

X2Rail-1

Project Title:	Start-up activities for Advanced Signalling and Automation Systems
Starting date:	01/09/2016
Duration in months:	36
Call (part) identifier:	H2020-S2RJU-CFM-2015-01-1
Grant agreement no:	730640

Deliverable D2.3

Terminology for the future Signalling and Automation System

Due date of deliverable	08-2017
Actual submission date	03-05-2018
Organization name of lead contractor for this deliverable	ALS
Dissemination level	PU
Revision	

Authors

Author(s)	ALSTOM Jacques PORE Benoît BIENFAIT
Contributor(s)	ALSTOM Francois HAUSMAN
	Ansaldo Claudio MONTI
	AZD Michal PAVEL
	BOMBARDIER Staffan PETTERSSON
	CAF José Antonio QUINTANO
	KAPSCH Ulrich GEYER Michael MIKULANDRA
	MERMEC Francesco INZIRILLO
	SIEMENS Craig McLELLAN Simon CHADWICK
	THALES Bettina DOETSCH Lisa-Marleen SCHEILE Belen LOSADA
	Deutsche Bahn Ralph MÜLLER Bernd EBERTS
	Network Rail Nicola FURNESS
	Trafikverket Ulf BOHLIN

Executive Summary

This document contains the first version of a harmonized glossary for the terminology used in X2Rail-1 and further X2Rail-projects. It is a living document which will be updated regularly.

Table of Contents

EXECUTIVE SUMMARY 4

TABLE OF CONTENTS 5

GLOSSARY 6

Glossary

Deliverable D2.3
Terminology for the future Signalling and Automation System

	Term	Definition	Source Document
	Colour used by WP6		
WP3_4.11	3GPP	The 3rd Generation Partnership Project (3GPP) is a collaboration of telecommunications associations that drive the standardization for mobile telecommunication standards (2G/GSM, 3G/UMTS, 4G/LTE).	
WP6_01	acceptance criteria	<u>[ISO/IEC/IEEE 24765, 2010]</u> 1. the criteria that a system or component must satisfy in order to be accepted by a user, customer, or other authorized entity. 2. those criteria, including performance requirements and essential conditions, which must be met before project deliverables are accepted. A Guide to the Project Management Body of Knowledge (PMBOK® Guide) — Fourth Edition cf. requirement, test criteria	[ISO/IEC/IEEE 24765, 2010]
WP6_02	acceptance testing	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> Formal testing with respect to user needs, requirements, and business processes conducted to determine whether or not a system satisfies the acceptance criteria and to enable the user, customers or other authorized entity to determine whether or not to accept the system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP8_001	access	1. Ability and means to communicate with or otherwise interact with a system in order to use system resources. <u>Note to entry:</u> Access may involve physical access (authorization to be allowed physically in an area, possession of a physical key lock, PIN code, or access card or biometric attributes that allow access) or logical access (authorization to login to a system and application, through a combination of logical and physical means).	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_002	access account	1. Access control function that allows the user access to a particular set of data or functions for certain equipment. <u>Note to entry:</u> Many times accounts are linked to user identification (IDs) and passwords. These user IDs and passwords may be linked to an individual or group of individuals such as control room work team performing the same set of operating tasks.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_003	access control	1. Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_004	accountability	1. Property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP6_03	accuracy	<u>[ISO/IEC/IEEE 24765, 2010]</u> 1. a qualitative assessment of correctness, or freedom from error. 2. a quantitative measure of the magnitude of error	[ISO/IEC/IEEE 24765, 2010]
WP6_05	actual result	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> The behavior produced/observed when a component or system is tested.	[ISTQB (http://glossar.german-testing-board.info/)]
WP3_2.1	Adaptability	In general, adaptability is the ability of a system to adjust its behaviour in an efficient manner to reflect changes in its environment or in parts of the system itself. Adaptability of a railway communication solution means, that such a system should be decoupled from the application, i.e., it should fit the needs and fulfil the expectations of several different heterogeneous applications. Future applications will be able to be integrated efficiently. Furthermore, such a communication system should be adaptable in terms of its multi-bearer capability, supporting a number of different radio access technologies and related networks.	
WP8_005	Administrative practices	1. Defined and documented practices or procedures that individuals are personally accountable to follow at all times. <u>Note to entry:</u> These are usually in the conditions of employment for the organization. In the IACS environment, these often have HS&E implications.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP6_09	anomaly	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> Any condition that deviates from expectation based on requirements specifications, design documents, user documents, standards, etc., or from someone's perception or experience. Anomalies may be found during, but not limited to, reviewing, testing, analysis, compilation, or use of software products or applicable documentation.	[ISTQB (http://glossar.german-testing-board.info/)]

WP4_132	API	The Automatic Programming Interface (API) is the functions/primitives required to complete the \emph{Runtime model}. It shall provide the remaining of the features listed hereabove which are not provided by the Runtime model.All these can be provided with or without safety properties.	
WP6_166	Architecture	<u>[ISO/IEC/IEEE 24765, 2010]</u> 1. fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution. ISO/IEC 15288:2008 (IEEE Std 15288-2008), Systems and software engineering — System life cycle processes.4.5. 2. the organizational structure of a system or component. 3. the organizational structure of a system and its implementation guidelines. Syn: architectural structure cf. component, module, subprogram, routine NOTE sometimes refers to the design of a system's hardware and software components	[ISO/IEC/IEEE 24765, 2010]
WP8_006	asset owner	individual or company responsible for one or more IACS Note 1 to entry: Used in place of the generic word end user to provide differentiation Note 2 to entry: This includes the components that are part of the IACS Note 3 to entry: In the context of this standard, asset owner also includes the operator of the IACS	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_007	asset(s)	1) physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization 2) physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization 3) physical or logical object having either a perceived or actual value to the IACS <u>Note 1 to entry:</u> In the case of industrial automation and control systems the physical assets that have the largest directly measurable value may be the equipment under control. <u>Note 2 to entry:</u> In this specific case, an asset is any item that should be protected as part of the cyber security management system.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_008	assurance	Attribute of a system that provide grounds for having confidence that the system operates such that the system policy is enforced.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP3_3.32	ATC On-board - Automatic Train Control – on board train	The system for automatically controlling train movement, enforcing train safety, and directing train operations. ATC must include ATP and may include ATO.	IEEE 1474.1-2004, Communications-Based Train Control (CBTC) performance and functional requirements
WP4_001	ATO (Train, Area) Hold	The functionality that allows trains to be held at a defined location for regulation purposes. This functionality can be applied to either one train only or a defined area with multiple trains or the whole service which may run through multiple traffic management controlled areas.	
WP4_002	ATO Area	The area where, for Grades of Automation (GoA) 2 to 4, Automatic Train Operation is possible, informed by real-time dynamic update of operational data via a telecommunications link between the ATO on-board and ATO trackside subsystems.	
WP4_003	ATO Available	ATO Available is the ATO state when the ATO-OB is ready for operation and is waiting for the Engagement Conditions to be fulfilled.	
WP4_004	ATO Configuration	ATO Configuration is the ATO state when the ATO-OB executes self-tests procedures and receives the required ETCS Train Data.	(definitions contained originally in “ATO over ETCS SUBSET-125 ATO system requirements specification” and developed in that work stream, which were moved to this document)
WP4_005	ATO Disengaged	The status of the ATO on-board sub-system when it is not controlling train functions.	
WP4_006	ATO Disengaging	ATO state when the ATO-OB losses the ATO Operational conditions while being engaged. The ATO-OB controls the braking command in order to bring the train to standstill waiting for the driver to disengage the ATO.	(definitions contained originally in “ATO over ETCS SUBSET-125 ATO system requirements specification” and developed in that work stream, which were moved to this document)
WP4_007	ATO Engage Button	Input that permits the driver to request to start automatic driving when the engagement conditions are fulfilled.	(definitions contained originally in “ATO over ETCS SUBSET-125 ATO system requirements specification” and developed in that work stream, which were moved to this document)
WP4_008	ATO Engaged	ATO state in which the ATO on-board is responsible for driving the train, controlling brake and traction according to the computed ATO Operational Speed Profile.	

Deliverable D2.3
Terminology for the future Signalling and Automation System

May 2018			
WP4_009	ATO Failure	ATO state when the ATO on-board has failed to power up, has failed its self-tests, has an in-service failure, or when it has detected a failure that does not allow it to perform its functions. This is applicable to the Failure state (FA).	
WP4_010	ATO Fitted Train	A train that is fitted with an ATO on-board sub-system.	
WP4_011	ATO Inhibition Zone	The prevention of the ATO functionality over a defined area of the railway in the direction of travel. It may be in either or both directions of a bi-directional section of track.	(definitions contained originally in "ATO over ETCS SUBSET-125 ATO system requirements specification" and developed in that work stream, which were moved to this document)
WP4_012	ATO Isolation Mode	ATO state when the ATO Isolation Switch is set to isolation position. In this state, some functions of ATO are inhibited.	(definitions contained originally in "ATO over ETCS SUBSET-125 ATO system requirements specification" and developed in that work stream, which were moved to this document)
WP4_013	ATO Not Available	ATO state when the ATO-OB is not ready for operation and it is waiting for the Operational Conditions to be fulfilled.	
WP4_014	ATO Not Selected	ATO Not Selected is the ATO state when the ATO Selector is in NS position.	
WP4_015	ATO On-board	The sub-system and set of automated non-safety-related driver functions, depending on the grade of automation.	
WP3_3.34	ATO On-board - Automatic Train Operation – on board train	The subsystem within the ATC system that performs any or all of the functions of speed regulation, programmed stopping, door control, performance level regulation, or other functions otherwise assigned to the train operator.	IEEE 1474.1-2004, Communications-Based Train Control (CBTC) performance and functional requirements
WP4_021	ATO Operated Train	A train that is fitted with ATO on-board sub-system and this sub-system is operational.	
WP4_016	ATO Operational Speed Profile	The most energy efficient speed profile calculated by the ATO on-board sub-system that fulfils the Journey Profile and respects the ETCS safe braking envelope.	
WP4_017	ATO over ETCS System (AoE)	The set of interrelated or interacting components that provides ATO and ATP functionalities.	
WP4_018	ATO Ready	ATO state when the ATO-OB is ready for operation and it is waiting for the engagement order.	(definitions contained originally in "ATO over ETCS SUBSET-125 ATO system requirements specification" and developed in that work stream, which were moved to this document)
WP4_019	ATO Selected	It is the ATO mode when the ATO-OB is in CO, NA, AV, RE, EM or DE state.	(definitions contained originally in "ATO over ETCS SUBSET-125 ATO system requirements specification" and developed in that work stream, which were moved to this document)
WP4_020	ATO Selector	Input from the driver to select "ATO Selected Mode" (SM) or "ATO Not Selected Mode" (NS).	(definitions contained originally in "ATO over ETCS SUBSET-125 ATO system requirements specification" and developed in that work stream, which were moved to this document)
WP4_022	ATO Trackside	A set of functions that interfaces with the necessary trackside systems which contain the operational data and infrastructure data that is required by the ATO on-board.	
WP4_023	ATO Trackside Handover	It is the process of passing the responsibility for an ATO train between two ATO trackside subsystems.	
WP4_024	ATO Unpowered	ATO state when the ATO on-board is powered off.	(definitions contained originally in "ATO over ETCS SUBSET-125 ATO system requirements specification" and developed in that work stream, which were moved to this document)
WP3_3.33	ATP On-board - Automatic Train Protection – on board train	The subsystem within the ATC system that maintains fail-safe protection against collisions, excessive speed, and other hazardous conditions through a combination of train detection, train separation, and interlocking.	IEEE 1474.1-2004, Communications-Based Train Control (CBTC) performance and functional requirements

May 2018			
WP8_009	attack	<p>Assault on a system that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of method or techniques) to evade security services and violate the security policy of a system.</p> <p><u>Note to entry:</u> There are different commonly recognized classes of attack:</p> <ul style="list-style-type: none"> * An "active attack" attempts to alter system resources or affect their operation. * A "passive attack" attempts to learn or make use of information from system but does not affect system resources. * An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider") , i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.. * An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (including insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments. 	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_010	attack potential	<p>measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation</p> <p>Authors note: TOE Target of Evaluation</p>	CC-1, CCMB-2012-09-001
WP8_011	attack tree	Formal, methodical way of finding ways to attack the security of a system.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP6_10	attack-based testing	<p>[ISTQB (http://glossar.german-testing-board.info/)]</p> <p>An experience-based testing technique that uses software attacks to induce failures, particularly security related failures.</p>	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_11	attacker	<p>[ISTQB (http://glossar.german-testing-board.info/)]</p> <p>A person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent.</p>	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_12	audit	<p>[EN 50126:1999]</p> <p>A systematic and independent examination to determine whether the procedures specific to the requirements of a product comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives.</p>	[EN 50126:1999]
WP8_012	Authentication	<p>1) Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.</p> <p>2) Action of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.</p> <p>3) Provision of assurance that a claimed characteristic of an identity is correct.</p> <p><u>Note to entry:</u> Authentication is usually a prerequisite to allowing access to resources in a control system.</p>	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_013	Authenticity	<p>1) Property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator (see "authentication").</p> <p>2) Property that an entity is what it claims to be.</p> <p><u>Note to entry:</u> Authenticity is typically used in the context of confidence in the identity of an entity, or the validation or a transmission, a message, or message originator.</p>	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_025	Automatic Joining	An automatic process to couple two or more train consists.	
WP4_026	Automatic Splitting	An automatic process to separate a train into two or more individual consists.	
WP4_027	Automatic Train Control System (ATC)	System which effects an emergency brake application if the driver does not react to certain signal aspects or speed restrictions.	IEC 60050-821:1998: International Electrotechnical Vocabulary - Part 821: Signalling and security apparatus for railways
WP4_028	Automatic Train Operation (ATO)	A method of operation in which different train operation tasks are automated, according to the Grade of Automation (GoA) level present, up to GoA 4 level, where the train is automatically controlled without the presence of staff on board.	
WP4_029	Automatic Train Protection (ATP)	A system that enforces obedience to signals and speed restrictions by speed supervision, including automatic stop at signals.	ERA Glossary of Railway Terms, 8th November 2010, available at http://www.era.europa.eu/Document-Register/Pages/Glossary-of-railway-terms.aspx .
WP4_030	Automatic Turnback	The functionality that allows trains to change direction for another journey which may include automatic unattended movement.	

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP6_14	availability	[EN 50126:1999] May 2018 The ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided.	[EN 50126:1999]
WP8_015	Availability	1) probability that an asset, under the combined influence of its reliability, maintainability, and security, will be able to fulfill its required function over a stated period of time, or at a given point of time 2) property of ensuring timely and reliable access to and use of information 3) property of ensuring timely and reliable access to and use of control system information and functionality	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_031	Awake Train	This function is intended to prepare a train for operation.	
WP7_001	Axle counter	A device for clear detection, based on the counting of axles entering and leaving a defined portion of track and comparing these values.	-
WP3_2.6	Backward Compatibility	Backward compatibility is a property of a system, product, equipment, service or technology that allows for interoperability with an older or legacy system, or with input designed for such a system.	
WP3_1.9	Bandwidth	Anticipated data rate when using a specific application.	
WP6_15	baseline	[ISO/IEC/IEEE 24765, 2010] 1. specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. ISO/IEC 12207:2008 (IEEE Std 12207-2008), Systems and software engineering — Software life cycle processes.4.6, ISO/IEC 15288:2008 (IEEE Std 15288-2008), Systems and software engineering — System life cycle processes.4.7. 2. formally approved version of a configuration item, regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle. ISO/IEC 19770-1:2006, Information technology — Software asset management — Part 1: Processes.3.1. 3. agreement or result designated and fixed at a given time, from which changes require justification and approval. 4. document or a set of such documents formally designated and fixed at a specific time during the life cycle of a configuration item 5. work product that has been placed under formal configuration management. 6. snapshot of the state of a service or individual configuration items at a point in time. ISO/IEC 20000-1:2005, Information technology — Service management — Part 1: Specification.2.2. 7. description of a system and its components (configuration items) at a particular period including any approved updates. 8. an approved plan (for a project), plus or minus approved changes. It is compared to actual performance to	[ISO/IEC/IEEE 24765, 2010]
WP6_16	behavior	[ISTQB (http://glossar.german-testing-board.info/)] The response of a component or system to a set of input values and preconditions.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_17	black-box test design technique	[ISTQB (http://glossar.german-testing-board.info/)] Procedure to derive and/or select test cases based on an analysis of the specification, either functional or non-functional, of a component or system without reference to its internal structure.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_18	black-box testing	[ISTQB (http://glossar.german-testing-board.info/)] Testing, either functional or non-functional, without reference to the internal structure of the component or system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP5_001	Block	A method of controlling the separation between trains by dividing the line into sections with, normally, no more than one train in each section. The block can either be a fixed block or a moving block.	Subset-023
WP4_032	Block section	A section of track in a fixed block system which a train may only enter when it is not occupied by other vehicles.	ERA Glossary of Railway Terms, 8th November 2010, available at http://www.era.europa.eu/Document-Register/Pages/Glossary-of-railway-terms.aspx .
WP6_19	boundary value	[ISO/IEC/IEEE 24765, 2010] 1. a data value that corresponds to a minimum or maximum input, internal, or output value specified for a system or component	[ISO/IEC/IEEE 24765, 2010]
WP6_23	bug	[ISTQB (http://glossar.german-testing-board.info/)] See defect	[ISTQB (http://glossar.german-testing-board.info/)]
WP4_033	Built In Test	The functionality that enables the AoE system to carry out its in-service health check.	
WP8_017	business continuity plan	Document with identified procedures for recovering from a disaster and restoring business operations.	[ISA/IEC 62443-1-2, D1E6, 2017]

Deliverable D2.3

Terminology for the future Signalling and Automation System

WP7_003	CAPEX	Capital expenditure, or CapEx, are funds used by a company to acquire or upgrade physical assets such as property, industrial buildings or equipment	-
WP7_002	Catenary	(also called Overhead line) Power distribution system formed by hanging electric power cables and used to transmit electrical energy to trains	-
WP3_3.16	Catering Schedulers	Staff tasked with scheduling on-train catering.	
WP3_3.6	Catering Staff	Catering staff on board trains	
WP6_171	Certification	<p><u>WP6 definition from Ed Morton:</u> the action or process of providing someone or something with an official document attesting to a status or level of achievement.</p> <p>It may refer to Sub-systems (e.g. Factory Acceptance certification) or complete Signalling Infrastructure Systems (e.g. a final Test Certificate [TC1] prior to Entry into Service in the UK).</p> <p>Certification may also refer to the process of gaining regulatory approval for the use of a System under European CSM-RA and Interoperability Legislation.</p>	WP6 definition from Ed Morton:
WP8_019	ciphertext	Data that has been transformed by encryption so that its semantic information content (i.e., its meaning) is no longer intelligible or directly available.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP5_002	Clear (a Signal)	To change a signal aspect from its most restrictive aspect to a less restrictive aspect.	Subset-023
WP8_021	client	Device or application receiving or requesting services or information from a server application.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_034	Coasting	The free running of a train with no traction and no brakes applied.	IEV 811: International Electrotechnical Commission – Electric traction
WP6_24	code	<p><u>[ISO/IEC/IEEE 24765, 2010]</u></p> <p>1. in software engineering, computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler, or other translator</p> <p>2. to express a computer program in a programming language.</p> <p>3. a character or bit pattern that is assigned a particular meaning</p> <p>cf. source code, object code, machine code, micro code</p> <p>EXAMPLE a status code</p>	[ISO/IEC/IEEE 24765, 2010]
WP4_035	Collision Detection	Functionality which detects an unexpected contact between the train and an obstacle.	
WP4_036	Command	<p>Order used to perform a function in a system.</p> <p>Adapted by replacing UGTMS with AoE</p> <p>Note 1 to entry: This order can originate from</p> <ul style="list-style-type: none"> - a system operator, - an external system, - inside AOE; <p>this order can be sent:</p> <ul style="list-style-type: none"> - to an external system - inside AOE. 	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP8_023	communication channel	<p>1) Logical or physical point-to-point or multi-point data flow between components in one zone to one or more components in another zone.</p> <p>2) Specific logical or physical communication link between assets.</p> <p><u>Note 1 to entry:</u> Zone as defined for ISA/IEC 62443.</p> <p><u>Note 2 to entry:</u> A channel facilitates the establishment of a connection.</p>	[ISO/IEC 62443-1-2, D1E6, 2017]
WP7_006	Communication protocol	A set of rules and conventions governing a transferred message. The defined elements are syntax, semantics and timing. A communication protocol consists of two parts: a data protocol and a transmission protocol.	-

Deliverable D2.3

Terminology for the future Signalling and Automation System

WP8_025	Communication Security	<p>1) measures that implement and assure security services in a communication system, particularly those that provide data confidentiality and data integrity and that authenticate communicating entities</p> <p>2) state that is reached by applying security services, in particular, state of data confidentiality, integrity, and successfully authenticated communication entities</p> <p><u>Note to entry:</u> This phrase is usually understood to include cryptographic algorithms and key management methods and processes, devices that implement them, and the life-cycle management of keying material and devices. However cryptographic algorithms and key management methods and processes may not be applicable to some control system applications.</p>	[ISA/IEC 62443-1-2, D1E6, 2017]
WP3_1.12	Communications Availability	The ability of a product (here: communication link) to be in a state to perform a required function under given conditions (here: allows communication with the given QoS parameters) at a given instant of time or over a given time interval assuming that the required external resources are provided. In this case, it includes the communications link being useable, i.e., free from interference.	EN 5126 - Railway applications- The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
WP6_25	Compatibility	<p>1) The ability of two or more systems or components to perform their required functions while sharing the same hardware or software environment</p> <p>2) The ability of two or more systems or components to exchange information.</p> <p>3) The capability of a functional unit to meet the requirements of a specified interface without appreciable modification.</p>	[ISO/IEC/IEEE 24765, 2010]
WP6_26	Compatibility tests	Tests regarding Compatibility. (used in the glossary of deliverable D6.1)	WP6 definition used in the glossary of deliverable D6.1
WP8_027	Compensating Countermeasures	<p>countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements</p> <p><u>Note to entry:</u> Examples include:</p> <p>1. (component-level): locked cabinet around a controller that doesn't have sufficient cyber access control countermeasures</p> <p>2. (system/zone-level): physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be unique identified by the IACS</p> <p>3. (component-level): a vendor's PLC can't meet the access control capabilities from an end-user, so the vendor puts a firewall in front of the PLC and sells it as a system</p>	[ISA/IEC 62443-1-2, D1E6, 2017]
WP6_28	compliance	<p>[EN 50126:1999]</p> <p>A demonstration that a characteristic or property of a product satisfies the stated requirements.</p>	[EN 50126:1999]
WP6_29	component	<p>[ISO/IEC/IEEE 24765, 2010]</p> <p>1. an entity with discrete structure, such as an assembly or software module, within a system considered at a particular level of analysis. ISO/IEC 15026:1998, Information technology — System and software integrity levels.3.1.</p> <p>2. one of the parts that make up a system. IEEE Std 829-2008 IEEE Standard for Software and System Test Documentation.3.1.6.</p> <p>3. set of functional services in the software, which, when implemented, represents a well-defined set of functions and is distinguishable by a unique name. ISO/IEC 29881:2008, Information technology — Software and systems engineering — FiSMA 1.1 functional size measurement method.A.4</p> <p>NOTE A component may be hardware or software and may be subdivided into other components. The terms "module," "component," and "unit" are often used interchangeably or defined to be subelements of one another in different ways depending upon the context. The relationship of these terms is not yet standardized. A component may or may not be independently managed from the end-user or administrator's point of view.</p>	[ISO/IEC/IEEE 24765, 2010]
WP6_30	component testing	<p>[ISTQB (http://glossar.german-testing-board.info/)]</p> <p>The testing of individual components/units/Subsystems.</p>	[ISTQB (http://glossar.german-testing-board.info/)]
WP8_029	compromise	<p>1) Unauthorized disclosure, modification, substitution, or use of information (including plaintext cryptographic keys and other critical security parameters).</p> <p>2) Violation of the security of a system such that an unauthorized disclosure or modification of sensitive information may have occurred.</p>	[ISA/IEC 62443-1-2, D1E6, 2017]

WP7_008	Computerized Maintenance Management System	Computerized Maintenance Management System (CMMS) is a means to perform maintenance tasks and to analyze collected data. It can also contain information to support fault handling and repairing	-
WP6_170	Concordance Tests	see Correspondance Tests	
WP7_004	Condition Base Maintenance	Condition Based Maintenance is maintenance when need arises. This maintenance is performed after one or more indicators show that equipment is going to fail or performance is degraded.	-
WP3_3.5	Conductors	Conductors on-board trains are responsible for operational and safety duties that do not involve actual operation of the train (e.g., ticket collection, customer service, observing door closure, performing safety tasks in case of emergency/accident...)	
WP8_031	Conduit	1) logical grouping of communication assets that protects the security of the channels it contains. 2) logical grouping of communication channels, between connecting two or more zones, that share common security requirements. <u>Note to entry:</u> This is analogous to the way that a physical conduit protects cables from physical damage. <u>Note to entry:</u> A conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone	[ISO/IEC 62443-1-2, D1E6, 2017]
WP6_32	Confidence testing	Confidence testing is a term used to define the repeat (duplicate) of any other test more than the absolute minimum to achieve it's given success criteria. The number of repeat or duplicate tests is an arbitrary number based on the user's experience and trust in the system. [mail from NR]	[mail from NR]
WP8_033	Confidentiality	1) assurance that information is not disclosed to unauthorized individuals, processes, or devices 2) preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (FIPS 199) 3) preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information <u>Note to entry:</u> When used in the context of an IACS, refers to protecting IACS data and information form unauthorized access.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_038	Configurable System	Capability of the system to allow users to select, from pre-programmed functions (modular software units), those which are necessary to accomplish a control strategy or other complex functions, without the use of computer language.	ISO 3511-4:1985: Industrial process measurement control functions and instrumentation -- Symbolic representation -- Part 4: Basic symbols for process computer, interface, and shared display/control functions
WP5_003	Confirmed Safe Rear End	Safe rear end of the train with integrity confirmed	--
WP6_35	Conformity	[ISO/IEC/IEEE 24765, 2010] 1. the fulfillment by a product, process or service of specified requirements. IEEE/EIA 12207.1-1997 IEEE/EIA Standard: Industry Implementation of International Standard ISO/IEC 12207:1995, Standard for Information Technology — Software Life Cycle Processes — Life cycle data.1.4.1	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_014	Consequence	1) result that occurs from a particular incident 2) condition or state that logically or naturally follows from an event	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_039	Consist	Single vehicle or a group of vehicles which are not separated during normal operation.	IEC 61375-2-3:2017-02: Electronic railway equipment - Train communication network (TCN) - Part 2-3: TCN communication profile
WP4_040	Constituent	Any elementary component, group of components, sub-assembly or complete assembly of equipment incorporated or intended to be incorporated into the AoE.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP7_005	Contactora	Electrically controlled switch used for switching an electrical power circuit, similar to a relay except with higher current ratings.	-
WP3_1.4	Content Type	The content type of applications is defined by four different categories (see table).	UIC FRMCS User Requirements Specification, V2.
WP8_016	Control	See security control.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP6_169	Correspondence Tests	<u>WP6 definition from Ed Morton:</u> The process of confirming an action from the Control Layer or Equipment element (e.g. button press, track circuit de-energisation, point movement) corresponds to the correct output at the required interface. (e.g. Signal 'off', track circuit indication illuminated. points indication 'out of correspondence').	WP6 definition from Ed Morton:

Deliverable D2.3
Terminology for the future Signalling and Automation System

May 2018			
WP8_018	Countermeasure Countermeasures	action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. <u>Note to entry:</u> The term "Control" is also used to describe this concept in some contexts. The term countermeasure has been chosen for this standard to avoid confusion with the world control in the context of "process control".	[ISA/IEC 62443-1-2, D1E6, 2017]
WP3_1.20	Coverage	Geographical coverage of tracks, stations, yards, tunnels.	
WP8_020	Critical	very important device, computer system, process, etc. that if compromised by an incident could have high financial, health, safety, or environmental impact to an organization	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_022	Critical Infrastructure	NO DEFINITION	-
WP5_004	Current position	The position of a train measured at a certain moment using defined system co-ordinates.	Subset-023
WP6_167	Customer acceptance testing	<u>WP6 definition from Giuseppe Savino:</u> Customer acceptance testing are testing activities conducted to determine if the requirements of a Customer specification or contract are met.	WP6 definition from Giuseppe Savino:
WP8_024	Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.	NIST SP 800-53 r4
WP8_028	Cybersecurity Cyber Security	Measure taken to protect a computer or computer system against unauthorized access or attack .	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_026	Cyberspace	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.	NIST SP 800-53 r4
WP7_007	Cycle Life	The number of load/charge cycles the energy storage can experience before it fails to meet specific performance criteria, usually about 80% of original performance. The measure is defined for specific charge and discharge conditions for example the rate and depth of the cycles	-
WP5_005	Danger (Aspect)	An indication given by a signal to stop.	Subset-023
WP6_39	data tests	The Data tests are performed to verify the correctness of the individual subsystem configuration data (e.g. MA Length, Static Speed Profile, ...) and they are related to a single subsystem in order to test its Specific Application (SA). (Refer to EN50128 (2011): Table A.11 – Data Préparation Techniques (8.4))	EN50128 (2011): Table A.11 – Data Préparation Techniques (8.4)
WP7_009	Data Throughput	Rate of successful message delivery over a communication channel	-
WP3_6.1	Dedicated Mobile Legacy Network	Single-purpose network dedicated and optimized mainly for railway applications based on legacy technology (e.g. GSM-R for mainline)	
WP3_6.2	Dedicated Mobile Network	Single-purpose network dedicated and optimized for railway applications only based on future X2Rail-1 technology	
WP3_6.3	Dedicated Network with Supplementary Public Network	Single-purpose network dedicated and optimized for rail only based on future X2Rail-1 technology in combination with a public mobile network with little or no adaptation to rail-specific needs	
WP3_6.4	Dedicated Network, RAN Sharing with Public Operator	Single-purpose Core Network (CN) dedicated to rail, Radio Access Network (RAN) (including both non-transmission related equipment (sites, masts, power supply...) and transmission related equipment) shared with public operator.	
WP6_42	defect	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> A flaw in a component or system that can cause the component or system to fail to perform its required function, e.g., an incorrect statement or data definition. A defect, if encountered during execution, may cause a failure of the component or system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP8_030	Defense-in-Breadth	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).	NIST SP 800-53 r4

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP8_032	Defense-in-Depth defense in depth	Provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack. <u>Note to entry:</u> Defense in depth implies layers of security and detection, even on single systems, and provides the following features: * attackers are faced with breaking through or bypassing each layer without being detected * a flaw in one layer can be mitigated by capabilities in other layers * system security becomes a set of layers within the overall network security	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_034	Degraded Mode	mode of operation in the presence of faults which have been anticipated in the design of the control system <u>Note to entry:</u> Degraded modes allow the control system to continue to provide essential functions despite the deficiency of one or several system elements, e.g. malfunction or outage of control equipment, disruption of communication due to failure or intentional system isolation in response to identified or suspected compromise of subsystems.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_041	Degraded Operation	Operation resulting from an unplanned event that prevents the normal delivery of train services.	ERA Glossary of Railway Terms, 8th November 2010, available at http://www.era.europa.eu/Document-Register/Pages/Glossary-of-railway-terms.aspx .
WP8_126	demilitarized zone DMZ	1) Perimeter network segment that is logically between internal and external networks. 2) Common, limited network of servers joining two or more zones for the purpose of controlling data flow between zones. <u>Note to entry:</u> The purpose of a demilitarized zone is to enforce the internal network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks. <u>Note to entry:</u> In the context of IACS, the term "internal network" is typically applied to the network or segment that is the primary focus of protection. For example, a control network could be considered "internal" when connected to an "external" business network. <u>Note to entry:</u> DMZ's are typically used to avoid direct connections between different zones.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_127	denial of service DoS	Prevention or interruption of authorized access to a system resource or the delaying of system operations and functions. <u>Note to entry:</u> In the context of IACS denial of service can refer to loss of process function, not just loss of data communications.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_042	Depot	A location used for maintenance and storage of rolling stock.	
WP3_3.22	Depot Staff	Staff based at a depot	
WP4_043	Derailment Detection	A functionality which detects a train derailment.	
WP8_035	Device	asset incorporating one or more processors with the capability of sending or receiving data or control to or from another asset <u>Note to entry:</u> Examples include controllers, HMIs, PLCs, RTUs, transmitters, actuators, valves, network switches, etc.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_044	Dispatch Order	The process whereby signallers or controllers can change the order or timing of trains to maximise overall train service performance in real time.	
WP4_045	Disruptive Event	Any event or circumstance which prevents or disrupts the operation of trains.	
WP8_036	Distributed Control System	type of control system in which the system elements are dispersed but operated in a coupled manner Note 1 to entry: Distributed control systems may have shorter coupling time constants than those typically found in SCADA systems. Note 2 to entry: Distributed control systems are commonly associated with continuous processes such as electric power generation; oil and gas refining; chemical, pharmaceutical and paper manufacture, as well as discrete processes such as automobile and other goods manufacture, packaging, and warehousing.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP3_1.7	Distribution	The distribution of applications is defined by three different categories (see table).	UIC FRMCS User Requirements Specification, V2.
WP8_037	Domain Security Domain(s)	Environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources	
WP4_046	Door Release	An external system command which permits the door open command. A release may include mechanical, electromechanical or electronic parts.	

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP3_3.1	Drivers	A person capable and authorised to drive trains, including locomotives, shunting locomotives, work trains, maintenance railway vehicles or trains for the carriage of passengers or goods by rail in an autonomous, responsible and safe manner	UIC FRMCS User Requirements Specification, V2.
WP5_006	Driving on sight	The driver driving at a speed that allows him to stop the train to avoid obstacles on the track.	Subset-023
WP4_047	Dwell Time	Time during which a train is stopped at a Stopping Point, it means the time period between wheel stop and wheel start.	
WP4_048	Dwell Timer	A function used to determine the amount of time left until departure.	
WP6_45	dynamic testing	[ISTQB (http://glossar.german-testing-board.info/)] Testing that involves the execution of the software of a component or system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP8_128	eavesdropping	Monitoring or recording of communicated information by unauthorized parties.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_038	Edge Device	communication security asset, within a zone or conduit, that provides an interface between a zone and a conduit	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_039	Electronic Security	actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets <u>Note to entry:</u> The objective is to reduce the risk of causing personal injury or endangering public health, losing public or consumer confidence, disclosing sensitive assets, failing to protect business assets or failing to comply with regulations. These concepts are applied to any system in the production process and include both stand-alone and networked components. Communications between systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control, or exchange data with any of these control systems. Electronic security includes the concepts of identification, authentication, accountability, authorization, availability, and privacy.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP6_48	EMC	The ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment [EN61000-2-2, 2002]	[EN61000-2-2, 2002]
WP7_010	Emergency Power System	Independent source of electrical power (backup) that supports important electrical systems on loss of normal power supply	-
WP4_049	Emergency Release	A device accessible under certain conditions which permits the operation of an apparatus in case of failure.	IEC 60050-821:1998: International Electrotechnical Vocabulary - Part 821: Signalling and security apparatus for railways
WP8_129	encryption	Cryptographic transformation of plaintext into ciphertext that conceals the data's original meaning to prevent it from being known or used (see "decryption"). <u>Note to entry:</u> If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP5_007	End of Authority	Location to which the train is permitted to proceed and where target speed = zero.	Subset-023
WP5_008	End of Movement Authority	Location to which the train is permitted to proceed according to an MA. When transmitting an MA, it is the end of the last section given in the MA.	Subset-023
WP8_040	End User	individual or company responsible for the components that make up the production process (see "asset owner")	[ISA/IEC 62443-1-2, D1E6, 2017]
WP3_2.13	Energy Efficient Operation	The design of a system or service should minimise energy and environmental impacts.	
WP7_011	Energy Harvesting	Energy harvesting is the process by which energy is derived from external sources (e.g. solar power, wind energy, etc., also known as Ambient Energy) and converted into electrical energy for its use (to supply a load) or storage	-
WP7_012	Energy Storage	Process and/or equipment suited to capture and retain energy for use a later time	-
WP3_3.19	Engineering Staff	Staff tasked with railway engineering research, development, maintenance duties	

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP6_46	Environment	<p style="text-align: center;">May 2018</p> <p>[ISO/IEC/IEEE 24765, 2010]</p> <p>1. anything affecting a subject system or affected by a subject system through interactions with it, or anything sharing an interpretation of interactions with a subject system. IEEE Std 1175.1-2002 (R2007) IEEE Guide for CASE Tool Interconnections — Classification and Description.3.6. 2. the configuration(s) of hardware and software in which the software operates. ISO 9127:1988, Information processing systems — User documentation and cover information for consumer software packages.3.2.8.</p> <p>3. the circumstances, objects, and conditions that surround a system to be built. IEEE Std 1362-1998 (R2007) IEEE Guide for Information Technology — System Definition — Concept of Operation Document.3.9.</p> <p>4. the circumstances, objects, and conditions that will influence the completed system. IEEE Std 1233-1998 (R2002) IEEE Guide for Developing System Requirements Specifications.3.9.</p> <p>5. a concept space, i.e., an area in which a concept has an agreed-to meaning and one or more agreed-to names that are used for the concept. IEEE Std 1320.2-1998 (R2004) IEEE Standard for Conceptual Modeling Language Syntax and Semantics for IDEF1X97 (IDEFobject).3.1.57</p>	[ISO/IEC/IEEE 24765, 2010]
WP8_041	Environment	<p>1) aggregate of external procedures, conditions and objects affecting the development, operation and maintenance of the IACS</p> <p>2) surrounding objects, region or circumstances which may influence the behavior of the IACS and/or may be influenced by the IACS</p>	[ISA/IEC 62443-1-2, D1E6, 2017]
WP6_47	Environmental tests	<p>Tests regarding environmental conditions. Environmental tests are a group of tests composed by climate tests, vibration tests, solar tests, tests with sand and dust, electromagnetic susceptibility and emission etc.</p> <p>[mail from MerMec]</p>	[mail from MerMec]
WP3_2.8	Equipment reliability	The probability that an item (here: equipment) can perform a required function under given conditions (here: allows communication with the given QoS parameters) for a given time interval.	EN 5126 - Railway applications- The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
WP3_4.14	ERC / EC	European Research Council / European Commission	
WP6_49	error	<p><u>EN 50128:2011:</u></p> <p>error, fault defect, mistake or inaccuracy which could result in failure or in a deviation from the intended performance or behaviour</p>	EN 50128:2011:
WP4_050	ERTMS Users Group	The European Economic Interest Group established in 1995 by the national railways of France, Germany and Italy. The group currently consists of the infrastructure managers: ADIF (Spain), Banedanmark (Denmark), Banverket (Sweden), DB (Germany), Infrabel (Belgium),	
WP3_4.16	ESA	European Space Agency	
WP8_042	Essential Function	<p>function or capability that is required to maintain health, safety, the environment, and availability for the equipment under control.</p> <p><u>Note to entry:</u> Essential functions include but are not limited to the safety instrumented function (SIF), the control function, and the ability of the operator to view and manipulate the equipment under control, The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively. In some industries additional functions such as history may be considered essential</p>	[ISA/IEC 62443-1-2, D1E6, 2017]
WP3_4.15	ETSI/TC RT	European Telecommunications Standards Agency / Technical Committee Railways Telecommunications	
WP7_013	European Train Control System (ETCS)	A subset of ERTMS providing a level of protection against over speed and overrun depending upon the capability of the line side infrastructure	-

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP8_044	Evaluation	assessment of a PP, an ST or a TOE, against defined criteria Authors note: PP Protection Profile ST Security Target ToE Target of Evaluation	May 2018 CC-1, CCMB-2012-09-001
WP8_043	Event	occurrence of or change to a particular set of circumstances <u>Note to entry:</u> In an IACS this may be an action taken by an individual (authorized or unauthorized), a change detected within the control system (normal or abnormal), or an automated response from the control system itself (normal or abnormal).	[ISA/IEC 62443-1-2, D1E6, 2017]
WP6_51	expected result	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> The behavior predicted by the specification, or another source, of the component or system under specified conditions.	[ISTQB (http://glossar.german-testing-board.info/)]
WP4_051	External systems	Any system that is outside of the ATO over ETCS system but which interfaces to it.	
WP4_052	External Train HMI	The interface between local operations staff not travelling on the train and the train. Also see Human Machine Interface.	
WP7_014	Facing points	Points where the moving end of the blades face approaching traffic.	-
WP6_52	factory acceptance testing	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> Acceptance testing conducted at the site at which the product is developed and performed by employees of the supplier organization, to determine whether or not a component or system satisfies the requirements, normally including hardware as well as software.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_53	failover testing	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> Testing by simulating failure modes or actually causing failures in a controlled environment. Following a failure, the failover mechanism is tested to ensure that data is not lost or corrupted and that any agreed service levels are maintained (e.g., function availability or response times).	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_54	failure	<u>EN 50128:2011:</u> unacceptable difference between required and observed performance	EN 50128:2011:
WP6_55	fault	<u>EN 50128:2011:</u> error, fault defect, mistake or inaccuracy which could result in failure or in a deviation from the intended performance or behaviour	EN 50128:2011:
WP7_015	Field elements	Summary term for signalling devices which are connected with the interlocking machine and are situated outside it, e.g. points, signals, track circuits and axle counters.	-
WP8_130	firewall	1) Inter-network connection device that restricts data communication traffic between two connected networks. 2) Hardware device or software package that provides filtering and/or provision of rules to allow or deny specific types of network traffic to flow between internal and external networks. <u>Note to entry:</u> A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), that forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP5_009	Fixed Block	A block in which the extremities of the block sections are at fixed locations. The signalling allows a train to move from one block to the next, normally only when the block ahead is clear.	Subset-023
WP3_3.30	Fixed System	Fixed communication system not on board a train (which may or may not be track-side).	
WP5_010	Fixed Virtual Block	A signalling system where trains are separated by virtual blocks configured when a scheme is engineered, and where virtual block occupancy is derived from Train Position Reports.	--
WP3_5.4	Freight	A dedicated freight line (no passengers) that spans between cities and possibly across nations.	
WP3_1.16	Frequency of Use	Frequency of use reflects how often and/or the duration the application is used by an active user at a certain location in a certain operational situation.	UIC FRMCS User Requirements Specification, V2.
WP7_016	Fuel Cell	Electrochemical device that converts the chemical energy from a fuel into electricity; in this context it is considered as a power supply source	-
WP5_011	Full Moving Block	A signalling system where trains are separated based only on Train Position Reports, without the use of virtual blocks.	--

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP4_053	Full Service Brake	Service Brake set at maximum allowed effort.	May 2018
WP4_133	Functional Architecture	This corresponds to the functional boundaries between the ATO System and the other functional components (Obstacle Detection, Antenna, ...). These boundaries are described in the FIS or FFFIS. It also includes the parting of the KERNEL into different functions.	
WP6_59	functional testing	Testing conducted to evaluate the compliance of a system or component with specified functional requirements. <u>[ISO/IEC/IEEE 24765, 2010]</u>	[ISO/IEC/IEEE 24765, 2010]
WP4_054	Generic Application	Application which contains all mandatory and all or a subset of optional functions, with predefined configurability and customisable for different specific applications.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP4_055	Global Navigation Satellite System	A worldwide position, time and velocity radio determination system comprising space, ground and user segments. (EN 61209:1999-08)	
WP3_4.3	Government	National or regional body mandating a governance and regulatory framework placing specific legal, financial, operational, strategic, social and contractual obligations on Infrastructure Managers and Railway Undertakings.	
WP4_056	Grade of Automation	Automation level of train operation, in which a train can be operated, resulting from sharing responsibility for given basic functions of train operation between operations staff and system.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP4_057	Grade of Automation 0 (GoA0) On-sight train operation	In this grade of automation, the driver has full responsibility and no system is required to supervise his activities. However, points and single tracks can be partially supervised by the system.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP4_058	Grade of Automation 1 (GoA1) Non-automated train operation	In this grade of automation, the driver is in the front cabin of the train observing the guideway and stops the train in the case of a hazardous situation. Acceleration ^[1] and braking are commanded by the driver in compliance with wayside signals or cab-signal. The system supervises the activities of the driver. This supervision may be done at specific locations, be semi-continuous or continuous, notably in respect of the signals and the speed. Safe departure of the train from the station, including door closing, is the responsibility of the operations staff. Note: Acceleration is used in this context as a common term for traction.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP4_059	Grade of Automation 2 (GoA2) Semi-automated train operation	In this grade of automation, the driver is in the front cabin of the train observing the guideway and stops the train in the case of a hazardous situation. Acceleration and braking is automated and the speed is supervised continuously by the system. Safe departure of the train from the station is the responsibility of the operations staff (door opening and closing may be done automatically).	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP4_060	Grade of Automation 3 (GoA3) Driverless train operation	In this grade of automation, additional measures are needed compared to GOA2 because there is no driver in the front cabin of the train to observe the guideway and stop the train in case of a hazardous situation. In this grade of automation, a member of the operations staff is necessary on-board. Safe departure of the train from the station, including door closing, can be the responsibility of the operations staff or may be done automatically.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP4_061	Grade of Automation 4 (GoA4) Unattended train operation	In this grade of automation, additional measures are needed compared to GOA3 because there is no on-board operations staff. Safe departure of the train from the station, including door closing, has to be done automatically. More specifically, the system supports detection and management of hazardous conditions and emergency situations such as the evacuation of passengers. Some hazardous conditions or emergency situations, such as derailment or the detection of smoke or fire, may require staff interventions.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP6_172	grey-box testing	<u>WP6 definition from Giuseppe Savino:</u> Grey Box testing is a combination of White Box and Glass Box Testing. In this type of testing, the tester has little knowledge about the internal working of the software, so he tests the output as well as process carried out to generate the output. Grey-box testing refers to a testing system by knowing limited information about the internals of the system. The knowledge is always limited for detailed design documents and architecture diagrams. In concise, it is a good blend of black and white box testing, which leverage the strengths of each. A little knowledge of the system is expected in Gray box testing.	WP6 definition from Giuseppe Savino:
WP6_60	Hardware	1) Physical equipment used to process, store, or transmit computer programs or data. 2) All or part of the physical components of an information system. <u>[ISO/IEC/IEEE 24765, 2010]</u>	[ISO/IEC/IEEE 24765, 2010]
WP6_61	Hardware tests	Tests regarding hardware.	
WP4_062	Hazard	Potential source of harm	ISO Guide 73:2009: Risk management – Vocabulary

Deliverable D2.3
Terminology for the future Signalling and Automation System

May 2018

WP4_063	Headway	The time interval between the passing of the front ends of successive vehicles or trains moving along the same lane or track in the same direction.	
WP4_064	Human Machine Interface (HMI)	Part of a system an operator interacts with. The interface is the aggregate of means by which the users interact with a machine, device, and system (the system). The interface provides means for input, allowing the users to control the system and output, allowing the system to inform the users.	EN 61924-2:2013: Maritime navigation and radiocommunication equipment and systems - Integrated navigation systems - Part 2: Modular structure for INS - Operational and performance requirements, methods of testing and required test results
WP8_045	Human-Machine Interface	aggregate of means by which people (the users) interact with a particular machine, device, computer program or other complex tool (the system) Note to entry: In many cases, these involve video screens or computer terminals, push buttons, auditory feedback, flashing lights, etc. The human-machine interface provides means of: * Input, allowing the users to control the machine * output, allowing the machine to inform the users	[ISA/IEC 62443-1-2, D1E6, 2017]
WP3_4.12	IEEE	The Institute of Electrical and Electronic Engineers (IEEE) is, amongst others, responsible for the standardization of the IEEE 802.11 Wi-Fi standard family.	
WP8_046	Impact	evaluated consequence of a particular event	ISA TR62443-1-2, D1E5
WP5_012	In advance of	A term indicating a point beyond a specific location on the track, with respect to a given direction.	Subset-023
WP5_013	In rear of	A term indicating a point on the approach to a specific location on the track, with respect to a given direction.	Subset-023
WP8_047	Incident	event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system	ISA TR62443-1-2, D1E5
WP8_048	Industrial Automation and Control Systems (IACS)	1) collection of personnel, hardware, and software that can affect or influence the safe, secure and reliable operation of an industrial process 2) collection of personnel, hardware, software and policies involved in the operation of the industrial process ant that can affect or influence its safe, secure, and reliable operation Note to entry: These systems include, but are not limited to: * industrial control systems, including distributed control systems (DCSs) * programmable logic controllers (PLCs) * remote terminal units (RTUs) * intelligent electronic devices * supervisory control and data acquisition (SCADA) * networked electronic sensing and control, and monitoring and diagnostic systems (In this context, process control systems include basic process control system and safety-instrumented system [SIS] functions, whether they are physically separate or integrated.) * associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems * associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_049	Industrial Control System (ICS)	see Industrial Automation and Control Systems (IACS)	WP8
WP8_050	Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. [CNSSI 4009] An instance of an information type. [FIPS 199]	NIST SP 800-53 r4
WP8_051	Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.	NIST SP 800-53 r4
WP8_052	Information System (IS)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. <u>Note to entry:</u> Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.	NIST SP 800-53 r4

Deliverable D2.3

Terminology for the future Signalling and Automation System

WP8_053	Information System Resilience	The ability of an information system to continue to: May 2018 (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.	NIST SP 800-53 r4
WP8_054	Information Technology (IT)	computer-related assets of an organization that represent nonphysical assets, such as software applications, process programs, and personnel files Note to entry 1: Throughout this document, this use of the term of information technology is not abbreviated. Note to entry 2: Another use of information technology (IT) refers to the company's internal organization (e.g., the IT department) or the items traditionally maintained by this department (i.e., the administrative computers, servers, and network infrastructure). Throughout this document, this use of the term information technology is abbreviated as IT.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_065	Infrastructure Equipment	Fixed installations of the railway system (e.g. tracks, power supply, signalling, communication).	LC/TS 50591:2013: Specification and verification of energy consumption for railway rolling stock
WP3_3.18	Infrastructure Manager	Any body or undertaking that is responsible in particular for establishing and maintaining railway infrastructure. This may also include the management of infrastructure control and safety systems. The functions of the infrastructure manager on a network or part of a network may be allocated to different bodies or undertakings.	ERA Glossary / Directive 21/14/EC On the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification
WP8_055	Initial Risk	risk before controls or countermeasures have been applied (See "risk")	ISA TR62443-1-2, D1E5
WP8_131	insider	"trusted" person, employee, contractor, or supplier who has information that is not generally known to the public (See "outsider").	[ISA/IEC 62443-1-2, D1E6, 2017]
WP3_2.7	Installability	Installability is the ease with which a system, a service or an application can be successfully installed in its environments in a timely and cost-efficient manner.	
WP6_63	integration test	The progressive linking and testing of programs or modules in order to ensure their proper functioning in the complete system. <u>[ISO/IEC/IEEE 24765, 2010]</u>	[ISO/IEC/IEEE 24765, 2010]
WP6_62	integration testing	[ISTQB (http://glossar.german-testing-board.info/)] Testing performed to expose defects in the interfaces and in the interactions between integrated components or systems.	[ISTQB (http://glossar.german-testing-board.info/)]
WP8_056	Integrity	1) quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data 2) property of protecting the accuracy and completeness of assets 3) guarding against improper modifications or destruction, and includes ensuring information non-repudiation and authenticity (FIPS 199) Note to entry: in a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_132	interception	Capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission, and other communication attributes.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_067	Interchangeability	Is the capability of system components identified in this document to be procured from any number of suppliers and replaced without any substantial change in functionality or performance.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP6_64	interface testing	Testing conducted to evaluate whether systems or components pass data and control correctly to one another. <u>[ISO/IEC/IEEE 24765, 2010]</u>	[ISO/IEC/IEEE 24765, 2010]
WP4_068	Interlocking	An arrangement of switches and signals interconnected in a way that each movement follows the other in a proper and safe sequence.	ERA Glossary of Railway Terms, 8th November 2010, available at http://www.era.europa.eu/Document-Register/Pages/Glossary-of-railway-terms.aspx .
WP5_014	Interlocking	A general term applied to the controlling of the setting and releasing of "signals" (<i>if any</i>) and "points" to prevent unsafe conditions arising, and equipment which performs this function. Note - Definition as from Subset-023: A general term applied to the controlling of the setting and releasing of "signals" and "points" to prevent unsafe conditions arising, and equipment which performs this function.	Derived from Subset-023

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP7_017	Interlocking	A system that, in accordance with commands from a signaling or signaling control system, manages track side equipment and the safe movement of rail traffic.	-
WP6_65	interoperability	1) The ability of two or more systems or components to exchange information and to use the information that has been exchanged 2) The capability to communicate, execute programs, and transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units. 3) The ability of a rail system to allow the safe and uninterrupted movement of trains which accomplish the required levels of performance. This ability depends on all the regulatory, technical and operational conditions which must be met in order to satisfy the essential requirements.	1) ISO/IEC/IEEE 24765, 2010 2) Interoperability Directive 2008/57/EC 3) ERA Glossary / Directive 2008/57/EC on the interoperability of the rail system within the Community
WP6_68	interoperability testing	1) Testing conducted to ensure that a modified system retains the capability of exchanging information with systems of different types, and of using that information. [ISO/IEC/IEEE 24765, 2010]	[ISO/IEC/IEEE 24765, 2010]
WP8_133	intrusion detection	Security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP7_018	IT Security	Protection of systems from the theft or damage to their software or information, as well as from disruption or misdirection of the services	-
WP6_164	IT security tests	System or component testing whose primary objective is to discover vulnerabilities. Vulnerabilities include those that cause denial of service [ISA-62443-2-4]	ISA-62443-2-4
WP4_070	Jerk	First derivative of the acceleration with respect to time.	
WP4_071	Jog	The functionality that provides low speed control in both forward and reverse directions to enable correction of a train's alignment with a defined stopping location.	
WP3_6.8	Join Mission Critical Network (shared with, e.g., PPDR)	Dedicated mobile network adapted to the needs of multiple mission critical sectors (rail, PPDR...)	
WP4_072	Journey	Scheduled movement of a vehicle along a single route.	EN 13816:2002: Transportation - Logistics and services - Public passenger transport; Service quality definition, targeting and measurement
WP4_073	Journey Profile	The Journey Profile contains the set of dynamic infrastructure data and operational data required by the ATO-OB in order to drive the train. The operational data contains the list of Timing Points to be traversed by the train along its journey. This list is defined in real time on the basis of the scheduled timetable and on-line traffic regulation. The Journey Profile may be updated during the journey.	
WP8_134	key management	Process of handling and controlling cryptographic keys and related material (such as initialization values) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the keys and related material.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_074	Kinematic Envelope	Kinematic load gauge further enlarged to allow for possible tolerances in the position of the track.	[RD18] EN 50119:2009: Railway applications - Fixed installations - Electric traction overhead contact lines
WP5_015	L3 On-board	An EVC which is capable of operating at ETCS Level 3. It will also operate at other ETCS Levels.	--
WP6_162	laboratory	WP6 definition from Oliver Röwer: A laboratory is a facility that provides a test environment and controlled environmental conditions for testing.	WP6 definition from Oliver Röwer:
WP3_1.8	Latency	The end-to-end user transport delay between the involved communication entities.	
WP8_057	Legacy System	existing industrial automation and control system in a facility that may not be available as a commercial off the shelf (COTS) item Note to entry: A legacy system may have been COTS at one time, but it may be no longer available and/or supported.	ISA TR62443-1-2, D1E5
WP3_2.17	Legal obligations	Ability to fulfil legal obligations (e.g. ownership of mission critical infrastructure)	

Deliverable D2.3

Terminology for the future Signalling and Automation System

WP5_016	Level 3	A level of ERTMS/ETCS that uses radio to pass movement authorities to the train. Level 3 uses train reported position and integrity to determine if it is safe to issue the movement authority.	Subset-023
WP7_019	Level crossing	An intersection at grade between roads and railway tracks that may or may not be protected by lights, barriers or other equipment.	-
WP7_020	Level crossing system	The driving and detection system of the protection devices of a level crossing	-
WP8_058	Life Cycle Life-Cycle	Evolution of a system, product, service, project or other human-made entity from conception through retirement. <u>Note to entry:</u> Sources include ISO/IEC 15288 and ISO/IEC 12207	[ISA/IEC 62443-1-2, D1E6, 2017]
WP7_021	Life Cycle Cost	Sum of all recurring and one-time (non-recurring) costs over the full life span or a specified period of a good, service, structure or system	-
WP8_059	Likelihood	quantitative chance that an incident may occur	ISA TR62443-1-2, D1E5
WP3_1.19	Line	Operation along a line setting between stations and yards, where line is defined as: One or more adjacent running tracks forming a route between two points. Where a section of network comprises two or more lines running alongside one another, there are as many lines as routes to which tracks are allotted exclusively.	ERA Glossary / Glossary for Transport Statistics
WP4_075	Line Clear Detection	Automatic proving or detection that a line is clear or occupied.	IEC 60050-821:1998: International Electrotechnical Vocabulary - Part 821: Signalling and security apparatus for railways
WP3_1.10	Link Reliability	The probability that an item (here: communication link) can perform a required function under given conditions (here: allows communication with the given QoS parameters) for a given time interval.	EN 5126 - Railway applications- The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
WP7_022	Load Levelling	A method for reducing the large fluctuations that occur in electricity demand, for example by storing excess electricity during periods of low demand for use during periods of high demand	-
WP6_69	load testing	[ISTQB (http://glossar.german-testing-board.info/)] A type of performance testing conducted to evaluate the behavior of a component or system with increasing load, e.g., numbers of parallel users and/or numbers of transactions, to determine what load can be handled by the component or system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP7_023	Load/charge Cycles	The process of accumulating energy in an energy storage system (e.g. Supercap or rechargeable battery) and discharging it providing supply to a load.	-
WP4_076	Lock	Force a functional unit to maintain a defined value of the output variable independent of all other input variables or state variables.	EC 60050-351:2013:International electrotechnical vocabulary - Part 351: Control technology
WP3_2.3	Longevity	The useful life of a system, unless otherwise agreed at the time of tendering between the equipment manufacturer and the user, shall be taken as 20 years.	EN5155:27
WP3_5.1	Mainline	A dedicated (high-speed) passenger line / train that spans between cities and possibly across the nations.	
WP3_2.4	Maintainability	The probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources.	EN 5126 - Railway applications- The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
WP7_025	Maintenance	The combination of all technical and administrative actions, including supervisory actions, intended to retain a product in, or restore it to, a state in which it can perform a required function.	-
WP4_077	Maintenance Staff	Maintenance staff are persons who are involved in maintenance of infrastructure and rolling stock.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP7_026	Maintenance System	composite of all maintenance resources that must be acquired for maintaining the system throughout its life cycle, including: Spare parts data/documentation/storage; Maintenance procedures; Maintenance manuals; Maintenance facilities (power supplies, offices, building of testing centres); External testing equipment; Special tools; Training of maintenance personnel.	-
WP8_135	malicious code	Programs or code written for the purpose of gathering information about systems or users, destroying system data, providing a foothold for further intrusion into a system, falsifying system data and reports, or providing time-consuming irritation to system operations and maintenance personnel. <u>Note to entry:</u> Malicious code attacks can take the form of viruses, worms, Trojan Horses, or other automated exploits. <u>Note to entry:</u> Malicious code is also often referred to as "malware".	[ISA/IEC 62443-1-2, D1E6, 2017]

Deliverable D2.3

Terminology for the future Signalling and Automation System

WP8_060	Management System	CSMS (cybersecurity management system) program designed by an organization to maintain the security of the entire organization's assets to an established level of confidentiality, integrity, and availability, whether they are on the business side or the industrial automation and control systems side of the organization.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP5_018	Max safe front end	The maximum safe front end position differs from the estimated position by the Under-reading Amount in the distance measured from the LRBG plus the Location Accuracy of the LRBG.	Subset-023
WP5_017	May	Is permissible.	Subset-023
WP3_5.2	Metro/Urban	A dedicated urban (mass transit) passenger line / train that spans part or all of a city and possibly as far as the neighboring towns (with sections both above and below ground).	
WP7_024	MIB: Management Information Base	A management information base (MIB) is a formal description of variables that can be managed using the Simple Network Management Protocol (SNMP). Characteristics of variables such as type of data and access criteria can be defined.	-
WP3_2.10	Migration	Necessity of a system to migrate from an existing one to a new one. This includes the possibility of co-existing with a legacy system and its applications.	
WP5_019	Min safe front end	The minimum safe front end position differs from the estimated position by the Over-reading Amount in the distance measured from the LRBG plus the Location Accuracy of the LRBG.	Subset-023
WP5_020	Min safe rear end	The min safe rear end position shall be calculated by subtracting the train length (acquired as Train Data) from the min safe front end position	CR940
WP4_078	Minimum Dwell Time	Minimum allowed value of dwell time, defined for each stopping point included in the journey profile, to be considered by the ATO-OB before departure. The minimum dwell time is applied during normal or degraded operation to aid service recovery	
WP5_021	Mission, ETCS	Any train movement started under the supervision of an ERTMS/ETCS on-board equipment in one the following modes: FS, LS, SR, OS, NL, UN, or SN. The ETCS mission is ended when any of the following modes is entered: SB, SH.	Subset-023
WP6_70	mistake	Mistake 1. a human action that produces an incorrect result NOTE: The fault tolerance discipline distinguishes between a human action (a mistake), its manifestation (a hardware or software fault), the result of the fault (a failure), and the amount by which the result is incorrect (the error). See Error	[ISO/IEC/IEEE 24765, 2010], ISTQB (http://glossar.german-testing-board.info/)
WP4_079	Modular Design	Is a design approach that subdivides a system into smaller parts called modules or skids, that can be independently created and then used in different systems. A modular system can be characterized by functional partitioning into discrete scalable, reusable modules; rigorous use of well-defined modular interfaces; and making use of industry standards for interfaces.	Wikipedia
WP6_72	monkey testing	[ISTQB (http://glossar.german-testing-board.info/)] Testing by means of a random selection from a large range of inputs and by randomly pushing buttons, ignorant of how the product is being used.	[ISTQB (http://glossar.german-testing-board.info/)]
WP7_027	Moveable frog	A pivoting or flexible frog (common crossing) that is operated by a point machine to close the rail gap at the frog in accordance to the route that is set up.	-
WP5_023	Movement Authority	Permission for a train to move to a specific location with supervision of speed. Note - Definition as from Subset-023: Permission for a train to run to a specific location within the constraints of the infrastructure.	Derived form Subset-023
WP5_024	Moving Block	A block whose length is defined by the position of the train occupying the section of track ahead. The minimum block length would be from the rear most part of the occupying train to a point on the track where, if the train braked from its current speed, the front of the occupying train would be when the train came to a stand.	Subset-023
WP6_73	negative testing	[ISTQB (http://glossar.german-testing-board.info/)] Tests aimed at showing that a component or system does not work. Negative testing is related to the tester's attitude rather than a specific test approach or test design technique, e.g., testing with invalid input values or exceptions.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_74	Net Access	In Switzerland the proof of operability of a system was done by so called " NetAcces" tests. Now they are called "Operational Interoperability Tests" (IOP tests).	[mail from Bombardier]

Deliverable D2.3
Terminology for the future Signalling and Automation System

		May 2018	
WP3_2.14	Network CAPEX	Network investment costs	
WP3_2.15	Network OPEX	Network operating costs	
WP3_2.11	Network Security Risk	Combination of the probability of occurrence of harm and the severity of that harm.	IEC 6158-4:21; ISO/IEC Guide 51:1999, definition 3.2
WP4_080	Neutral Section	An arrangement of insulators in the Overhead Line Equipment designed to ensure that two sections are kept electrically separate even during the passage of a pantograph.	
WP7_028	Non Vital Data	Data communication that is not safety critical	-
WP4_081	Non-ATO Train	Non-ATO equipped trains and trains with inoperative ATO on-board equipment.	
WP6_75	non-functional requirement	[ISTQB (http://glossar.german-testing-board.info/)] A requirement that does not relate to functionality, but to attributes such as reliability, efficiency, usability, maintainability and portability.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_77	non-functional testing	[ISTQB (http://glossar.german-testing-board.info/)] Testing the attributes of a component or system that do not relate to functionality, e.g., reliability, efficiency, usability, maintainability and portability.	[ISTQB (http://glossar.german-testing-board.info/)]
WP8_136	non-repudiation	1) Security service that provides protection against false denial of involvement in a communication. 2) Ability to prove the occurrence of a claimed event or action and its originating entities. 3) Assurance that the sender of information is provided with proof of delivery and the recipient is viny processed the information. <u>Note to entry:</u> The purpose of non-repudiation is to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_082	Obstacle Detection	A sub-system able to supervise the area in front of or around the train in order to detect and identify objects on or close to the track that might adversely affect safe train operation.	
WP5_025	Occupied	A portion of track (i.e a track section if Track Vacancy Detection devices are used) having any part of a train present upon it.	Derived from Subset-023
WP3_3.31	On-board System	Communication system on-board of a train excluding application(s).	
WP7_029	Open System Interconnection (OSI)	Conceptual and logical layout (composed of 7 layers) that defines network communication used by systems open to interconnection and communication with other systems	-
WP3_1.14	Operational Maximum Speed of Device	Maximum speed that a user (which can be a human or a system) is travelling at, and the application remains operational.	UIC FRMCS User Requirements Specification, V2.
WP4_083	Operations	Operation covers all functions which deal with the safety and regular exploitation of the transportation service.	FprEN 62580-1:2013: Electronic railway equipment - On-board multimedia and telematic subsystems for railways - Part 1: General Architecture (IEC 9/1775/CDV:2013)
WP4_084	Operations Control Centre (OCC)	Is the centre from which operation of the line or the network is supervised and managed.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP4_085	Operations Staff	Staff authorised to perform tasks concerning train operation or direct service to passengers.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP8_061	Operator	particular type of user that is usually responsible for the correct operation of the equipment under control	ISA TR62443-1-2, D1E5
WP7_030	OPEX	An operational expenditure (OPEX) is the money a company spends on an ongoing, day-to-day basis in order to run a business or system.	-
WP8_137	outsider	Person or group not "trusted" with inside access, who may or may not be known to the targeted organization (See "insider"). <u>Note to entry:</u> Outsiders may or may not have been insiders at one time.	[ISA/IEC 62443-1-2, D1E6, 2017]

Terminology for the future Signalling and Automation System

WP8_062	Overlay (<i>Security Control Overlay</i>)	A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.	NIST SP 800-53 r4
WP6_78	pass/fail criteria	[ISTQB (http://glossar.german-testing-board.info/)] Decision rules used to determine whether a test item (function) or feature has passed or failed a test.	[ISTQB (http://glossar.german-testing-board.info/)]
WP4_086	Passenger Information Systems	The on-board train or infrastructure based systems which provide passengers with real-time information relation to the operation of the railway.	
WP4_087	Passengers	People travelling or intending to travel on a train whose activities are not related to operating the train.	
WP4_088	Passing point	A Timing Point defined in the Segment Profile, where the train is planned to pass within a given time window defined in the Journey Profile.	
WP8_063	Penetration	successful unauthorized access to a protected system resource	ISA TR62443-1-2, D1E5
WP8_064	Penetration Testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.	NIST SP 800-53 r4
WP6_79	performance	The degree to which a system or component accomplishes its designated functions within given constraints, such as speed, accuracy, or memory usage. [ISO/IEC/IEEE 24765, 2010]	[ISO/IEC/IEEE 24765, 2010]
WP3_1.13	Permanent Virtual Connection	A permanent virtual connection is a connection that is permanently established between two or more users. It enables the creation of a logical connection on top of a physical connection between nodes that communicate frequently or continuously.	
WP3_3.4	Persons at Level Crossings	People (public) at level crossings, without specific activities related to the transport	
WP3_3.3	Persons on Platforms	People (passengers and non-travelling public) on platforms, without specific activities related to the transport.	
WP4_089	Perturbation	The operation of a transport system outside of the timetable, such that delays in arrival and departure from defined locations are present.	
WP4_090	Planning System	A system or set of systems using methods for scheduling or planning. Based on infrastructure, asset data and planning rules it provides timetables for both passenger and freight train operation.	
WP4_092	Platform / Train Interface (PTI - Predominantly used in the UK)	The interface between the platform and the train, gap included. It can include Platform Edge Doors, Platform Gates, Platform Screen Doors or platform edges equipped with none of these.	
WP4_091	Platform Barrier System	The system that keeps passengers at a safe distance from the platform edge, outside of boarding times. E.g. Platform Edge Doors, Platform Gates or Platform Screen Doors	
WP4_093	Platform Doors	The doors fixed to the platform forming a barrier between the passengers and the train and track. They include Platform Edge Doors, Platform Gates and Platform Screen Doors.	
WP4_094	Platform Edge Doors	Full height screens forming a barrier between the passengers and the train and track. They are only present on platform edges and have a gap of varying height above them to the ceiling of the station.	
WP4_095	Platform Gates	Commonly referred to as "half height" barriers, they separate passengers from the train and track at a platform. They are usually designed to be of reduced height, with a minimum height of 1 metre.	
WP4_096	Platform Screen Doors	Are full height screens which are fixed at the top and bottom of a platform to separate passengers from the train and track. They form a climatic barrier between the platform and track to facilitate cost effective platform climate control.	
WP4_097	Platform Skip	Is the functionality that enables a train to continue driving without stopping at a platform that had previously been scheduled as a stopping point.	
WP3_3.9	Platform Staff (Dispatchers)	Platform-based staff tasked with dispatching a train	
WP3_3.10	Platform Staff (Security)	Security staff on platforms	
WP5_026	Point	A section of track equipped so that train routes may converge or diverge.	Subset-023
WP7_032	Point heater	A device that caresses the blades against the freeze.	-
WP7_033	Point machine	A machine in the field equipment for the physical operation, locking and detection of points or other moveable track elements.	-
WP7_031	Points	Assembly of rails, blades and of auxiliaries, certain ones being movable, which effect the tangential branching of tracks and allows to run over either one track or another.	-

Deliverable D2.3
Terminology for the future Signalling and Automation System

		May 2018	
WP6_80	portability	<p><u>[ISO/IEC/IEEE 24765, 2010]</u> portability 1. the ease with which a system or component can be transferred from one hardware or software environment to another. 2. the capability of a program to be executed on various types of data processing systems without converting the program to a different language and with little or no modification. ISO/IEC 2382-1:1993, Information technology — Vocabulary — Part 1: Fundamental terms.01.04.06. Syn: transportability cf. machine-independent</p>	[ISO/IEC/IEEE 24765, 2010]
WP8_065	Potential Impact	loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect, a serious adverse effect, or a severe or catastrophic adverse effect on organizational operations, organizational assets, IACS or individuals	ISA TR62443-1-2, D1E5
WP7_035	Power consumption	Energy demand of a system (load) during operation. In this context is consumption that uses electric energy to manage object controllers and field elements and measured in Watt-hours [Wh]	-
WP7_036	Power Supply	A system that manages and provides electric energy to an electrical load. In this context, the power supply is mainly batteries and (super) capacitors together with electronics to convert electrical power to supply to its load. And equipment mainly to SWOC and Object Controller. The power supply obtains the energy from an energy source, e.g. from the power harvesting or from the electrical grid.	-
WP7_034	Powered points	A set of points operated by a machine.	-
WP4_099	Powerless section	A section where no electrical traction power is available.	
WP6_82	Principle Tests	<p><u>WP6 definition from Ed Morton:</u> The process of testing a Signalling System (in the UK) to ensure compliance with the requirements of UK Signalling Principles (contained within NR/L2/SIG/30009/GKRT0060).</p>	WP6 definition from Ed Morton:
WP3_1.15	Priority	Level of priority required for a specific application.	
WP6_83	problem	<p><u>[ISO/IEC/IEEE 24765, 2010]</u> problem 1. unknown underlying cause of one or more incidents. ISO/IEC 20000-1:2005, Information technology — Service management — Part 1: Specification.2.8 2. a negative situation to overcome NOTE risk factor becomes a problem when a risk metric (an objective measure) crosses a predetermined threshold (the problem trigger).</p>	[ISO/IEC/IEEE 24765, 2010]
WP5_027	Proceed aspect	Any signal aspect which permits the driver to pass the signal.	Subset-023

Deliverable D2.3
Terminology for the future Signalling and Automation System

May 2018

WP6_84	product	<p>[ISO/IEC/IEEE 24765, 2010] product</p> <p>1. an artifact that is produced, is quantifiable, and can be either an end item in itself or a component item. A Guide to the Project Management Body of Knowledge (PMBOK® Guide) — Fourth Edition.</p> <p>2. complete set of software and documentation. ISO/IEC 26514, Systems and software engineering — Requirements for designers and developers of user documentation.4.36.</p> <p>3. output of the software development activities (e.g., document, code, or model). IEEE Std 1074-2006 IEEE Standard for Developing a Software Project Life Cycle Process. Annex E. 4. result of a process. ISO/IEC 15939:2007, Systems and software engineering — Measurement process.3.33. Syn: material, goods</p> <p>cf. activity, deliverable, result</p> <p>NOTE [ISO 9000:2005] There are four agreed generic product categories: hardware (e.g., engine mechanical part); software (e.g., computer program); services (e.g., transport); and processed materials (e.g., lubricant). Hardware and processed materials are generally tangible products, while software or services are generally intangible. Most products comprise elements belonging to different generic product categories. Whether the product is then called hardware, processed material, software, or service depends on the dominant element.</p>	[ISO/IEC/IEEE 24765, 2010]
WP8_066	Product Supplier	<p>manufacturer of hardware and/or software product</p> <p>Note to entry: Used in place of the generic word “vendor” to provide differentiation.</p>	ISA TR62443-1-2, D1E5
WP6_86	product tests	Testing of a product.	WP6 definition
WP4_100	Progressive Shutdown of Train Service	Function designed to stop operation of trains in a safe and controlled way in case there is a failure.	
WP3_3.27	Public Emergency Operator	The nominated user who is responsible for answering public emergency calls.	UIC FRMCS User Requirements Specification, V2.
WP3_6.6	Public Network	Public mobile network with little adaptation to rail-specific needs	
WP3_6.5	Public Network with IM as MVNO	Public mobile network used for rail application with rail acting as Mobile Virtual Network Operator (MVNO)	
WP6_87	qualification	<p>[ISO/IEC/IEEE 24765, 2010] qualification</p> <p>1. process of demonstrating whether an entity is capable of fulfilling specified requirements. ISO/IEC 12207:2008 (IEEE Std 12207-2008), Systems and software engineering — Software life cycle processes.4.31; ISO/IEC 15288:2008 (IEEE Std 15288-2008), Systems and software engineering — System life cycle processes.4.22.</p> <p>2. the process of determining whether a system or component is suitable for operational use</p>	[ISO/IEC/IEEE 24765, 2010]
WP6_88	quality	<p>[ISO/IEC/IEEE 24765, 2010] quality</p> <p>1. the degree to which a system, component, or process meets specified requirements. IEEE Std 829-2008 IEEE Standard for Software and System Test Documentation.3.1.25.</p> <p>2. ability of a product, service, system, component, or process to meet customer or user needs, expectations, or requirements.</p> <p>3. the totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs. ISO/IEC 9126-1:2001, Software engineering — Product quality — Part 1: Quality model.B.21.</p> <p>4. conformity to user expectations, conformity to user requirements, customer satisfaction, reliability, and level of defects present. ISO/IEC 20926:2003, Software engineering — IFPUG 4.1 Unadjusted functional size measurement method — Counting practices manual</p> <p>5. the degree to which a set of inherent characteristics fulfils requirements. A Guide to the Project Management Body of Knowledge (PMBOK® Guide) — Fourth Edition.</p> <p>6. the degree to which a system, component, or process meets customer or user needs or expectations. IEEE Std 829-2008 IEEE Standard for Software and System Test Documentation.3.1.25</p>	[ISO/IEC/IEEE 24765, 2010]

Deliverable D2.3
Terminology for the future Signalling and Automation System

May 2018			
WP6_89	quality gate	[ISTQB (http://glossar.german-testing-board.info/)] A special milestone in a project. Quality gates are located between those phases of a project strongly depending on the outcome of a previous phase. A quality gate includes a formal check of the documents of the previous phase.	[ISTQB (http://glossar.german-testing-board.info/)]
WP4_101	Rail Adhesion	The friction between the wheels of a vehicle and the rails, which makes possible the transmission of tractive effort and braking force.	IEV 811: International Electrotechnical Commission – Electric traction
WP7_037	Rail changer	Motorised moveable element that enables the third rail of a mixed track to change sides.	-
WP3_3.23	Rail Network Operator	An organisation that operates a rail network which can be understood as a combination of RU (see 3.17) and IM (see 3.18), e.g., a metro operator who manages both trains and the underlying infrastructure.	
WP3_3.26	Railway Application Operator (Comms)	An organisation that operates an application for communicating to part / all of a railway(e.g., a department of an Infrastructure Manager).	
WP3_3.25	Railway Application Operator (Control)	An organisation that operates an application for controlling part or all of a railway (e.g., a department of an Infrastructure Manager).	
WP3_4.9	Railway Data & Information managers and developers	Those that collect data and information sourced from railway IMs and RUs, that is they process and pass on to users.	
WP3_4.8	Railway Infrastructure Manager (IM)	Any body or undertaking that is responsible in particular for establishing and maintaining railway infrastructure. This may also include the management of infrastructure control and safety systems. The functions of the infrastructure manager on a network or part of a network may be allocated to different bodies or undertakings.	ERA Glossary / Directive 21/14/EC On the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification
WP3_4.13	Railway Standard Bodies	Standardization bodies tasked with the development of railway specific standards.	
WP3_3.17	Railway Undertaking	Any public or private undertaking, licensed according to applicable Community legislation, the principal business of which is to provide services for the transport of goods and/or passengers by rail with a requirement that the undertaking must ensure traction; this also includes undertakings which provide traction only.	ERA Glossary / Directive 21/14/EC On the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification
WP6_90	random testing	[ISTQB (http://glossar.german-testing-board.info/)] A black-box test design technique where test cases are selected, possibly using a pseudo-random generation algorithm, to match an operational profile. This technique can be used for testing non-functional attributes such as reliability and performance.	[ISTQB (http://glossar.german-testing-board.info/)]
WP3_5.3	Regional	A remote low-capacity passenger line with few connections that spans between cities.	
WP6_91	regression testing	[ISTQB (http://glossar.german-testing-board.info/)] Testing of a previously tested program following modification to ensure that defects have not been introduced or uncovered in unchanged areas of the software, as a result of the changes made. It is performed when the software or its environment is changed.	[ISTQB (http://glossar.german-testing-board.info/)]
WP4_103	Remaining Dwell Time	Is the amount of time left before a train resumes moving.	
WP8_138	remote access	1) Use of systems that are inside the perimeter of the security zone being addressed from a different geographical location with the same rights as when physically present at the location. 2) Communication with assets that are outside the perimeter of the security zone being addressed. 3) Access to a control system by any user (human, software process or device) communicating from outside the perimeter of the zone being addressed. Note to entry: The exact definition of "remote" can vary according to situation. For example, access may come from a location that is remote to the specific zone, but still within the boundaries of a company or organization. This might represent a lower risk than access that originates from a location that is remote and outside of a company's boundaries.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP3_3.35	Remote Vehicles	Vehicles (not including trains) that are operated remotely, e.g., survey drones or maintenance robots.	
	Repeated or similar terms		
WP8_140	repudiation	Denial by one of the entities involved in a communication of having participated in all or part of the communication.	[ISA/IEC 62443-1-2, D1E6, 2017]

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP6_93	requirement	<p style="text-align: center;">May 2018</p> <p><u>[ISO/IEC/IEEE 24765, 2010]</u> 1. a condition or capability needed by a user to solve a problem or achieve an objective. 2. a condition or capability that must be met or possessed by a system, system component, product, or service to satisfy an agreement, standard, specification, or other formally imposed documents 3. a documented representation of a condition or capability as in (1) or (2) 4. a condition or capability that must be met or possessed by a system, product, service, result, or component to satisfy a contract, standard, specification, or other formally imposed document. Requirements include the quantified and documented needs, wants, and expectations of the sponsor, customer, and other stakeholders. A Guide to the Project Management Body of Knowledge (PMBOK® Guide) — Fourth Edition cf. design requirement, functional requirement, implementation requirement, interface requirement, performance requirement, physical requirement</p>	[ISO/IEC/IEEE 24765, 2010]
WP8_067	Requirement	<p>need or expectation that is stated, generally implied or obligatory Note 1 to entry: “Generally implied” means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied. Note 2 to entry: A specified requirement is one that is stated, for example in documented information</p>	ISO/IEC 27000:2016
WP8_068	Residual Risk	remaining risk after the security controls or countermeasures have been applied	ISA TR62443-1-2, D1E5
WP8_069	Resilience	see Information System Resilience	NIST SP 800-53 r4
WP3_1.21	Resilience to Interference	The ability to provide and maintain an acceptable level of service even in case of out-of-band interference	2) Non-functional Attributes
WP6_94	result	<p><u>[ISTQB (http://glossar.german-testing-board.info/)]</u> The consequence/outcome of the execution of a test. It includes outputs to screens, changes to data, reports, and communication messages sent out.</p>	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_95	Re-testing	<p><u>[ISTQB (http://glossar.german-testing-board.info/)]</u> Testing that run tests that failed the last time they were run, in order to verify the success of corrective actions</p>	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_96	risk	<p><u>[EN 50126-1:2016]</u> combination of expected frequency of loss and the expected degree of severity of that loss</p>	[EN 50126-1:2016]
WP8_070	Risk	<p>A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.</p>	[NIST SP 800-53 r4]
WP8_071	Risk Analysis	see Risk Assessment	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_072	Risk Assessment	<p>1) Process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure; 2) Process of identifying and evaluating risks to the organization's operations (including mission, functions, image, or reputation), the resulting impact, and additional countermeasures that would mitigate this impact. <u>Note 1 to entry:</u> Types of resources include physical, logical and human. <u>Note 2 to entry:</u> Risk assessments are often combined with vulnerability assessments to identify vulnerabilities and quantify the associated risk. They are carried out initially and periodically to reflect changes in the organization's risk tolerance, vulnerabilities, procedures, personnel and technological changes. <u>Note 3 to entry:</u> Synonymous with risk analysis, and incorporates threat and vulnerability analyses.</p>	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_073	Risk Evaluation	<p>process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable Note 1 to entry: Risk evaluation assists in the decision about risk treatment.</p>	ISO/IEC 27000:2016

		May 2018	
WP8_074	Risk Identification	process of finding, recognizing and describing risks Note 1 to entry: Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.	ISO/IEC 27000:2016
WP8_075	Risk Management	Process of identifying and applying countermeasures commensurable with the value of the assets protected based on a risk assessment	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_141	risk mitigation	Actions to reduce the likelihood and/or severity of an event.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_076	Risk Tolerance	risk the organization is willing to accept	ISA TR62443-1-2, D1E5
WP3_2.5	ROI	Return on Investment (ROI) is the benefit to an investor resulting from an investment of some resource. This may be a direct or indirect benefit.	
WP5_028	Roll away	An unintended and non-powered movement of the train in a direction, which conflicts with the current position of the direction controller in the active desk.	Subset-023
WP4_104	Rolling Stock	General term covering all vehicles with or without motors.	IEV 811: International Electrotechnical Commission – Electric traction
WP5_029	Route	Path commanded by the Signaller (or by a Automatic Train Supervision System) to be run by a train from an entry point to an exit point. A Route is considered as established by Trackside when it fulfils all conditions, i.e.: route compatibility checks, point locking... Note - Definition as from Subset-023: The particular section or sections of track, from a starting point to a point of destination, prepared for train operation.	Derived from Subset-023
WP4_135	Runtime model	This is the abstract layer required to "run" the formal model. It shall provide in the formalism part or all of the following (but not restricted to): - memory management, - execution of state machines (or of the chosen formal objects), - failures, - communication between processes and concurrence, - real time clock.	
WP4_134	Runtime Model/API	This corresponds to the Runtime Model plus API. Therefore it should provide all the services needed to emulate at abstract level the hardware platform that could run the software.	
WP4_105	Safe Braking Model	An analytical representation of a train's performance while decelerating to a complete stop, allowing for a combination of worst-case influencing factors and failure scenarios.	
WP3_2.12	Safe Operation	Compliance to safety standards, whereas safety is defined as: The freedom from unacceptable levels of risk of harm.	EN 5126 - Railway applications- The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
WP4_106	Safe Places	Areas within the network of an operator where evacuation of passengers can be performed, depending on current operational conditions, with a minimum of risks to the passengers (e.g. stations, refuges on the line).	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP6_100	Safety	[ISO/IEC/IEEE 24765, 2010] 1. the expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered. ISO/IEC 15026:1998, Information technology — System and software integrity levels.3.14	[ISO/IEC/IEEE 24765, 2010]
WP8_077	Safety	freedom from unacceptable risk	ISA TR62443-1-2, D1E5
WP8_078	Safety Instrumented System	1) system used to implement one or more safety-instrumented functions 2) system specifically designed to monitor certain conditions and act on those conditions to maintain the safety of the personnel and the facility 3) system used to implement one or more safety-related functions Note to entry: A Safety Instrumented System is composed of any combination of sensor(s), logic solver(s), and actuator(s)	ISA TR62443-1-2, D1E5
WP7_038	Safety Integrity Level	Concept of classes of safety requirements for functions, systems, sub-systems or components	-

Deliverable D2.3
Terminology for the future Signalling and Automation System

May 2018

WP8_079	Safety Integrity Level	discrete level (one out of four) for specifying the safety integrity requirements of the safety-instrumented functions to be allocated to the safety-instrumented systems Note to entry: Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest	ISA TR62443-1-2, D1E5
WP8_080	Safety Network	network that connects safety-instrumented systems for the communication of safety-related information	ISA TR62443-1-2, D1E5
WP6_101	Safety Tests	Safety Qualification Tests (Section 6 of the Technical Safety Report) This section shall contain evidence to demonstrate successful completion of the Safety Qualification Tests under operational conditions. The purpose of these tests is - to gain increased confidence that the system/sub-system/equipment fulfils its specified operational requirements, - to gain increased confidence that the specified reliability and safety targets have been achieved, - to allow systems/sub-systems/equipment to be put into operational service before final Safety Approval, subject to provision of appropriate precautions and monitoring. NOTE These tests only provide increased confidence and are not the unique means for demonstration of safety. <u>[CENELEC Standard EN50129]</u>	[CENELEC Standard EN50129]
WP3_2.9	Scalability	Scalability is the capability of a service or application to handle a growing or decreasing amount of users (people or devices) or its potential to be adjusted to accommodate that growth or decrease.	
WP3_3.15	Schedulers	Staff tasked with scheduling train operations (e.g., generate time-tables, manage track availability...).	
WP6_102	scripting language	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> A programming language in which executable test scripts are written, used by a test execution tool (e.g., a capture/playback tool).	[ISTQB (http://glossar.german-testing-board.info/)]
WP8_142	secret	Condition of information being protected from being known by any system entities except those intended to know it.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP5_030	Section	A part of the movement authority.	Subset-023
WP8_081	Security	1) measures taken to protect a system 2) condition of a system that results from the establishment and maintenance of measures to protect a system 3) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss 4) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet ensure that this is not denied to authorized persons and systems 5) prevention of illegal or unwanted penetration of or interference with the proper and intended operation of an industrial automation and control system <u>Note to entry:</u> Measures can be controls related to physical security (controlling physical access to computing assets) or logical security (capability to login to a given system and application)	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_082	Security Assurance	measure of confidence that the IACS those computer systems and data are free from vulnerabilities and the computer systems function in the intended manner	ISA TR62443-1-2, D1E5
WP6_103	security attack	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> An attempt to gain unauthorized access to a system or component, resources, information, or an attempt to compromise system integrity.	[ISTQB (http://glossar.german-testing-board.info/)]
WP8_083	Security Attribute	property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs Authors note: SFR Security Functional Requirements	CC-1, CCMB-2012-09-001
WP8_084	Security Capability	A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).	NIST SP 800-53 r4

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP8_085	Security Category	Characterization of IACS components based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of the capability required to support applicable foundational requirements would have on organizational operations, organizational assets, IACS, or individuals.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_143	security components	Assets such as firewalls, authentication modules, or encryption software used to improve the security performance of an industrial automation and control system (See "countermeasure").	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_086	Security Control	see countermeasure	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_087	Security Control Assessment	(Assessment) (Security Assessment) The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.	NIST SP 800-53 r4
WP8_088	Security Event	occurrence in a system that is relevant to the security of the system	ISA TR62443-1-2, D1E5
WP8_089	Security Function	function of a zone or conduit to prevent unauthorized electronic intervention that can impact or influence the normal functioning of devices and systems within the zone or conduit	ISA TR62443-1-2, D1E5
WP8_090	Security Incident	adverse event in a system or network or the threat of the occurrence of such an event Note to entry: The term "near miss" is sometimes used to describe an event that could have been an incident under slightly different circumstances.	ISA TR62443-1-2, D1E5
WP8_091	Security Level	1) level corresponding to the required effectiveness of countermeasure and inherent security properties of devices and systems for a zone or conduit based on an assessment of risk for the zone or conduit 2) measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner Note to entry: Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle, or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.	ISA TR62443-1-2, D1E5
WP8_092	Security Objective	1) aspect of security which to achieve is the purpose and objective of using certain mitigation measures, such as confidentiality, integrity, availability, user authenticity, access authorization, accountability 2) confidentiality, integrity or availability required to support the applicable foundational requirements	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_093	Security Policy	set of rules that specify or regulate how a system or organization provides security services to protect its assets	ISA TR62443-1-2, D1E5
WP8_094	Security Problem	statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address This statement consists of a combination of: - threats to be countered by the TOE and its operational environment, - the OSPs enforced by the TOE and its operational environment, and - the assumptions that are upheld for the operational environment of the TOE. Authors note: TOE Target of Evaluation, OSP Operational Security Policy	CC-1, CCMB-2012-09-001
WP8_095	Security Procedures	definitions of exactly how practices are implemented and executed Note to entry: Security procedures are implemented through personnel training and actions using currently available and installed technology.	ISA TR62443-1-2, D1E5
WP8_096	Security Requirement	A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. Note: Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.	[NIST SP 800-53 r4]
WP3_3.7	Security Staff	Security staff on board trains	
WP8_097	Security Target (ST)	implementation-dependent statement of security needs for a specific identified TOE Authors note: TOE Target of Evaluation	CC-1, CCMB-2012-09-001

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP8_098	Security Zone	Grouping of logical or physical assets that share common security requirements Note 1 to entry: All unqualified uses of the word "zone" in this standard should be assumed to refer to a security zone. Note 2 to entry: A zone has a clear border with other zones. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone. Zones can be hierarchical in the sense that they can be comprised of a collection of subzones.	ISA TR62443-1-2, D1E5
WP4_107	Segments Profile	Set of static infrastructure data required by the ATO on-board to compute the Operational Speed Profile.	
WP8_099	Self Assessment	review of an organization (i.e., policies, procedures, operations, equipment, and personnel) by a group inside the organization Note to entry: This group may be either directly associated with the organization's business process or may be in another part	ISA TR62443-1-2, D1E5
WP8_100	Service Provider	organization (internal or external organization, manufacturer, etc.) that has agreed to undertake responsibility for providing a given support service and obtaining, when specified, supplies in accordance with an agreement Note to entry: This term is used in place of the generic word "vendor" to provide differentiation.	ISA TR62443-1-2, D1E5
WP3_1.3	Service Type	The serviced type of applications is defined by two different categories (see table).	UIC FRMCS User Requirements Specification, V2.
WP7_039	Set of points	A section of track equipped so that train routes may converge or diverge.	-
WP3_1.11	Setup Time	The time to establish a voice or data communication session with the application that would be acceptable to a user, and is sufficient to perform the railway operation.	UIC FRMCS User Requirements Specification, V2.
WP5_031	Shall	Is mandatory.	Subset-023
WP4_109	Shall not	The use of "shall not" is restricted to formal requirements statements. It indicates obligation not to do something or to make sure that something does not happen, or not having permission / not being permitted to do something.	
WP5_032	Should	Is recommended.	Subset-023
WP3_3.14	Shunters	Staff tasked with operation of moving a rail vehicle or set of rail vehicles inside a railway station or other railway installations (depot, workshop, marshalling yard, etc.).	ERA Glossary / Glossary for Transport Statistics
WP5_033	Signal	A visual display device that conveys instructions or provides advance warning of instructions regarding the driver's authority to proceed.	Subset-023
WP7_040	Signal	A visual display device that conveys instructions or provides advance warning of instructions regarding the driver's authority to proceed.	-
WP5_034	Signaller (signalman)	A person responsible for the operation of the Signalling System, to safely control the movement of trains.	--
WP7_041	Simple Network Management Protocol	Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks	-
WP6_104	simulation	<u>[ISO/IEC/IEEE 24765, 2010]</u> 1. a model that behaves or operates like a given system when provided a set of controlled inputs. 2. the process of developing or using a model as in (1). 3. the use of a data processing system to represent selected behavioral characteristics of a physical or abstract system. ISO/IEC 2382-1:1993, Information technology — Vocabulary — Part 1: Fundamental terms.01.06.01 cf. emulation	[ISO/IEC/IEEE 24765, 2010]
WP6_105	simulator	<u>[ISO/IEC/IEEE 24765, 2010]</u> 1. a device, computer program, or system that behaves or operates like a given system when provided a set of controlled inputs cf. emulator	[ISO/IEC/IEEE 24765, 2010]
WP6_106	site acceptance testing	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> Acceptance testing by users/customers at their site, to determine whether or not a component or system satisfies the user/customer needs and fits within the business processes, normally including hardware as well as software.	[ISTQB (http://glossar.german-testing-board.info/)]
WP7_042	Sleep mode	Power-saving state that a device can enter when not in use	-

Deliverable D2.3
Terminology for the future Signalling and Automation System

May 2018			
WP6_175	Soak testing	<p><u>WP6 definition from Ed Morton:</u> Soak testing involves testing a system with a typical operational load, over a continuous availability period, to validate system behaviour under operational use. (For example, in software testing, a system may behave exactly as expected when tested for one hour. However, when it is tested for three hours, problems such as memory leaks cause the system to fail or behave unexpectedly).</p>	WP6 definition from Ed Morton:
WP6_107	Software	<p><u>[EN 50128:2001]</u> intellectual creation comprising the programs, procedures, rules and any associated documentation pertaining to the operation of a system NOTE Software is independent of the media used for transport.</p>	[EN 50128:2001]
WP6_109	Software testing	<p>The dynamic verification of the behaviour of a program on a finite set of test cases, suitably selected from the usually infinite executions domain, against the expected behaviour. <u>[ISO/IEC/IEEE 24765, 2010]</u></p>	[ISO/IEC/IEEE 24765, 2010]
WP4_110	Specific Application	Is an application designed for a particular realisation based on a customised generic application.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP7_043	Specific Energy	Energy per unit mass. In this context it is used to quantify energy stored in a battery or other energy storage device, related to its mass	-
WP6_110	specification	<p><u>[ISO/IEC/IEEE 24765, 2010]</u> 1. a detailed formulation, in document form, which provides a definitive description of a system for the purpose of developing or validating the system. ISO/IEC 2382-20:1990, Information technology — Vocabulary — Part 20: System development.20.01.03. 2. a document that fully describes a design element or its interfaces in terms of requirements (functional, performance, constraints, and design characteristics) and the qualification conditions and procedures for each requirement. IEEE Std 1220-2005 IEEE Standard for the Application and Management of the Systems Engineering Process.3.1.28. 3. a document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system, component, product, result, or service and, often, the procedures for determining whether these provisions have been satisfied. Examples are: requirement specification, design specification, product specification, and test specification. A Guide to the Project Management Body of Knowledge (PMBOK® Guide) — Fourth Edition</p>	[ISO/IEC/IEEE 24765, 2010]
WP3_4.10	Spectrum Regulators	<p>The Electronic Communications Committee (ECC) is part of the European Conference of Postal and Telecommunications Administrations (CEPT) and is the European regulatory body responsible for radio communications and telecommunications. Radio Spectrum Policy Group (RSPG) has been established under Commission Decision 22/622/EC and is a high-level advisory group that assists the European Commission in the development of radio spectrum policy.</p>	
WP6_111	Stability tests	Method to check how an operational system and its quality (software, hardware) behaviour with time elapsing, in a defined environment, monitoring any unexpected event that occurs during the duration of the test. (used in the glossary of deliverable D6.1)	
WP8_101	Stakeholder	<p>individual or group with an interest in the success of an organization in delivering intended results and maintaining the viability of the organization's products and services Note to entry: Stakeholders influence programs, products, and services. In this particular case, stakeholders are personnel in an organization responsible for promoting and overseeing the cyber security process. These personnel include the manager of the cyber security program as well as the cross-functional team of individuals from all of the departments affected by the cyber security program.</p>	ISA TR62443-1-2, D1E5
WP7_044	State of the Art	The most recent stage in the development of a product or technology, incorporating the newest ideas and features	-
WP6_112	state transition testing	<p><u>[ISTQB (http://glossar.german-testing-board.info/)]</u> A black-box test design technique in which test cases are designed to execute valid and invalid state transitions.</p>	[ISTQB (http://glossar.german-testing-board.info/)]

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP6_113	static testing	[ISTQB (http://glossar.german-testing-board.info/)] Testing of a software development artifact, e.g., requirements, design or code, without execution of these artifacts, e.g., reviews or static analysis.	May 2018 [ISTQB (http://glossar.german-testing-board.info/)]
WP3_1.17	Station	Operation within a station setting, where station is defined as: A railway location where a passenger train can start, stop or end.	ERA Glossary / TAP TSI Glossary
WP5_035	Station	A place where trains stop, or where loading and unloading occurs, and where assistance may be available. Where there can be points (facing or trailing) that makes it possible for the train to use different routes.	Subset-023
WP3_3.20	Station Managers	The Station Manager is the entity responsible for day-to-day management of a station. This role may be discharged by the Railway Undertaking, the Infrastructure Manager or a third party.	ERA Glossary / Commission Decision 28/164/EC concerning the TSI relating to persons with reduced mobility in the trans-European conventional and HS rail system
WP3_3.21	Station Staff	Staff with station-based duties, other than dispatchers and managers	
WP4_111	Status	State condition of a component or system.	Directive 2001/16/EC of the European Parliament and of the Council of 19 March 2001 on the interoperability of the trans-European conventional rail system
WP5_036	Stop aspect	Any signal aspect that does not allow the driver to pass the signal.	--
WP4_112	Stopping Point	A Timing Point defined in the Segment Profile where the train is planned to stop within a given time window defined in the Journey Profile, usually to carry out a specific activity such as allowing passengers to join and leave the train.	
WP6_114	stress testing	[ISTQB (http://glossar.german-testing-board.info/)] A type of performance testing conducted to evaluate a system or component at or beyond the limits of its anticipated or specified workloads, or with reduced availability of resources such as access to memory or servers.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_115	Subsystem	part of a system, which is itself a system [SOURCE: IEC 60050-192:2015, 192-01-04]	[SOURCE: IEC 60050-192:2015, 192-01-04]
WP6_116	Subsystem testing	[ISTQB (http://glossar.german-testing-board.info/)] See component testing	[ISTQB (http://glossar.german-testing-board.info/)]
WP7_045	Super capacitor	(also called super cap) High-capacity capacitor able to store 10 to 100 times more energy per unit volume or mass than electrolytic capacitors	-
WP4_113	Supervision	Activity, performed either manually or automatically, intended to observe the state of an item.	IEV 191-04-01: International Electrotechnical Commission - Dependability and quality of service
WP6_176	Supervision tests	WP6 definition from Giuseppe Savino: Testing activities related to system monitoring (i.e.: QoS, alarms, notification).	WP6 definition from Giuseppe Savino:
WP8_102	Supervisory Control And Data Acquisition (SCADA) System	type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems Note to entry: Supervisory control systems are also used within batch, continuous, and discrete manufacturing plants to centralize monitoring and control activities for these sites.	ISA TR62443-1-2, D1E5
WP7_046	SWOC: Smart Wayside Object Controller	The Smart Wayside Object Controller (SWOC) is a piece of equipment that is directly connected to the Wayside Objects, on one side, and to the Route Management Systems (Interlocking, TMS, ATP, etc.), on the other side; and to other SWOCs	-
WP3_1.5	Symmetry (Up/Down)	Ratio between uplink traffic and downlink traffic. Up-link refers to "mobile to infrastructure", and down-link refers to "infrastructure to mobile".	
WP6_117	system	set of interrelated elements considered in a defined context as a whole and separated from their environment [SOURCE: IEC 60050-351:2013, 351-42-08]	[SOURCE: IEC 60050-351:2013, 351-42-08]
WP8_103	System	interacting, interrelated, or interdependent elements forming a complex whole	ISA TR62443-1-2, D1E5
WP6_177	System Acceptance	Phase of System Lifecycle in which following activities are performed: a) Assessment of compliance of the total combination of subsystems, components and external risk reduction measures with the overall RAMS requirements of the complete system. b) Acceptance of the system for entry into service. [EN 50126: 2011]	[EN 50126: 2011]

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP6_165	System Approval	See System Acceptance	May 2018
WP8_104	System Integrator	person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications	ISA TR62443-1-2, D1E5
WP8_105	System Security Level	measure of confidence that computer systems and data are free from vulnerabilities and able to report anomalies in a timely manner; and, the computer systems function in the intended manner Note to entry: See the definitions of target security level, capability security level, and achieved security level.	ISA TR62443-1-2, D1E5
WP6_118	system testing	Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. <u>[ISO/IEC/IEEE 24765, 2010]</u>	[ISO/IEC/IEEE 24765, 2010]
WP8_106	System Under Consideration	collection of IACS and related assets for the purpose of security risk analysis	ISA TR62443-1-2, D1E5
WP6_119	system under test	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> See test object.	[ISTQB (http://glossar.german-testing-board.info/)]
WP8_107	Target of Evaluation (TOE)	set of software, firmware and/or hardware possibly accompanied by guidance	CC-1, CCMB-2012-09-001
WP8_108	Target of Evaluation (TOE) evaluation	assessment of a TOE against defined criteria	CC-1, CCMB-2012-09-001
WP8_109	Target Security Level	measure of confidence based on security policy and consequence analysis	ISA TR62443-1-2, D1E5
WP3_3.24	Telecoms Bearer Operator	An organisation that operates one or more telecoms bearers (e.g. a public Mobile Network Operator (MNO) or the communications department of an Infrastructure Manager).	
WP3_4.2	Telecoms Equipment Manufacturers	A company or organization that is responsible for developing and manufacturing telecoms equipment.	
WP3_2.16	Terminal CAPEX	Costs for terminal / on-board costs	
WP6_160	test automation	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> The use of software to perform or support test activities, e.g. test management, test design, test execution and results checking.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_120	test automation architecture	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> An instantiation of the generic test automation architecture to define the architecture of a test automation solution, i.e., its layers, components, services and interfaces.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_121	test automation strategy	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> A high-level plan to achieve long-term objectives of test automation under given boundary conditions.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_122	test case	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> A set of input values, execution preconditions, expected results and execution postconditions, developed for a particular objective or test condition, such as to exercise a particular program path or to verify compliance with a specific requirement.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_123	test case result	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> The final verdict on the execution of a test and its outcomes, such as pass, fail, or error. The result of error is used for situations where it is not clear whether the problem is in the test object.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_125	Test design	<u>[ISO/IEC/IEEE 24765, 2010]</u> 1. documentation specifying the details of the test approach for a software feature or combination of software features and identifying the associated tests. IEEE Std 1012-2004 IEEE Standard for Software Verification and Validation.3.1.32 NOTE commonly includes the organization of the tests into groups	[ISO/IEC/IEEE 24765, 2010]
WP6_126	test design specification	<u>[ISO/IEC/IEEE 24765, 2010]</u> 1. a document specifying the details of the test approach for a software feature or combination of software features and identifying the associated tests	[ISO/IEC/IEEE 24765, 2010]
WP6_127	test environment	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> An environment containing hardware, instrumentation, simulators, software tools, and other support elements needed to conduct a test.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_128	test execution	<u>[ISTQB (http://glossar.german-testing-board.info/)]</u> The process of running a test on the component or system under test, producing actual result(s).	[ISTQB (http://glossar.german-testing-board.info/)]

		May 2018	
WP6_129	test execution automation	[ISTQB (http://glossar.german-testing-board.info/)] The use of software, e.g., capture/playback tools, to control the execution of tests, the comparison of actual results to expected results, the setting up of test preconditions, and other test control and reporting functions.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_130	test execution tool	[ISTQB (http://glossar.german-testing-board.info/)] A type of test tool that is able to execute other software using an automated test script, e.g., capture/playback.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_131	test implementation	[ISTQB (http://glossar.german-testing-board.info/)] The process of developing and prioritizing test procedures, creating test data and, optionally, preparing test harnesses and writing automated test scripts.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_132	test input	[ISTQB (http://glossar.german-testing-board.info/)] The data received from an external source by the test object during test execution. The external source can be hardware, software or human.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_133	test item	[ISTQB (http://glossar.german-testing-board.info/)] The individual element to be tested. There usually is one test object and many test items.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_134	test level	[ISTQB (http://glossar.german-testing-board.info/)] A group of test activities that are organized and managed together. A test level is linked to the responsibilities in a project. Examples of test levels used in WP6 (see D6.2) are subsystem test, integration test and system test.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_135	test management	[ISTQB (http://glossar.german-testing-board.info/)] The planning, estimating, monitoring and control of test activities, typically carried out by a test manager.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_136	test manager	[ISTQB (http://glossar.german-testing-board.info/)] The person responsible for project management of testing activities and resources, and evaluation of a test object. The individual who directs, controls, administers, plans and regulates the evaluation of a test object.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_137	test object	[ISTQB (http://glossar.german-testing-board.info/)] The component or system to be tested.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_138	test objective	[ISTQB (http://glossar.german-testing-board.info/)] A reason or purpose for designing and executing a test.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_140	test phase	[ISO/IEC/IEEE 24765, 2010] 1. the period of time in the software life cycle during which the components of a software product are evaluated and integrated, and the software product is evaluated to determine whether or not requirements have been satisfied	[ISO/IEC/IEEE 24765, 2010]
WP6_141	test plan/test strategy	[ISO/IEC/IEEE 24765, 2010] test plan 1. a document describing the scope, approach, resources, and schedule of intended test activities. IEEE Std 1012-2004 IEEE Standard for Software Verification and Validation.3.1.33. 2. a document that describes the technical and management approach to be followed for testing a system or component. IEEE Std 1012-2004 IEEE Standard for Software Verification and Validation.3.1.33. 3. a plan that establishes detailed requirements, criteria, general methodology, responsibilities, and general planning for test and evaluation of a system. ISO/IEC 2382-20:1990, Information technology — Vocabulary — Part 20: System development.20.06.09 NOTE It identifies test items, the features to be tested, the testing tasks, who will do each task, and any risks requiring contingency planning. Typical contents identify the items to be tested, tasks to be performed, responsibilities, schedules, and required resources for the testing activity.	[ISO/IEC/IEEE 24765, 2010]
WP6_142	test script	[ISTQB (http://glossar.german-testing-board.info/)] Commonly used to refer to a test procedure specification, especially an automated one.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_143	test sequence	see use case: WP6_150	#WERT!
WP6_144	test specification	[ISTQB (http://glossar.german-testing-board.info/)] A document that consists of a test design specification, test case specification and/or test procedure specification.	[ISTQB (http://glossar.german-testing-board.info/)]

		May 2018	
WP6_159	test strategy	[ISTQB (http://glossar.german-testing-board.info/)] A high-level description of the test levels to be performed and the testing within those levels for an organization or programme (one or more projects)	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_145	test tool	[ISTQB (http://glossar.german-testing-board.info/)] A software product that supports one or more test activities, such as planning and control, specification, building initial files and data, test execution and test analysis.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_146	test type	[ISTQB (http://glossar.german-testing-board.info/)] A group of test activities aimed at testing a component or system focused on a specific test objective, i.e. functional test, usability test, regression test etc. A test type may take place on one or more test levels or test phases.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_147	tester	[ISTQB (http://glossar.german-testing-board.info/)] A skilled professional who is involved in the testing of a component or system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_148	testing	[ISO/IEC/IEEE 24765, 2010] 1. activity in which a system or component is executed under specified conditions, the results are observed or recorded, and an evaluation is made of some aspect of the system or component. IEEE Std 829-2008 IEEE Standard for Software and System Test Documentation.3.1.46	[ISO/IEC/IEEE 24765, 2010]
WP8_110	Threat	1) potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm 2) circumstance or event with the potential to adversely affect organizational operations (including mission, functions, image or reputation), organizational assets, IACS, or individuals via unauthorized access destruction, disclosure, modification of data and/or denial of service 3) circumstances or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_111	Threat Action	assault on system security	ISA TR62443-1-2, D1E5
WP8_112	Threat Agent	Method, including a surrogate, used to breach the security of a facility, operation or system by exploiting a vulnerability	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_113	Threat Assessment	Formal description and evaluation of threat to an information system.	NIST SP 800-53 r4
WP8_114	Threat Scenario	situation and manner in which an attacker (or Threat Agent) attempts to cause harm	ISA TR62443-1-2, D1E5
WP8_115	Threat Source	intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability (synonymous with threat agent)	ISA TR62443-1-2, D1E5
WP8_116	Threat Vector	a threat vector is a path or means by which a threat agent can gain access to an asset resulting in a negative outcome	ISA TR62443-1-2, D1E5
WP4_114	Timetable	Planned chronological occupation of rail infrastructure for train movements.	
WP4_115	Timing Points	A location and stopping accuracy defined in the Segment Profile for which a type (Stopping or Passing Point) and specific time is identified in the Journey Profile. This time may be an arrival time, a departure time, or in the case of a train not scheduled to stop at that location, the passing time.	
WP7_050	Track Circuit	An electrical circuit of which the rails of a track section form a part and which is used to positively detect the absence of trains over that section of the Station or Line.	-
WP5_037	Track free	A route being detected clear of obstacles such that permission may be given for a train to enter that route.	Subset-023
WP5_038	Track occupied	An object in a route that prevents that route being offered to a train.	Subset-023
WP5_039	Track Portion	Connected and bounded section of a track. Note: This does not necessarily correspond to a track vacancy detection related track section. To be clarified	--
WP5_040	Trackside equipment	The equipment with the aim of exchanging information with the vehicle for safely supervising train circulation. The information exchanged between track and trains can be either continuous or intermittent according to the ERTMS/ETCS level of application and to the nature of the information itself.	Subset-023
WP3_3.13	Trackside Maintenance Staff	Staff tasked with maintaining the track and railway infrastructure	
WP3_3.28	Track-side Systems	System placed near to the track	

Deliverable D2.3
Terminology for the future Signalling and Automation System

			May 2018
WP3_3.29	Track-side warning System	System that warns track-side workers of approaching trains	
WP3_3.12	Traffic Controller	A traffic controller (also: dispatcher) is an employee who supervises the train movements of a line or a certain area. In territories with centralized traffic control (CTC) the dispatcher also controls train movements.	IFEV Glossary of railroad operation and control
WP4_118	Traffic Management System	A non-safety-critical system which advises the control command and signalling system, based on the current traffic situation and other internal or external information, in order to improve the level of service.	
WP4_119	Traffic Operation and Management	The procedures and related equipment enabling a coherent operation of the different structural subsystems, both during normal and degraded operation, including in particular train driving, traffic planning and management.	Directive 2007/59/EC of the European Parliament and of the Council
WP7_047	Trailing points	Points where the fixed end of the blades face approaching traffic.	-
WP4_116	Train Control Management System	Train subsystem managing the interfaces with traction/braking controls and other train devices e.g. train doors.	
WP4_120	Train Coupler	The mechanical interface that enables vehicles to be operated together.	PD IEC/TS 62580-2:2016: Electronic railway equipment. On-board multimedia and telematic subsystems for railways. Video surveillance/CCTV services
WP5_041	Train detection	The proof of the presence or absence of trains on a defined section of line.	Subset-023
WP7_048	Train Detection	The proof of the presence or absence of trains on a defined section of line.	-
WP4_121	Train Driver	A person capable and authorised to drive trains, including locomotives, shunting locomotives, work trains, maintenance railway vehicles or trains for the carriage of passengers or goods by rail in an autonomous, responsible and safe manner.	Directive 2007/59/EC of the European Parliament and of the Council
WP4_122	Train Driver Identity	A unique code which identifies a train driver.	
WP4_117	Train Holding Brake	Function ensuring that the train will not move while it is at standstill.	
WP4_123	Train Inauguration	Inauguration is an automated process of train bus configuration that includes detecting all bus nodes and their orientation, assigning the numbers to particular bus nodes and collecting their properties.	UIC code 556 4th edition, August 2005
WP5_042	Train integrity	The level of belief in the train being complete and not having left coaches or wagons behind.	Subset-023
WP3_3.11	Train Maintenance Staff	Staff tasked with maintaining trains	
WP7_049	Train Management System		-
WP3_4.1	Train Manufacturers	A company or organization that is responsible for developing and manufacturing new trains.	
WP3_4.6	Train operating companies (commuter / sub-urban)	A train operating company is a public or private undertaking whose principal business is to provide services for the transport of passengers by rail (via commuter / sub-urban lines).	
WP3_4.7	Train operating companies (freight)	A train operating company is a public or private undertaking whose principal business is to provide services for the transport of goods by rail.	
WP3_4.5	Train operating companies (national/regional)	A train operating company is a public or private undertaking whose principal business is to provide services for the transport of passengers by rail (via national / regional lines).	
WP3_4.4	Train operating companies (urban / metro)	A train operating company is a public or private undertaking whose principal business is to provide services for the transport of passengers by rail (via urban / metro lines).	
WP4_124	Train Operation	The control command of routes, loading and unloading (of passengers and freight), driving of trains and shunting.	
WP5_043	Train orientation	If there is an active cab, this one defines the orientation of the train, i.e. the side of the active cab is considered as the front of the train. If no cab is active, the train orientation is as when a cab was last active.	Subset-023
WP3_3.8	Train Preparation Staff	Staff that takes care of preparing a train (e.g., cleaning, preparing seats...) prior to public operation.	
WP4_125	Train Separation	The means of keeping successive trains at a safe braking distance. The safe braking distance is the minimum distance in which a train can be guaranteed to be brought to a standstill.	
WP4_126	Train Splitting	The process by which multiple units are detached mechanically (which may also include pneumatically and electrically) to form a new number of train consists.	
WP7_051	Treadle	A track device, possibly complementing a TVP section, that is used to detect the wheels of a train passing a particular point on the track.	-

Deliverable D2.3
Terminology for the future Signalling and Automation System

WP8_117	Trust	<p style="text-align: center;">May 2018</p> <p>1) attribute of an entity that is relied upon to a specified extent to exhibit an expected behavior 2) confidence that an operation or data transaction source, network or software process can be relied upon to behave as expected Note 1 to entry: Generally, an entity can be said to 'trust' a second entity when it (the first entity) makes the assumption that the second entity will behave as the first entity expects. Note 2 to entry: This trust may apply only for some specific function.</p>	ISA TR62443-1-2, D1E5
WP8_118	Trustworthiness	Attribute or trait of the system which causes it to be deserving of trust	[ISA/IEC 62443-1-2, D1E6, 2017]
WP4_127	Turnback Move	A train movement at the end of a mission, where the train changes direction.	
WP7_052	TVP Track Vacancy Proving	The function which proves that a defined section of track is not occupied	-
WP6_163	type test	[EN 50215: 2008] a test of one or more devices, system or complete vehicle to show that the design meets the 264 required specifications and the relevant standards	[EN 50215: 2008]
WP4_128	UNISIG	Union Industry of Signalling - an associated member of UNIFE, created to develop the ERTMS/ETCS technical specifications.	
WP4_129	Unit	A set of one or more vehicles which cannot be decoupled during train operation.	
WP6_149	Unit testing	[ISTQB (http://glossar.german-testing-board.info/)] See component testing	[ISTQB (http://glossar.german-testing-board.info/)]
WP3_2.2	Upgradability	The potential ability of a system, subsystem or component to respond to changes in operational requirements and anticipated or foreseeable technical changes such as software upgrades without affecting the basis of its structure	EN 932:215-3
WP7_053	UPS	Uninterruptible Power Supply, is an electrical apparatus that provides near-instantaneous protection (i.e. supplies the load) from main input power interruptions	-
WP3_1.2	Usage Type	The use of applications is defined by three different categories (see table).	UIC FRMCS User Requirements Specification, V2.
WP6_150	use case	[ISTQB (http://glossar.german-testing-board.info/)] A sequence of transactions in a dialogue between an actor and a component or system with a tangible result, where an actor can be a user or anything that can exchange information with the system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_151	use case testing	[ISTQB (http://glossar.german-testing-board.info/)] A black-box test design technique in which test cases are designed to execute scenarios of use cases.	[ISTQB (http://glossar.german-testing-board.info/)]
WP8_119	User	person, organization entity, or automated process that accesses a system, whether authorized to do so or not	ISA TR62443-1-2, D1E5
WP6_152	user acceptance testing	[ISTQB (http://glossar.german-testing-board.info/)] Acceptance testing carried out by future users in a (simulated) operational environment focusing on user requirements and needs.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_153	user interface	[ISTQB (http://glossar.german-testing-board.info/)] All components of a system that provide information and controls for the user to accomplish specific tasks with the system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_154	user test	[ISTQB (http://glossar.german-testing-board.info/)] A test whereby real-life users are involved to evaluate the usability of a component or system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_155	validation	confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled Note 1 to entry: The term "validated" is used to designate the corresponding status. Note 2 to entry: The use conditions for validation can be real or simulated. Note 3 to entry: In design and development, validation concerns the process of examining an item to determine conformity with user needs. Note 4 to entry: Validation is normally performed during the final stage of development, under 745 defined operating conditions, although it can also be performed in earlier stages. Note 5 to entry: Multiple validations can be carried out if there are different intended uses. [SOURCE: IEC 60050-192:2015, 192-01-18, modified]	[SOURCE: IEC 60050-192:2015, 192-01-18, modified]
WP6_168	validation tests	WP6 definition from Giuseppe Savino: validation tests are the testing activities executed in order to demonstrate that the product meets in all respects its specified requirements.	WP6 definition from Giuseppe Savino:

May 2018

WP6_156	verification	confirmation, through the provision of objective evidence, that specified requirements have been fulfilled Note 1 to entry: The term “verified” is used to designate the corresponding status. Note 2 to entry: Design verification is the application of tests and appraisals to assess conformity of a design to the specified requirement. Note 3 to entry: Verification is conducted at various life-cycle phases of development, examining the system and its constituents to determine conformity to the requirements specified at the beginning of that life-cycle phase. [SOURCE: IEC 60050-192:2015, 192-01-17, modified]	[SOURCE: IEC 60050-192:2015, 192-01-17, modified]
WP6_155_a WP6_156_a	Verification and validation - difference between both	<p>The diagram is a V-model. The top left box is 'Requisiti del Sistema / System Requirements'. The top right box is 'Accettazione del Sistema / System Acceptance'. The bottom left box is 'Ripartizione / Apportionment'. The bottom right box is 'Validazione del Sistema / System Validation'. Arrows point from 'Requisiti del Sistema' to 'Ripartizione' and 'Validazione del Sistema'. Arrows point from 'Ripartizione' to 'Accettazione del Sistema'. Arrows point from 'Validazione del Sistema' to 'Accettazione del Sistema'. A double-headed arrow connects 'Requisiti del Sistema' and 'Accettazione del Sistema'. A double-headed arrow connects 'Ripartizione' and 'Validazione del Sistema'. The text 'Rappresentazione a "V" del Ciclo di Vita "V" Representation of the Life Cycle' is written below the diagram. The words 'Verifica Verification' are written on the left and right sides of the V-shape.</p>	from EN50126 standards
WP6_161	virtualization	The process of changing something that exists in a real form into a virtual version (= one that is created using a computer). [Cambridge Dictionary, http://dictionary.cambridge.org/dictionary/english/virtualization , 19.07.2017]	
WP7_054	Vital Data	Data communication that is safety critical and that ensures the safe operation of a system	-
WP8_120	Vulnerability	1) flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy 2) weakness in a system function, procedure, internal control or implementation that could be exploited or triggered by a threat source, either intentionally designed into computer components or accidentally inserted at any time during the lifecycle.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP8_121	Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in a system.	[ISA/IEC 62443-1-2, D1E6, 2017]
WP7_055	Wayside Object	Generic for trackside objects as point, level crossing, etc.	-
WP6_157	white-box test design technique	[ISTQB (http://glossar.german-testing-board.info/)] Procedure to derive and/or select test cases based on an analysis of the internal structure of a component or system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP6_158	white-box testing	[ISTQB (http://glossar.german-testing-board.info/)] Testing based on an analysis of the internal structure of the component or system.	[ISTQB (http://glossar.german-testing-board.info/)]
WP7_056	Wireless Communication	Transfer of information or power between two or more points that are not connected by an electrical conductor. I.e Wi-Fi, Radio, Satellite etc.	-
WP3_1.18	Yard	Operation within a yard setting, where yard is defined as: An arrangement of tracks, other than main tracks, used for making up trains (shunting), storing cars and trains and other purposes NOTE: Could not find this definition in the ERA Glossary (RR)	ERA Glossary / IFEV Glossary of railroad operation and control
WP4_130	Yards	An arrangement of tracks, other than main tracks, used for making up trains, storing cars and trains and other purposes.	ERA Glossary of Railway Terms, 8th November 2010, available at http://www.era.europa.eu/Document-Register/Pages/Glossary-of-railway-terms.aspx .
WP8_122	Zone	1) grouping of logical or physical assets that share common security requirements (see “security zone”) Note to entry: A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.	ISA TR62443-1-2, D1E5
WP4_131	Zone of Protection	A zone where no train is allowed to run as a result of various kinds of incidents except identified hazardous situations for which trains can leave the zone.	IEC 62290-1:2014: Railway applications - Urban guided transport management and command/control systems, Part 1: System principles and fundamental concepts.
WP8_123	Zones Contained In Zones	collection of entities that take credit for, or are conditioned on, the security assurance provided by the entities in the containment zone	ISA TR62443-1-2, D1E5