OCORA

Open CCS On-board Reference Architecture

PoC Configuration Management
Concept

Document ID: OCORA-TWS15-060

Version: 0.10

Date: 07.06.2023

Management Summary

This concept describes the approach and the state of TWS15: Prototyping Configuration Management Concept is described. Within this workstream a proof of concept of the OCORA Configuration Management Concept in the form of a prototype is carried out.

In the first, currently ongoing phase, the underlying Configuration Management Concept discussion paper is reviewed by the industry partner. This finalised concept, as well as the test cases to be carried out to prove its suitability, will subsequently be used by the industry partner to develop the necessary specifications for the prototype to be implemented.

Following the construction of the prototype hardware and the implementation of the necessary software functions, tests are carried out to prove the feasibility of the OCORA Configuration Management Concept from the proof of concept are documented and taken into account in the Configuration Management Concept.

Revision history

Version	Change Description	Initial	Date of change
0.1	▪ Initial draft		07.06.2023

Table of contents

Table of figures

Table of tables

Empty.

References

Reader's note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references to external documents. Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). OCORA always reference to the latest available official version of the SUBSET, unless indicated differently.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-040 – Feedback Form

[3] OCORA-TWS07-060 – OCORA Configuration Management - Concept

1 Introduction

1.1 Purpose of the document

The purpose of this document is to describe the proof of concept of the OCORA Configuration Management Concept.

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [2].

1.2 Applicability of the document

The document is currently considered informative but may become a standard at a later stage for OCORA compliant on-board CCS solutions. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

1.3 Context of the document

This document is published as part of the OCORA Release 4, together with the documents listed in the release notes [1]. This document describes the concept and the way forward to gain the expected experience in Workstream 15 of the OCORA project.

2 Objectives of TWS15: Prototyping Configuration Management

Within the framework of the OCORA project, a concept [3] for configuration management was developed and published in the previous release within the Technical Workstream TWS07 Modular Safety, CENELEC, RAM. The concept describes how updates to the software of Building Blocks of the CCS subsystem and their configuration are prepared, initiated, executed and validated.

The goal of the Technical Workstream TWS15: Prototyping Configuration Management is to implement and validate the OCORA Configuration Management Concept by setting up a demonstrator. Gains in knowledge and experience are to be incorporated into the concept of TWS07.

The demonstrator is being carried out together with an experienced company from the railway industry supplying hardware and software components for safety-relevant functions on rail vehicles. The Lyss (CH)-based company Selectron Systems AG could be contractedfor its implementation.

3 ApproachProceeding

3.1 Review of OCORA Configuration Management Concept

The first step of the TWS is a review of the existing version of OCORA Configuration Management Concept by Selectron Systems staff.

Up to now, remote updates on SW parts of rail vehicles have only been implemented to a very limited extent in the railway sector. The workstream is not aware of any examples of over-the-air software updates, particularly for functionalities that are relevant to safety.

Therefore, the aim of the review is to compare the view and procedures of the OCORA concept with the knowledge and experience of the industry and to adapt the concept to best practices as far as possible without negative influence on the functionality. This would simplify later consideration of the concept on a broad scale.

The discussion in detail concerns the following content:

Review and discussion of the process management under the following conditions

- Delineation of the concept's horizon of consideration
- Ensuring remote updates from different HW hierarchy levels
- Ensuring remote updates for functionally dependent Building Blocks
- Analysis and adaptation of the procedure to ensure the highest possible availability".

Definition of activation conditions for the distribution and installation of an update

- for the Configuration Manager
- for the Building Blocks

Definition of the exported integration, operation and deployment constraints

- Narrowing down the applicability of the concept
- Definition of integration conditions
- Monitoring, checks and tests by personnel
- Necessity of manual procedures and processes in case of failure

Assignment of resulting responsibilities per role

Following the review and the associated discussion, the concept will be adapted, the findings incorporated and

then published as an updated version.

3.2 Developing and setting up objectives of the demonstrator and the test cases

A set of specifications drawn up by SBB detailing the objectives is to serve as the basis for the development of the test cases. The achievement of the objectives is to be demonstrated by means of these test cases..The elaboration of the contents is still ongoing. An excerpt of the list of objectives is shown below.

Validation of all possibilities of the statuses of the flow chart of the OCORA concept for configuration management

Carrying out the updates for the listed cases:

- Update of software of a non-safe Building Block
- Update of software of a safe Building Block
- Updates of software of safe and non-safe Building Blocks
- Update of software of a building block, which is functional unidirectionally linked with another Building Block, taking into account the possible combinations of two safe and non-safe Building Blocks
- Update of software of a building block, which is functional bidirectionally linked with another Building Block, taking into account the possible combinations of two safe and non-safe Building Blocks

Simplified creation and compilation of the update files according to the necessity of the update case and roles

Simplified dispatching the update to the Configuration Manager

Checking of the update files by the Configuration Manager on:

- Correctness
- Completeness

Transmission of the software update to Building Block according to activation conditions

Checking of the software update files by the Building Block on:

- Correctness
- Completeness

Execution of the software update according to activation conditions

Consideration of error management

Status feedback from the Building Block to the Configuration Manager

Status feedback of the Configuration Manager to the update server

3.3 Requirement specification for the demonstrator

In the following, joint specification of the procedure, elements and activation conditions for distribution, authorization and activation of safe and non-safe app updates (and rollbacks) for the demonstrator shall be elaborated. Basically, the specification are based on the revised OCORA Configuration Management Concept. However, a complete implementation would be very extensive and time-consuming. Therefore, the specification shall reduce the extent in a matter, that the objectives of the proof of concept are still fulfilled and the test cases can be carried out. To increase efficiency, the demonstrator should enable the integration of existing software components of Selectron Systems.

The specification is to be developed by Selectron Systems. The OCORA team's task is to carry out regular reviews and ensure the project objectives are met.

The specification will be professionally reviewed by an ISA before finalisation. The review is limited to the identification of safety and security deficiencies and gaps in the safety and security concept. Within the proof of concept no certification is sought, but the certifiability should also be considered.

A key element is the definition of the activation conditions of the updates, i.e. compliance with the necessary conditions for update notification, software download, as well as the installaion of the update.

3.4 Implementation of the demonstrator and execution of the test runs

The demonstrator will then be implemented based on the developed and reviewed specification. A simplification of the demonstrator's structure is shown in Figure 1.

Two demonstrators will be implemented, whereas one will be located at SBB and the other at Selectron Systems. Each of the demonstrators will have two CCUs. Applications with and without safety-related functions are implemented on each of these. A training for the SBB employees by Selectron Systems should enable SBB to carry out the test runs independently.

The findings from the testing will be edited in a concept validation report and incorporated into the next OCORA release. If necessary, the OCORA concept for configuration management will be updated based on the outcome of the prototyping.

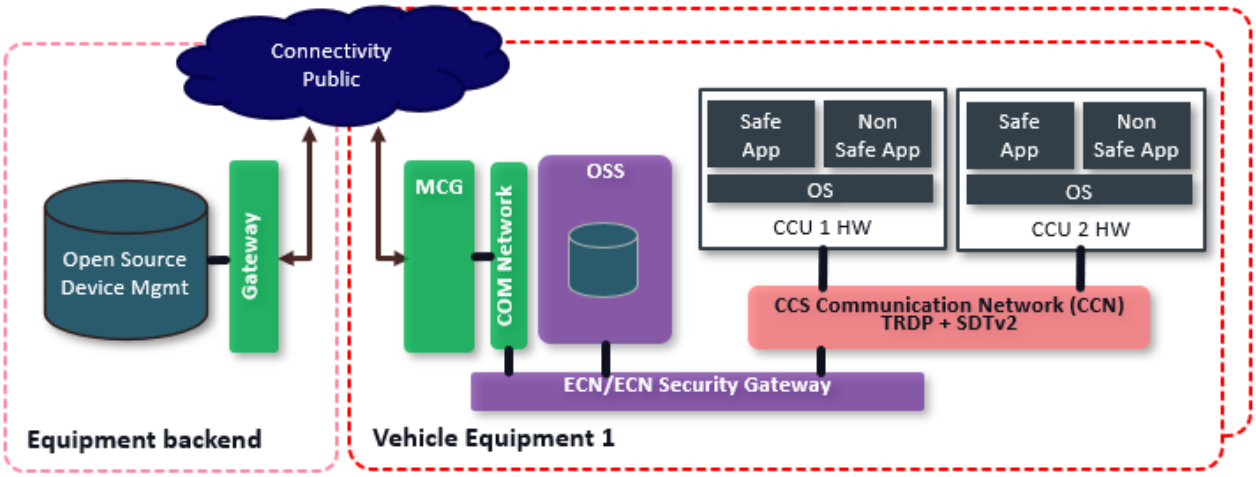

Figure 1: Schematic diagram of the demonstrator from the tender agreement with Selectron Systems AG