and the client shall be agreed between the client and the general contractor. They will be prioritized by the client.

The contractor shall coordinate the market-specific start-up curves with the market launch deadline in detail with the client.

Throughout the entire development period, the contractor shall analyze and reveal weight-reducing measures.

Weight figures shall be broken down by the contractor on the basis of the parts list. They serve as the basis for future optimizations and the documentation thereof. Note that the components/item numbers at interfaces to adjacent modules are to be given full consideration.

In addition, the contractor shall offer at least one lightweight design variant of the subject component, this variant weighing less than the specified maximum weight. Consideration shall here be given to alternative materials, manufacturing processes and weight-optimized design.

The contractor shall reveal the weight reduction potential and any additional costs of the lightweight solution versus the conventional manufacturing process to the client.

1.3 Complementary VAN-Specific Standard Requirements

This scope of supply is also used for Mercedes-Benz Vans. For this purpose, the complementary VAN-specific requirements from [Van MGU] shall be observed. If conflicting requirements between the supplementary VAN-specific requirements and the present Mercedes-Benz Cars component specifications are identified by the contractor, the

client shall be notified of these immediately for clarification.

2 2 Scope of Services

2.1 Component-Specific Requirements

2.2 Service Life and Reliability

2.3 Important Gen20x project specific requirements

The client follows a agile working model within this Gen20x project. The following chapters therefore describe the requirements of the client regarding this new working model.

2.3.1 Agile Project Work

The working model of Gen20x project for Software is agile. SW development will be done as AGILE SCRUM.

Due to the size of the project a customised version of SCALED AGILE SAFe is basis of our working model. Additionally to the SCALED AGILE SAFe in the Gen20x Project we have a customised Project Organisation. Details about the Way of Working are described in "Way of Working".

Therefore the contractor shall enable an agile working model and team setup.

The contractor is responsible for providing the required applicable roles needed at Team, Domain and Project level mentioned in 2.3.6.2.1 Roles within Way of Working (SW20X-rm1_3286379)

The contractor shall setup an agile project management aligned with Mbition Project Management Office and the roles mentioned in 2.3.6.2.1 Roles within Way of Working (SW20X-rm1_3286379)

The contractor shall work with the client on a common backlog inside the Gen20x project "Apricot". Planning and Development must be done according to the "Way of Working" and transparent for the Project Organisation. The client always hast to explain and adapt the status of the backlog to show the development and planning status.

This backlog consists out of Jira tickets issuetype "function", "architecture measures", "diagnostic requirement", "epics", "bug", "task" and "story". The status of these tickets must always be up to date, latest in the end of the sprint.

The refinement of this backlog will be done as part of AGILE SCRUM.

The contractor is responsible to refine this backlog in alignment with the client.

Supplier shall maintain security requirements as part of their product backlog.

Non-functional security requirements shall be included in the definition of done and/or acceptance criteria of respective user stories.

2.3.2 Offer

The offer of the contractor shall consider at least the following pricing relevant content:

The contractor shall describe the setup of the project team according to the roles mentioned in 2.3.6.2.1 Roles within Way of Working (SW20X-rm1_3286379)

The contractor shall list all occurring license cost of the provided software module or of software submodules which are part of this software module.

The contractor shall name and list any fixprice content.

2.3.3 Architecture and Responsibilities

For the IVI i4 project, several companies are involved and contracted by the client. Each company contributes to the overall IVI i4 product. Responsibility is spread to different partners. The overall architecture and responsibilities are described in the picture attached to chapter 2.1.3.2 and the following requirements.

The CarComputer component containing the IVI part consists of Software and Hardware.

Tier 1a is mainly responsible for product delivery (HW and HW-near SW), Hardware development, production and production-ready SW.

Tier 1B Premium is mainly responsible at the system level for SW Integration, SW Quality, CI/CD, SW Testing as well as SW Supplier Management. The role of Tier 1B Premium is described in the following chapter "Software Integrator" in more detail.

The contractor is responsible for the delivery of his SW function which is described in this SW-KLH.

Due to several partners being involved in this project, the contractor shall cooperate with other partners where needed.

2.3.3.1 RASIC

The responsibilities of the software integrator, the contractor as well of other project involved roles are defined in Gen20x RASIC document [MBITION_RASIC].

Document [MBITION_RASIC] is part of agile CI/CD work process which means that this document will continuously be improved and adjusted. Therefore this document reflects only today's version. The document is provided by MBition.

The contractor will get direct access to the database were document [MBITION_RASIC] is sourced.

All changes in this document which affect the contractor will only be done in vote with the contractor.

2.3.3.2 Obligations of the Contractor

The contractor shall ensure compliance with all the provisions of these requirement specifications.

2.3.3.2.1 Representatives Regulation

Communication between contractor and client shall be through the representatives nominated by both parties for the provision of services on each assignment. These representatives will be documented in the project insigts database

Issue-specific communication between experts of contractor and Mbition and client shall be allowed. Both parties shall strictly refrain from the reciprocal issuing of work instructions.

Prior to commencement of provision of the services, both parties undertake to convey to everyone involved in active project work (individuals involved in the active, regular communication process) an understanding compatible with the requirements of a service contract (Dienstvertrag) in relation to the character of functional communication.

The representatives of contractor and client shall advise the involved individuals of the requirement to strictly refrain from issuing labor-law instructions and shall guarantee compliance therewith.

The contractor shall specify in the quotation a representative structure appropriate to the scope of the work and keep this up-to-date.

The list of representatives from the client are listed in the project database "Insigts" from Apricot project

The client reserves the right to not consider quotations that do not comply with this specification.

The data of the representatives named in this requirement specifications document shall be used only for the processing of the services described in this document.

The control and coordination of the employees appointed by the contractor is the sole responsibility of the contractor.

2.3.3.2.2 Subcontractors

The contractor shall ensure that its own personnel fulfill the stipulated contracted service. Partial or complete contract award to/sub-contracting of third parties is not permitted. Deviations from this provision require the written approval of the client.

2.3.3.2.3 Acceptance Criteria

The following described Acceptance Criteria is only valid for the agile content described in this SWLH and not for fix price content.

The in chapter 2.4.3 "Scope of function" and 2.4.4 "High Level Backlog" defined content with its resulting deliveries and deliverables are subject to an aligned continuous refinement as part of the Way of Working. This will lead into a detailed sprint and PI planning for each sprint and each milestone content. The achievements of each sprint will be accepted by each sprint demonstration. This will be done by the approval the of corresponding clients representative and deputy of the representative based on the aligned content of each sprint.

The detailed execution of acceptance will be defined between the client and the contractor.

The SW shall reach the level of end customer readiness at least in the SW release planned for the SW delivery milestone PRO1 for the individual carline. The detailed milestone are desribed in the Project plan.

2.3.4 Software Integrator

For Gen20x project the overall software responsibility and software integration is done by software integrator which is MBition GmbH.

The software integrator is contracted separately by the client.

MBition is a 100% subsidiary company of Mercedes-Benz.

The contractor must work in close contact with MBition along the project organisation. The contractor must always represent the status of development and planning towards the Mbition Project Management Office. Furthermore in case of defect the contractor must align with Mercedes-Benz and Mbition Project Organisation a solution path.

2.3.5 Locations

The following locations are the places where the development for Gen20x takes place:

- Mercedes-Benz project lead development: Sindelfingen, Germany

- MBition software development: Berlin, Germany

- Mbition software development: Sofia, Bulgaria

Only whoever provides an operating facility that meets the following requirements can be considered as a contractor:

- criterion 1: software development location

- criterion 2: located in Berlin

The contractor shall install his team of experts in a location in Berlin close to the MBition office or Sindelfingen Office, in order to enable a close collaboration in working

This is to enable the contractor to work as an integrated team within the software development aligned to the Way of Working.

The contractor shall support worldwide testdrives if needed.

2.3.6 Way of Working

This chapter describes how software will be developed in Gen20x project. It is called Way of Working and defines the agile software development in this project.

The contractor shall work in close collaboration with MBition who is the owner of the Way of Working and the Project Organisation

2.3.6.1 Qualification of 3rd Party Suppliers

The contractor shall develop software according to [MBITION_Q3PS].

The contractor shall work according to chapter 2.1.1 "General" in [MBITION_Q3PS] as INTEGRATED DEVELOPMENT TEAM.

[MBITION_Q3PS] gives you an overview about the Way of Working in this project. Detailled and complete information about the Way of Working can be found in [SWF_WOW] which is the Way of Working document.

Document [MBITION_Q3PS] is part of agile CI/CD work process which means that this document will continuously be improved and adjusted. Therefore this document reflects only today's version. The document is provided by MBition.

2.3.6.2 Way of Working Document

The contractor shall develop software according to [WOW] which is Way of Working.

[SWF_WOW] shows detailed and complete the Way of Working. Purpose is to establish a common understanding among project members how to work within the project.

Document [SWF_WOW] is part of agile CI/CD work process which means that this document will continuously be improved and adjusted. Therefore this document reflects only today's version. The document is provided by MBition.

The contractor will get direct access to the database were document [SWF_WOW] is sourced.

2.3.6.2.1 Roles within Way of Working

To fulfill the above tasks, the contractor shall assign his personnel to the roles of Way of Working accordingly. The client and contractor shall agree on the assignment.

If a contractor is responsible for a full domain he must assign the domain roles. If they are part of the domain with it teams they need to apply the team roles.
In the following the most important roles are described. A full overview of all roles you can

find in [SWF_WOW].

(Domain) Product Manager (PM) - Defines who is doing what, how and why, until when, i.e. overall planning, staffing and financial control of the project within a domain.

(Domain) Architect (DA) - Defines how Features shall be constructed and Attributes shall be maintained in the Sub-Systems of a domain.

Developer Representative (DR) - Accountable for documentation of detailed design and Sub-System-Architecture and source code quality. Design, document, implement / integrate and test.

Developer (DE) - Develops end-user features. Design, document, implement / integrate and test.

Product Owner (PO) - the product owner owns the product on behalf of the company and is responsible for the business value of the project within the team's domain. The Product Owner is the voice of the customer and defines the details (User Stories) that realize a feature. There is one dedicated Product Owner per team in the project organization.

Product Owner (PO) shall also be responsible for business case level threat analysis in order to define abuse cases / misuse stories for certain user stories. These abuse cases shall be analyzed by development team during backlog grooming and further security user stories may be created and included in the product backlog based on this analysis.

Scrum Master (SM) - The Scrum Master facilitates the everyday work in the team and make sure the team lives by the values and practices of Scrum and the processes defined in Way of Working.

For teams other than development teams, the roles should met the roles defined for Teams or Domains in Way of Working.

2.3.6.2.2 Meetings

The content in this chapter describes existing regular meetings. As Way of Working is updated according to the changing requirements, contractor is also expected to adapt to the changes in the Meeting Structures

Depending on the role assignments, the contractor’s personnel has to join respective meetings. The following meetings currently are happening on a regular basis.

Internal meeting within team. All team members participate in meeting. One meeting per team

Backlog Refinement (team level)- Identification and estimation of possible work to be done by the team in upcoming sprints

Sprint Planning (team level) - Definition of team's sprint goal and definition of team's sprint backlog

Sprint Retrospective (team level) - Establishment of a common understanding of the health of the team, to serve as a basis for continuous improvement

Daily (team level)- Establishment of a common understanding regarding team's ongoing work and possible impediments to be resolved outside of team. Project global information shared with team members.

Sprint Review (team level)- get feedback about the work done within a sprint and monitor the team’s progress

Internal meeting on project level. At least one representative from each team participate in meeting, typically the Scrum Master. Customer representatives may attend:

Technical Alignment (domain level) - Establishment of a common understanding regarding system architecture design and potential design issues

Process Alignment (project level) - Continuous improvement of way of working on a project level, i.e. over team boundaries.

360° Domain Sync (Domain Level) - Ensuring the project interest inside the domains and integrate the domain into the projects

Sprint Retrospective (project level) - Establishment of a common understanding of the health of the project, to serve as a basis for continuous improvement.

Townhall - Project global information shared with all project members

Milestone Kick-off (project level) - alignment of all teams with the project goals for the upcoming quarter. The goal here is to offer all interested parties clarity on the project's direction

External meeting. Representatives from customer and supplier participate in meeting:

Project Steering (a.k.a. Operational) - Establish a common understanding between meeting participants regarding project status and issues experienced in the project that requires actions to be taken outside the actual project organization

Sprint Review (project level) - Establishment of common understanding of system status and project status across team boundaries and company boundaries. Project global evaluation of sprint and sprint review session

Change Control Board (CCB) (project level) - Meeting for agreements on change requests, scope discussions and other issues not resolved in project member's continuous dialogue with stakeholders outside project organization.

360° Project Sync (Project Level) - gathering a project status out of every domain status and is preparing the escalations and further measures for the domain.

Technical Alignment (project level) - establishment of a common understanding regarding system architecture design and potential design issues at project level

Milestone Review (project level) - establishment of a common understanding of the achievements of the preceding milestone (quarter) across all personnel, teams, and stakeholders. The goal is to inspect and adapt as a basis for planning the next Milestone

2.3.6.3 Architecture Principles

The contractor shall develop software according to [MBITION_ARPRI] which is Architecture Principles.

[MBITION_ARPRI] contains the architecture principles based on which MBiENT and Gen20x is developed. These architecture principles are also binding for the contractor.

Document [MBITION_ARPRI] is part of agile CI/CD work process which means that this document will continuously be improved and adjusted. Therefore this document reflects only todays version. The document is provided by MBition.

The contractor will get direct access to the database were document [MBITION_ARPRI] is sourced.

2.3.6.4 Test Plan

The contractor shall develop software according to [MBITION_SFTP] which is Test Plan in Way of Working

[MBITION_SFTP] contains all definitions for testing in this project.

Document [MBITION_SFTP] is part of agile CI/CD work process which means that this document will continuously be improved and adjusted. Therefore this document reflects only todays version. The document is provided by MBition.

The contractor will get direct access to the database were document [MBITION_SFTP] is sourced.

The Tier 1B is responsible for Basic and Extended Feature Test of his Application.
These Tier 1B test shall also be performed in the (partly or fully) integrated system on the target. For details please refer to [MBITION_SFTP].

2.3.6.5 Softwarefactory Documentation

The contractor shall develop software according to [SW_FA_DOC].

[SW_FA_DOC] contains guidelines how to program software in this project and at MBition.

Document [SW_FA_DOC] *is part of agile CI/CD work process which means that this document will **continuously** be **improved** and adjusted. Therefore this document reflects only todays version. The document is provided by MBition.*

The contractor will get direct access to the database were document [SW_FA_DOC] is sourced.

The Tier 1B is responsible for Basic and Extended Feature Test of his Application.
These Tier 1B test shall also be performed in the (partly or fully) integrated system on the target. For details please refer to [MBITION_SFTP].

The contractor must comply with the integration process and provide a component test with the MR.

2.3.7 Tools and CI/CD

In Gen20x project the CI/CD-toolchain is provided by MBition.

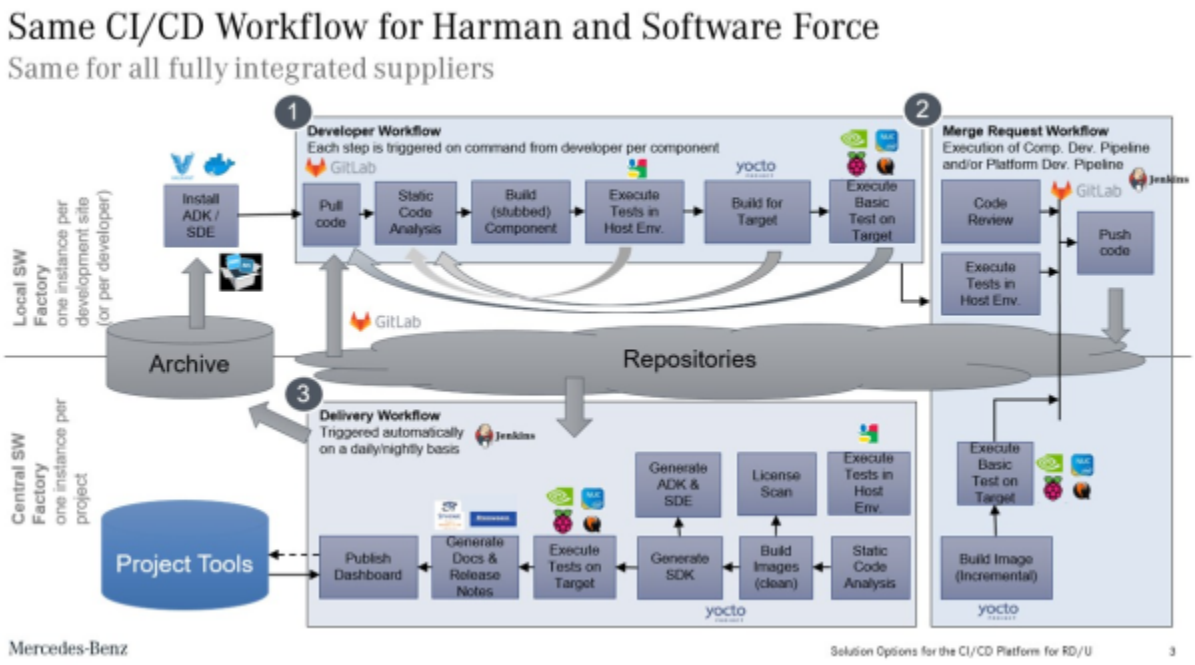
Contact persons for the CI/CD-toolchain are listed in chapter 3 "Contacts and Responsibilities".

Whereever possible the contractor shall use the CI/CD toolchain provided by Mercedes-Benz.

The contractor shall provide continuous software releases to Mercedes-Benz according to CI/CD.

The following illustration shows the CI/CD workflow.

CI/CD workflow

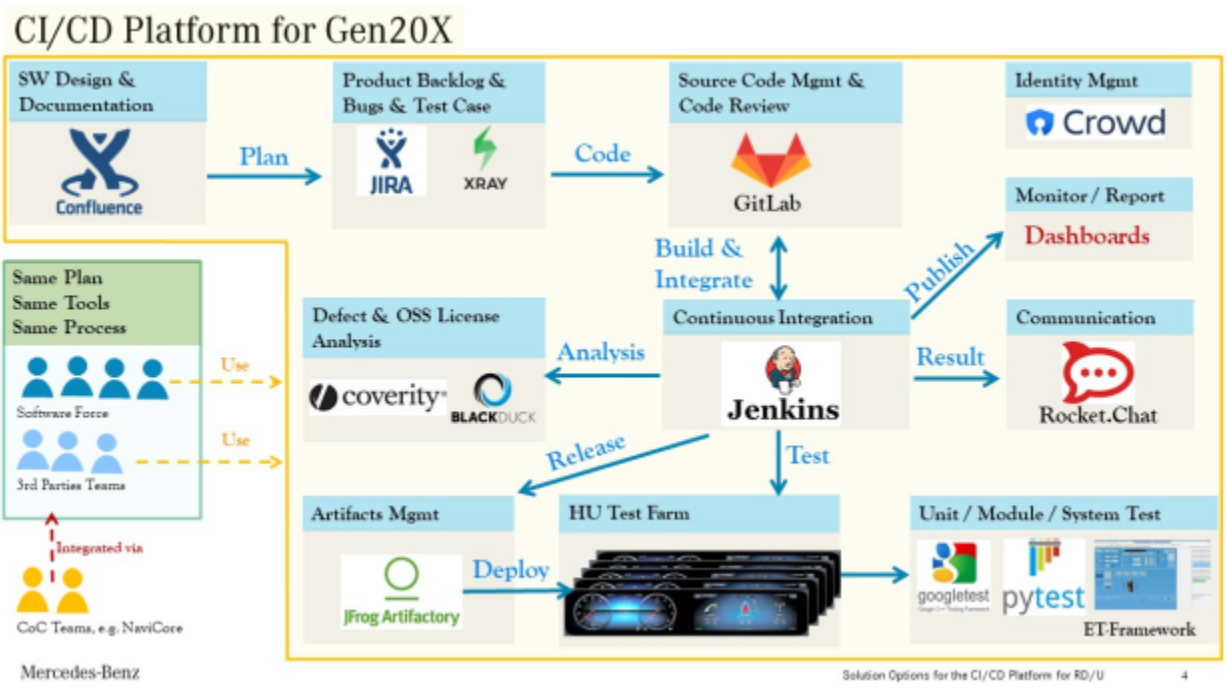


Version of embedded object: 1.0

2.3.7.1 Toolchain

The following illustrations shows the CI/CD toolchain including the used tools.

Toolchain



Version of embedded object: 1.0

The toolchain will be continuously improved according to the needs of the project driven by Mercedes-Benz and Mition

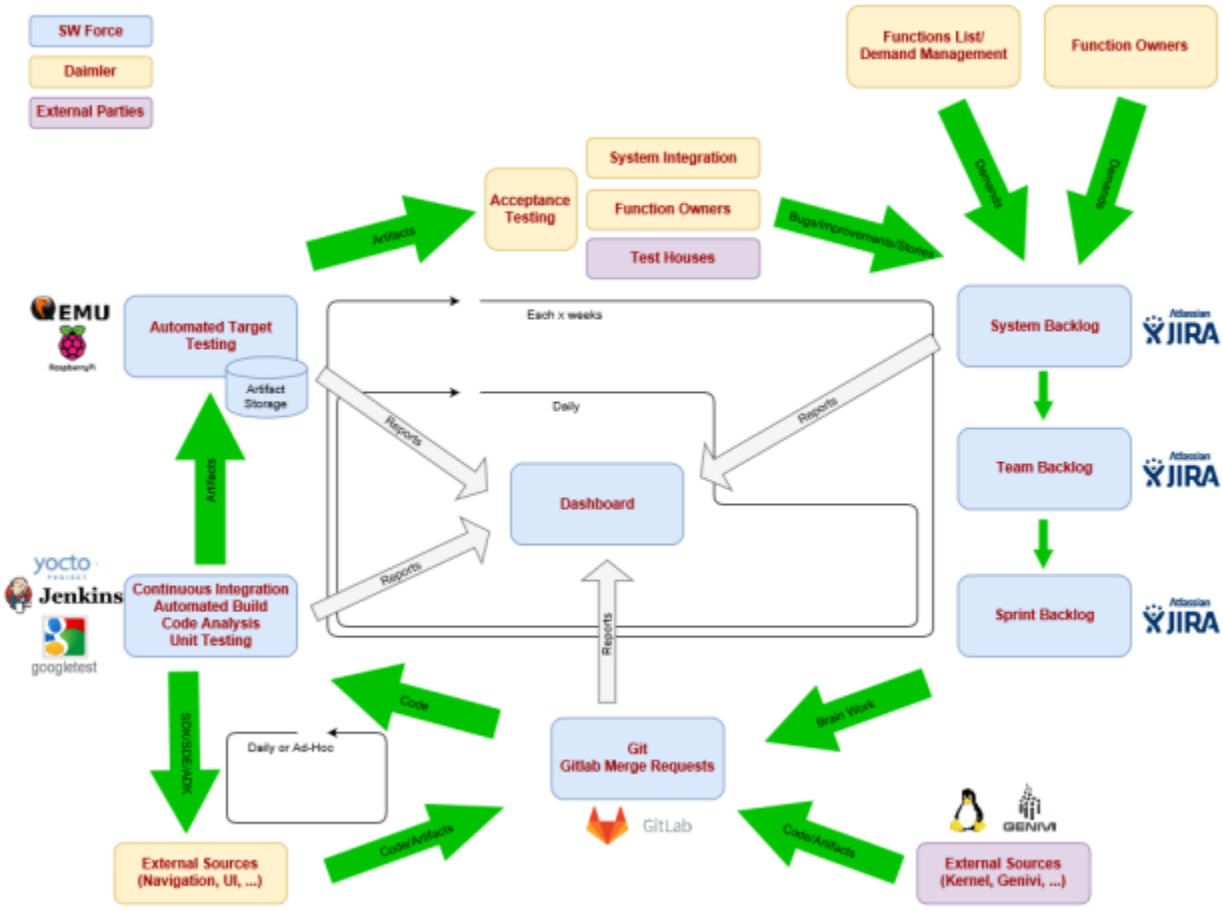
The contractors suggestions for improvement is welcome and will be considered according to the project needs.

2.3.7.2 Continuous Integration and Testing Cycle

The following graph shows Continuous Integration and Testing Cycle.

The latest valid version is defined in Confluence (https://wiki.swf.daimler.com/display/PDC1218/Continuous+Integration+and+Testing+Cycle)

The picture below describes the initial version for the contractor.



Version of embedded object: 1.0

Sprint duration is 2 weeks which means that "each x weeks" means two weeks cycle.

2.3.8 IT Infrastructure

The contractor shall take care to provide a sufficient IT Infrastructure to fullfill the requirements in this specificaition.

The contractor shall also take care to provide a sufficient IT Dataconnection to Mercedes-Benz Network.

The contractor shall take care that all his involved locations support a bandwidth of at least 1 GBit/sec.

To fullfill this the contractor shall establish an IT Infrastructure and -connection in coordination with Mercedes-Benz RD Partner Connect. (http://pcn.e.corpintra.net/dashboard).

Further information about Mercedes-Benz RD Partner Connect can be found on PCN - Partner Connect Navigator page (@PCN, @RDPC in Daimler Intranet) and on Supplier Portal (supplier.daimler.com).

The RD Partner Connect (RDPC) RD Supplier Integration team will coordinate the IT integration of external partners upon request by the assigning Mercedes-Benz department.

In the course of the RDPC integration process, a so-called IT integration concept will be created. This concept consolidates the applications, system access, etc. (integration demand) mentioned by the Mercedes-Benz department to be provided to the contractor's users in order to fulfill these requirement specifications.

RDPC will expand this integration need by appropriate access paths and solutions and derive the fundamental prerequisites and conditions which the contractor shall meet for the described IT integration (and hence for the fulfillment of these requirement specifications).

2.3.9 Test-Equipment and Hardware

The contractor is responsible for procurement of the test-equipment including testbenches and HW-samples for his own use.

2.3.10 Defect Management

For defect management the contractor shall also use the toolchain of Mercedes-Benz.

Defect Management will be done with StarC and SWF JIRA tool.

The contractor shall manage and response all defects related to his software responsibility.

If support is needed the contractor shall participate on testing and analyzing workshops.

If the contractor hosts its own defect management system the contractor is responsible for synchronisation.

Mercedes-Benz internally also HP ALM Dante or its successor STARC will be used as second tool for defect management.

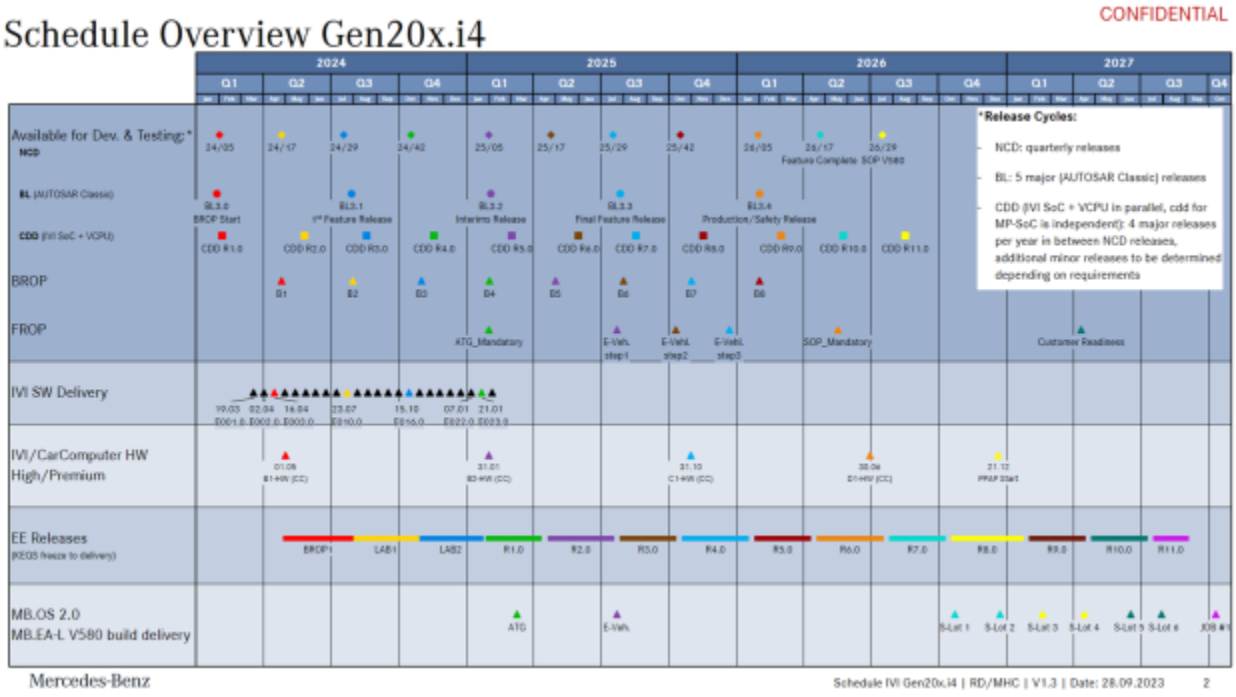
Mercedes-Benz keeps the right to use also HP ALM Dante or its successor STARC as backup-system for defect management and the contractor shall be prepared to also support this system if needed.

2.4 Specific Requirements for Camera Base SW

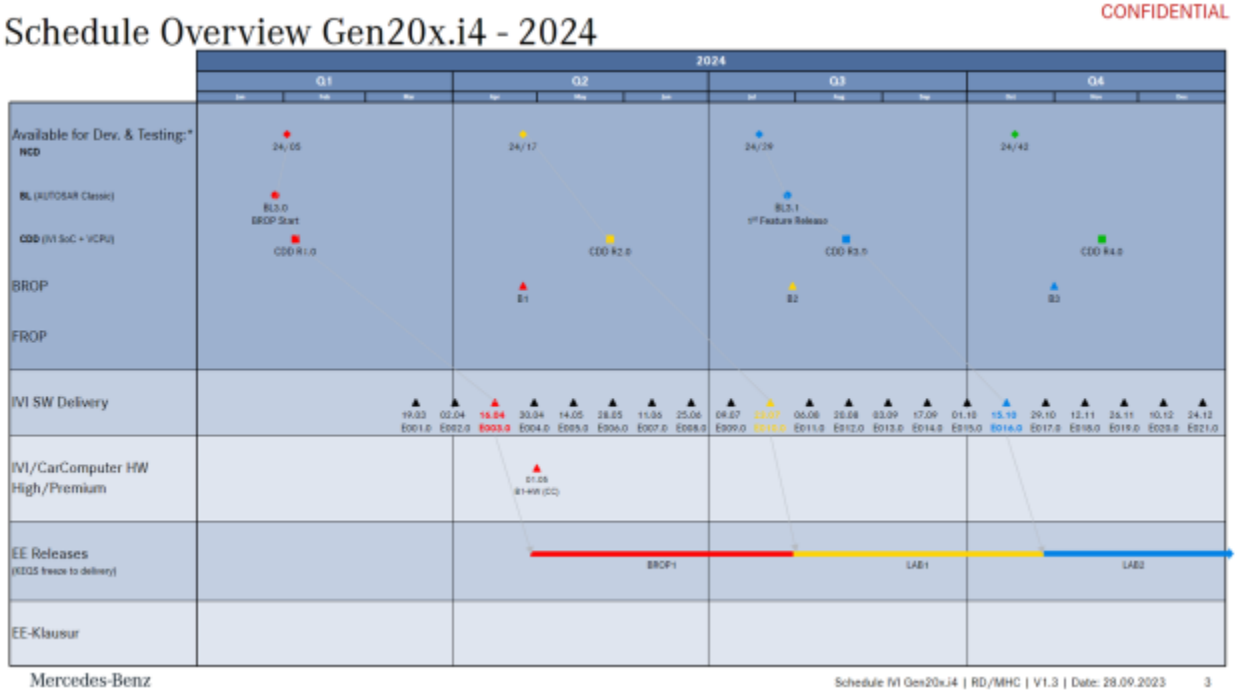
2.4.1 Time span of assignment

The following pictures shows the IVI i4 project schedule

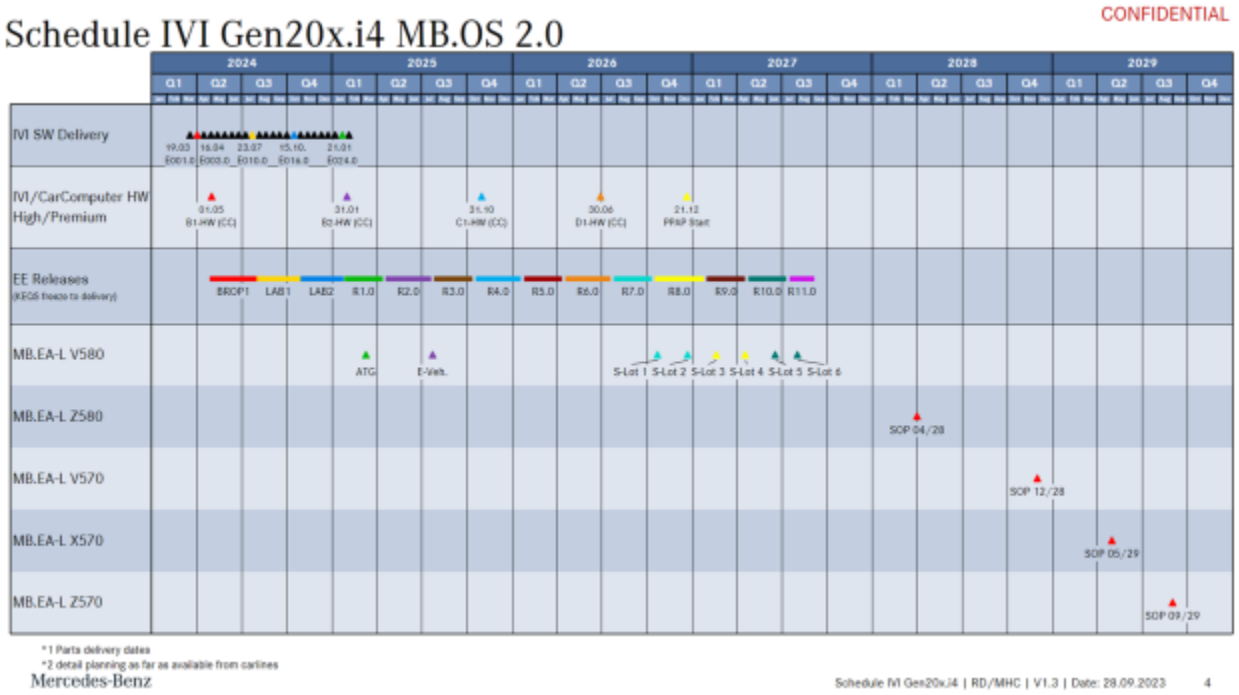
Gen20x IVI i4 project schedule v1.3



Gen20x IVI i4 project schedule v1.3



Gen20x IVI i4 MB.OS 2.0 project schedule v1.3



The Software project schedule for the RSU will follow the SW schedule and cadenz for the CIVIC I3 MB.OS 0.7 the RSU will be built in the vehicle.

The Software for the RSU should be provided together with the Software for the CIVIC.

The contractor shall provide the possibility to the client to extend the project scope of this development before end date is reached.

For project extension the client will provide a request for extension to the contractor.

The contractor shall also take care for bugfixes which exist based on his implementation even after end of project. Further details are defined in the contracts between client and contractor.

2.4.2 Agile Development Setup

The contractor shall structure the agile development according to the WoW, with a camera domain specific addition, related to to the deployment to Gen20x.i4 platform.

The contractor shall establish one team dedicated to vertical SW deployment into Gen20x.i4 platform.

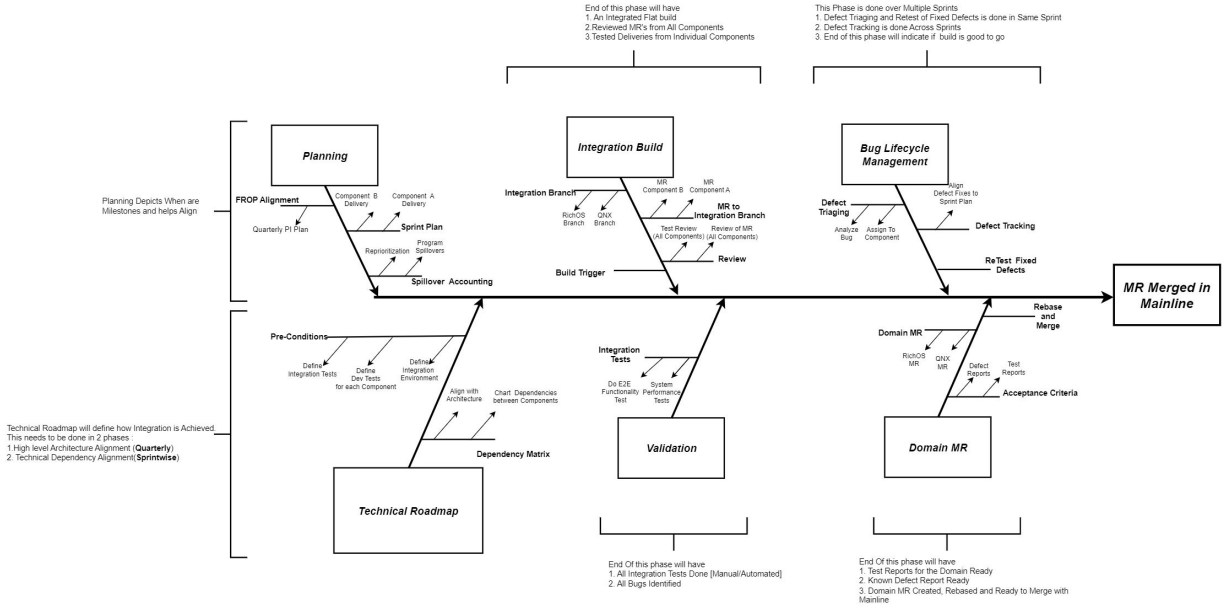
This SW deployment team should be the main point of contact between the contractor internal SW development/testing teams and all other teams involved with i4 SW development. This team has the mission of ensuring E2E availability and functionality of the cameras and their streams into the i4 platform to Camera applications.

This team should have experience with driver integration in QNX, usage of SoC HW specific accelerated resources, integration of services in QNX, debugging and performance profiling. This team should be capable of validating the deployed functionality in the i4 SIL and HIL environments.

This team should create, automate and run SW integration tests, also identify, triage and

analyze bugs related to SW integration in i4 platform and coordinate the resolution with other teams as necessary.

The following diagram 1778685: Integration_flow.JPG describes the agile development and SW integration flow for the camera domain to be followed by the contractor. Further revisions to this flow may apply during the development phase if needed.



The recommended size of the deployment team working on SW integration is 2-3 FTE, with a minimum of 1 FTE.

2.4.3 Scope of function

PLEASE DESCRIBE HERE THE APPLICATION OR FUNCTION FOR THIS SWLH.

PLEASE DESCRIBE HERE THE SUBFUNCTIONS OF THIS FUNCTION (e.g. messaging, adressbook for application phone)

PLEASE LIST HERE SPECIFICATION DOCUMENTS YOU WANT TO REFERENCE.

2.4.4 High level Backlog

PLEASE ADD HERE THE HIGH LEVEL BACKLOG FOR YOUR APPLICATION OR FUNCTION. IN THE FOLLOWING YOU FIND ALREADY PROPOSALS FOR BACKLOG ITEMS REQUIRED BY GEN20X PROJECT.

The contractor shall adapt the function to MBiENT by considering specification XY.

OR The contractor shall develop a new function XY by considering specification XY.

The contractor shall redesign the function to a SW module which has clear interfaces as defined by MBiENT.

The contractor shall refactor existing code based on MBiENT Architecture Principles.

The contractor shall implement innovations as definec now or later in the Backlog.

The contractor shall adapt existing code to upcoming derivative of MBiENT.

The contractor shall take care that his function supports all needed MBiENT functions as there are e.g. Diagnosis, Logging, SW-Update, Coding, Audiohandling, Containerization, Performance Measuring, KPI, Personalisation, Stability, Persistence, ... (further details see in SW system architecture).

2.4.5 SoC support

IVI SW must support multiple SoCs and all SoC platforms.

Note: At the current point in time, SoC supplier is not determined yet. Until awarding no detailed information about the SoC platform can be given.

The contractor shall take care that the provided function or application supports all HW supported by MBiENT.

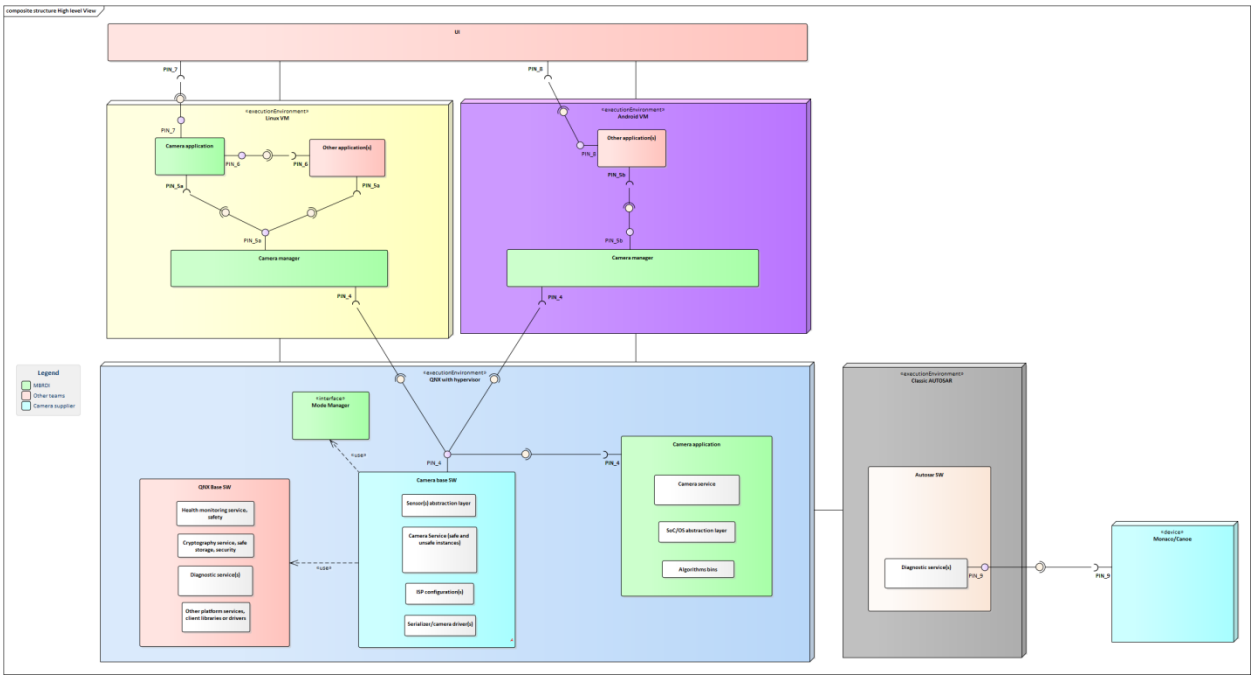
2.5 Electromagnetic Compatibility

2.6 Software

2.6.1 Camera Architecture

2.6.1.1 High level and interfaces

The following overview 1705956: High level View.bmp explains the overall high level view of the ISS SW and its execution environments and the teams responsible for each component. It also introduces so called “Pins” which are required key interfaces of the system.



The contractor of the Camera base SW is responsible of providing and testing the output of PIN_4 interface.
This interface includes both the data/image and control interface and is the implementation of the interface specified by the sensor abstraction layer specification.

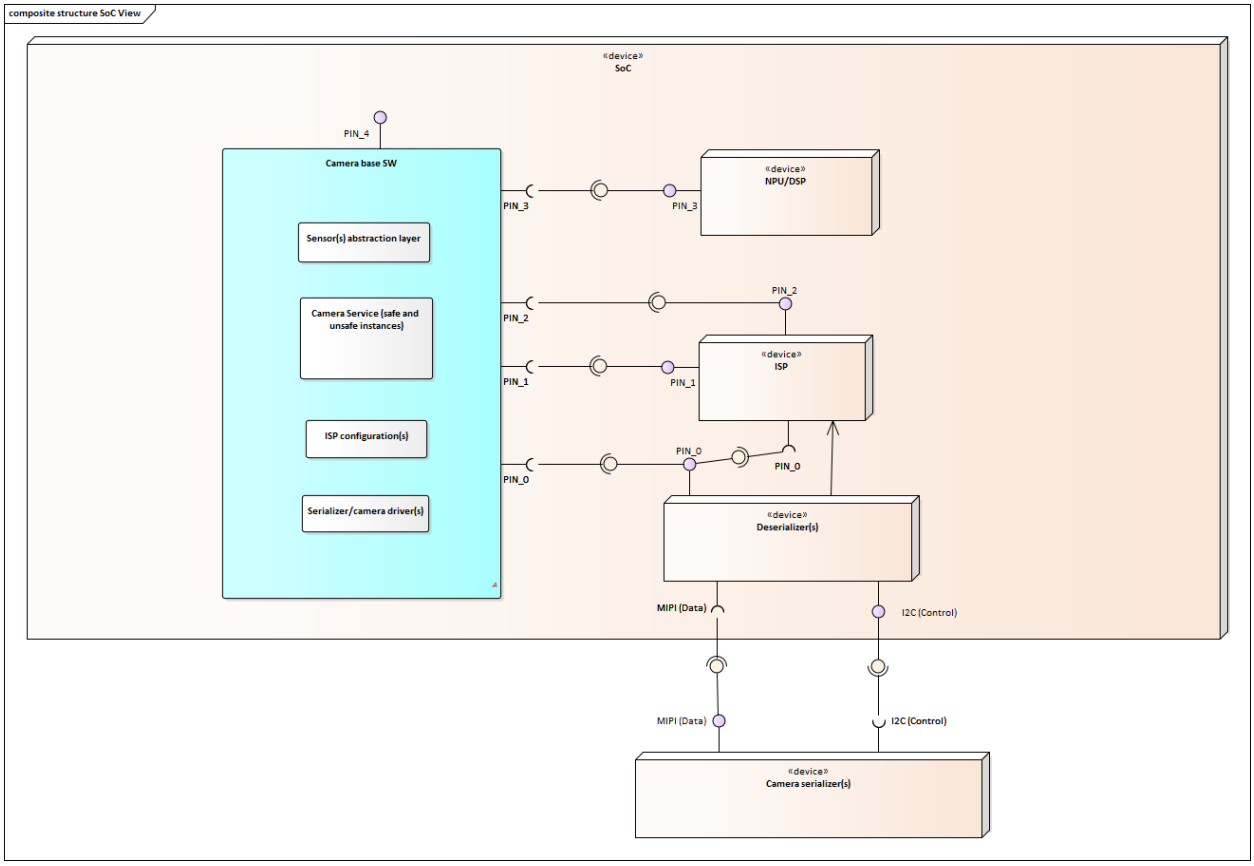
Adaptation to PIN_4 interface specification shall be jointly specified and agreed based on the expected E2E functions between the contractor and other relevant teams.

The contractor of the camera base SW is responsible of testing PIN_9 interfaces.

This is the diagnostic interface exposed from the car computer to the Telematic network and the contractor has the responsibility of verifying all its specified diagnostic functionality also trough this interface.

PIN_9 can be tested during development with Monaco or Canoe tools, however the final test result must be verified using Monaco.

The following overview 1705968: SoC View.bmp illustrates the expected interaction between the camera base SW and the HW components of the camera and i4 platform.



The contractor of the Camera base SW is responsible of jointly defining with relevant teams the interfaces for PIN_0, PIN_1, PIN_2 and PIN_3. The contractor is also responsible of independently testing PIN_0, PIN_1, PIN_2 and PIN_3 and to run automated integration tests on those PINs.

PIN_0 is the interface with the Deserializer(s), meaning I2C and MIPI communication with the camera are accessed via this PIN.

PIN_0 shall be set up additionally to support video and metadata dump for analysis during the development phase. In production code the video and metadata shall go back to back directly to the ISP without memory or CPU access in between.

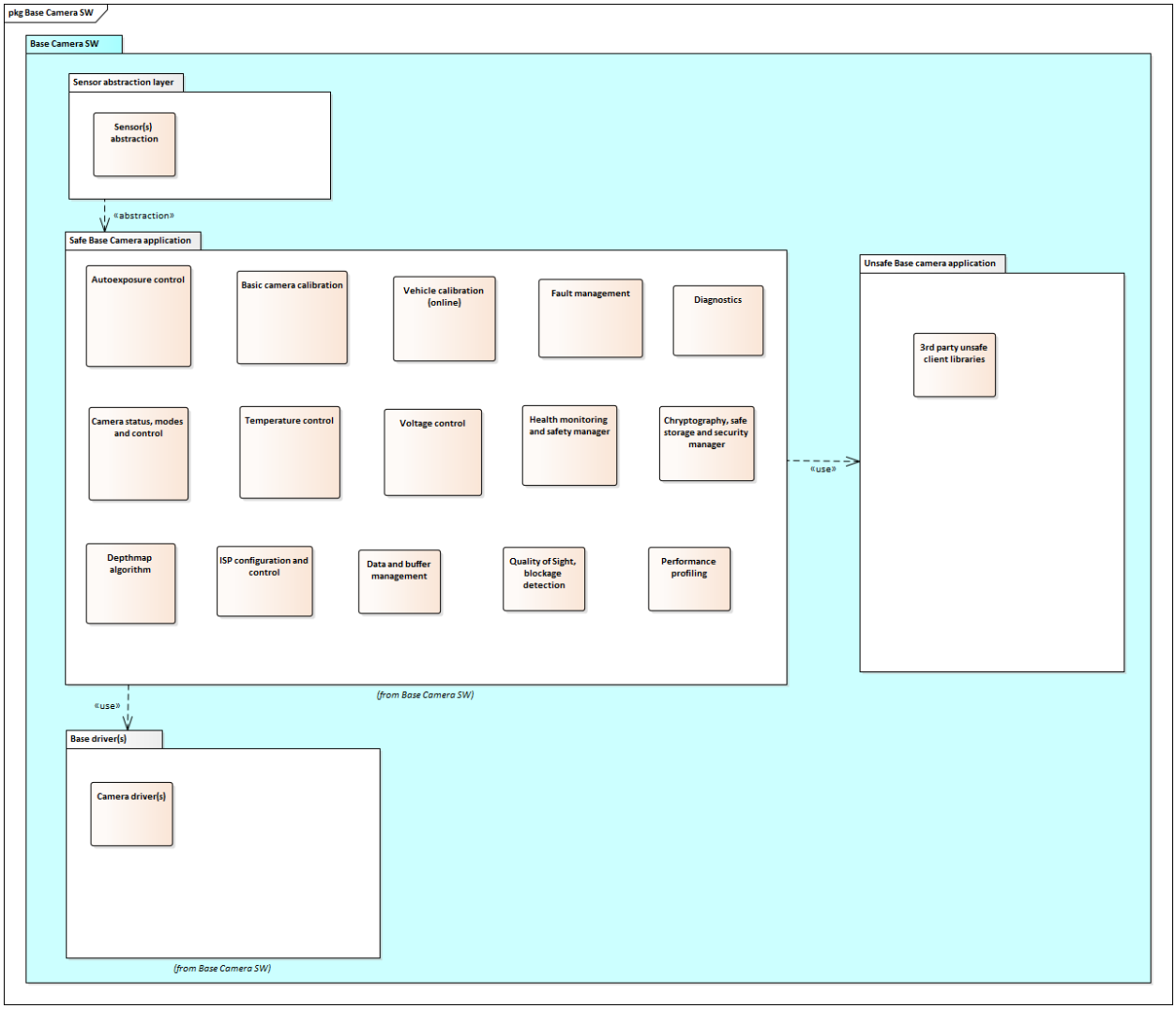
PIN_1 is the interface to configure or reconfigure the ISP functions. This interface is expected to be used during initialization of the camera base SW.

PIN_1 is to be used to define one or more individual configurations for each virtual camera. This means that a single input virtual camera can result in multiple output virtual cameras if required by the client use cases.

PIN_2 is the interface to access the data output of the ISP. PIN_2 shall also be used to re-inject data to ISP in case multiple passes trough the ISP are required for any given virtual camera.

PIN_3 is the interface to be used in case of image or data post-processing operations which have to be accelerated, in case they are not CPU friendly or the CPU budget is exceeded.

The following overview [1731349: Base Camera SW.bmp] represents the breakdown of the base camera SW in terms of SW components and macro features each component must provide.



The Base Camera SW component consists of four sub-components (which again may consist of several parts):

- Sensor abstraction layer

- Safe Base camera application
- Unsafe Base camera application
- Base drivers

The Base Camera SW must be released as a binary runnable on both i4 platform, but also on x86 (PC version).

The x86 binary version shall be bit accurate, including ISP processing and any contractor algorithms. Latency shall be similar at full frame rate for all cameras between x86 version and the embedded version running on the i4 platform.

The x86 version may be released as a docker container, the exact type of virtual container or delivery practice shall be discussed between MB and the contractor until B sample production.

The Sensor abstraction layer is the interface exposing video/data access and control APIs to client applications.

The Safe Base Camera application software contains all core functionalities and services and shall not include 3rd party libraries or code not safe according to ISO26262 or the safety specification.

The Unsafe Base camera application software contains all 3rd party libraries or code which could not be made safe according to ISO 26262, but is required to function as interface within the i4 platform. This shall run in a different process spaces from the safe version.

The Base drivers block includes all drivers which are required to operate the HW provided by the contractor (eg: cameras, sensors, illumination, etc...).

The source code of the contractor software can be in MISRA C:2012 with 2020 compliance and/or C++20 following the MISRA C++:2020. The versions may be updated during the development phase.
Any specific hardware accelerated implementation needs to be agreed upon in writing with the client during the quarterly architecture alignments.

The contractor shall propose a software architecture to the client shortly after the awarding of the component including a mapping of software parts to the available hardware components. At the client's request, the contractor shall organize, conduct and support joint meetings with the client to present and discuss the software architecture until a common agreement on the software architecture has been reached.
This agreement shall be reached before the first hardware or software release after the awarding.

Software updates include, but are not limited to: Integration of new client software, including the change of the softwares interfaces and integration of new communication matrices.

All configuration data that is used to parametrize the SW, HW blocks (e.g. ISP, illumination control) is part of the SW.

The contractor must provide all software, hardware and documentation to the client, that are needed for the integration of client software incl. changed interfaces. The contractor must enable the client to perform a complete software build to create new software flash files on his own without the contractor involved.

The client will share exact project setup, project partners and all relevant stakeholders to the contractor at project kickoff after project award.

The contractor needs to share a preliminary overview of used resources (at least computational resources, memory resources and bandwidth requirements) during the RFQ. Any special resource demands by the contractor (e.g. from special accelerator hardware, ISP, ...) needs to be included by the contractor and agreed by client.

The contractor needs to provide computational resource information for every release to the client.

During recording or replay of video streams for measurement/testing or data collection, the Camera Base SW shall operate as normal, meaning the measurement system shall be transparent to the Camera base SW and this shall be able to handle this scenario.

2.6.1.2 Base drivers

The base driver shall provide the low level communication between the cameras, sensors and any other required HW component provided by the contractor to the Safe base camera application software in the i4 platform

The base drivers shall provide at least the following functions:

- Read out of all the raw 2D and 3D images (RGB and IR depending on the imager) based on the timing diagram provided to the contractor
- Read out of all relevant temperatures from the sensors
- Read out of all relevant voltages
- Read out all available calibration data (intrinsic and/or extrinsics if applicable)
- Read out all relevant configuration data, status and error information
- Read out all relevant HW information like partnumbers, serial numbers and patchlevels
- Write configuration data to the HW registers and/or memory
- Set camera modes according to mode state machine provided to the contractor
- Apply all relevant safety and security settings and act as feature enabler
- Check all relevant parameters to fullfill eye safety requirements and disable the camera if eye safety is not fullfilled
- Fulfill all diagnostic requirements

2.6.1.3 Safe base camera SW

The safe base camera application provides all core SW logic and functionalities required from the contractor, it runs as a process in the QNX environment of the i4 platform.

The Camera Application Software shall provide at least the following functions:

- Autoexposure control (individual for each virtual camera)
- Frame configuration control (eg: starting line for the crop frame readouts)
- Basic camera calibration (geometrical based on CAD data for each vehicle variant and relevant style)
- Vehicle Calibration (inside the vehicle during vehicle production and afterwards during operations)

- Fault Management
- Diagnostic functions and interface
- Camera status mode and control
- Temperature control and over-temperature protection
- Voltage control with under-over voltage protection
- Health monitoring and safety features according to MB safety architecture and SW specification
- Cryptography, safe storage and security features according to MB security architecture and SW specification
- Depthmap algorithm to extrapolate car coordinates 3D data
- ISP configuration and runtime control
- Quality of sight with blockage detection and IQ requirement fulfillment
- Performance profiling

2.6.1.4 Unsafe base camera SW

The unsafe base camera application shall be used, in order to fulfill the ISO26262 requirements, whenever a client library is required to implement a functionality expected out of the base camera SW, which is not and cannot be made safe.

The Unsafe base camera application, shall be avoided at all whenever possible, but if not it should run in its own process space.

2.6.1.5 Sensor abstraction layer

The sensor abstraction layer is the expression of PIN_4 and it shall abstract all drivers, virtual cameras and core functionalities of the Base camera SW.

It also represents the interface between camera Application, Camera manager and Mode manager to the Base Camera SW.

2.6.2 Component Functions

2.6.2.1 Core functions

The following requirements and information details the expected functionalities to be provided by the contractor as part of the Camera base SW running on the i4 platform.

2.6.2.1.1 Camera status, modes and control

The contractor shall implement the concept of virtual camera defined as any frame readout from a physical camera with its own individual configuration or settings. Any physical camera may have multiple virtual cameras, the amount and configuration is defined by the timing diagram provided in the HW KLH: FI: 1490131

A virtual camera is expected to be represented as such also at all interface levels, from SerDes to ISP core components, but also as system/user devices to be finally exposed to other camera applications running on the i4 platform.

The contractor shall implement the concept of camera status as a state machine. This state machine is used to understand in which operating state the camera is (eg: idle, initializing, ready, streaming, etc...) and to change or control its status based on the appropriate conditions. Details in FI: 1622853

Client application shall be able to change the camera status, for example by starting/stopping camera streams or turn specific active illumination on/off.

The contractor shall be able to set the camera into different modes, this is a different concept to the camera status.
While the camera status reflects the pure state of the camera, the camera modes describes the operating mode of the Camera Base SW, including which virtual cameras are available and/or streaming.

Changing modes may also require reconfiguration of the ISP, by requesting to add/remove/reconfigure virtual camera outputs.

Camera mode change request or any client application request affecting the virtual cameras and their configuration has to be always routed trough the meta-application mode manager which includes policing/authentication features and may approve or deny the request for mode changes.

The camera modes shall also be used to optimize the resource consumption by selectively activate/deactivate/reconfigure individual virtual cameras when requested by the mode manager meta-application. This means, but not only, that a frame readout may not need to be processed in case there is no active client application reading it.

The camera status can impact the camera modes, for example if the camera streaming is OFF, this should be reflected in the camera modes and the mode manager shall be informed.

The contractor shall support at least the following modes of operation:

- self-test mode
- measurement/recording mode
- replay mode
- calibration mode
- pairing mode
- diagnostic mode

Eventual adjustments to this list shall be discussed and agreed with MB during the development phase until B sample production.

2.6.2.1.2 ISP configuration and control

The contractor shall work together with the SoC supplier to configure the ISP such that all required virtual cameras can be processed in parallel and all IQ requirements for image processing are fulfilled.

The contractor shall configure the ISP during the i4 platform initialization and design it such that the initialization of the Base Camera SW is indipendent from the initialization of the ISP, which shall be faster.

In case a single virtual camera stream requires to be processed in parallel in different way due to client application requirements, the ISP shall be configured such that for a single input multiple N appropriate outputs are generated in parallel.

The ISP processing shall never exceed the latency of 15ms for any frame of any virtual camera. Ideally this latency should be less than 10ms.

The contractor is responsbible of setting the right configuration for the ISP and getting correctly processed images and finally fulfilling the IQ requirements.

The contractor shall reconfigure the ISP at runtime, for all (IQ or not) relevant runtime parameters. It must also be possible to add/remove virtual cameras and their ISP configurations at runtime, without the need to re-initialize the ISP pipeline.

Changing the parameter values shall happen at runtime on a frame by frame basis on the next frame. This includes reconfiguration or re-initialization of the ISP pipeline for any virtual camera.

The contractor shall provide all relevant configuration data in case of the ISP shall be used. This shall be part of the release mechanism.

The contractor shall provide a SW component to perform image color transformation from sensor domain into different color spaces. The exact video streams shall be defined jointly with the client. It shall include as a minimum:

* a YUV or RGB stream (colored image)
* a IR image

The client software must have access to all relevant parameters. The contractor has to document the parameters and to include them in the regular release documentation.

The contractor must implement all relevant preprocessing functions (filters) to meet the required image quality performance.

The contractor shall provide all necessary configurations for the ISP which shall be integrated in the file system of the CIVIC. This shall happen for every release.

The relevant parameters must be discussed and agreed with the client.

2.6.2.1.3 Data and buffer management

The contractor shall implement highly optimize data and buffer management for all virtual cameras and both video and data processing.

There shall be no read/write of frames between Deserializer and ISP in production code. Only after ISP completes its processing shall the data be read from memory.

Memory has to be allocated at compile time, no dynamic memory allocation shall happen at runtime.

Buffers may only be shared trough pointers or memory address, and the contractor must fulfill a 0-copy policy for all buffers, be them video data or metadata.

Access to video data and metadata to other application also has to be done via sharing pointers and/or memory addresses.

The contractor may implement cyclical buffers or queues to ensure no frame drops happens and to give enough time to let frames pass trough the video processing pipeline and be consumed by the client applications. Proper mechanisms shall be put in place to prevent reading corrupted memory or writing memory being read.

the sizing of buffer queues for each virtual camera, shall be done based on the expected latency of the whole Camera base SW. This is detailed in the chapter dedicated to performance and resources.

2.6.2.1.4 Fault management

The Base Camera SW shall read, store and/or report any abnormal/fault state of the camera and detect abnormalities in its Base Camera SW execution including but not only, error returned when executing a 3rd party function or excessive latency when running a function.

The errors shall be detailed and categorized in:

- HW non-recoverable errors
- HW recoverable state (eg: over temperature, over voltage)
- SW non-recoverable errors
- SW recoverable errors (eg: by restart or re-initialize)
- SW temporary error (eg: excessive latency due to system load)
- Frame loss and video errors
- Performance errors
- Security errors
- Safety errors

  The contractor shall discuss and agree with MB during the RFQ phase on a degradation matrix.

All faults shall be reported via diagnostics, details in the Diagnostic chapter.

At least the error category shall be reported to the client applications on the i4 platform and additionally this may be applicable to some specific errors to be discussed and agreed during the development phase with relevant i4 platform teams.

2.6.2.1.5 Diagnostics

The Camera base SW shall interact with i4 platform diagnostic services and use them to provide information about the Camera HW and the camera Base SW including its status, data, faults, etc...

The contractor shall fulfill the Diagnostic specification chapter in terms of DID, RID and DTC functions to be provided via the i4 platform diagnostic services.

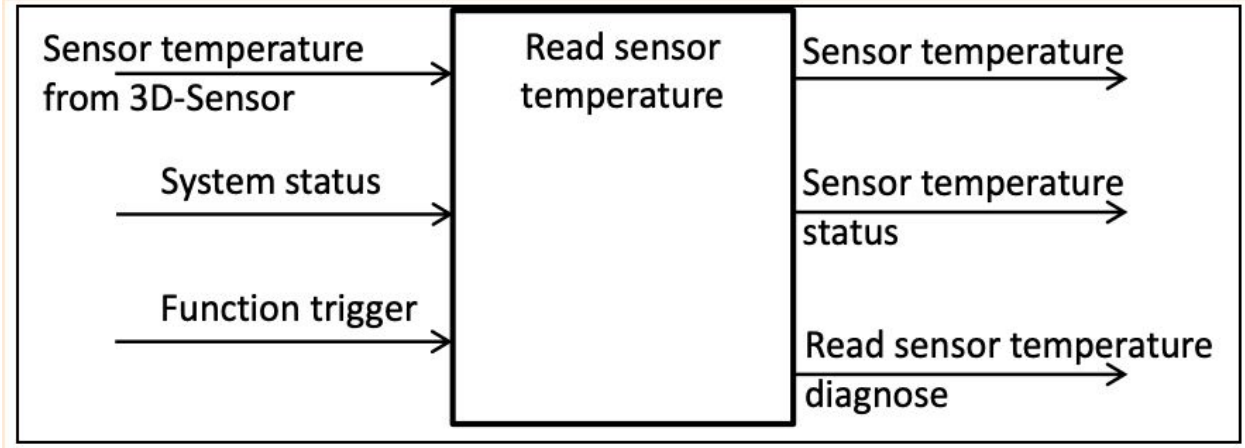
It is the contractor responsibility to ensure that the diagnostic functions are working as specified. The contractor must finally test this also using both Monaco and ET Framework Tools. In case of SW integration issues, it is the contractor responsibility to provide proof via SW component test cases that their diagnostic code works correctly.

If the diagnostic services of the i4 platform are not implemented according to ISO26262 standard, then the interaction shall happen trough the unsafe camera base application first.

2.6.2.1.6 Temperature control

This function reads the sensor temperature from the camera head and disable the camera if the temperature is critical. This function provides the temperature und the status of the camera to all other applications.

The following figure shall explain interaction with the temperature sensor.



The function must read the sensor temperature from the camera.

The temperature value must be linearized

The linearized temperature value of all temperature sensors must be provided to all other functions

The function must check the feasibility of the temperature values

If the temperature value is not feasible an error flag must be set

Exact error flags will be defined during development phase.

Camera enable and disable conditions for each camera:
Disable camera: Camera temp >= Tmax_Disable
Enable camera: Camera temp <= Tmin_Enable

The values for "Tmax_Disable" and "Tmin_Enable" shall be discussed and agreed with the client.

The alignment regarding the TMax_Disable and Tmin_Enable shall happen before B-sample.

If the temperature has an impact on the IQ requirement, the temperature values shall be used by the ISP control function to tune the IQ parameters to achieve the best possible quality.

2.6.2.1.7 Voltage control

The contractor shall measure all relevant internal voltage levels of the camera to ensure its normal running operation and that no damage is caused to it or by the camera itself.

In case the voltage is out of the specification for the camera head HW components, additionally to any HW requirement, also the Camera base SW shall be informed about the voltage levels and change the camera state in order to safeguard the HW component. If the voltage levels are again back within the normal range then operations shall be reused and the camera shall be reinitialized accordingly.

The voltage values must be linearized and provided to all other functions.

The function must check the feasibility of the voltage values and in case those era not feasible an error flag must be set. Exact error flags will be defined during the development phase.

The alignment regarding Vmax, Vmin, and the hysteresis parameters shall be discussed and agreed with the client before B-sample.

If the voltage has an impact on the IQ requirement, the voltage values shall be used by the ISP control function to tune the IQ parameters to achieve the best possible quality.

2.6.2.1.8 Basic camera calibration

The camera optics are expected to be calibrated at the contractor EOL facility, generating a set of intrinsic calibration data which have to be stored in the camera EEPROM.

The contractor shall also generate a set of extrinsic calibration data to convert camera coordinate system to car coordinate system. The basic version shall use CAD data provided by MB.

The extrinsic calibration data has to be stored in the i4 platform persistent memory and loaded based on the vehicle and variant information signals available in the i4 platform.

The function and SW design has to be discussed and agreed with MB during the RFQ phase.

2.6.2.1.9 Vehicle calibration

The contractor shall implement a mechanism and/or algorithm to generate a set of extrinsic calibration data without usage of CAD data.
This mechanism could be split into 2 parts:

- EOL vehicle calibration at MB car production via the usage of a diagnostic routine
- Online vehicle re-calibration which is computed at runtime on-the-fly during vehicle operations

The contractor shall propose a way to calibrate cameras, generate and store a set of extrinsic calibration data using computer vision algorithms during the EOL vehicle calibration. The whole operation shall take at most 1000ms.

The contractor shall propose a way to re-calibrate dynamically the cameras, generate and store new extrinsic calibration data using computer vision algorithms during vehicle operations. This operation scope is to compensate for mechanical, temperature and aging adjustments during the lifetime of the vehicle.

The precision compared to ground truth 3d measurements shall be of +-10mm at 120cm distance from the camera mount position.

The algorithms shall work also with moving parts like the seats and different interior variants with different elements positions, colors and trim parts.

The online re-calibration may not exceed the allocated resources given to the Camera base SW, unless a special low-system computational scenario is available where more resources could be temporarily allocated.

The online re-calibration may run with low priority and low resource consumption over long periods of time, for example 1hour or longer, storing intermediate data to safeguard the scenario of i4 platform being turned off due to user activity.

The function and SW design has to be discussed and agreed with MB during the RFQ phase.

2.6.2.1.10 Autoexposure control

The contractor shall implement a mechanism to process the video data and statistics

processed by the ISP in order to continuosly adjust the gain, exposure and other camera/illumination parameters.

The autoexposure control shall be configured and the output applied to every single individual virtual camera.

The autoexposure control has to happen after every frame read-out of any virtual cameras.

The autoexposure control shall be influenced not only by the IQ requirements, but also by client application, by usage of dynamic ROIs concept and the complete architecture shall be jointly discussed and agreed between MB and the contractor during the RFQ phase.

Purpose of dynamic ROIs within AEC is to enhance specific areas of the image, which are most important by the algorithm functions running at application level. This improves the flexibility and overall algo performance.

The autoexposure control shall be able to support N ROIs, of which the piority, origin and size are define at runtime on a frame by frame basis.

These ROIs shall be used by the autoexposure and gain control mechanism of the camera to ensure the best possible image quality within the given ROIs. In case it is not possible to enhance all the ROIs at the same time and at the same quality, or if this may create artifacts or degradations, priority should be followed. Still the whole image shall fulfill the image quality requirements.

Each of these ROIs may have different origin and dimensions (height and width).

Each of these ROIs may have different priority.

In case the priority is FF (255), this means the area should be ignored for the overall autoexposure control and image statistics.

The maximum number of ROIs, defined as N can be up to 32.

When the number of ROIs is 0, then a default AEC configuration and default AEC ROIs should be used.

The default configuration shall be parametrizable in SW or in Variant Coding and depends on the car model and variant and on the camera variant fi applicable.

The number of ROIs, their priority, their origin (top-left corner) and their dimensions (height and width) shall be given from application layer to MPIC camera framework at runtime on a frame by frame basis.

APIs definition shall be agreed between MB and the supplier, before start of implementation.

An adequate hysterisis function (temporal information) shall be implemented to avoid flickering when the ROI changes are significant enough.

This function has to be proven effective based on an image database and/or ground truth provided by MB.

The timing between a new AEC ROI set of parameters and reaction to the camera autoexpsoure is expected within the next available frame.

2.6.2.1.11 Depthmap algorithm

The contractor shall provide an algorithm that is able to generate a 3D depthmap based on the camera active dot illumination.

This function shall expose an asyncronous interface to client applications to provide the

computed depthmap data.

The interface shall allow multiple clients to select:

- quality level (precision)
- ROI crop (origin and dimensions of the area for which 3D coordinates are requested)
- downscaling factor

Whenever requesting access to depthmap data.

The depthmap algorithm shall be HW accelerated in the SoC via either usage of ISP (whenever possible), NPU or DSP.

Depending on the quality level, the contractor may reduce the precision requirements for depthmap computation.
The expectation is that the algorithm shall offer at least 3 levels:

- HIGH: where the IQ requirements are fully met or exceeded
- MEDIUM: where the precision could be reduced by 50%
- LOW: where the precision may be reduced by 200%

The ROI interface for depthmap computation shall accept any size ranging between the full image resolution and a single pixel.

The algorithm shall accept also a direct request to downscale first the image by a downscaling factor, thus reducing the overall amount of pixels to be computed. The factor may go from 1x (no downscaling), to 10x (scaled down 10 times).

The depthmap algorithm is required to run at the same fps rate of the input image provided by the imager for the full image resolution at HIGH quality.

The depthmap algorithm execution time shall not exceed 15ms on the i4 platform.

2.6.2.1.12 Quality of Sight

The contractor shall develop a blockage detection for the camera head to guarantee the quality of sight.
The fps rate of this feature shall be defined jointly between MB and the contractor.

This algorithm shall be able to distinguish between temporary blockage (eg: user blocking the camera fov while typing on the display) and a permanent blockage (a sticker is put on the camera).

This algorithm shall be able to provide individual blockage detection information for every camera head and whenever applicable to all visible car seats individually. This means that in case a camera FOV can see 2 seats, then it should report blockage detection for 2 individual areas.

The contractor shall implement the blockage detection before B-sample.

The contractor shall implement a supervision software to monitor that the diffuser of the active IR illumination is still attached and not defective. This shall be implemented before B-sample.
The fps rate of this feature shall be defined jointly with the client before B-sample.

2.6.2.1.13 Health monitoring and safety manager

The contractor shall implement all relevant safety measures described in the safety SW requirement specification. In case additional measures or adaptation to the safety specification would be required during the development phase, those shall be done at no additional cost until C sample production.

The contractor shall at least implement an heartbeat and provide health status and safety status data to safety monitoring applications as per the safety SW requirement specification.

The contractor has to collaborate and contribute to the specification of the safety measures, whenever the contribution is requested by MB safety architects.

The contractor shall provide a detailed SW design fulfilling the SW safety specification and submit this to MB for review and approval. This shall be done no later than B sample production.

2.6.2.1.14 Cryptography, safe storage and security manager

The contractor shall implement all security measures described in the MB cybersecurity specification.

Additionally the contractor has to fulfill all security measures described in this document under the security chapter. In case additional measures or adaptation would be required during the development phase, those shall be done at no additional cost until C sample production.

The contractor has to collaborate and contribute to the specification of the security measures, whenever the contribution is requested by MB security architects.

The contractor shall provide a detailed SW design fulfilling the security specification and submit this to MB for review and approval. This shall be done no later than B sample production.

2.6.2.1.15 Performance profiling

The contractor shall develop detailed performance profiling mechanisms, which can be enabled or disabled at runtime with minimal or no performance impact.

The contractor shall at least provide runtime measurements for the following elements:

- Latency of each individual core function
- Latency of frame processing for each individual virtual camera at all PINs (PIN_0 to PIN_4)
- Latency between function call and response or callbacks from and to 3rd party libraries
- ROM, RAM (stack and heap) usage
- Percentage of CPU core utilization with breakdown by core function
- Latency and percentage of NPU/DSP used (if used)
- Latency of each ISP function and percentage of ISP HW resources used with detailed breakdown
- Amount of context switches
- Initialization latency and CPU load spikes

The contractor shall optimize all the above aspects in order to fulfill the non functional

performance, latency and resource consumption requirement in its dedicated chapter.

The contractor shall work together with MB and other development teams to ensure an optimal SoC and system level configuration for its own processes.

2.6.2.2 Diagnostics

There are different types of functional diagnostic requirements. We differentiate

- DIDs (identifiers for read and write purpose)
- RID (routines identifiers to execute functions)
- DTC (diagnostic trouble code)
- VC (variant coding, which stores configuration data, car variant sensible)

The Camera Base SW is responsible of executing the diagnostic functions based on the requirements below and to expose the results via diagnostic services of the i4 platform.

Security and safety SW requirements are also applicable for diagnostics, some functions may have specific requirements.

All security services shall be protected with security mechanisms. The contractor shall provide this as part of the security concept of the MPIC.

All status information shall be accessible via the link to classical diagnostic interface and also on the PIN_4. Details of which exact information is relevant have to be discussed and agreed between MB and the contractor before B sample production.

Diagnostic functions are applicable to all contracted HW parts (eg: all camera heads, imagers, active illumination, etc..). In case of possible confusions, the diagnostic interface shall be implemented as individual diagnostic interface for each individual camera head or relevant HW part.

All diagnostic implementations shall be integrated according to MGU "DDS - Daimler Diagnostic Specifications" and implemented according to “Diagnosis and Flash Programming” STM-868338

The contractor shall support changes to the diagnostic function list described in this chapter according to changes in concept or software architecture. The final concept shall be agreed and implemented until C sample production.

2.6.2.2.1 Camera Hardware

There shall be a diagnostic service (DID) to read temperature information of the camera Hardware. All available temperature sensors shall be included (at least imager sensors).

There shall be a diagnostic service (DID) to read the MB HW A-part number, Mercedes HW Version (Year/Week/PatchLevel), contractor HW serial numbers and manufacturing data. Information read via Diagnostic shall match eventual physical labels on the camera hardware.

There shall be a diagnostic service (DID) to read SW version from the camera. This shall include the Mercedes Mercedes SW A-part number and Mercedes SW Version (Year/Week/PatchLevel) inf applicable.

There shall be a diagnostic service (DID) to read calibration information for all available calibrations, both intrinsics and extrinsics.
In case of running online calibration, the last 10 extrinsic calibration matrix and parameters

shall be provided too.

There shall be a diagnostic service (routine) to write intrinsic and extrinsic calibration information into the cameras.
This can be combined with the respective functional routine to perform a camera calibration. The contractor shall include this into the functional concept.

There shall be a diagnostic service (DID) to read the status of the eye safety mechanism.

In case the Camera HW hosts updatable firmware or software, there shall be a diagnostic service (DID) to read the SW and firmware versions.

There shall be a diagnostic service (DID) to read the current state of the active illuminations (eg: activation status, illumination scheme).

There shall be a diagnostic service (DID) to read the current illumination intensity of the illumination. The scale shall be defined during development until B sample production.

There shall be a diagnostic service (DTC) to set a fault in case the illumination fails. If the active illumination was turned off via diagnostics, the DTC shall set an event instead of a fault.

There shall be a diagnostic service (DID) to set values for the active illumination and to activate/deactivate the active illumination.

There shall be a diagnostic service (DTC) for over temperature of the camera head.

There shall be a diagnostic service (DID) to read out a temperature histogram of the camera head.
The entries per histogram bin shall be noted in hours. The temperature histogram shall stay persistent within the camera head.
At least 10 bins shall be used whereas the bins shall be adapted according to the relevant temperature areas.
Details shall be presented to the client for final agreement before C sample production.

There shall be a diagnostic service (DTC) for under and for over voltage for each individual camera head or separate active illumination parts.

There shall be a single diagnostic service (DTC) for each camera that summarizes all HW-defects of the camera head to decide if the camera needs to be replaced.
The reason shall be part of the DTC possible enum values.

2.6.2.2.2 Camera Interfaces

There shall be a diagnostic service to set a DTC in case of line faults, this shall include at least:

* short to bat
* short to ground
* open
* Input Image not correct or missing
* bad link quality
* PRBS (pseudo random bit stream) fail

SW design and interface has to be agreed together with relevant parties of the i4 platform to ensure the data is available to all.

There shall be a diagnostic service to set a DTC in case power supply is missing or power

good signal is not available.

There shall be a diagnostic service (routine) to start/perform a pairing between camera head and CIVIC. The scope and functional requirements are defined in the pairing section of the security concept.

There shall be a diagnostic service (routine) to undo the pairing and remove stored keys or relevant information for pairing.

There shall be a diagnostic service (DTC) active if the pairing was not processed successfully (only if the corresponding camera head is connected)

There shall be a diagnostic service (DTC) to set a fault state in case the authorization process/pairing between camera head and CIVIC fails.
If this DTC is active, the specific camera video streams shall be disabled.

There shall be a diagnostic service (DTC) to set a fault state in case of an unauthorized attack of the video link or frames being injected between camera HW and the i4 platform (eg: signal calculation failure).
If this DTC is active, the specific camera video streams shall be disabled.

2.6.2.2.3 Self tests routines

There shall be a routine to perform a PRBS test. This is to test the interface between Camera Hardware and Camera base SW
In case of failure a "PRBS fail" DTC shall be set.

There shall be a diagnostic service to perform a SERDES self test (routine).
In case of failure a "SERDES self test fail" DTC shall be set.

There shall be a diagnostic service (RID) to perform a Camera head self test (routine). In case of failure, a DTC shall be set.

There shall be a diagnostic service (RID) to start/perform an image check and detect if the camera's FOV or active illuminations are fully or partially blocked.

There shall be a diagnostic service (Routine) to start/perform a security test, which shall ensure that security requirements of all camera streams and controls are properly implemented (eg: HMAC, certificates exchange, watermarking, encryption of frames, etc..) . To this end, the CIVIC security mechanisms shall also be utilized.

There shall be a diagnostic service to perform a Built-in Image Quality test (routine) and provide the results. In case of failure, a DTC shall be set.
This requirement shall ensure its functionality for all camera head, design cover and mounting position variants.

Info: The Built-in Image Quality test is specified in Chapter Other Functions

There shall be a diagnostic service to start/perform a Field Image Quality test (routine). In case of failure, a DTC shall be set.
This requirement shall ensure its functionality for all camera head, design cover and mounting position variants.

Info: The Field Image Quality test is specified in Chapter Other Functions.This diagnostic service is intended for client and contractor development activities.

There shall be a diagnostic service (routine) to perform a self test of the active illumination. The contractor shall present the implementation concept of this self test before B-sample production.

There shall be a diagnostic service to perform a Camera Base SW self test (routine). This test shall prove that the driver and applications are running properly and all required video streams are received and sent out to 3rd party applications correctly. In case of failure, a DTC shall be set.

There shall be implemented diagnostic services (RID), which will be used to start/perform and to stop "Test Pattern Mode" of the camera hardware.
The "TestPattern Mode" shall tell the targeted camera head to generate specific test patterns and send them to Camera Base SW.

It shall be possible to activate the "Test Pattern Mode" with three different pattern (three activation commands, one deactivation command) when applicable:

- moving/rolling
- IR
- RGB

The final concept for test patterns shall be discussed and agreed with MB before C sample production.

2.6.2.2.4 Camera Base SW

There shall be a diagnostic service (DID) to read the status of the cameras and the current mode, incl streaming status and format information.

There shall be a diagnostic service (routine) to store a frame from the camera. This shall include a raw image (before pre-processing or ISP) and post-ISP. This shall be stored in a non-volatile memory of the CIVIC.
This function shall be security and access protected.
The exact location of the memory shall be defined during development.

2.6.2.2.5 Variant coding

The contractor shall implement as variant coding all relevant parameters. The complete set of parameters shall be discussed and agreed until C sample production and shall at least include all the data of this chapter.

There shall be a variant coding service read/write for distortion correction, crop and upscaling of frames for each virtual camera.

There shall be a variant coding service read/write for the cameras intrinsic calibration data.

There shall be a variant coding service read/write to set the authentication timeout.

2.6.2.2.6 Others or generic

There shall be a diagnostic service (DID) to read the currently used configuration.

There shall be a diagnostic service (DID) to read generic device properties. The exact list of properties shall be defined during development until C sample production.

There shall be a diagnostic service (DID) to read the available adjustment functions for the camera. Exact services shall be defined during development until C sample production.

There shall be a diagnostic service (DID) to read the information from manufacturing. The scope and values shall be defined during development.

If the customer switches off the cameras, all controls, read-out services and diagnostic service (DTC) of the camera head shall stay active and operable.

The DTCs shall be raised based on a priority tree and whenever technically possible, only the father of all following tree branches shall be raised.

All controls and DTC-settings shall be active according to required startup time after activation of the camera head. This shall ensure that diagnosis is available from the beginning when the camera head is operational.

All relevant variant parameters shall be part of each release according to the Mercedes-Benz diagnostics requirements.

All possible combinations of variant coding parameters shall be protected to ensure that only tested combinations are accepted to the camera system (e.g. with check sums).

2.6.2.3 Security

The contractor shall analyze and support a security solution which addresses all applicable attack surfaces.

The contractor shall follow the Need to follow Telematics IT Security system and process specifications: "SYS_CIVIC_MMA_IT_Security_v1.0.pdf" and "SYS_CIVIC_MMA_IT_Security_Process_v1.0.pdf"

The contractor shall run a joint TARA analysis with MB security architects and include any additional required countermeasures not listed below as part of this contract.

The Security Goals are to:

- Ensure that the system does not cause a safety hazard even if under attack.
- Protect the functions of the ECU against unauthorized modifications
- Protect sensitive data that will be stored in or processed by the ECU.
- Sensitive data are defined as private personal data (e.g.images of persons), OEM secret data (e.g.keys) andintellectual property (e.g. implementations of valuable algorithms).
- For the contractor Software components Standard secure coding guidelines and secure software development lifecycle rules to be followed. Additional guidelines captured in external interfaces page based on recent inputs from MB Security team.

The following attack surfaces are considered.

AS.1: Android applications inside Android VM
AS.2: Linux applications inside Linux VM
AS.3: external communication interface to the i4 platform (e.g. network interface, OBDII interface)
AS.4: Video input from camera heads to i4 platform
AS.5: input into the camera heads.

Security critical data shall be identified, listed and discussed with MB until C sample production.

The contractor shall include especially AS.4 and AS.5 in the security concept (responsibility). The other attack surfaces (AS.1-3) shall be analyzed, too, however here the contractor shall support the relevant stakeholders responsible for the i4 platform.

The contractor shall include possible man in the middle attacks into the security concept and prevent this attack surface from happening.

The contractor shall include latest cyber security, encryption and authentication technology. The proof shall be part of the security concept and process.

The camera shall support a protected mode which shall restrict access to the video stream to previously authenticated (certified) applications only. The exact exchange of keys and security mechanisms shall be defined jointly with the client in the context of the available & supported security mechanisms of the i4 platform.
By default, this mode shall always be active and only via additional authentication (e.g. for R&D) it shall be possible to deactivate this mode temporarly.

The contractor shall support mechanisms which prevent not authenticated storage of image & video data. Here supported mechanisms of the i4 platform platform shall be used.

The access for the Camera base SW shall be protected via an authentication mechanism. This shall enable a secure “beachhead” inside the i4 platform.
The contractor shall propose an implementation concept based on the underlying mechanisms of the i4 platformplatform and implement in combination with the i4 platform development partners.

It shall be ensured that all privacy relevant data cannot be stored by any application without proper authentication to the "beachhead". This shall include also further configuration and vehicle information data.

Any persistent storage of information must be authenticated and encrypted. Here the available and supported mechanisms of the i4 platform shall be used.

The contractor shall support a concept of certified applications if requested by the client. Certified applications shall include an auditing process organized by the client.

During the diagnostics routine the Camera Base SW shall store the sensor proprietary certificate (public key) in a secure location of the i4 platform.
The exact location shall be defined jointly with the Mercedes-Benz team during development.

During device activation after reset or reboot or power cycle the Camera base SW shall compare the results with the stored certificate from pairing mode to confirm the device is the paired device.
Here the calculation of the HMAC based on the retrieved sensor public key shall be compared with the stored (paired) public key.

All applications access the control interface of the Camera base SW shall be authenticated by a service of the i4 platform.
The authentication concept shall be defined between the contractor, MB and any other relevant teams during development based on available service of the i4 platform.

The SW interface to the host command interface via the SERDES shall be part of the security concept and inside the beachhead.

The Camera base SW shall be able to retrieve a secret session key and NONCE from the i4 platform to enable authentication mechanism with the camera head (and imager). This shall be part of the security concept.

The secret session key shall have at least 256-bit.

During every power cycle the Camera base SW shall read the sensor public key to generate

the SSK. This shall support RSA-2048 encryption.

The Camera base SW shall only enable streaming interface once full authentication mechanism incl. comparison of stored public key information is completed.

It shall be possible to update the SSK during streaming. This shall be possible on a frame by frame basis depending on the security concept.

During the authentication the Camera heads shall only send a sparse image information (e.g. selected rows only) which prevents authentication of private information from persons in front of the camera (privacy protection).

The Camera base SW shall support HMAC generation based on received (sparse) video data to authenticate the camera head based on exchanged SSK and NONCE.

The contractor shall develop a security concept including all relevant security threats. This shall be delivered including respective updates at each release to the client.

The Camera base SW shall generate a NONCE that shall be used compared with a SSK to enable device authentication.

The contractor shall include all components of the Camera system (camera head and MPIC support SW package) in their organizational security process to track potentially known security breaches throughout the lifetime of the vehicle.

It shall not be possible to compromise Image Quality (IQ) via cyber security attacks. The contractor shall discuss and agree on a concept with MB before B sample production.

2.6.2.3.1 Camera authentication and application

The camera sensors shall support mutual authentication between camera heads and i4 platform.

The i4 platform shall provide tamper resistance checks from the Security Module to the Camera base SW. The Modules will be part of package prepared for i4 platform which will be signed by Mercedes.

The Diagnostic services (services listed at a later side) are protected by the i4 platform Security unlock to allow these critical services only to authorized entities.

2.6.2.3.2 Video stream authentication

The image sensors captures image frames, then shall calculate HMAC with the HMAC generator using SSK(Secret Session Key) and NONCE(Seed) from i4 platform and appends the same as part of meta-info with each frame.

The Image sensors shall have a security IP within the same, which has the dedicated cryptomemory and RAM.

The image sensors shall support Encrypted key exchange of the SSK(Secret Session Key) and NONCE(Seed) from i4 platform. The encrypted session key from i4 platform is decrypted and stored within the crypto RAM of security IP.

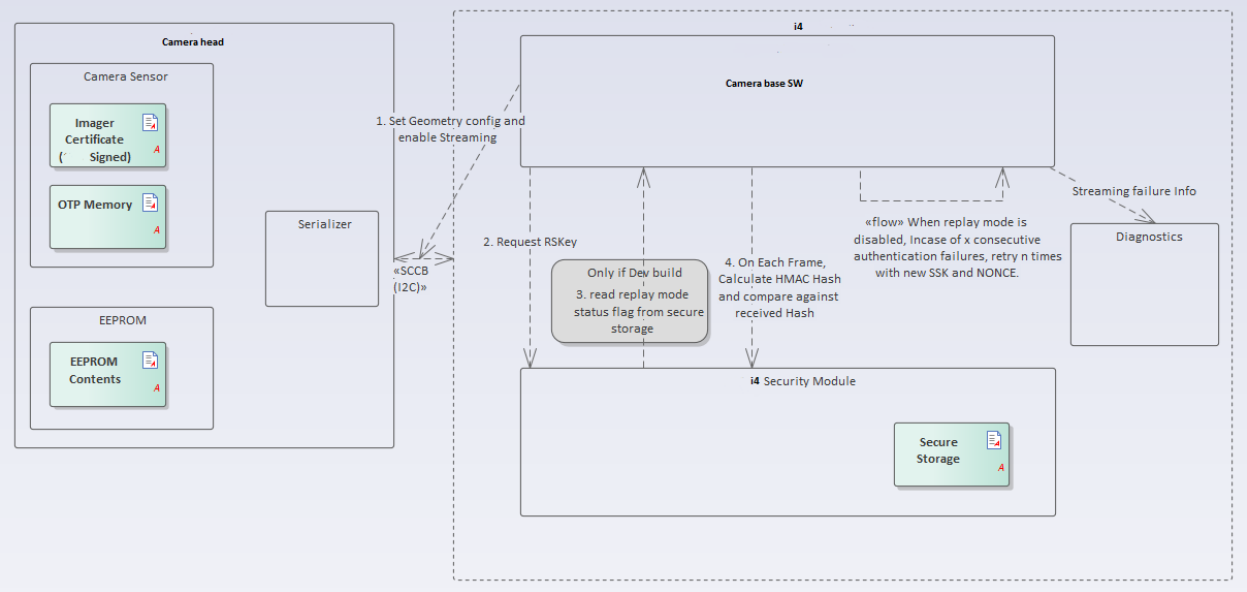
The Camera Base SW shall receive the HMAC, re-calculate it and compare it against the HMAC appended in meta-info to validate the authenticity of the image frame.

The Camera Sensor shall support both full frame and partial random frame for the HMAC generation. The mode configured will have direct impact on the CPU Load of the crypto block.

In case the contractor camera hardware provides ISP functionality, then the contractor shall discuss and agree with MB on a security concept for it before B sample production.

The following process defines the Stream Authentication between camera heads and i4 platform and is shown by the diagram below:

- On Successful Key Exchange, The Camera Base SW Makes sure the Geometry config is set in the Camera and enables the stream capture.
- For Each frame, Camera Base SW requests the Crypto module for the Row Select Key(RSKEY) based on which it passes the data to crypto module for authentication.
- The TEE Crypto module replicates the state machine of Camera sensor to compute the AKEY and RSKEY based on the Unique ID and the Session specific SSK and NONCE.
- Read the Replay Mode status flag(always disabled in production software) from secure storage.
- For Each frame, Camera Base SW uses the RSKEY based on geometry set to pass the authentication payload and the sensor computed HMAC available in meta info of image frame to the crypto module.
- The crypto module using the computed AKEY, and the data received from the Camera Base SW calculates the HMAC(HMAC SHA256) and compares with the received HMAC to authorize the frame as valid.
- In case of failures when Replay Mode is Disabled(in development builds), the Camera Base SW can perform n tries by generating new SSK and NONCE for each x consecutive retries. (Currently considering value of n and x as 3). Capture the Streaming failure Info when replay mode is disabled.



2.6.2.3.3 EEPROM authentication

The camera heads EEPROM Unique Information (eg: UID of Image Sensor, Serializer ID,

PartNumber…) shall by signed by the contractor.

Any updatable Calibration or data stored in EEPROM of the Camera heads shall be validated by the Camera base SW by comparing the copy in i4 platform secure storage.

2.6.2.3.4 Data access

The i4 platform Memory Management Unit(MMU) and Mandatory Access Control(MAC) are configured in order to restrict the access of Image frames from Camera heads only to the Camera base Software and the ISP Pipeline used by the contractor.

The Contractor may use the i4 platform security services (eg: Crypto operations, Secure Storage, Key Handling, RNG) to fulfill and/or accelerate execution of the security functions.

For the Images storage within i4 platform , it is required to use the Secure Storage capability managed by the TEE to store the image in encrypted form. The keys for encryption can be self provisioned using the RNG. The frame can be decrypted and sent back to user on request.

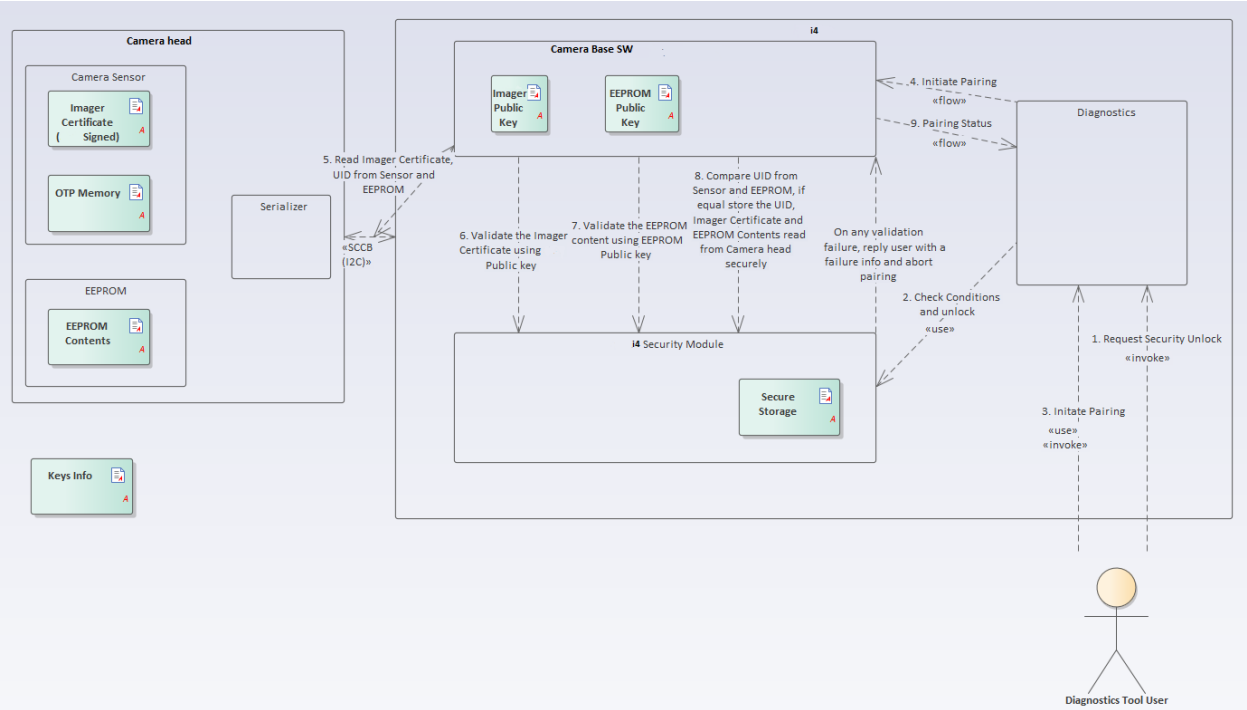
2.6.2.3.5 Camera Control Signals

The contractor shall propose a mechanism to ensure authentication of the I2C commands, in particular commands which are eye safety relevant.

2.6.2.3.6 Pairing and Unpairing

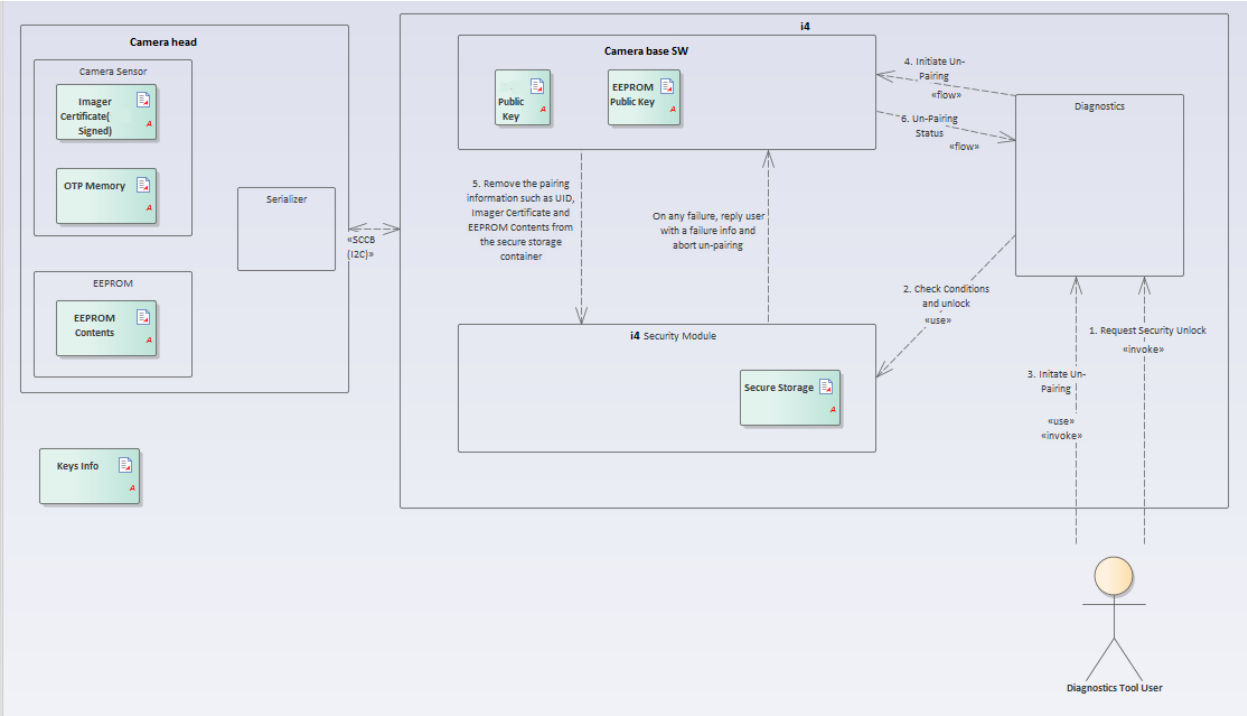
The following process defines the pairing between camera heads and i4 platform and is shown by the diagram below:

- The Pairing process involves Authorization of user by a Security Unlock and triggering the Pairing routine in CIVIC.
- The MPIC Interface SW receives this request from Diagnostics and reads the Imager Certificate, Unique Id from imager Sensor and EEPROM Contents(unique for each MPIC and partially signed by the contractor)
- Imager Certificate is validated by signature verification using the imager public key
- EEPROM signed part is validated by Signature verification using the contractor EEPROM Signing Public Key.
- Unique ID read of Sensor is compared against the UID in EEPROM.
- After the Successful validations, the Imager Certificate, Unique Id and EEPROM Contents are stored in i4 platform Secure Storage to finish the pairing.
- In case of any failure, the failure information is captured, and the pairing process is aborted.



The following process defines the unpairing between camera heads and i4 platform and is shown by the diagram below:

- The UnPairing process is like pairing process and can be done only on a paired unit.
- It involves Authorization of user by a Security Unlock and triggering the Un Pairing routine in i4 platform.
- The Camera base SW receives this request from Diagnostics and removes all the paired information such as Imager Certificate, Unique Id and EEPROM Contents stored in i4 platform Secure Storage to finish the Un pairing.
- In case of any failure, the failure information is captured, and the unpairing process is aborted.



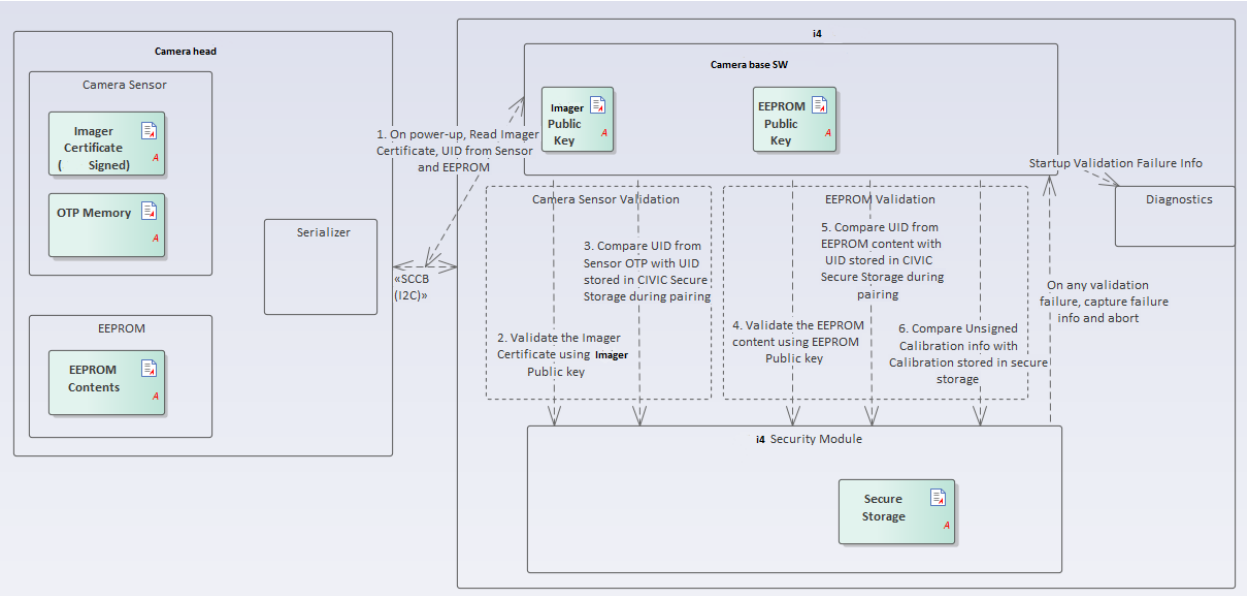
2.6.2.3.7 Security activation

The security activation shall happen at each power cycle, each reset and also during the streaming itself. Security activation shall include the authentication between the Cameras and the i4 platform. This shall be analyzed and extended to protect relevant attack surfaces. This includes M/W-ITM (man/women-in-the-middle) attack patterns.

The following process defines the Startup Validation between camera heads and i4 platform and is shown by the diagram below:

- On power up, the Camera base Software checks for availability of paired camera information in secure storage.
- If pairing information available, read the Imager Certificate, Unique Identifier of the Sensor and the EEPROM contents from the Camera Head.
- If no pairing information is available, then camera head is untrusted till a pairing is done successfully.
- The Signature of the Imager Certificate is validated using the Imager Public Key which is embedded in the Camera base Software.
- Compare the Unique ID of Sensor with the Unique ID of Camera Sensor available as part of the Secure Storage of i4 platform, if they are same then the Camera Sensor is successfully validated.
- The Signature of the EEPROM is validated using the EEPROM Public Key which is also embedded in the Camera base Software.
- Compare the Unique ID of Sensor in EEPROM with the Unique ID of Camera Sensor available as part of the Secure Storage of i4 platform.

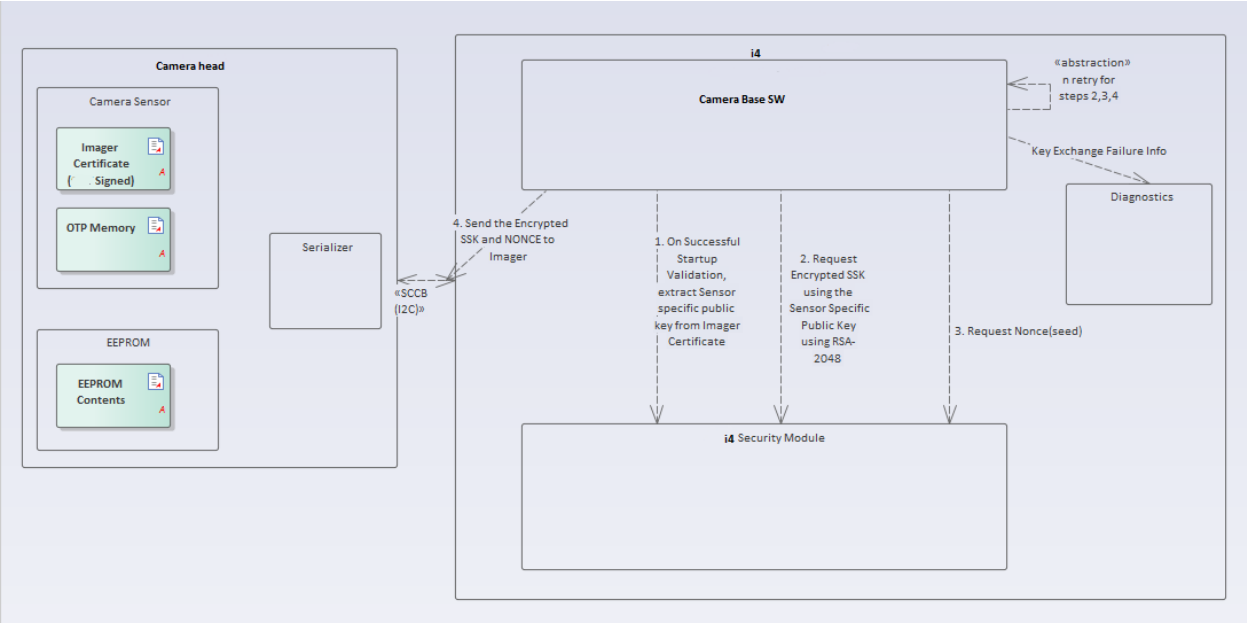
- Compare the Updatable Calibration Info read from EEPROM with the copy of same available in Secure Storage of i4 platform with these validations the EEPROM contents are validated.
- In case of any Start up validation failures, the Camera head is not trusted and the same will be unavailable. The failure information is captured via diagnostics.
- Please be noted that when replay mode is enabled, the consecutive power/ignition cycles startup Validation will be by passed till replay mode is disabled in development builds.



The following process defines the Session Key Exchange between camera heads and i4 platform and is shown by the diagram below:

- On Successful Startup Validation, The Camera Base SW extracts the Sensor specific public key from Imager Certificate and Provisions the same as temporary RAM key in TEE.
- Camera Base SW requests Crypto module to generate the Secret Session Key(SSK) custom TA service of TEE and NONCE(Seed for randomization) by using the RNG services of QNX Host. The Session Key is generated and saved within the i4 platformTEE and only the RSA public key encrypted(RSA 2048) SSK is shared to Camera Base SW from TEE, which is then sent to Camera sensor.
- The generated SSK is encrypted using the provisioned RAM key by TEE and returned to the Camera Base SW which in turn is forwarded to the Imager.
- The Image sensor security IP decrypts this message and holds the Session key from CIVIC within the Crypto RAM. The Imager decryption Status is monitored to get the Key Exchange done successfully.
- In case of failure, we can do the retry and once the retries are exhausted the same is declared as failure and the Camera is not trusted further. The failure information is passed to diagnostics.
- Please be noted that when replay mode is enabled(in development builds), the

consecutive power/ignition cycles Key Exchange will be by passed till replay mode is disabled.

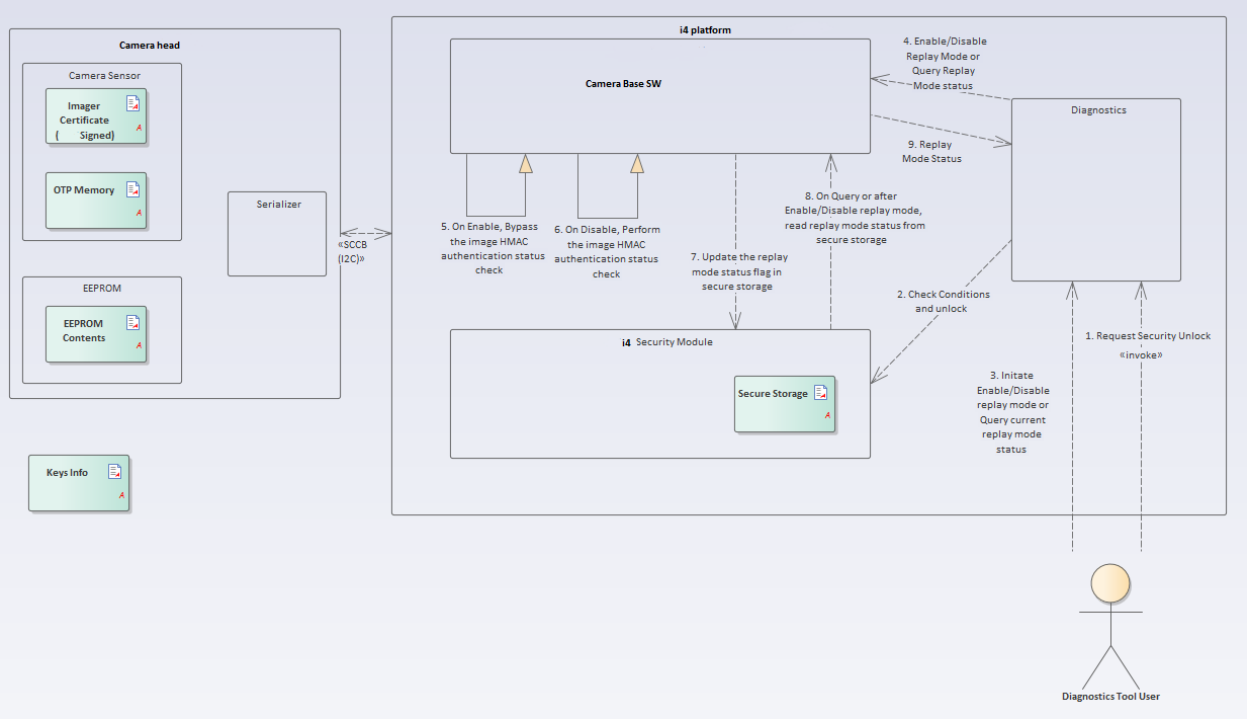


2.6.2.3.8 Replay mode

The following process defines the Replay mode between camera heads and i4 platform and is shown by the diagram below:

- The Replay mode change or status request process involves Authorization of user by a Security Unlock and triggering the Replay mode change or status query routine in i4 platform.
- The Camera Base SW receives this request from Diagnostics.
- On replay mode Enable request, the replay mode status flag is updated to bypass the HMAC image authentication and startup validation/key exchange in consecutive cycles till replay mode is disabled.
- On replay mode Disable request, the replay mode status flag is updated to enable the HMAC image authentication, it is a must to perform a restart of the system to have the start up validation and key exchange performed.
- On any of the above, the replay mode status flag is updated in secure storage.
- After Successful change or on query of replay mode status, the flag is read from secure storage and responded to the user.
- Please note that this feature will be available only during development for debug. It will be removed for production software.
- Open points:
    - Replay mode to be enabled across power cycles till disabled or carried for any certain number of cycles or to enabled by user for every cycle or disable automatically when Odometer reports speed above 7 mph.

- Any DTC reporting to be done when replay mode is activated.



2.6.2.4 Privacy

The contractor shall develop a concept to support different configurations of the camera where at least one meets legal privacy protection requirements for the target markets. This shall be agreed with Mercedes-Benz team.

The applicable privacy standards will be finalized before B-sample. This process shall happen without additional cost to the client.

The contractor shall support the maintenance of the privacy features during the regular lifetime management procedure in case standards change for certain regions.

It shall not be possible to store an image inside the the MPIC system while privacy protection mode is active.

The contractor shall support mechanisms to prevent storage of image information also inside the CIVIC.

Vehicle configuration data, vehicle status data and video data must not be stored together.

Only authorized requests shall be able to receive a full image / video stream. These requests shall be performed according to the security mechanisms of the MPIC support SW package.

The minimal mode (see recording modes) shall be used to transfer video data while not enabling identification of persons inside the vehicle. Any change into another mode that could enable identification shall be protected with authentication measures which the contractor need to define jointly with the client during development (handshake).

The contractor shall propose other de-identification mechanisms (beyond a minimal mode) during development and shall offer this as an option integrated in the MPIC support SW

package.

The contractor shall develop a concept that proofs privacy concerns from the target markets and regions are protected.

This shall be tested at each major release.

The client will deliver target markets and regions upon request to the contractor.

The contractor shall include all privacy relevant mechanisms in an overall privacy concept. This shall be in conjunction with the security authentication methods and protected against misuse. Here latest technology shall be used (see security section).

If requested by the client the contractor shall include encrypted video transmission from the MPIC support SW package to receiving applications and use available encryption techniques of the CIVIC. This shall happen without additional cost.

2.6.3 Other Functions

2.6.3.1 Diagnosis and Flash Programming

Contact for diagnostic / flash standards
Last name, first name: Pfaff, Ralf
Department: GSP/TPF
Email: ralf.pfaff@daimler.com

The contractor shall implement the interfaces for diagnosis and flash programming as specified in the [Daimler Diagnostic Specifications]. These specifications contain all relevant requirements regarding implementation of diagnosis and flash reprogramming (including variant coding, fault management, etc.).

When applying for this document in DocMaster, the contractor shall provide the following information of the client in the comment field:
- Name of the component developer
- Name of the control unit
- Model series in which the control unit is to be used
- Release date of the required document

Missing information leads to a longer processing time of the document release.

The functionality of a component may not be limited during diagnostic communication with this or other components.
Functional limitations are only permissible if write or actuation intervention is carried out due to diagnostic commands.

2.6.3.1.1 1.2.1.1 Diagnosis Documentation and Testing

The contractor shall perform the diagnostic data (CDD-file or ODX data), the documentation of the diagnosis and the diagnostic communication data safeguarding as described in the Diagnostic Data Authoring Guidelines [A0030027199].

The contractor shall perform and provide diagnostic/reprogramming testing and reporting of test results as described in the Diagnostic Test and Reporting Requirements [DTRR].

2.6.3.1.2 1.2.1.2 Flash Programming

If technically possible, control units with diagnostic functionality shall be flashable as defined in [DDS].

If the ECU will be flash reprogrammable in series production, it shall be flash reprogrammable with already while in development phase.

2.6.3.2 Over The Air Software Update (OTA-Update)

To ensure OTA updateability, ECU's that are flashable according to [Daimler Diagnostic Specifications] shall implement the requirements from [MGU00000836].

When preparing quotations, the requirements of the [Mercedes-Benz Software Remote Update] document shall be taken into account

2.6.3.3 Software Distribution

The contractor must co-ordinate with the client all basic functions, which are necessary for the distribution of the software.

2.6.3.4 Test and Initial Startup

Functions in the context of test and initial startup shall be generally available with the B-samples.

Deviations shall be negotiated with the contractor.

In detail the following functions shall be implemented (in each case including temporal requirements and surrounding field requirements such as temperature, pressure, density of light, combustion engine run,...):

- Initial startup functions, for example normalisations, learning journey, adaptations, (self) calibrations

- Test functions, for example for vehicle manufacturing, onboard error recognition of all I/O and periphery

- Error recognition functions, checks and their preconditions, supply of measurements over diagnosis interface

- Support functions for check and initial startup in the overall vehicle

The component's total software update must be able to be performed within 300 seconds via the OBD port.

Flash operations must work with each ECU at terminal 15=Off.

If the ECU is a gateway, its performance per bus shall be dimensioned in such a way that all ECUs behind the gateway can be updated at the same time, even at full parallelism.

If the ECU is a gateway, its performance per bus shall be dimensioned in such a way that all ECUs behind the gateway can be diagnosed at the same time, even at full parallelism.

The coding time of an ECU in the vehicle topology from OBD port to the individual ECU must not exceed 10 seconds.

The total time needed to calibrate and teach a ECU must not exceed 10 seconds.

ECU electronics and plugs must be designed in such a way that it is possible to plug and unplug under voltage in production.

The ECU software must be partitioned in such a way that a separate software update for basic functions/basic functions, diagnostic functions and customer functions is possible.

The contractor must prepare a cause-effect analysis (Ishikawa) including limit values and tolerances for the identification of interference factors of the test and initial setup procedures running in the control unit. This cause-effect analysis must be passed before

implementation time, or with the B-smaple at the latest. For the C-sample, a proof of measurement from the supplier has to be delivered, which proves the suitability and reproducibility of the process (MSA1).

The contractor must develop calibration procedures that allow assessable conclusions to be drawn about the quality of the calibration process or the calibration result. (e.g. replay rate, deviation, ambient parameters, ...). The quality criteria of each calibration must be made available through diagnosis.

The flow of the ECUs internal calibration process (calibration algorithm) from a software and hardware point of view must be described in a process diagram.

Calibrations with external equipment and devices must be avoided in favour of simple, automatic calibration procedures without plant technology and special targets.

All test, initial setup routines or condition queries for the success of a test, initial setup must provide a clear identification of the cause of the error in the event of an error.

DThe peripherals on the ECU and the ECU itself (e.g. sensors, USB ports, etc.) must enable an automated contacting test. This can be done either via a cyclic ECU internal check including diagnostic trouble codes or a diagnostic-triggered test with the corresponding return value.

For each release, a initial setup testat is must be delivered by the contractor, which documents the initial setup steps ok/nok. The basis is the test and initial setup regulations to be developed.

User settings shall not restrict, deactivate or interfere with test or commissioning procedures. All tests and integration activities shall be possible even with deactivated user function.
For example: Sensors or cameras must not be disconnected from power supply or deactivated in order to ensure diagnostic responses and onboard error detections.

2.6.3.5 Built-in Image Quality Test

This test shall inspect the Quality of Service (QoS) of the MPIC system while mounted in the vehicle at its target position/orientation after every iginition cycle, after installation and pairing is completed.
Crucial for QoS is image quality, thus this test shall focus on key IQ KPIs.
The scope includes all optically relevant components (including cover glass).

The Built-in Image Quality test shall detect stains and dust particles between the camera head (lens) or the illumination and the design cover / display glass.

In case of failure, a DTC shall be set.

The Built-in Image Quality test shall work targetless, i.e., no dedicated IQ target shall be required.

MPIC camera pairing shall trigger the Built-in Image Quality test.

The Built-in Image Quality test shall function for all car lines and all vehicle interiors.

Detailed implementation of the Built-in Image Quality test shall be suggested by the contractor and discussed with the client during development.

The Built-in Image Quality test shall function under all lighting condition.
The lighting conditions include at least:
- aftificial light in a workshop

- artificial lighting in an assembly line
- low light (e.g. garage, parking lot)
- darkness
- indirect sunlight
- direct sunlight

The Built-in Image Quality Test software shall detect if the ambient lighting condition are suitable for complete execution of the Built-in Image Quality Test.

In case of failure, a DTC shall be set.

The Built-in Image Quality Test software shall detect if the scene is suitable for execution of the Built-In Image Quality Test.
The scene detection includes at least:
- Blockage
- Persons or living beings in the vehicle
- Objects in the camera field-of-view

The Built-in Image Quality test shall function under all environmental conditions.
The environmental conditions include at least:
- Ambient temperature 0°C < T_ambient < 60°C
- Relative Humidity RH = 0% < RH < 70%

The measurement error of the Built-in Image Quality test shall be <5% over all external illumination conditions that might be present.

The Built-in Image Quality test shall enable predictive maintenance w.r.t. IQ KPIs.

A relative measure over time shall be presented by the contractor and reviewed by the client.

The contractor shall present a measurement system analysis (MSA) study to the client for each of the Built-in Image Quality test KPIs.

The MSA shall include at least:

- repeatability

- reproducibility

- stability

The degradation over lifetime of Image Quality of the MPIC system is described in the Image Quality chapter.

If the Built-in Image Quality test detects a further degradation that is seen as significant deviation from mentioned IQ data (i.e., >20%) it shall generate a DTC.
Information: Further details can be found in the Diagnostics chapter.

The Built-in Image Quality test shall measure cross-talk (stray light from the active illumination to the image sensor).

In case of failure, a DTC shall be set.

The Built-in Image Quality test shall measure the spatial frequency response (SFR) as defined in chapter "Image Quality".

In case of failure, a DTC shall be set.

The Built-in Image Quality test shall measure the image noise as defined in chapter "Image Quality".

In case of failure, a DTC shall be set.

The Built-in Image Quality test shall measure the non-uniformity as defined in chapter "Image Quality".

In case of failure, a DTC shall be set.

The Built-in Image Quality test shall detect pixel defects as defined in chapter "Image Quality".

In case of failure, a DTC shall be set.

The Built-in Image Quality test shall measure IR and RGB image quality.

In case of failure, a DTC shall be set.

The Built-in Image Quality test shall include testing of the active IR illumination.

In case of failure, a DTC shall be set.

The function shall support triggering via the measurement system or diagnostics commands.

2.6.3.6 Field image quality test

Information: The Field Image Quality test shall allow for capturing of image quality relevant information during development as an approximation of lab tests. Especially, if issues are present in a certain vehicle and illumination scenario, the field image quality test and the underlying capturing of related mobile IQ targets shall allow for generating relevant and meaningful data for further analysis.

The Field Image Quality test shall cover target based image quality tests in the vehicle. The target (e.g. test chart) may be placed manually in the vehicle (e.g. driver seat, passenger seat, rear middle seat, head rest, etc.)

The contractor shall provide mobile Image Quality (IQ) targets that can be transported and utilized in a vehicle. This shall include miniature versions of
- dead leaves target
- SFR target
- color checker target
- target to measure horizontal & vertical field-of-view

Additional targets shall be presented by the contractor to the client.

The field image quality test shall allow triggering from the measurement systen and diagnostics.

The 20 most recent measurements of the field image quality test shall be stored on the i4 platform persistent storage with meta data e.g. date, time, location, part numbers, ambient conditions.

2.6.3.7 Event Data Recorder

This component shall not contain event data recorder (EDR) functionality. In control units without event data recorder functionality no dynamic vehicle data with time reference to a crash event may be stored in a non-volatile memory.

2.6.3.8 Data Protection

The contractor is obliged to provide the client with documentation of all data points (e.g. aggregated or internal signals, CAN signals, error codes, load collectives) stored in the control unit over an ignition run and bus silence (i.e. non-volatile) using the form [MGU00001737] for each release; this also applies to encrypted data points or data

points in storage areas accessible only to the contractor.

The above mentioned documentation obligation begins with the release which is provided 18 months before the start of production and is also required for any subsequent releases. The documentation requirement ends with the last release made available or the end of production of the component, whichever is later. Changes (new additions, deletions or changes) to the previous version of the release documentation shall be clearly marked (e.g. in red).

Excluded from this are data points that are requested/stored for storage by software components provided by the client.

In case of questions, in particular regarding the scope and execution of the documentation obligation, the client must be contacted at an early stage in order to avoid possible ambiguities and misunderstandings from the outset.

2.6.3.9 Collection of Vehicle Data

ECUs shall provide a generic mechanism for collection of ECU-internal as well as communication data.
To enable data collection for different purposes and users, generic and flexible configuration interfaces have to be provided.
This also decouples the definition of individual data collections from the development process of the ECU.
The contractor shall implement the requirements specified in [MGU00001754].

2.6.4 Interfaces

2.6.4.1 1.3.1 Human-Machine-Interface (HMI)
2.6.4.2 1.3.2 Interfaces with other Software Modules
2.6.4.3 1.3.3 Signal Names

All signal names, which are used within this document and applicable documents, are to be understood as substitute symbols without claim on continuous usage of exactly this name. If the designation of a signal changes after award of contract, no change costs may be charged.

2.6.4.4 1.3.4 Measuring Technology Interface

The contractor shall process measuring technology signals using the CAN Calibration Protocol (CCP/XCP) and can obtain a current example for this purpose from Vector Informatik GmbH.

An ASAP file is required from the contractor for the description of measuring technology signals. Each SW status shall include an ASAP file for the frame SW and the functional SW. These files are placed in a project frame in order to configure the application tool.

The CAN-IDs for the CCP/XCP messages of the control unit are described in the current Network Communication Description (NCD).

In combination with the use of a security class the measuring technology interface shall be removed at the beginning of production. This shall be coordinated with the client.

2.6.4.5 1.3.5 Application and Parameterization Interface

As with the measuring technology signals, the application of parameters is done using the CAN Calibration Protocol (CCP/XCP) and/or the Unified Diagnostic Services (UDS).

In combination with the use of a security class, the application and parameterization interface shall be removed at production start-up. This shall be coordinated with the client.

For the description of the parameters, the contractor shall likewise provide an ASAP file, which shall be structured in the same way as for the measuring technology signals.

The contractor shall provide a Candela file for the description of parameters.

The contractor shall ensure ASAP conformity to CAN Calibration Protocol (CCP/XCP) and Calibration Data [ASAM].

Type definitions for the interfaces CCP/XCP/KWPon-CAN, -K-Line/ETK shall be created based on the client's definitions.

The client makes the definitions available as a ASAP2 file. The contractor shall request the latest version of the ASAP2 file from the responsible specialist department.

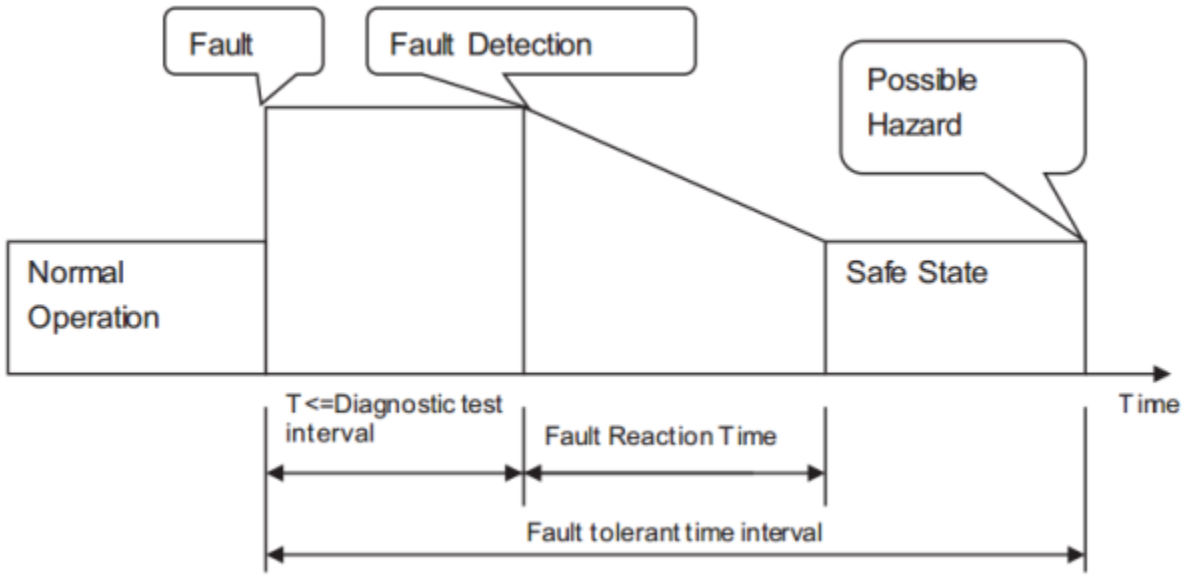
The RAM memory for the measurement data tables of the application and parameterization interface (DISTAB, OLDA) shall be placed in the emulation memory (EMEM) of the microcontroller in the control unit.

2.6.4.5.1 1.3.5.1 Scalability of the Application Interface

All microcontroller debug interfaces such as DAP / JTAG, DAPE and AURORA (AGBT) must be available via connectors in the application control units.

The contractor shall provide for series application ECUs with standard interface modules (e.g., 100BASE-T1 modules), that support only the DAP / JTAG interface. For more complex application requirements or external bypassing, it must be possible to implement interface modules that also support the AURORA interface (such as ETAS FETK-T or Vector VX145x).

The application and bypass interface driver in the control unit basic software must automatically recognize the built-in interface module variant (DAP / JTAG and AURORA) and activate the corresponding module variant.



2.6.4.5.2 1.3.5.2 Standard Application

In the standard application control units, application interface modules with 100BASE-T1

(Automotive Ethernet) and XCP protocol ≥ XCP V1.3.0 are used:

Measurement performance: 2000 bytes per rate

Maximum size of a single measurement vector is 3 KB

Ignition key and cold start capability shall be ensured

Reconfiguration in the application tool (for example, adding or deleting measured variables or measurement windows) while the bypass is running must not lead to a crash of the bypass connection and thus lead to a control unit reset (for example due to high utilization of the interface hardware).

The application interface driver software provides the rates, DAQ, and STIM lists for external bypass, and provides the Bypass Preparation and Definition Tool vendor with information about accessing the communication drivers.

2.6.4.5.3 1.3.5.3 High Speed Application

The contractor shall provide application control devices that support the trace interface (AURORA, AGBT) for applications where high user data rates or the measurement of very large quantities are required.
Measurement performance: ≥ 15 Mbytes/s.
Otherwise, the same requirements apply as for the standard applications.

2.6.4.5.4 1.3.5.4 XCP-Debugging

To enable debugging for control units or control unit networks in the vehicle, XCP debugging shall be provided in the control unit base software.

The debug software (for example TRACE32 from Lauterbach) runs on a host computer. Debug commands are not sent directly to the target CPU. All debugging commands are encoded in XCP. These XCP commands are sent from the host computer to the Application Interface Module (100BASE-T1 pod). The application interface module translates the XCP commands back into a low-level debug protocol (JTAG, DAP, Nexus, ...). An Ethernet switch allows multiple control units to be connected to the debugger.

For measuring the data flows between software components (e.g., for monitoring cross-module data consistency) or observing chains of effects across module boundaries, the control unit supplier must provide an additional description file (A2L file) that describes measuring signals in the control unit basic software (OS, driver, etc.).

2.6.4.5.5 1.3.5.5 High-speed Datalogging and Online Debugging

For high-speed data logging and real-time observation (such as continuous non-intrusive runtime analysis of control unit microcontrollers), the trace interface data of the microcontroller must be delivered with max. data rate, without loss of data on the host interface or on a second interface.

The interface for the trace data is unidirectional. The configuration of the application interface module for the trace mode is carried out by the application tool (for example INCA) via the application interface.

In data trace mode data from control units with application interfaces from different tool manufacturers must be merged with temporal correlation into a data sink (eg data logger), a

host interface with open protocol and time synchronization is required (such as XCP protocol ≥ V1.3.0).

The trace mode must work in parallel to the standard application.

2.6.4.5.6 1.3.5.6 Physical Design of the Host Interface

The standard application control units use application interface modules with 100BASE-T1 (Automotive Ethernet) and XCP protocol ≥ V1.3.0.

The more powerful application interface modules require a host interface that provides for high-speed data logging and online debugging the maximum data rate of the trace interface (AURORA interface) without data loss. Currently, a data rate of ≥ 5 Gbit/s is needed here (25 Gbit/s in the future and more).In the future, data rates of ≥ 5 Gbit/s are required (for example, 10 Gbit Ethernet 10GBaseT).
In the future, data rates of ≥ 25 Gbit/s are required.

If the data for application and data logging can not be combined on a common host interface, separate interfaces can be used (for example, 1 GBit Ethernet for the application and 10 GBit for data logging).

2.6.4.5.7 1.3.5.7 Interface Module Driver

The application and bypass interface driver in the control unit base software shall be conform to the ASAM MCD-1 POD ≥ V1.0.0 standard.

The application interface driver software provides the rates, DAQ, and STIM lists for external bypass, and provides the Bypass Preparation and Definition Tool vendor with information about accessing the communication drivers.

The driver software for the application interface contains the safety concept for the bypass interface.

2.6.4.5.8 1.3.5.8 Prioritization of the measuring and bypass rates

The DAQ events in the control unit should be prioritized as follows:
- Bypass events have higher priority as measurement events
- 1 ms bypass events (or faster time-synchronized bypass events) have the highest priority
- Then come the angle synchronous bypass events
- This is followed by the time-based bypass events such as 10 ms and 100 ms
- Then comes the 1 ms measurement event (or faster time-synchronous measurement events)
- Then comes the angle-synchronous measurement event
- The lowest prio have the time-based measurement events such as 5 ms, 10 ms and 100 ms

2.6.4.5.9 1.3.5.9 Measurement labels for task runtimes

In order to be able to monitor the runtime of the time- and angle-synchronous tasks, in particular for the integration of on-target bypasses, the control unit software must provide measurement labels for all time- and angle-synchronous tasks:
- Current gross runtime
- Maximum runtime
- Maximum runtime over lifetime. This value is stored in the EEPROM when the Engine is switched off and can be reset via application parameter.

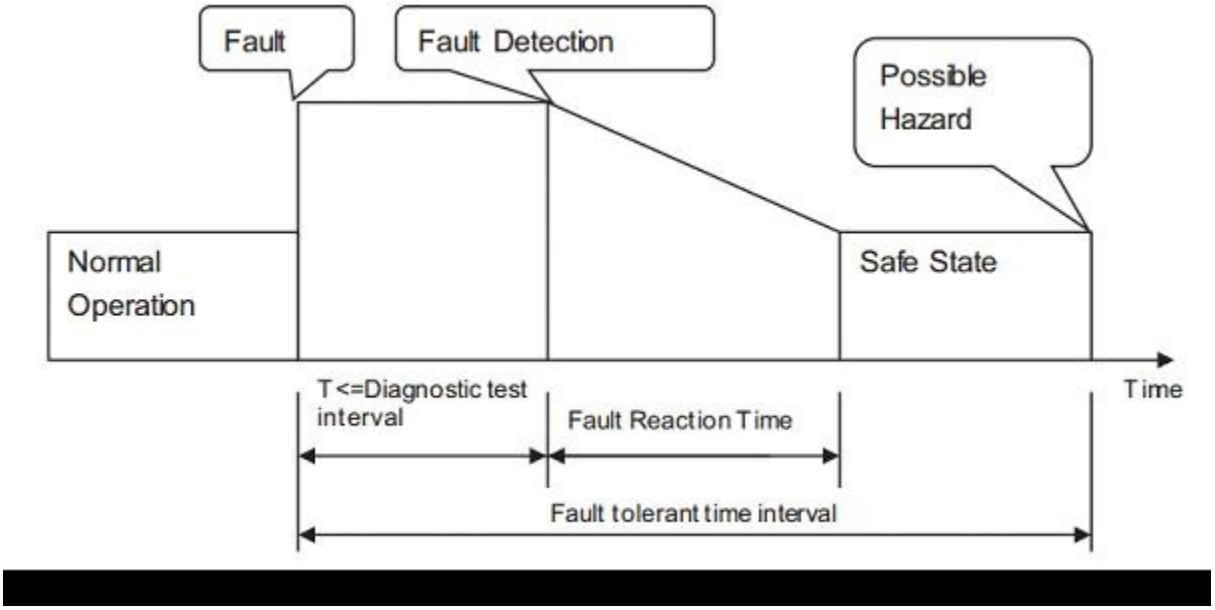
- Application parameter for resetting the maximum values

In addition, information which maximum runtime the individual tasks may not exceed (via on-target bypassing) is supplied by the Tier1 (for example in the A2L file in the long identifier of the task runtime labels).

2.6.4.5.9.1 1.3.5.9.1 Measurement and Bypassing of several control units

With a bypass controller, functions must be externally bypassed in multiple ECUs (e.g., engine control unit and common powertrain controller) using application interfaces from different tool manufacturers. At the same time, measurement data are still being read out of the two ECUs by the application tool.

The bypassing must be able to be started via ignition key or power-on (i.e., by applying the supply voltage). When connecting and initializing an already started bypass system with the application tool, the bypassing continues without interruption.



2.6.4.5.10 1.3.5.10 Bypassing

External bypass uses the existing application interface of the control unit.

Number of data bytes per bypass rate: max. 255 bytes (DAQ or STIM data)

Up to 3 bypass rates can be active at the same time (independent of measuring rates).

Bypass roundtrip time: 400 µs (with 255 bytes for each DAQ and STIM) for standard application control units and 100 µs (with 255 bytes for each DAQ and STIM) for application control units with the high-speed application interface.

Dynamic allocation of the available memory of the bypass input and output tables to the individual rates.

DAQ and STIM events for bypassing and measurement must be handled separately. No DAQ or STIM events defined for bypassing may be used for measurement or application. Also, no DAQ or STIM events defined for bypassing may be used for measurement or application.

The bypassing must be implemented in such a way that it is possible to start and stop the measurement and the bypasses independently.

Each measurement data can be used as input for a bypass.

Ignition key and cold start capability must be ensured.

Internal and external bypassing is only activated in control units with application interface.

2.6.4.5.10.1 1.3.5.10.1 Safety Concept Bypass Interface

Bypass consistency check must be performed according to XCP protocol V1.4.0.

All bypass event channels are triggered exactly once per bypass cycle.

All bypass event channels are always triggered in the same order.

All bypass event channels have in the DAQ direction a 1: 1, 1: n, or n: 1 relationship with the STIM channels.

The number of consecutive rate losses must be monitored. A parameter can be used to specify the maximum permissible number of consecutive rate losses in the range from 0 to 255.

When a rate loss occurs, the last received value is used. This requires double buffering of the stimuli data in the control unit.

When booting, depending on an applicable parameter, the bypass is either automatically enabled when the connection is established successfully (ignition key start), or it remains switched off initially and must be activated by an application parameter.

Depending on another parameter, bypassing is not enabled until a valid data frame has been received from each used bypass rate. If this parameter ist set to another value, the bypassing for each rate is enabled independently to the others.

2.6.4.5.10.2 1.3.5.10.2 Measurement Labels for Bypass Runtimes

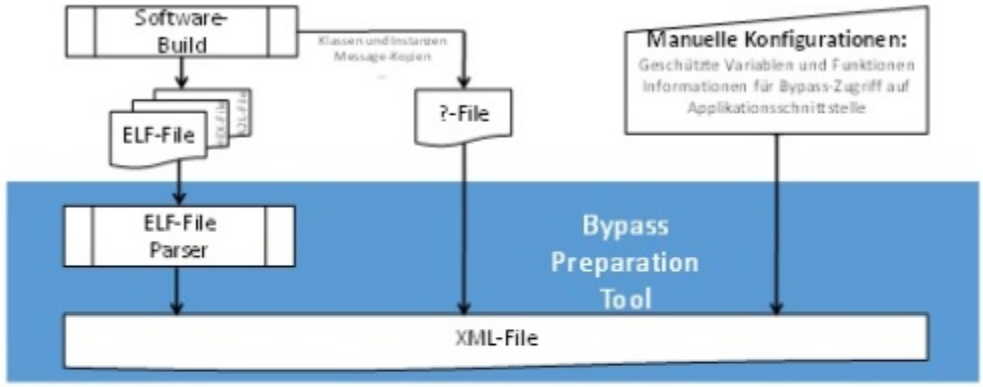
The Measurement / Calibration / Bypass interface provides debug information or a measurement for each bypass rate, indicating the amount of time between the occurrence of a Bypass DAQ event and the successful writing of the corresponding STIM buffer.

2.6.4.5.10.3 1.3.5.10.3 Tool and Control Unit Supplier-independent Bypass Creation

For the rapid integration of bypass hooks (internal or on-target bypassing and external bypassing) into the control unit software by the customer, a tool and control unit supplier independent bypass creation must be provided. For this, the contractor must provide additional information to the customer or the bypass tool supplier.

2.6.4.5.10.4 1.3.5.10.4 Bypass Preparation Tool

The Bypass Definition Tool requires information out of the software in the control unit to quickly integrate bypasses into the control unit software for internal or external bypassing. This information is generated during the software build and written by the Bypass Preparation Tool in encrypted form into an XML structure in accordance with the exchange format adopted by AUTOSAR RCP. The Bypass Preparation Tool is provided by the tool supplier and is integrated by the contractor into the software build environment.



2.6.4.5.10.5 1.3.5.10.5 Bypass Definition Tool

The bypass definition tool is provided by tool suppliers and is used by the client to integrate the internal and external bypasses into the control unit software.

The following tools for model-based software development for on-target bypasses must be supported:
- Simulink
- ASCET
- Targetlink

The Bypass Definition Tool supports the following hook types:
- Fixed value hook
- Application hook
On Target Bypass (internal bypass) based on Simulink, ASCET or Targetlink models
- External bypass via the existing application interface

It must be possible to prioritize the RAM memory areas if they have different access times.

It must be possible to call existing control unit functions in the Bypass Definition Tool e.g. by providing functional containers for integration into Simulink, ASCET or Targetlink.

It must be possible to use existing (scalar) adjustment parameters from the control unit in the software development tool (Simulink, ASCET, Targetlink).

The bypassing tool must provide the user the option of overwriting the corresponding CPU register of a bypassed variable.

Support of class parameters that are multiply instantiated (transfer of data structure generation, for example, from ASCET to Bypass Definition Tool).

The Bypass Definition Tool generates measured variables in the OTB bypass code so that for

maps the actual working point can be displayed in the application tool.

The external bypassing accesses the existing (and with regard to software driver for bypassing prepared) application interface of the control unit.

2.6.4.5.10.6 1.3.5.10.6 Shared Build Environment

The build environment at the contractor and at client (Shared Build Environment) contains the bypass preparation tool. At software build, additional information (in encoded form) is written in an XML file. This information is used by the Bypass Definition Tool to generate internal or external bypasses.

The contractor provides the client with a shared build environment that includes the bypass preparation tool. In this way, with the bypass definition tool, internal or external bypasses can be inserted into contractor software and client's in-house software. The Bypass Definition Tool is procured by the client.

2.6.4.6 1.3.6 Security and Protection

This chapter does not represent a complete list of the security requirement, but forms the basis on which security-features of functions are defined in other specification parts.
In this respect, the contractor is required to analyze and evaluate the complete requirement specifications with regard to security.
The individual subchapters describe the security aspect and not the whole function.
If further requests are made to the security in other parts of the requirement specifications, they apply.
However, the requirements from this chapter shall not be undershot.

The General Terms and Conditions for Car IT Security (GTC for DCS certificates and GTC for ZenZefi) must be complied with:
For the fulfillment of the assignment, the diagnosis of security-relevant ECUs is necessary. In order to do this, the contractor will require Diagnostics, Coding and Security Onboard Communication Certificates (DCS Certificates).
In the event that no contractor owned software to manage the DCS certificates is available, it is possible to use the Central Certificate Management Tool (ZenZefi) of the contracting authority.
The DCS certificates and ZenZefi are subject to the General Terms and Conditions for Car IT Security, consisting of the following documents:
- GTC for DCS certificates with the attachments mentioned therein [MSS 10902]
- GTC for ZenZefi with the attachments mentioned therein [MSS 10903]

In the case of a residual bus simulation, a SecOC calculation for selected signals may be required.

Appropriate measures must be taken by the contractor to protect the provided crypto material. These are:
- Implementation of a security concept including Security Incident Management by the contractor and inspection by the contacting authority.
- Need to Know Principle (only employees who need the provided information directly for the fulfillment of a specific task get access)
- Training and awareness-raising activities for employees
- Rules for using client's Security Tools
- Rules for registering users in client's Directory

When the ECUs are delivered to the contracting authority it must be ensured that
- the date and time are not in the future.

- the Tick Count" is less than 1 year.
- the "SecOC Standard Keys" are set (delivery status of the ECU manufacturer).
- the default VIN is set (delivery status of the ECU manufacturer).
- the ECU certificates are stored in the ECU (ensured by ECU supplier).
- the appropriate Private Key to the Public-Key/ECU Certificate is stored.
This applies both to series deliveries and to development samples.

2.6.4.6.1 1.3.6.1 Referenced Documents

[MSS 10796] - Standard Security Specification

[MSS 10809] - Standard Flashloader Specification

[MSS 10815] - Standard Security Architecture - Implementation Specification

[MSS 10820] - Requirement Specification for SHA512 and Ed25519ph

[MSS 10824] - Requirement Specification for Certificate Structure

[MSS 10866] - Specification for Key-Format CCCv2

[MSS 10872] - Specification for ZIP-CertificateBag V1.0

[MSS 10902] - DCS-Zertifikate AGB

[MSS 10903] - ZenZefi AGB

[MSS 20208] - Ethernet Networking Performance Specification

[Daimler Diagnostic Specifications] - Daimler Diagnostic Specifications

[MSS 10816] - Standard Security Architecture for AUTOSAR Adaptive - Implementation Specification

[MSS 10799] - Standard Security Architecture for AUTOSAR Adaptive

The contractor shall take into consideration any applicable standard, and/or regulation, and/or legislation, even in draft state, if it is foreseable to be applicable at the start of production or at the start of sale.

This applies in particular to ISO standard (e.g. ISO 27000, ISO 21434) or SAE standard (SAE J3061), but is not only restricted to these.

2.6.4.6.2 1.3.6.2 General Basica

Flashware protection shall be implemented according to the applicable reference documents [MSS 10809].

The component shall provide security mechanisms to prevent remote attacks (e.g. through remote interfaces).

The component shall provide mechanisms, which prevent an attacker from unauthorized manipulation of software and/or data of the component.

The component shall provide mechanisms to protect the integrity of the software and data of the system and its components.
The behavior in the case of a detected manipulation shall be coordinated with the client.
In case of a multiprocessor system, this mechanism must be examined individually for each processor / memory.

The component shall not store user private data unless the confidentiality of the data is

protected and the user consent was given. In any case private data storage shall be approved by the customer.

The component shall only contain the function described in the requirement specifications.

A security solution for the component shall be developed by the contractor and approved by the client.

Components having increased security needs, shall additional reserve 150 kB ROM and 32 kB RAM.
Rationale: For future cryptographic updates.

Components having increased security needs, shall reserve a 192 kB ROM block for flashbootloader.
Rationale: For future cryotographic updates of flashbootloader.

Components having increased security needs, shall have a minimum of 192 kB RAM for flashware signature verification while flash rom update is active. An additional amount of ram for extra cryptographic functions shall be taken into account.
Rationale: For future cryotographic updates of flashbootloader.

2.6.4.6.3 1.3.6.3 Hardware Security

Internal parameters which relate to the condition of the system with regard to security shall not be manipulated via diagnosis or debug mechanism.

Sensitive information shall be protected against unauthorized use. Examples of sensitive information are cryptographic keys and passwords.

The communication between the MPIC and the matching CPU inside the CIVIC shall be protected using state of the art authentication and encryption equivalent to AES256/SHA256 and TLS1.2

The contractor shall present the concept to secure the communication between cameras and car computer. This concept needs to be reviewed and approved by client.

In case that findings are identified in the review additional requirements can be added by client without cost.

2.6.4.6.4 1.3.6.4 Hardware Security Module

The ECU shall contain a hardware security module (HSM).

If the microcontroller has a HSM, the following Requirements are mandatory: STLH-7167 to 7171) as well as the Section „Asymmetric Crypto“ (STLH-7173) resp. (STM-1317006).

The following requirements are mandatory for the cameras, regardless if the HSM is included in a microcontroller or a different hardware component (e.g. image sensor): STLH-7167 to 7171 as well as the Section „Asymmetric Crypto“ (STLH-7173) resp. (STM-1317006).

All cryptograpic operations which use keys stored inside the HSM shall be implemented inside the HSM. Any exceptions shall be approved by the client in written form.

Private/symmetric key material stored in the HSM shall not be exported or exportable from the HSM during runtime.

Unauthorized access to the HSMs functions and data shall be protected by the HSM, e.g. using access control.

The HSM shall povide secured storage mechanism that is resilient to physical attacks.

The HSM shall provide means to perform crypto related operations using internally stored keys on data that is provided via an external interface.

Private / public key pairs must be generated in HSM.

All used symmetric keys - if they are not session keys - and all private keys must be hold in a HSM.

All public keys must be integrity protected by use of the HSM.

All cryptographical operations that uses keys which are hold in HSM shall be implemented in HSM.

Key materials which are stored in HSM shall not leave the HSM.

Key material shall not be able to be changed via diagnosis or debug mechanisms, unless it is explicitly specified and protected by further security measures.

Access to the HSM must be limited to authorized function (access control).

2.6.4.6.5 1.3.6.5 Supported Crypto Primitives and Functions

2.6.4.6.5.1 1.3.6.5.1 Asymmetric Crypto

If asymmetric key material is generated during runtime, this shall be done in an HSM. Any exceptions shall be approved by the client in written form.

The HSM shall support crypto primitives and algorithms as specified by reference documents.

The HSM shall provide random number generators as specified by reference documents.

The HSM shall provide sufficient storage capacity as speficied by refernce documentation and specific component requirements.

2.6.4.6.5.2 1.3.6.5.2 Debug Interfaces

All low-level debug interfaces (e.g. JTAG, SWD, XCP, serial) shall be protected by a strong authentication mechanism that utilizes a key or password that provides a security strength of at least 112 bit symmetric equivalent. If the protection is not feasible for a specific interface an alternative solution shall be discussed and approved by the client.

All high-level debug interfaces (e.g. adb shells, CLIs, GUIs) shall be protected by a strong authentication mechanism that utilizes a key or password that provides a security strength of at least 128 bit symmetric equivalent. If the protection is not feasible for a specific interface an alternative solution shall be discussed and approved by the client.

In case of protected debug-interfaces the authentication mechanism shall utilize device individual secrets that are not directly derived from publicly known data (e.g. the ECUs serial number) but rather be derived involving a strong secret or randomly generated.

2.6.4.6.5.3 1.3.6.5.3 Miscellaneous Secure Hardware Requirements

HW Security requirements shall be implemented as specified by reference documents.

2.6.4.6.6 1.3.6.6 Operating System and application hardening

Operating System and application hardening shall be done according to the referenced

doucments and according to the component specific requirements

Processes and applications shall be limited to the least possible rights required to fulfill their respective use-case.

Processes shall be prevented from manipulating or influencing other processes by suitable mechanisms.

The operating system shall be hardened if applicable according to the specific hardening requirements suggested by the contractor and approved by the client.

The security mechanisms provided by the hardware (e.g. NX bit) shall be activated in the operating system.

Access rights shall be defined according to the least privilege prinicple.

If Address Space Layout Randomization (ASLR) is supported by the operating system, this shall be used.

All userspace binaries shall be compiled as Position Independent Executables (PIE) to support ASLR.

Features of the operating system which are not requiered shall be deactivated. This applies particularly to debug features.

Drivers which are not required shall be deactivated, and if technically possible, deleted from the operating system.

Driver features which are not requiered shall be deactivated, if technically possible, or deleted from driver.

If a multi user operating system is used, applications and services shall be distribute meaningfully, to systemusers with restricted rights.

Information on the exact configuration of the operating system must be removed from the software release if technically feasible.

Login credentials shall be unique and individual. Exceptions to this requirements shall be approved by the customer.

If the component manages sessions, the period of validity of the session shall be selected as small as possible.

Third-party software that contains publicly-known, unfixed vulnerabilities shall not be used in the component.

The contractor shall use the most up-to-date software components and OS versions unless otherwise approved by the client.

Production grade software shall not contain any debug symbols and debug information.

Software components which are only created for debuging-, developing- or testing-reasons shall be removed in production grade software releases.

The software components shall utilize the security mechanisms provided by the compiler and/or runtime environment.

The supplier shall use compiler options to protect against buffer overflows if applicable.

The application shall use mechanisms to prevent code injections.

Software shall be protected against reverse engineering.

If key material is not stored in a HSM, unencrypted key material shall only be held in RAM or file system for the shortest possible time required to perform crypto operations with it.

If key material is not stored in a HSM, the key material is to be stored and processed in a Trusted Execution Environment (TEE), if this is technically possible and the hardware platform used provides a TEE.

2.6.4.6.7 1.3.6.7 Diagnosis

Diagnosis functions shall not disclose any information beyond the legally required dimension without any previous authentication.

The component shall not contain any undocumented diagnostic services.

Diagnosis services created by the contractor for their own use (e.g. Production) shall be disclosed to the client and require explicit approval by the client.

While driving diagnostic services must be reduced to the statutory minimum. See DDS, DRECU Chapter Security.

2.6.4.6.8 1.3.6.8 Communication channels

The component shall only provide access interfaces which are required by relevant specifications.

The component shall provide mechanisms to establish and maintain secure communication channels to external services.

Mutual authentication shall be used to setup secure communication channels.

Mutual authentication shall be used for wireless interfaces.

Communication interfaces and their drivers are to be limited to the feature and protocol required for operating the control unit.

Communication interfaces that are not used in a certain control unit configuration or operating state shall be switched off during operation. This applies especially to radio interfaces.

Communication interfaces that are generally not used in a certain hardware variant are to be deactivated in a irreversibly hardware manner (e.g. due to missing contact on the PCB, short circuit, fuses, etc.).

The component shall provide mechanisms to enforce the separation of different in-car networks.

The component shall provide mechanisms to restrict the communication between in-car and external connected networks only to the necessary content and communication patterns.

The component shall reject faulty or unexpected messages, packets and data. The function of the components shall not be influenced.

The component shall perform input validation.

The component shall correctly code all output signal ("output encoding").

The functionality implemented by all interfaces shall be minimal, i.e. the interfaces shall only offer the explicitly specified functionality.

Remote interfaces shall be isolated from vehicle internal bus.

The component shall provide protection against replay attacks on its interfaces.

Consumer electornic interfaces which are not customer accessible, shall be secured with cryptographicaly strong passwords. Default passwords are not allowed.

Credentials shall be transferred confidentially (by means of encryption) on the vehicle bus.

Secured interfaces shall be protected against brute-force-attacks.

Messages routing mechanisms shall be implemented by using the "whitelist" approach (with "default-deny").

During the implementation of standard protocols, it shall be ensured, that no "downgrade" (e.g. Cipher-downgrade) is possible, i.e. the security mechanisms cannot be lowered by the level specified by the client.

Cryptographic and security mechanisms known as vulnerable and/or weak shall not be used. This also aplies to the mechanisms which are expected to be vulnerable and/or weak by the start of production and/or start of sales.

Every component which includes a cryptographic routine, shall have a means to update or replace the underlying algorithm.
Rationale: Once a cryptographic algorithm gets broken it has to be updated or replaced to a stronger one.

2.6.4.6.9 1.3.6.9 Logging/Monitoring

Credentials or other security parameters shall not be logged.

The contractor should make further suggestions for events that also be held in the security log.

Debug information (in whatever form) that reveals any detailed information regarding components functionality shall not be logged in the production grade device. Any exceptions shall be approved by the client in the written form.

In the course of development, the contractor and the client shall define when and in which form events shall sent to the Event Collector (directly when the event occurs, aggregated, cyclical, ...).

2.6.4.6.10 1.3.6.10 Debugging

The production grade component shall not contain any unprotected maintenance interfaces .

2.6.4.6.11 1.3.6.11 Random numbers

2.6.4.6.12 1.3.6.12 3rd-Party software

The contractor is obliged to check the origin of software, libraries or source code, from third parties and to obtain via secure channels. If cryptographic signature are used for the software components, they must be checked.

The contractor shall integrate regular updates of the 3rd-party software.

The contractor shall ensure that all 3rd-party software is free of any known vulnerability and/or backdoors.

The contractor shall disclose to the client all used 3rd-party software software.

The contractor shall disclose the configuration of the operating system cores (kernel) to the client.

2.6.4.6.13 1.3.6.13 Security Process requirements

2.6.4.6.13.1 1.3.6.13.1 Secure Development process

The contractor shall appoint a contact person responsible for the security risk management.

The contractor shall provide detailed information in a format coordinated with the client with each software release regarding used FOSS.

The contractor shall provide detailed information in a format coordinated with the client regarding all software and hardware components used.

The contractor shall disclose upon request all implemented security measures to the client.

Software components shall be distinguishable by uniquely identifiable software version. When using FOSS, the version numbers from the original source shall be taken over. For the adaptation of FOSS components, the deviation to the original template shall be documented and communicated to the client.

If FOSS components are used, the underlying source code shall be available to the client when requested, if the corresponding FOSS-license permits this.

On request the contractor shall confidentially make available information and documents about implementations on external interfaces (e.g. Bluetooth, Air-Interface), including protocols going through this interfaces and the relevant target applications, to the client for a security review.

The contractor shall provide the client with all needed documents and information about the deployed operation system, services and applications (concepts, design, API etc.).

The contractor shall ensure that the product is only able to be changed by authorized developers and that all changes to the product are understandable at any time (when, who, what has been changed, etc.).

The contractor shall define and apply "secure coding guidelines". These shall be approved by the client.

2.6.4.6.13.2 1.3.6.13.2 Data handling outside of control units

The contractor shall protect the data of the client against unauthorized access, misuse, loss, destruction or change.

The security concept shall be approved by the client. The client reserves the right to check the security concept and its implementation.

Change to the security concept shall be communicated to the client in writing.

User data shall be protected and be used only for the intended purpose.

Data of different users shall be stored separately.

Access to the client's data-base is only permitted after written approval. Access to client's data shall not be passed on to third parties. Subcontractors can only access the data-base as part of their contracting and only and after written approval by the client. In case of the subcontracting ends or the assigned employees leave the project or the subcontractor, access permissions shall be canceled accordingly

The contractor shall inform the client immediately in case of information security or data breach and to coordinate the next steps.

For the information transfer with the client's systems or at the locations of the client, the contractor shall follow the specifications from the Supplier Portal.

The contractor is obligated to inform the client if third parties (insolvency, investigation, etc.) access to the data of the client.
Furthermore, the contractor shall inform the accessing third party that the data belong to the client.

The contractor is obliged to inform the employees and subcontractors with access to data centers of the client, about information security relevant topics.

The contractor shall ensure that the data of the client cannot be accessed by other customers.

The contractor is obliged to further education all employees for information security regularly.

All data classified by the client as "secret" or "confidential" shall be protected by cryptographic measures.

Test data shall be removed from production grade components.

The contractor shall retain the data of the client for two years after termination of the service contract. After the deadline, the data shall be deleted. Upon request from the client, an earlier deletion of the data shall be done by the contractor.

Source code secuirty shall be validated using code analysis tools according to industry best practices.

The contractor is obliged to use the specified security tool and the supplied crypto material (key / certificate) of the client. The used crypto material and Security Tool can be changed in the lifecycle of the control unit / project. The contractor shall be obliged to implement and confirm the update according to the client's specifications.

The contractor agrees that all users which needs access to diagnosis certificates of the client, recorded in it's user repository, and have to apply for access to the certificates. The access rights are issued according to the principle of "least privilege".
The contractor agrees to inform promptly about changes that affect this principle (change of role, termination of employment, etc.).

The contractor shall ensure, that control units do not accept any date/time that is available before the production date.

The contractor shall not store any passwords or secrets in plain text.

2.6.4.6.13.3 1.3.6.13.3 Risk management

The contractor is obliged to perform and document a complete risk analysis for the product to be developed (including the clients requirements specifications and contractors platforms).

In particular, the contractor shall point out, privacy- and safety- threats that results from security compromises.

The contractor is obliged to check for security vulnerabilities ("CVEs") and to monitor them during the life cycle of the product. If a vulnerability is detected, the contractor shall inform

the client immediately and discuss necessary mitigations.

2.6.4.6.13.4 1.3.6.13.4 Pen test

The contractor grants consent that the client may test the items supplied by the contractor (including but not limited to products, systems, hardware, software, data), or have these tested by third parties, for compliance with information technology security requirements, in particular by means of penetration tests. The tests are aimed at individual items or complete systems. The test may include accessing, and hence possibly reproducing and/or editing computer programs, including the source code or other data. This may include data that is not intended for the client and that is specially secured against unauthorized access. To the extent that such testing may violate the rights of third parties to the articles supplied by the contractor, the contractor hereby grants consent also in the name of and on behalf of these third parties.

The contractor is obliged to perform a penetration test. The penetration test shall include all component developed and deployed by the client. The result of the penetration test shall be provided to the client before C-sample phase.

The contractor is obliged to grant the client access to selected source code and related documents for security reviews by the client and by 3rd party companies assigned by the client.

The contractor is required to provide the client or an commissioned third party with the source code as well as all necessary for an automated code scan (SCAS, Source code analysis service).

The contractor is obliged to contribute to partial source code analyses related to the part of the source code owned by the contractor.

The contractor is obliged to assess the analyses’ outcomes in cooperation with the client and, if necessary, to discuss appropriate measures in cooperation with the client.

2.6.4.6.13.5 1.3.6.13.5 Incident management

The contractor is obliged to inform the client of any known vulnerabilities of his products.

The contractor is obliged to cooperate with the client to mitigate known vulnerabilities.

The contractor is obliged to inform the client of vulnerabilities in any 3rd party software within the contractor’s products applied for the client.

2.6.5 Standard Software Architecture

Contact for Standard software
Last name, first name: Koser, Steffen
Department: RD/FEA
Email: Martin.Huber@daimler.com

The contractor shall produce a software architecture for the individual control units / control unit groups in coordination with the client. The following illustration shows an example of software architecture.

2.6.5.1 1.4.1 Block Diagram of Software Components

The contractor shall draw a block diagram with the different software components (e.g. I/O, application and frame software, communication, gateway) and coordinate this with the client.

2.6.5.2 1.4.2 Inclusion of Standardized Software Modules

Standard software modules according to the AUTOSAR standard are used. A complete list and a short description of the standard software modules for a classic AUTOSAR platform are located in the standard [MSS 10730].
A complete list and a brief description of the standard software modules for an Adaptive AUTOSAR platform can be found in [MSS 10731].

The always updated requirements on configuration and integration of an AUTOSAR 4.x stack are available in the Diagnosis Portal in Section “Standard Software / Star 3 / Documentation” within the Document “Integration of AUTOSAR 4.x”. These requirements shall be adhered to.

2.6.5.3 1.4.3 End-To-End Communication Protection (E2E)

All safety relevant signals shall be protected in accordance to: End-to-End Communication Protection [QEV111AES5MSS]

The parameters t_{FD} and t_{FR} shall be agreed with the client for safety-relevant signals:

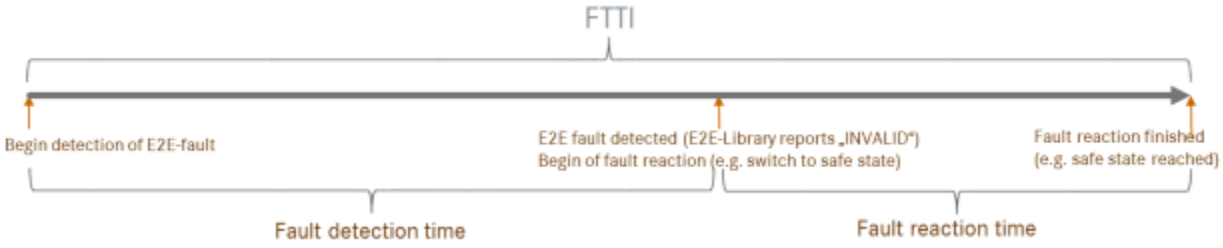


Image: Fault detection time, fault reaction time and fault tolerance time interval

Fault detection time (t_{FD}) is the time span for error detection according to [ISO 26262-1]. In the E2E context: t_{FD} is the basis for E2E parametrization. If t_{FD} is documented in XDIS dialog "Edit Safety Parameters", it can be referenced here.
Fault reaction time (t_{FR}) is the time from fault detection to reaching a safe state according to [ISO 26262-1].
Fault tolerance time interval (FTTI) is the time span in which one or more faults can be present in a system without a dangerous event occurring, according to [ISO 26262-1]. FTTI is defined in the system specification and referenced here.

2.6.5.4 1.4.4 Global Time Synchronization

All control units connected via CAN, CANFD, fLexray or Ethernet take part in global clock synchronization. In addition to the component and system requirement specifications, [MSS 21001] shall be observe.

2.6.5.5 1.4.5 Frame Software Requirements

2.6.5.5.1 1.4.5.1 System-specific functions which have to be mapped to the frame software

- A task configuration under AUTOSAR OS. The tasks record the function calls of the functions which are generated. In addition, a data exchange concept shall be realized for secure data exchange between tasks (e.g. by means of message services)

- Variant decoding allowing selection between different parameter sets and the related initialization.

- Signal conditioning for analog as well as digital input and output signals – for both HW and CAN signals. The signal interface to the functional software includes a substitute value generation for all signals as well as a status byte

- Self test (at system start and cyclical) of RAM/ROM, EEPROM, periphery and CPU

- A function for operating one or several watchdogs. The watchdog can be bound internally (SW watchdog) or externally (HW watchdog). Further a function for releasing a system reset and for the recognition of the reset cause (e.g. power on reset, soft reset, reset by diagnosis request).

- Function for monitoring the system/processor load (e.g. runtime monitoring of tasks) allowing a controlled intervention in the operational sequence if required (e.g. switching off of non-critical functions in case of processor overload)

2.6.5.5.2 1.4.5.2 Interfaces Between Frame and Functional Software

The interface between the frame and the functional software shall be described unambiguously. The mechanisms of data exchange shall be defined and coordinated with the client.

The interface between frame and functional software shall be designed in such a way that the functional software can be developed as independently from HW as possible.

2.6.5.6 1.4.6 Functional Model of the Tasks and Interrupts

The contractor shall subdivide the tasks and interrupts and describe the interfaces between them. This shall be done in coordination with the client.

2.6.5.7 1.4.7 Description of the Time Dependencies

The contractor shall draft a description of the time dependencies between the various tasks and interrupts and coordinate it with the client.

2.6.5.8 1.4.8 Description of Operating Modes

The contractor shall draft a description of the operating modes of the control unit (e.g. normal operation, emergency mode, diagnosis, etc.) and of mode switching and coordinate it with the client.

2.6.5.9 1.4.9 Start-up and Shut-down Behavior

The contractor shall draft a description of the start-up/shut-down behavior and coordinate it with the client.

2.6.5.10 1.4.10 Description of Hardware-Level Interfaces

The contractor shall draft a description of the interfaces of HW-oriented functions which are not covered by standard software (e.g. PWM actuation, analog/digital I/O, SPI, etc.) and coordinate it with the client.

2.6.5.11 1.4.11 Memory Layout

The contractor shall draft a description of the memory layout (definition of global and local variables, visibility/encapsulation, consistent data for interruptible tasks, applicable parameters) and coordinate it with the client.

2.6.5.12 1.4.12 Requirements for the Use of Resources

The contractor shall plan and determine the resource usage in coordination with the client.

At the time of production start-up, no more than 80% of the processor resources (RAM, ROM,

EEPROM and calculating time) shall be used up. At the beginning of the C-sample phase, no more than 60% of the processor resources shall be in use.

2.6.5.13 1.4.13 Compliance with Standards

The following guidelines and standards shall be taken into account at least in the software development.

- MISRA C Guidelines [MISRA C]

- ISO/ANSI C Programming

2.6.5.14 1.4.14 Variant Manager

The contractor shall introduce a variant manager, which is able to recognize the vehicle model and the national variant on the basis of the related communication message. If this involves a MOST component, the contractor shall coordinate initialization with the client.

2.6.6 Implementation Defaults

2.6.6.1 1.5.1 Sub Module Structure

2.6.6.2 1.5.2 Sub Module Requirements

2.6.7 Quality Requirements

2.6.7.1 1.6.1 Quality Management

Contact for Software quality management
Last name, first name: 1935267: VAR_SWQM_NAME_1502Klink , 1935266: VAR_SWQM_VORNAME_1502Andreas
Department: 1935265: VAR_SWQM_ABTEILUNG_1502MP/EK4
Email: 1935264: VAR_SWQM_EMAIL_1502andreas.a.klink@daimler.com

The contractor must keep the standardized requirements in Chapter "Elements of the EE and software quality management system" of the document [LHV 310 001] at the requirements ID CRQ-2005.

2.6.7.2 1.6.2 Performance

Quality performance KPIs shall be suggested by the contractor and discussed with the client.

The quality performance KPI report shall be available latest 4 weeks after project start.

The quality performance KPI report shall be available at any time. KPIs shall be updated at least once per day.

2.6.7.3 1.6.3 Operational Safety

All items of this chapter are treated as “operational safety”.

The contractor shall ensure that the illuminators of the MPIC causes no damage to eyes. We call this eye safety.

The contractor shall evaluate if the illuminators of the MPIC can cause damage to eyes. This evaluation shall consider normal operation, all relevant single point failures and common cause failures affecting the illumination (e.g. lighting permanent on, damage of front cover of the MPIC).

The requirement described in this chapter shall apply in all situation (e.g. all driving scenarios, leaning towards the MPIC, car assembly, component replacement in service, child playing in vehicle, cockpit cleaning, usage of optical aids such as magnifiers or binoculars).

Eye Safety shall be certified with the assistance of an independent external and certified measurement service provider.

The details of the evaluation described in this chapter shall be discussed with the customer.

A report of the evaluation described in this chapter shall be provided to the customer.

The illuminators of the MPIC shall work in conformance with DIN EN 62471/IEC 62471, so that there is no impairment of the driver, any passenger, any person in or outside the vehicle, and any animal in or outside the vehicle and at any time.

The illuminators of the MPIC shall work in conformance with IEC 60825, so that there is no impairment of the driver, any passenger, any person in or outside the vehicle, and any animal in or outside the vehicle and at any time.

The operational safety shall be fulfilled independent of the distance of the eyes of any person to the MPIC.

Operational safety shall be fulfilled independent of the duration of exposure by the MPIC of the eyes of any person.

Operational safety shall be fulfilled independent of the configuration settings (e.g. false exposure settings) of the MPIC.

Measures to fulfill operational safety shall be reported to the customer.

The contractor shall provide documentation and measurement reports showing the operational safety that is fulfilled with any hardware delivery (e.g. A-sample, B-sample, C-sample, D-sample, series production sample).

The contractor shall implement measures to avoid eye damage during operation and in case of any single point failure or common cause failure. (e.g. detachment of the diffuser, damage or partial damage of the diffuser, damage to the illumination driver).

The requirement described in operational safety shall be fulfilled in combination with any connected hardware (e.g. FrameGrabber, CIVIC ECU, other ECUs)

The requirement described in operational safety shall be fulfilled with measures only in the MPIC camera head. No ECU software shall be required.

Eye safety shall be guaranteed indepentently of the camera software running on the connected ECU.

The contractor shall implement measures to decrease the light emission (average power and/or peak power) below the limits described in operational safety if the MPIC detects complete or partial blockage.
(e.g. by decresing the frame rate, by decreasing the emitted optical power)

The measures described in operational safety shall be suggested by the contractor and coordinated with the customer.

The contractor shall implement and verify the measures defined in operational safety to ensure eye safety for all samples delivered to the customer.

All required measures to guarantee eye safety shall be implemented in the MPIC.

The contractor shall design the illumination supply and control circuit such, that eye safety is guaranteed with any illumination setting.

The MPIC shall guarantee eye safety in any operating mode (e.g. any configuration, any frame rate, any exposure time).

All touchable surfaces of the driver camera shall be safe to touch.

The contractor shall evaluate if the touchable surfaces of the driver camera are safe to touch.
This evaluation shall consider normal operation, all relevant single point failures and common cause failures.

The surface of the driver camera shall be safe to touch in accordance with IEC 60950-1, so that there is no impairment or injury of the driver, any passenger, any person and any animal and at any time.

2.6.8 Scope of Delivery

2.6.8.1 1.7.1 Contractor's Software Components

The contractor shall supply all function-necessary software components, which he provides.

2.6.8.2 1.7.2 Third Party Software Components

The contractor shall supply all function-necessary software components, which a third party provides. Deviations are to be coordinated with the client.

2.6.8.3 1.7.3 Licenses

The contractor shall supply all licenses software components, which are necessary for the use of the software. Deviations are to be coordinated with the client.

2.6.8.4 1.7.4 Free and Open Source Software

Free and Open Source Software (FOSS) encompasses all software that is, in principle, available at no cost and which is subject to a license or other contractual provision (FOSS License) that, as a requirement for modifying and/or distributing the software and/or any other software associated with or derived from this software (FOSS Derivative), contains at least one of the following conditions:
- the source code of such software and/or FOSS Derivatives must be made freely available to third parties; and/or
- third parties must be allowed to create products derived from such software and/or FOSS Derivatives; and/or
- third parties must be provided with authorization keys required for the installation of such software; and/or
- certain information or documents, such as license text, must be included in the product documentation and/or other materials provided along with the software.

Examples: FOSS Licenses include, e.g., the "Berkeley Software Distribution License" (BSD license), the "GNU General Public License" Version 2 (GPL V2) or the "GNU Lesser General Public License" Version 2.1 (LGPL V2.1).

Goods or services from the contractor may include FOSS only after a prior approval of the client and by observing the procedure described in [FOSS0001].

The contractor shall provide the fully and correctly completed form [FOSS0002] to the client prior to the usage of FOSS or to state that no FOSS is used at all.

2.6.8.5 1.7.5 Software Compliance

Software development shall be based on the principles specified in the Software Compliance Guide. This can be obtained via the Daimler Supplier Portal [ALD00001132].

In the documentation, it must be understandable for third parties how the software Compliance Guide is applied and the application has led to the result. The documentation must be complete and correct.

2.6.8.6 1.7.6 Software Data

A standard file designation is defined for the software data (and, if applicable, for the Zip files). This corresponds to the convention defined in the document [LHV 310 001], Chapter "Supplements for E/E Processes" at the requirements ID CRQ-486.

The following scope of delivery of the software data is required:

Software source file (*.hex, *.bin, *.mot, etc), scope of delivery

Software source file (*.hex, *.bin, *.mot, etc.), container format: zip

Telematics file, scope of delivery

Telematics file, container format: zip

Data application files for software source file in an ODX-F file (format 2.2.0), scope of delivery

Data application files for software source file in an ODX-F file (format 2.2.0), container format: zip

Delivery notes, scope of delivery

Delivery notes, container format: zip

Checksums for software source file, ODX-F, Security.def, scope of delivery

Checksums for software source file, ODX-F, Security.def, container format: zip

2.6.8.7 1.7.7 Software Documentation

The contractor shall carry out documentation of the component software according to the requirements in the technical KLH and shall take the following points into consideration:

- Tool (software tool, version, etc.)

- Program listing

- Module description

- Flow chart

- Interrupt structure

- Description of variables with standardization and range of values

- Description of the range of values

- Test specification

- Quality assurance measures (definition regarding type and scope at start of project)

- Software back-up / storage

- ECU diagnostic specifications (diagnostic protocol, supported diagnostic services, diagnostic data)

- Result of the software check in accordance with [MISRA C], including detailed description and justification of all deviations.

2.6.8.8 1.7.8 Interface Documentation

The contractor shall deliver a documentation of all interfaces between the software components involved.

2.6.8.9 1.7.9 Test Documentation

The contractor shall deliver a test documentation in accordance with CRQ-2016 chapter "Tests of E/E and Software" in the document [LHV 310 001].

2.6.8.10 1.7.10 User Documentation

The contractor shall deliver a user documentation.

2.7 General E/E Requirements
2.8 Fire Prevention
3 Contacts and Responsibilities

The contractor shall provide his contacts and responsibilities in his offer. Especially shall the contractor shall name his Representative, substitute of the Representative as well as all Subrepresentatives.

3.1 Client's Contacts

The contact persons for the client are listed in the following section.

PLEASE ADD HERE CONTACT DATA OF FUNCTION OWNER, TEAMLEADER, REPRESENTATIVE and SUBREPRESENTATIVES OF FUNCTION XY.

Component Manager
E-mail: 7179155: VAR_KOMPVERANTW_EMAIL_1498»...«

After-Sales
E-mail: 7178057: VAR_AFTERSALES_EMAIL_2698»...«

Product Cost Engineering
E-mail: 7176494: VAR_KAUFTEILEPL_EMAIL_3949»...«

Small Part Optimization (KTO)
E-mail: 7176348: VAR_KTO_EMAIL_2696»...«

Logistics
E-mail: 7178190: VAR_LOGISTIK_EMAIL_1507»...«

Materials Purchasing
E-mail: 7178673: VAR_MATERIALEK_EMAIL_1506»...«

Assembly
E-mail: 7175497: VAR_MONTAGE_EMAIL_3950»...«

Test Equipment (Geometry)
E-mail: 7175691: VAR_PRUEFMITTEL_EMAIL_2697»...«

Test Equipment (E/E)
E-mail: 7178117: VAR_PRUEFMITTEL_EMAIL_6814»...«

Quality Management
E-mail: 7178050: VAR_QUALIMANAG_EMAIL_1504»...«

Tool Specification for Prototype Parts
E-mail: 7178451: VAR_WERKZEUGSPEZ_PROTO_EMAIL_4199»...«

Functional Safety
E-mail 7177406: VAR_FUSI_EMAIL_5387»...«

3.1.1 Client's Contacts Mercedes-Benz

Representative

Last name, first name:

Email:

Substitute Representative

Last name, first name:

Email:

Subrepresentative

Last name, first name:

Email:

Function Owner

Last name, first name:

Email:

Project Manager CIVIC I2 and RSU (Gen20x - project overall)

Last name, first name: Hammori, Markus

Email: markus.hammori@mercedes-benz.com

Project Manager IVI i4 (Gen20x - project overall)

Last name, first name: Watermann, Stefan

Email: stefan.watermann@mercedes-benz.com (Extracted an unsupported link: mailto:stefan.watermann@mercedes-benz.com)

Software Project Lead IVI i4

Last name, first name: Schuster, Detlef

Email: detlef.d.schuster@mercedes-benz.com (Extracted an unsupported link: mailto:detlef.d.schuster@mercedes-benz.com)

Software Architect

Last name, first name: Thaler, Andres

Email: andres.thaler@mercedes-benz.com (Extracted an unsupported link: mailto:andres.thaler@mercedes-benz.com)

Infotainment Security Gen20x CIVIC I2

Last name, first name: Karger, Martin

Email: martin.karger@mercedes-benz.com (Extracted an unsupported link: mailto:martin.karger@mercedes-benz.com)

Infotainment Security Gen20x CIVIC I3

Last name, first name: Shenoy, Murali Nagarkar

Email: murali_nagarkar.shenoy@mercedes-benz.com (Extracted an unsupported link: mailto:murali_nagarkar.shenoy@mercedes-benz.com)

Materials Purchasing

Last name, first name:

Email:

3.1.1.1 Software Quality Management

Last name, first name:

Email:

Last name, first name:

Email:

Last name, first name:

Email:

3.1.2 Client's Contacts MBition

Head of Ececutive Body/ CEO

Last name, first name: Preidel, Frank

Email: frank.preidel@mercedes-benz.com

Software Architect

Last name, first name: Thelin, Johan

Email: johan.thelin@mercedes-benz.com

Software Architect

Last name, first name: Hakki, Sadri

Email: sadri.hakki@mercedes-benz.com

Project Manager MBiENT, Gen20x CIVIC I2 Software

Last name, first name: Sturza, Bogdan-Iancu

Email: bogdan-iancu.sturza@mercedes-benz.com

Project Manager MBiENT, Gen20x CIVIC I3 Software

Last name, first name: Alokbi, Nourhan

Email: nourhan.alokbi@mercedes-benz.com

Project Manager MBiENT, Gen20x RSU Software

Last name, first name: Völzke, Christian

Email: christian.voelzke@mercedes-benz.com

External Partner Management

Last name, first name: Andreadis, Simon

Email: simon.andreadis@mercedes-benz.com

Quality

Last name, first name: Kallur, Sachin

Email: sachin.kallur@mercedes-benz.com

Security

Last name, first name: Islam, MoinulEmail: moinul.islam@mercedes-benz.com

Software Factory, CI/CD

Last name, first name: Kremer, AlexanderEmail: Alexander.Kremer@mercedes-benz.com

3.2 Project Responsibilities

The contractor shall maintain an "open points" list, to include a measure tracking system. On request, the contractor shall allow the client to inspect the open points list and the measure tracking system. On request, the contractor shall provide the scopes relevant to the client once or at intervals to be defined (e.g. weekly) to the client in electronic form.

The contractor shall designate a project manager for the project who shall coordinate and monitor the processes within the contractor's organization and act as the interface to the client.

Which project partner assumes which responsibilities in the project is defined in the following list.

The following designations are used in the responsibilities list.

Abbreviation	Description
I = information	It is absolutely essential that the partner concerned be informed by the party responsible about any changes or new results
C = cooperation	Provision of appropriate support for the party responsible on request by one or more of the companies involved in the project
A = acceptance	The partner concerned shall accept the result or decision-making basis
C/A = check & approve	Checking/approval of results or decision-making bases
R = responsibility / execution	Is responsible for the provision of the services for providing results or the facts of the decision

Parts history

Client: A, I

Contractor: R

Process FMEA

Client: C/A, I

Contractor: R

Product FMEA

Client: C/A, I

Contractor: R

Functional safety

Client: C/A, A

Contractor: R

In the event of a system break-up (tier-n is specified by client), the following regulations apply to development cooperation.

A,C,K = directed part type according to directed part mark of system agreement from the source package (A = standard)

Item	Description	Client			Tier 1			Tier n		
		A	**C**	**K**	**A**	**C**	**K**	**A**	**C**	**K**
1	Creation and release of deadlines, milestones, target corridors, functional scopes, quality standards, dimensional specifications, data records for the tier-n scope	R	R	R	I	I	I	C	C	C
2	Design engineering responsibility for the overall tier-1 function (incl. tier-n scope)	A	A	A, C	R	R	R	C	C	I
3	Design engineering responsibility for the function of the tier-n scope (= directed part)	A	A	R	C	C	C	R	R	C
4	Creation and approval of specifications and requirement specifications for tier-n scope	R	R	R	C	C	I	C	C	C
5	Responsibility for tier-n component, functional properties in accordance with the stipulations of the requirement specifications	-	-	R	-	-	I	R	R	C
6	Responsibility for achieved performance: Integration (installability) of tier-n scope into tier-1 scope	C	A	A, C	R	R	R	C	C	I
7	Function testing of tier-n scope in accordance with the stipulations of	A	A	R	R	I	I	C	R	C

	the requirement specifications									
8	Tier-1 responsibility for the tier-n scope regarding quality characteristics (e.g. gap dimensions)	A	A	R	R	R	I	C	C	C
9	Responsibility for the tier-1 scope (incl. overall tolerances and interaction with vehicle)	C/A, A	C/A, A	A	R	R	R	I	I	I
10	Commissioning and payment of prototype parts & tools for the clientincl. tier-n scopes The criterion is the receipt of tier-n scope goods at the client	R	R	R	-	-	-	I	I	I
11	Provision of trial parts, tools, and fixtures for meeting the component requirement specifications & function specifications (LEK-E content) incl. tier-n scope (in line with DC Calc) The criterion is no receipt of tier-n scope goods at the client	A	A	A	R	R	R	I	I	C
12	Change management for the tier-n scope. Important: Changes may also be necessary in the tier-1 scope	A	A	R	R	C	C, I	C	R	C
13	Change management for tier-1 scope	A	A	A	R	R	R	I	I	I
14	Performance of design FMEA for tier-n scope (if required)	I	A	R	A	I	I	R	R	C
15	Performance of design FMEA for tier-1 scope incl. tier-n scope	A	A	A	R	R	R	-	-	C
16	Execution of the issue resolution process for tier 1 including tier-n scope (= component part) in the case of flaws in design engineering	A	A	A, C	R	R	R	C	C	I
17	Execution of the issue resolution process for tier-n scope in the case	A	A	R	R	I	I	C	R	I

	of flaws in design engineering									

3.3 Requirements for Development-Related Services

Definitions to reaction time and supporting functions are described in chapter 2.6 "Important project specific requirements" (20XSW-486).

Requirements pertaining to the deployment of contractor staff at the client's operations for work that is not specifically related to the contract are void. The costs thereof shall not be included in the quotation submitted by the contractor. The contractor shall explicitly reject such requirements.

The following section describes tasks that shall be performed by the contractor as part of the development of the scope specified in these requirement specifications.

Specification of a response time means that the contractor, following receipt of the facts of the situation from the client, shall be able to carry out the described task or to begin processing by no later than the end of the required response time.

Specification of a processing time means that the contractor, following receipt of the facts of the situation from the client, shall have fully completed the given task within the given processing time.

In cases where a processing time is given but the contractor is not able to complete the task within the requirement processing period, the contractor shall provide prompt notification of this to the client.

The communication of problems or feedback on results shall often be done using vehicle parts or measuring equipment located on the premises of the client. For the following tasks, it shall be ensured that communication can take place on the premises of the client.

The contractor shall conduct fault analyses (e.g. vehicle measurements).
Response time: 7176747: VAR_FEHLER_REAKTIONSZEIT_4665»One workday«

The contractor shall troubleshoot and eliminate faults in the overall system (as part of the system integration hardware-in-the-loop and/or in the vehicle).
Response time: 7175793: VAR_BESEITIGUNG_REAKTIONSZEIT_4666»One workday«

The contractor shall identify faulty components that are part of the overall system.
Response time: 7176327: VAR_IDENT_REAKTIONSZEIT_4667»One workday«

The contractor shall participate in/carry out the detection and description of faulty performance, in particular in cases of failures in the field, in such a way that the fault can be processed in an optimum manner using the contractor's procedures.
Response time: 7177419: VAR_ERFASSUNG_REAKTIONSZEIT_4668»One workday«

The contractor shall participate in/carry out the execution of vehicle campaigns/vehicle updates aimed at the elimination of identified faults by the client's workshops.
Response time: 7176707: VAR_ORGA_REAKTIONSZEIT_4669»One workday«

The contractor shall participate in and/or execute board tests and system/vehicle integration tests, including EMC vehicle tests.
Response time: 7178436: VAR_TEST_REAKTIONSZEIT_4670»One workday«

In cases where the expertise of the contractor is absolutely essential as part of a test drive, the contractor shall provide a contact to participate in such a test drive.
Response time: 7175578: VAR_VERSUCH_REAKTIONSZEIT_4671»One workday«

The contractor shall carry out the flash programming and coding of development samples on

the client's premises.
Response time: 7176965: VAR_FLASHEN_REAKTIONSZEIT_4672»One workday«

The contractor shall prepare, check and maintain vehicle checklists for the scopes concerning the contractor.
Processing time: 7178639: VAR_CHECKLISTEN_REAKTIONSZEIT_4673»Within one work week«

For scopes under the contractor's charge, the contractor shall perform data input for the client's data systems. The following systems shall be considered in detail:
7178954: VAR_SYSTEME_4674»Systems«

Data input for wiring harness using LCable.
Response time: 7176227: VAR_KABEL_REAKTIONSZEIT_4675»One workday«

Data application for EPDM (for component data, especially pinning) Response time: 7175530: VAR_KOMPDATEN_REAKTIONSZEIT_4676»One workday«

The contractor shall prepare, check and maintain the component testing station on the premises of the client.
Processing time: 7176587: VAR_KOMPLATZ_REAKTIONSZEIT_4677»Within one work week«

7178107: VAR_AUFGABEN_4678»Additional task«

3.4 Protection Requirements for Handling Vehicles and/or Components before Press Announcement Day (PAD)

If the services described in these specifications require the contractor's and/or subcontractor to handle vehicles and/or components before the respective PAD, the contractor shall meet the "Minimum Requirements for Prototype Protection for Third Parties (incl. Suppliers)" or demonstrate TISAX certification with the "Prototype Protection" add-on module.
The current version can be obtained from the Supplier Portal: https://supplier.mercedes-benz.com > General Supplier Documents

4 Deadlines, Tools and Components in the Development Process

4.1 Parts Delivery and Commissioning of E/E Scopes

4.1.1 Delivery for Virtual E/E Integration

The objective of the virtual E/E integration model is to virtually validate product functions as completely and realistically as possible. To increase the maturity level of the functions for integration in the vehicle at an early stage, the control units are required in the form of a virtual ECU. This is intended to eliminate faults in advance and virtually validate basic technologies as a component test or with customer functions already in combination.

For virtual E/E integration, the contractor shall provide the client with control unit software and the associated other simulation data in a coordinated format. Details on this are provided in the [SW-HB] in the MB.OS Portal ".

Virtual ECUs (or parts thereof) can be created with different programs, which are additionally available in different version statuses. The client shall therefore define the version and the compatibility matrix of the program/tool environment at the start of the project and coordinate this with the contractor.

4.1.1.1 Documentation

The contractor shall provide a release description for each virtual ECU (or part thereof)

delievered. The exact format and content of the release description shall be agreed with the client at the beginning of the project.

The contractor shall document the validation of the virtual ECU (or parts thereof) and provide it to the client.

4.1.1.2 Scope of virtual ECU (vECU)

Specific levels of the virtual ECUs should be created for different project phases. For the definition of the level, see CRCS - 5949058 in [LHV 310 00x].

If the contractor is only responsible for part of the virtual ECU, it shall deliver its share of the control unit software in digital form for integration into a virtual ECU in different expansion stages. Details on this will be provided in the [SW-HB] in MB.OS Portal.

If basic technologies are required and must be tested, at least one Level 3 control unit (see CRCS - 5949058 in [LHV 310 00x]) containing the software components relevant for the respective BROP release shall be supplied. Details shall be discussed with the client.

If application software and functions are required and must be tested, a Level 3 control unit (see CRCS - 5949058 in [LHV 310 00x]) shall be supplied. However, a level 1 control unit can also be supplied. Details shall be coordinated with the client.

4.1.1.3 Creation Process

The virtual ECU must be created as vTT, QEMU, Silver Unit or FMU 3.0 (A combination of complex control units is also permissible; this shall then be delivered individually or integrated in coordination with the client).

Development shall take place in accordance with the AUTOSAR standard and the version agreed in advance between the client and contractor. Deviations from this shall be discussed with the client and documented.

The contractor shall provide proof of its virtualization strategy. This contains at least one insight into the organizational structure for virtualization and the virtual ECU build process.

If it is a vTT virtual ECU, the vector approach with regard to the basic software configuration shall be used for the simultaneity formation of the virtual and the real control unit. Reconfiguration or reconfiguration shall be avoided. If this approach is not applicable for any reason, the resulting deviations shall be coordinated with the client.

If it is a vTT virtual ECU, the latest version of vVIRTUALtarget must be used. Deviations from this shall be coordinated with the client.

If it is a Level 3 Silver control unit, the client shall provide a virtual ECU build and simulation environment. This contains the MB.OS base layer and must be used to create a virtual ECU. Deviations in development with the environment shall be discussed with the employer.

The build and simulation environment provided serves as the basis for the integration, testing and validation of the delivery of a Level 3 Silver control unit of the contractor. It sets standards for handling this type of virtual ECUs and thus ensures integration capability in the MB.OS environment.

The following 3 criteria must be observed when developing a Level 3 Silver control unit:

- One-layer architecture for complex device drivers and other non-standard components to enable porting.
- Hardware-dependent code shall be developed closed in the smallest possible functions with a defined static interface.

- The contractor shall ensure substitute functions with equivalent functionality for target-specific codes.

4.1.1.4 Delivery of a virtual ECU

A virtual ECU, including its simulation and metadata, is delivered in the MB.OS portal, see [SW-HB].

The delivery times are determined by the milestones in the project schedule and can be taken from it.

Virtual ECUs can also be delivered between the required delivery times in order to utilize the existing test infrastructure in the MB.OS portal.

The one-time delivery of an "A-shaller" is due after one third of the time between the assignment of the control unit to the contractor and the first hardware delivery. This A-sample is used to assess the functionality and state of development of the virtual ECU. The client can thus detect problems in virtual development at an early stage.

The A-sample should support the core scope of the control unit buses and selected applications that are defined by the supplier. This definition must be documented.

4.1.1.5 Testing of Virtual ECUs

Virtual ECUs are used to intercept faults at an early stage and provide test support in the event of a hardware defect. The MB.OS portal can be used for testing. In the test area of the portal, more precise details in the [SW-HB], virtual ECUs can run through test pipelines.

If basic technologies are to be validated, they must be tested according to [MSS 30003]. This also describes the required tests for a virtual ECU.

In the case of virtual ECUs with basic technology, an automatic SMOKE test is performed in the MB.OS portal to ensure a minimum requirement for the quality of the delivery. This SMOKE test is described in [SW-HB].

If the virtual ECU has an application part, a SMOKE test must be defined with the client. It should ensure for both Level B and Level 3 that the vECU is accessible and simple communication can take place. Everything else is component-specific and shall be agreed between the contractor and client. The test reports of the SMOKE test must be submitted at the point specified by the client.

For diagnostic capable ECU, the diagnostic interface shall be implemented in the virtual ECU for communication with an external tester. The scope of diagnosis shall be agreed in advance with the client.

4.2 E/E Maturity Management

The development of the component is release-based.

The Excerpt from the Process Master Plan for suppliers contains the dates for the hardware cycles (HWC) and main releases at the beginning of development (e.g. BROP B1) and minor releases (e.g. BROP B1.1). In the course of development, software provision will be switched to sprint-based development. The sprints, named S-<YY><KW> (where <YY> year and <KW stands for calendar week, e.g. S23-17) are also shown in the process master plan.
It is mandatory that a new software version will be provided for each sprint after an NCD change. Additional new software versions can be deployed in subsequent sprints.

The planning of the content required per release is carried out in two release plans, namely the FROP (Feature Rollout Plan), which describes the assignment of the required functions to

the individual releases, and a BROP (Basic Technology Rollout Plan) that provides the assignment of the required basic technology to the individual releases.

The FROP is component-specific and is provided as an Excel table.

The BROP is uniform across components and is described in the document [MSS 30003].

If a test suite is referenced in the BROP [MSS 30003], the contractor is obliged to hand over the results of the test suite together with the respective release status.

In accordance with the requirements CRCS-3340091 in document [LHV 310 00x], the contractor is obliged to incorporate the requirements of FROP and BROP in its release planning and to inform the client immediately in event of deviations.

Six weeks before the respective release date, the contractor shall notify the client of the degree of maturity of the required content for the release date.

5 Documentation

The contractor shall continuously document the development status of the scope of supply as specified in the requirements given here. On request, the contractor shall allow the client to inspect this documentation.

The contractor shall prepare thorough and comprehensive documentation of the scope of supply and services described in these requirement specifications. This shall comply with all legislation, regulations and technical standards applicable to the full performance or partial performances.

The contractor shall deliver the technical documentation at the latest upon acceptance by the client of the supplies and services. If requested to do so prior to acceptance, the contractor shall deliver completed sections of the technical documentation covering both the full performance or individual performance units.

Prior to acceptance of the full performance or of any one performance unit, the client can demand to examine the methods, systematics and internal processes that the contractor used or will use to produce the technical documentation.

For this component, requirements with integrity levels exist. These shall be developed and documented as specified in the document [LHV 310 00x] under Requirement ID CRCS-3340251.

5.1 Special Characteristics (Part 1) - Safety-Relevant Characteristics

As it currently stands, DS identification on the drawings or in the documentation systems is not compulsory for this component. If DS characteristics prove relevant to documentation for the client or the contractor during the course of development, the type and time of identification shall be coordinated and documented in writing in an agreement – more detailed instructions will be issued in this respect if required.

5.1.1 Implementation of Safety-Relevant Characteristics

This component is subject to obligatory identification and documentation with regard to safety relevance using code DS at the drawing level and in the documentation systems in accordance with chapter "Safety-Relevant Characteristics" in the document [LHV 310 00x] under requirement ID CRCS-3340230.

The following list contains further subdivisions and the corresponding DS characteristics to be identified and documented for the client in accordance with [MBN 10317-0] and [MBN 10317-4] . Multiple items may be named.

Part: 7176063: VAR_TEIL_1545»...«

Characteristic with DS: 7178399: VAR_MERKMAL_MIT_DS_1546»...«

The required standards are as follows:

[MBN 10317-0]: CAD Drawings/ 3D-CAD-Models - Documentation Requirement - Identification of Parts, Assemblies, and Special Characteristics - Principles - Obligation to Component/Assembly Documentation

[MBN 10317-4]: CAD Drawings/ 3D-CAD-Models - Documentation Requirement - Identification of Parts, Assemblies, and Special Characteristics Specific Values and Application Cases (MBC, VAN)

If, during the course of development (incl. further development during the series production phase), further characteristics prove identification- and documentation-relevant for the client or the contractor, the type and time of identification shall be coordinated and documented in writing in an agreement.

5.2 Special Characteristics (Part 2) - Certification Relevant Characteristics (DZ)

As it currently stands, DZ identification on the drawings or in the documentation systems is not compulsory for this component. If DZ characteristics prove relevant to documentation for the client or the contractor during the course of development, the type and time of identification shall be coordinated and documented in writing in an agreement – more detailed instructions will be issued in this respect if required.

5.2.1 Implementation of Certification Relevant Characteristics

This component is subject to obligatory identification and documentation with regard to safety relevance (incl. emission relevance) using code DZ at the drawing level and in the documentation systems in accordance with Chapter "Certification Relevant Characteristics (DZ)" in the document [LHV 310 00x] under requirement ID CRCS-3340241.

The contractor shall moreover take into account the general certification requirements (e.g. CCC = China Compulsory Certification,Voluntary Certification or Self Declaration) in Chapter "Laws, Standards and Regulations" of the document [LHV 310 00x] under requirement ID CRCS-3341065 (see also [MBN 10317-2]).

The following list contains further subdivisions and the corresponding DZ characteristics to be identified and documented for the client in accordance with [MBN 10317-0] and [MBN 10317-2]. Multiple items may be named.

Part: 7176063: VAR_TEIL_1545»...«

Characteristic with DZ: 7176909: VAR_MERKMAL_MIT_DZ_1548»...«

The required standards are as follows:

[MBN 10317-0]: CAD Drawings-Zeichnung / 3D-CAD Models - Documentation Requirement - Identification of Parts, Assemblies, and Special Characteristics - Principles - Obligation to Component/Assembly Documentation

[MBN 10317-2]: CAD Drawings/ 3D-CAD Models - Documentation Requirement - Identification of Parts, Assemblies, and Special Characteristics Specific Values and Application Cases MBC, VAN , and Buses)

If, during the course of development (incl. further development during the series production

phase), further DZ characteristics prove identification- and documentation-relevant for the client or the contractor, the type and time of identification shall be coordinated and documented in writing in an agreement.

5.3 CAD Product Data Management and Documentation
5.4 Digital Development

The document [LHV 310 00x] lists general requirements pertaining to the provision of simulation data under CRCS-3340488.

6 Supplementary Specifications

This chapter is not relevant for SW deliveries in Headunit.

6.1 Agreed Deviations

If agreed deviations have been defined, delete this object and fill in the chapter accordingly.

6.2 Additional Information

If additional information has been defined, delete this object and fill in the chapter accordingly.

7 List of Abbreviations
8 Other Applicable Documents

The following list contains documents created by the client or external bodies. If a version or issue date is specified for a document, this version applies.
If no version or issue date is specified for a document, the following regulation applies:

- If the document is an external or company standard (namely MBN, DBL, software manual [SW-HB] or function specification), the latest version applies to ensure that the standardization subject corresponds to the recognized state of the art at the time of publication and after revision of the standard.
- If it is another document, the version of the document that was current at the time of signing the development contract belonging to the requirement specifications applies.

The contractor shall check that the referenced standards are up-to-date and take them into account in the tender. Should these standards change during the course of development, the contractor shall reveal the significance of such changes in terms of scheduling and costs.

Documents, standards and other applicable documents referenced in the KLH created by the client are made available to the contractor in the Standards Information System (DocMaster). Externally created standards (e.g. ISO, DIN, VDA, etc.) shall not be provided by the client to the contractor for copyright reasons. Externally created standards shall be independently obtained by the contractor.

The system can be accessed from the supplier portal in the Internet at the following link:
https://contractor.mercedes-benz.com

List of Other Applicable Documents: