OCORA

Open CCS On-board Reference Architecture

Glossary
Gamma Release

Document ID: OCORA-90-002-Gamma

Version: 2.00

Date: 04.12.2020

Status: Final

Revision history

Version	Change Description	Name (Initials)	Date of change
0.00	Initial release	JH	2020-05-15
0.01	Release for final review	TM	2020-06-12
1.00	Final version	TM	2020-06-26
1.01	Includes changes of Core Team review	JH	2020-06-27
1.02	Includes updates based on OCORA Beta release feedback & additions for OCORA Gamma release	TM	2020-11-15
1.10	Final version for Review	TM	2020-11-19
2.00	Final version	RM	2020-12-04

Table of terms and definitions

Terms	Definition
Architecture	The fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution. (ISO 42010) *Describes the structure of a coherent ensemble of building blocks and the glue (e.g. interfaces, bus system) between these building blocks that maintains structure consistency and coherence.*
Basic Software	Provides a replica-deterministic environment to the ETCS Kernel - typically using a super-loop architecture. *The Basic Software is usually vendor specific and handles all input/output with peripheral functions.*
Building Block	A building block is a top-level unit of the CCS on-board system (hardware and/or software), having well defined tasks to be performed to achieve a predefined result and interfaces towards other building blocks of the CCS system. *Building blocks consist of 1 – n component(s) and are regression free modifiable / adaptable and therefore portable / replaceable. As a result, every building block can be designed to be "plug & play"-like exchangeable, without impacting other building blocks.* *OCORA building blocks shall be an optimal balance between "number of interfaces between building blocks" and "desire to exchange building blocks at a low granularity".*
CCS Computing Unit	A computing unit hosting all or parts of the CCS on-board and eventually other software. *The unit consists of 1 to n processors and has a single connection to the UVCCB.*
Component	Specifically, for OCORA, a component is the 1st level of decomposition of the CCS on-board system. *Components are grouped into building blocks for defining the granularity of the "plug & play"-like exchangeability. Components consist of 1 – n sub-components.*
Device	A physical entity performing a predefined (set of) task(s). It consists of software integrated on a hardware.
Diesel Multiple Unit	Diesel Multiple Unit: combustion engine powered, self-propelled integrated combination of two or more rail cars for the transportation of passengers. *Also known as 'train set'. Once broken, the combination can no longer perform its function. Propulsion can be direct (diesel hydraulic) or indirect (diesel electric) and distributed over the combination or concentrated in e.g. power heads or locomotives.*
Electrical Multiple Unit	Electrical Multiple Unit: external power driven, electrically propelled integrated combination of two or more rail cars for the transportation of passengers.

Terms	Definition
	Also known as 'train set'. Once broken, the combination can no longer perform its function. Propulsion can be distributed over the combination or concentrated in e.g. power heads or locomotives.
European standard	A standard adopted and formally ratified by a European standardisation organisation (CEN, CENELEC or ETSI).
European Vital Computer	Device for performing the designated ETCS function of safe train operation. *It includes the logic needed to perform the ETCS tasks, i.e. data exchange management between internal and peripheral functions like odometry or DMI.*
Evolvability	Evolvability (Flexibility) is the ability to easily adopt to new technologies or to extend the functionality of an on-board CCS system without the involvement of the original supplier. *Evolvability is an architecture design principle, to be realised in the engineering concept of concrete products.*
Example	Any physical, graphical or textual representation of a concept, object or abstraction used for explaining or clarifying that concept, object or abstraction. *Examples shall not in any way be limitative or perceived as limitative and are not in any way to be understood as prescriptive or as a requirement.*
Exchangeability	Exchangeability (Interchangeability) is the ability to replace one or multiple building blocks with (a) respective building block(s) of (an)other supplier(s), without affecting other building blocks or the overall CCS on-board system. *Exchangeability is an architecture design principle that has to be achieved on the engineering concept of concrete products (hard- or software). Replaceability is the realisation of this design principle in concrete products.*
Formal Model	A Formal Model is the description of a Functional Model using formal grammar and the symbolism of a logical language. *A precise mathematical set of rules by which a valid Functional Model description is constructed that eventually can be (directly) transformed into computer code.*
Function	A (coherent set of) task(s) to be performed in order to achieve a defined result. *Functions express actions that are executed. They are usually embedded in structural elements of a system.*
Functional Application	Functional Application refers to the software that implements the actual (Business) Logic of a railway Function. *Examples would be the Vehicle Locator or the Vehicle Supervisor. Functional Applications shall be platform independent and make use of a "generalized abstraction" (API) to the Computing Platform.*
Functional decomposition	The partition of a system into single structural elements that each represent one or more coherent functions to be performed that together fulfil the design objective of the system. *Describes how (clusters of) Functions are embedded into the structural elements of a system.*

Terms	Definition
Functional Model	Abstraction of a system, describing interaction between individual functions of a system. *OCORA targets using a formal language for functional modelling.* *Describes the actions performed by a coherent ensemble of building blocks and the glue between these building blocks (e.g. interfaces, bus system) that together constitute a System.*
Functional Vehicle Adapter	The Functional Vehicle Adapter (FVA) is a piece of software deployed on the OCORA computing platform, or on the OCORA Gateway. Its job is to provide an OCORA unified and standardized interface towards the CCS applications and services for vehicle functions and vehicle information needed by the OCORA on-board applications and services.
Future Railway Mobile Communication System	Railway specific radio communication system based on global 5G telecommunication standards and technologies.
OCORA-Gateway	A hardware device providing communication capabilities between the UVCCB (CCS-ECN) and the legacy train control network or bus or the legacy actors and sensors residing outside the CCS domain but important to CCS.
Harmonised standard	A harmonized standard is a European standard elaborated on the basis of a request from the European Commission to a recognized European Standards Organisation (CEN, CENELEC or ETSI) to develop a European standard that provides solutions for compliance with a legal provision. (Source: CENELC) *Its application can be mandatory (referenced standard) or voluntary (standard listed in the Official Journal of the EU in the New Legislative Framework).*
International standard	A standard adopted and ratified by an international standardisation body. Examples are: ISO, IEC and ITU.
Interoperability	Interoperability is the ability of a train service to run seamlessly, i.e. without the need to change either rolling stock or train staff, on any ERTMS equipped rail network. *Interoperability is an architecture design principle, to be realised in the engineering concept of concrete products.*
(ETCS) Kernel	The prime task to be performed by the EVC (Vehicle Supervisor), including data exchange management with peripheral Systems like DMI and odometry.
(Business) Logic	Systematic set of principles for retrieving, dispatching, storing, modelling, analysing and predicting information so as to perform a specified task. *Pertains specifically to the management of data by a System, both internal as in exchange with peripheral Systems.*
Migrateability	The property of a system to allow changes to one or multiple building blocks, without affecting other building blocks or the overall system. *Migrateability is an architecture design principle, to be realised in the engineering concept of concrete products. It is a prerequisite for upgradeability.*

Terms	Definition
Mobile Communication Gateway	The Mobile Communication Gateway (MCG) provides train to track-side communication for the on-board CCS and depending on the vehicle, it may also provide track-side connectivity for the systems of the Train Control bus (VCS and PIS).
Model	A consistent digital representation of an Architecture, allowing to generate different views for documenting and explaining different aspects of the Architecture.
Modularity	The property of a system being composed of a coherent whole of single, independent building blocks or modules. *Modularity is a prerequisite for having "plug & play"-like exchangeability of an on-board CCS system or its subsystems without the need to involve either the original supplier of the vehicle, of the CCS system or one of its subsystems.*
Modular Safety	Is the concept to reduce the overall safety case workload by using modularity, not only for the technical design of components, but also to use modularity to foster independent, re-usable, composable safety cases. *Overall, it means to reduce the workload of the impact analysis for changes and end2end corrections to a possible minimum.*
Non-Safe	Adjective indicating that a system or function in itself is not designed to protect against bodily harm or material damage when it fails. *In general, the qualification of a system or function as 'non safe' indicates that the safety function, protecting both the involved animate or inanimate entities, is allocated to other safety systems or functions.*
Non-Vital	See Non-Safe
(Computing) Platform	Refers to the environment on which Functional Applications are executed. *Comprised of* • *Hardware (i.e. Compute Nodes, Memory, etc.) and* • *Software (i.e. the Runtime Environment)*
Platform Independence	The property of allowing a functional application to work on different Computing Platform implementations. *Platform Independence is the fact of using a "generalized abstraction" between Functional Application logic and the underlying (Computing) Platform.* *To concretely attain Platform Independence, the following elements are needed:* • *A definition of a "generalized abstraction" (in the form of an API specification)* • *At least one provider implementation of the "generalized abstraction" in form of a concrete (Computing) Platform* • *One or more Functional Applications applying the specification and being able to run on the (Computing) Platform.* *Platform Independence is achieved when a Functional Application, based on the generalized abstraction, runs un-changed on different (Computing) Platform implementations. For this, the Functional Application shall only use external functions through a defined application programming interface (API).*

Terms	Definition
	Platform independence is a design principle, used in the development of the engineering (concept) of concrete products.
Portability	The property that allows migrating a software from one concrete Computing Platform implementation to another concrete Computing Platform implementation. *See also Platform Independence.*
Presumption of conformity	Condition of per se demonstrating product, service or process compliance with relevant EU legislation in case of consistent application of EU harmonized standards by manufacturers, other economic operators or conformity assessment bodies. *The presumption of conformity is a concept that is widely used in the context of the European "New Approach" for better regulation. The presumption of conformity means that a manufacturer who has complied with a harmonised standard listed in the OJEU can legally assume he has met the requirements of the directive (or TSI) covered by that standard, as described in its Annex Z.* *ANNEX Z of standards and the Official Journal of the European Union* *The listing of a European standard in the OJEU requires a positive assessment of the Harmonized Standard Consultant and a corresponding positive statement of the EC desk officer. Furthermore, it is required that the listed standard contains an Annex Z detailing to which requirements of the directive (or TSI) it provides presumption of conformity.*
Radio Block Centre	The RBC is a centralised, radio communication enabled safety system to manage safe train movement based on train position information. *The Radio Block Centre (RBC) is a specialised computing device with Safety integrity level 4 (SIL) for generating Movement Authorities (MA) and transmitting it to trains. It gets information from Signalling control and from the trains in its section. It hosts the specific geographic data of the railway section and receives cryptographic keys from trains passing in. According to conditions the RBC will attend the trains with MA until leaving the section. RBC have defined interfaces to trains but have no regulated interfaces to Signalling Control and only follow national regulation.*
Referenced Standard	A standard or a part of a standard referenced in a Technical Specification for Interoperability (TSI). (Website EIM) *Furthermore, article 4.8 of Directive (EU) 2016/797 sets out that normative documents, such as specifications or technical documents can also be referenced in a Technical Specification for Interoperability (TSI). When referenced, their nature changes from voluntary to mandatory.*
Replaceability	He property of a component or a device to be removed and installed without support of the OEM. Replaceability is *the technical implementation of* exchangeability*, enabling components and devices to be removed and installed without support of the OEM.* *Replaceability is a design principle, used in the development of the engineering (concept) of concrete products.* See also: Exchangeability.

Terms	Definition
Runtime Environment	The Runtime Environment represents the execution context of Functional Applications. It consists of all software aspects required to provide that execution context including safety and security services, communication stack and if applicable Operating System and Virtualization. It provides a Platform Independent API - a general abstraction that allows *Functional Applications* to run unchanged on different Computing Platform implementations.
Safe / Safety	Safety is defined as a property of railway functions or systems that safeguards humans, physical assets and environment against (fatal) injury or damage in conformity with predefined acceptable risk thresholds. *Safe systems ensure that the defined risk levels are not exceeded and that the function or system enters its fail-safe state in case of failure. Since risks can never be completely mitigated, acceptable risk levels have to be established. Determining such levels is subject to ethical considerations and is, therefore, not within OCORA scope.*
(Cyber) Security	(Cyber) Security is the protection of (especially safety related) communication and data used in on-board CCS systems against threats (like cyber-attacks and hacks). To achieve this, all main security functionality like identify, protect, detect, respond and recover are considered. *(Cyber) security is a design principle, used in the development of the engineering (concept) of concrete products.*
Service	Services are specialized Functional Applications providing common functionality used by multiple other Functional Applications or an "input-output" conversion from and to other Functional Applications in coherence with the data model. An example of a Service is the "Vehicle Locator" (VL) which is used by the "Vehicle Supervisor" (VS) and the "ATO vehicle" (AV).
Specific Vehicle Interface	Data exchange function between the on-board CCS system and the vehicle that defines data and data formats that are not otherwise defined in either formal TSI specifications or published UNISIG or OCORA proposals for TSI specifications.
Standard	A technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory, except when referenced in a Technical Specification for Interoperability, or any other regulatory text (e.g. national rule, law, …)
System	A coherent group of interacting or interrelated entities that form a unified whole, described by its structure and purpose and expressed in its functioning. *A System is described by its spatial and temporal boundaries as surrounded and influenced by its environment.* *Refer to OCORA-40-001-Gamma, System Architecture for a definition of the OCORA system under consideration.*
Train Control and Management System	The Train Control and Management System (TCMS) is an on-board distributed control, communication and train management system that provides data communications interfaces to other train-borne systems and is designed to control and monitor train equipment. The TCMS also includes wired control logic.

Terms	Definition
	At interface level it refers to all aspects of the integration into the "Train": conceptually it groups together the two types of interfaces "serial interface" and "hard-wired interface" indicated in SUBSET -119.
Train Interface Unit	The Train Interface Unit (TIU) defines the interface between the ERTMS / ETCS on-board equipment and the train. *To avoid confusion, the term TIU is no longer used in context of OCORA as it would also be used in another context than only ERTMS / ETCS. The newly introduced Functional Vehicle Adapter (FVA) incorporates the full TIU functionality and ensures standardized communication with the TCMS on OSI layer 7. It is accessible to all OCORA applications like VS, ATO and any possible future extension.*
Train Set	See Diesel Multiple Unit, Electrical Multiple Unit
Vehicle Supervisor	The (Business) Logic enabling calculating location specific speed limits and activation of the braking system in case of speed limit overshoot. *Describes the prime task to be performed by the EVC (ETCS Kernel functions), including data exchange management with peripheral Systems like DMI and odometry.*
Vital	See Safe

Table of abbreviations and acronyms

Abbreviation	Definition
API	Application Programming Interface
APS	Advanced Protection System
APS-MOT	APS Mobile Object Transactor
APS-MT	APS Movement Authority Transactor
AsBo	Assessment Body
AT	ATO Transactor
ATC	Automatic Train Control
ATO	Automatic Train Operation
ATO-AT	ATO Transactor
ATO-AV	ATO Vehicle
ATP	Automatic Train Protection
AV	ATO Vehicle
BIU	Break Interface Unit
BTM	Balise Transmission Module
CAN	Controller Area Network
CCS	Control-Command and Signalling
CCU	CCS Computing Unit
CER	Community of European Railway and Infrastructure Companies
CiA	CAN in Automation
CMD	Cold Move Detection
CoC	Code of Conduct
COTS	Commercial off-the-shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CS	Consist Switch
DAS	Driver Advisory System
DCM	Device & Configuration Management
DDS	Data Distribution Service / Real-time Publish-Subscribe
DeBo	Designed Body
DM	Diagnostics & Monitoring
DMI	Driver Machine Interface
DMU	Diesel Multiple Unit
EB	Emergency Braking

EBA	Euro Balise Antenna
ECN	Ethernet Consist Network
ED	End Device
EDOR	ETCS Data Only Radio
EMU	Electrical Multiple Unit
ERA	European Union Agency for Railways (former European Railway Agency)
ERORAT	EULYNX RCA OCORA Risk Assessment Tool
ERTMS	European Rail Traffic Management System
ETB	Ethernet Train Backbone
ETBN	Ethernet Train Backbone Node
ETCS	European Train Control System
EUDD	European Driver's Desk
EUG	ERTMS User Group
EVC	European Vital Computer
FAT	Factory Acceptance Test
FFFIS	Form Fit Function Interface Specification
FM	Formal Model
FIS	Functional Interface Specification
FME(C)A	Failure Mode Effect (and Criticality) Analysis
FRMCS	Future Railway Mobile Communication System
FVA	Functional Vehicle Adapter
GASC	Generic Application Safety Case
GNSS	Global Navigation Satellite System
GoA	Grade of Automation
GPSC	Generic Product Safety Case
GSM-R	Global System for Mobile Communications - Railway
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HW	Hardware
I/O	Input/output
IAM	Identity & Access Management
IM	Infrastructure Manager/Management
ISMS	Information Security Management System
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IF	Interface
IM	Infrastructure Manager

IPv4	Internet Protocol version 4
ISA	Independent Safety Assessor
IU	Interface Unit
IVV	Integration, Verification and Validation
IXL	Interlocking (new APS)
JRU	Juridical Recording Unit
LAN	Local Area Network
LTM	Loop Transmission Module
MAC	Message Authentication Code
MBSE	Model Based Systems Engineering
MCG	Mobile Communication Gateway
MD	Message Data
ML	Maturity Level
MOT	Mobile Object Transactor
MoU	Memorandum of Understanding
MT	Movement Authority Transactor
MTC	Manoeuvre Train Control
MQTT	Message Queuing Telemetry Transport
MVB	Multifunction Vehicle Bus
NG-TCN	Next/New Generation TCN
NNTR	Notified National Technical Rules
NoBo	Notified Body
NTC	National Train Control
OBU	On-board Unit
OCORA	Open CCS On-board Reference Architecture
OD	Object Detection
ODO	Odometry
OEM	Original Equipment Manufacturer
OPC-UA	Open Platform Communications Unified Architecture
OS	Operating System
OTIS	Onboard Train Integrity System sometimes also referred to as TIMS
PD	Process Data
PS	Perception (Sub-)System
PIN	Passenger Information Network
QA	Quality Assurance
QoS	Quality of Service
RACI	Responsibility, Accountability, Consulted, Informed

RAMS	Reliability, Availability, Maintainability and Safety
RBC	Radio Block Center
RCA	Reference CCS Architecture
RDH	Railway Duty Holder
RFID	Radio-frequency identification
RIM	Radio Interface Module
RIU	Radio In-fill Unit
ROS	Robot Operating System
RTM	Real Time Model
RU	Railway Undertaking
S2R	Shift2Rail
SASC	Specific Application Safety Case
SB	Service Brakes
SC	Safety Case
SDT	Safe Data Transmission
SDTv2	SDT Version 2
SDTv4	SDT Version 4
SFERA	Smart Communications for Efficient Rail Activities
SFM	Semi-Formal Model
SIEM	Security Information and Event Management
SIL	Safety Integrity Level
SL	Security Level
SMI	Source Message Identifier
SOC	Security Operation Centre
SOME/IP	Scalable Service-Oriented Middleware over IP
SRAC	Safety Related Application Condition
SRP	Stream Reservation Protocol
SRS	System Requirements Specification
SSRS	Sub-System Requirement Specification
STM	Specific Transmission Module
SuC	System under consideration
SW	Software
TCMS	Train Control and Management System
TCN	Train Communication Network
TCO	Traction Cut-Off
TCP	Transmission Control Protocol
TFFR	Tolerable Functional Failure Rate (i.e. new naming for THR in CENELEC standards)

THR	Tolerable Hazard Rate
TI	Track Intrusion
TIMS	Train Integrity Monitoring System sometimes also referred to as Onboard Train Integrity System (OTIS)
TIU	Train Interface Unit
TLS	Transport Layer Security
TMS	Traffic Management System
TOBA	Telecom On-Board Architecture
TRB	Train Born
TRDP	Train Real-Time Data Protocol
TSI	Technical Specification for Interoperability
TSN	Time Sensitive Networking
TSN-PD	TSN Process Data
UDP	User Datagram Protocol
UI	User Interface
UIC	Union Internationale des Chemins de Fer
UVCCB	Universal Vital Control and Command Bus
V&V	Verification and Validation
VCU	Vehicle Control Unit
VLAN	Virtual Local Area Network
VL	Vehicle Locator
VLS	Vehicle Localisation (Sub-)System
VS	Vehicle Supervisor
WTB	Wired Train Bus