# SR40 Preliminary Customer Requirements

Version 1.0_published, 30.4.2018

## 1 Disclaimer

This document is a DRAFT version which is still under construction. Its content may change in the ongoing concept phase of SmartRail 4.0. The document is not completely verified and is not finalized by now. The document is published to enable an open discussion of the ongoing work of the SmartRail 4.0 program.

Links and references inside of this document may refer to other documents inside of the program SmartRail 4.0, that may not be published at this stage.

## 2 SR40 Preliminary customer requirements

The following requirements derived from the preliminary study "Bahnproduktion 3.5", which was the Basis for the decision for the program SmartRail 4.0. The following requirements build part of the mission and the objective for the program SmartRail 4.0 and contain the main premises, main customer requirements, constraints and dimensioning factors.

The term "SR40" is used

**SRP-3551 - SR40 Preliminary Customer Requirements [awaiting approvals ]**

**SRP-3622 - Functional requirements of the functional blocks [awaiting approvals ]**

**SRP-3701 - Requirements for Traffic Management (TMS) [**awaiting approvals **]**

**SRP-3624 -** Requirements for Planning, scheduling and production preperation (TMS-PAS) **[**awaiting approvals **]**

**SRP-3646 -** TMS shall provide functionality to create commercial schedules and production plans in a highly automated manner **[**awaiting approvals **]**

**SRP-3648 -** TMS shall provide functionality to work with all planning processes on an integrated planning system that avoids manual data transfer and that stores the dependencies between all type of plans. **[**awaiting approvals **]**

**SRP-3663 -** TMS shall provide planning functionality that works for longterm, midterm and shortterm planning in mostly the same way **[**awaiting approvals **]**

**SRP-3649 -** TMS shall provide functionality to check the feasibility of plans and schedules in an early stage **[**awaiting approvals **]**

**SRP-3650 -** TMS shall provide functionality to create and assess planning and schedule versions **[**awaiting approvals **]**

**SRP-3664 -** TMS shall provide a electronical access (e.g. Web-Portal) for customers, planners und partners, that are involved in the planning process, to retrieve their requests or commitments electronically **[**awaiting approvals **]**

**SRP-3665 -** TMS shall provide an open interface for systems of customers und partners, that are involved in the planning process, to retrieve their requests, plans or commitments electronically **[** awaiting approvals **]**

**SRP-3651 -** TMS shall provide functionality to assess plans and schedules concerning their impact on cost, punctuality and capacity and to optimize them **[** awaiting approvals **]**

**SRP-3652 -** TMS shall provide functionality to tune or correct the parameters of the automated planning **[** awaiting approvals **]**

**SRP-3758 -** TMS shall provide functionality to identify future traffic conflicts **[** awaiting approvals **]**

**SRP-3759 -** TMS shall provide functionality to solve future traffic conflicts with a high automation grade **[** awaiting approvals **]**

**SRP-3656 -** TMS shall provide functionality for direct manual commands in form of a short-term planning to EI **[** awaiting approvals **]**

**SRP-3657 -** TMS shall provide functionality to handle every type of track user (trains, persons, construction sites etc.) concerning the control or allowance for their movements **[** awaiting approvals **]**

**SRP-3666 -** TMS shall provide functionality to automate the communication between all persons in the production in the highest possible economical way **[** awaiting approvals **]**

**SRP-3667 -** TMS shall provide functionality to automatically process requests from production personal in the field **[** awaiting approvals **]**

**SRP-3725 -** Adaptive Steering: TMS shall optimize the usage of the steering possibilities (Triage) speed, distance and isolating safety elements on the track **[** awaiting approvals **]**

**SRP-3760 -** TMS shall allow every track user to start and end a movement at any point **[** awaiting approvals **]**

**SRP-3625 -** Requirements for Automatic train operation and driver assistance (TMS-ATO) **[** awaiting approvals **]**

**SRP-3653 -** TMS-ATO shall provide functionality to steer C-DAS-systems and ATO GoA2-Units in the train over open standardized interfaces **[** awaiting approvals **]**

**SRP-3654 -** TMS-ATO shall be upwards compatible to GoA3 and GoA4 **[**

awaiting approvals **]**

**SRP-3655 -** TMS-ATO shall provide a flexible functionality to communicate with the trains over alternate communication Systems (like GSM-R or public mobile Radio), which can build a redundant communication architecture **[** awaiting approvals **]**

**SRP-3761 -** The ATO onborad unit shall provide open interfaces to automation systems, that steer train formation, brake-checks, train preparation, coupling/decoupling, preparation for parking, parking etc.) **[** awaiting approvals **]**

**SRP-3762 -** TMS-ATO shall provide open interfaces to automation systems, that handle the passenger exchange at plattforms or passenger movements inside of stations **[** awaiting approvals **]**

**SRP-3763 -** TMS-ATO (Onboard Unit) shall provide the information of onboard sensors over an open interface. This includes sensors that collect information about the environment around the train, about the situation in the train, and about the technical diagnostic of the train. **[** awaiting approvals **]**

**SRP-3764 -** TMS shall provide open interfaces to the planning systems in shunting yards **[** awaiting approvals **]**

**SRP-3626 -** Requirements for the control of the CCS systems (TMS-L) **[** awaiting approvals **]**

**SRP-3658 -** TMS-L shall provide functionality to steer EI by transmitting the elements of a given plan to it as single commands step by step **[** awaiting approvals **]**

**SRP-3659 -** TMS-L shall provide functionality to use plans sent by for example TMS, RCS or other planning systems, sent over an open and flexible interface **[** awaiting approvals **]**

**SRP-3677 -** TMS-L or other TMS functions shall provide the functionality that today is resided in electronic interlockings or their control-systems today but not safety relevant **[** awaiting approvals **]**

**SRP-3727 -** TMS-L must be a realtime system able to steer EI in the right speed and with high precision ("meters and seconds") **[** awaiting approvals **]**

**SRP-3728 -** TMS-L must be able to calculate very short movement commends in a high frequency to allow a dynamic steering via EI. **[** awaiting approvals **]**

**SRP-3627 -** Requirements for Steering of processes in the field (TMS-GLAT, GLAT-Tablet ) **[** awaiting approvals **]**

**SRP-3660 -** TMS-GLAT shall provide functionality to inform persons in the field about the production status over a mobile GLAT enddevice **[** awaiting approvals **]**

**SRP-3661 -** TMS-GLAT shall provide functionality for user inputs to TMS over a mobile GLAT enddevice **[** awaiting approvals **]**

**SRP-3628 -** Requirements for production status visualization and information in TMS (N.N.) **[** awaiting approvals **]**

**SRP-3668 -** TMS shall show the production status delivered by EI in different views that are suitable for different operational procedures (e.g. logical track view, geometric track view, statistical view, conflict-view, etc.) **[** awaiting approvals **]**

**SRP-3669 -** TMS shall provide an open interface to steer and inform systems for customer information **[** awaiting approvals **]**

**SRP-3662 -** Requirements for Monitoring and Diagnostics (N.N.) **[** awaiting approvals **]**

**SRP-3670 -** TMS shall provide functionality to show the diagnostic status of trackside assets **[** awaiting approvals **]**

**SRP-3671 -** TMS shall provide functionality to show the diagnostic status of track users **[** awaiting approvals **]**

**SRP-3672 -** TMS shall provide functionality to show the diagnostic status given by third party systems over an open interface **[** awaiting approvals **]**

**SRP-3629 -** Requirements for Topology management (TMS-TOPO) **[** awaiting approvals **]**

**SRP-3673 -** TMS-TOPO shall provide the topology information needed in TMS **[** awaiting approvals **]**

**SRP-3682 -** TMS-TOPO shall be able to synchronize its topology with EI-TOPO **[** awaiting approvals **]**

**SRP-3683 -** -TOPO shall have an open interface to synchronize information with third party systems **[** awaiting approvals **]**

## SRP-3630 - Requirements for the SR40 Safety System (ETCS Interlocking, EI) [awaiting approvals ]

**SRP-3631 -** Requirements for EI [awaiting approvals ]

**SRP-3674 -** EI is the gatekeeper between all trackside management systems (TMS) and on the other hand all track users und trackside assets (moving and fixed objects). [awaiting approvals ]

**SRP-3688 -** EI guarantees, that no command is sent from TMS to moving or fixed objects that results in an unsafe situation in terms of the configured safety rules, as long as the track user can guarantee to follow the commands fail-safe and the trackside assets are reacting fail-safe to. [awaiting approvals ]

**SRP-3689 -** EI guarantees, that TMS receives the full and actual status of all moving and fixed objects including timestamps and outrun status information (e.g. because of lost connection) [awaiting approvals ]

**SRP-3690 -** EI must be able to achieve the safety in every communication based cab signalling train control system, especially and in the first step fully compliant to ETCS L2/L3 (TSI CCS) [awaiting approvals ]

**SRP-3691 -** EI shall be an integrated safety system, where interlocking and RBC functionality is combined [awaiting approvals ]

**SRP-3765 -** EI shall allow the start and end of movements at any point [awaiting approvals ]

**SRP-3766 -** EI shall provide functionality to safely control any type of movement (from A to B, multiple movements in a range, with/withoput stop allowed, etc.) [awaiting approvals ]

**SRP-3692 -** EI shall calculate safety risks at runtime for every requested operation in a safe manner [awaiting approvals ]

**SRP-3702 -** EI shall be able to work safe with a minimum of prepared configurational data [awaiting approvals ]

**SRP-3703 -** EI shall work safe only with imported topology information (geometric layout, capabilities of sensors and actors), danger patterns, rules for safe reactions, safety assessment rules and exclusion patterns [awaiting approvals ]

**SRP-3704 -** EI shall provide functionality to manually improve its configuration only in a safe direction on runtime **[** awaiting approvals **]**

**SRP-3705 -** EI shall use the information of third party systems (no SIL) improve its configuration only in a safe direction on runtime **[** awaiting approvals **]**

**SRP-3706 -** EI shall be able to validate its configuration concerning safety on runtime **[** awaiting approvals **]**

**SRP-3675 -** EI shall have as less as possible non-safety critical functionality **[** awaiting approvals **]**

**SRP-3678 -** EI should be able to be hosted in larger and redundant datacenters **[** awaiting approvals **]**

**SRP-3679 -** EI must be able to connect to legacy interlockings, RBC and trackside assets (excluding main signals) in a safe way **[** awaiting approvals **]**

**SRP-3680 -** EI shall be able to achieve the safety independent from trackside asset layouts **[** awaiting approvals **]**

**SRP-3681 -** EI must be able to achieve the safety at all times independent from operational processes as long as the necessary set of sensor-information and actor-capabilities is provided for this and as long a correct topology-representation is given **[** awaiting approvals **]**

**SRP-3684 -** EI shall be able to be configured to fulfil different safety levels, that fit  to  the capabilities set of the available sensor information **[** awaiting approvals **]**

**SRP-3685 -** EI shall be able to be configuredto fulfil different safety levels, that fit  to  the capabilities set of the available actors **[** awaiting approvals **]**

**SRP-3686 -** A correct topology representation is given if it has no faults that can provoke an unsafe situation **[** awaiting approvals **]**

**SRP-3687 -** EI must be able to handover the safety responsibility to local safety actors in a safe way **[** awaiting approvals **]**

**SRP-3729 -** EI shall provide a function for safe movements in absolute and relative braking distance **[** awaiting approvals **]**

**SRP-3749 -** Requirements for EI-MTC **[**awaiting approvals **]**

- **SRP-3694 -** EI shall have an open interface to mobile traffic control systems ("MTCs", e.g. systems that use a safe tablet for signalisation or as an command MMI, which have localisation functionality) **[**awaiting approvals **]**
- **SRP-3695 -** EI shall provide an open interface to traffic control systems only based on mobile tablets and safety servers. **[**awaiting approvals **]**
- **SRP-3750 -** EI-MTC shall provide functionality to get rid of shunting signals and boards **[**awaiting approvals **]**
- **SRP-3751 -** EI-MTC shall provide warning functionalities for trackusers with GLAT-compatible enddevices **[**awaiting approvals **]**
- **SRP-3700 -** EI shall provide the server functionality as a MTC server, providing an open interface to MTC clients **[**awaiting approvals **]**
- **SRP-3734 -** EI-MTC shall be available alone (minimum dependencies) to be a redundant safety layer and a fallback in the case of system failures in SR40. **[**awaiting approvals **]**
- **SRP-3697 -** EI shall provide the functionality to automate the shunting process over MTCs **[**awaiting approvals **]**
- **SRP-3696 -** EI shall provide the functionality to provide warning functions over MTCs **[**awaiting approvals **]**

**SRP-3676 -** Requirements for Safety control (EI-SL) **[**awaiting approvals **]**

- **SRP-3730 -** EI-SL shall provide a functionality, where the safety of a requested operation (TMS) is assed at runtime by a generic rule based risk-function. **[**awaiting approvals **]**

**SRP-3632 -** Requirements for Actor control (ES-COM) **[**awaiting approvals **]**

- **SRP-4752 -** ES-COM shall provide functionality to send a operational command to different actors (Systems or people) with different capabilities **[**awaiting approvals **]**

**SRP-3633 -** Requirements for Object identification (EI-OI) **[**awaiting approvals **]**

- **SRP-3731 -** EI-OI shall deliver the Identification, trackusage (footprint), speed, status, capabilties and type-information of every track user that is registered **[**awaiting approvals **]**

**SRP-3732 -** EI-OI shall deliver the information, when a registered track user can't be localized **[**awaiting approvals **]**

**SRP-3733 -** EI-OI shall provide open interfaces and a sensor fusion functionality, that allows the combined usage of legacy train detection systems and new geometric or block bases localisation systems (onboard or trackside) **[**awaiting approvals **]**

**SRP-3634 -** Requirements for Monitoring of danger patterns (EI-SM) **[**awaiting approvals **]**

**SRP-4753 -** EI-SM shall allow the definition of danger patterns in the production as configuration data. A danger pattern is a constellation of conditions of track users and trackside assets and their change in time. **[**awaiting approvals **]**

**SRP-4754 -** EI-SM shall invoke the appropriate safe reaction for a danger pattern. The safe reaction can be described via configuration data. **[**awaiting approvals **]**

**SRP-4755 -** EI-SM monitors the completion of safe reactions **[**awaiting approvals **]**

**SRP-3635 -** EI Requirements for safe operations in the field **[**awaiting approvals **]**

**SRP-4756 -** EI shall have functionality to control safe movements of people on the track **[**awaiting approvals **]**

**SRP-3636 -** Requirements for correct topology data for safe applications (EI-TOPO4) **[**awaiting approvals **]**

**SRP-4757 -** TOPO4 shall provide a data representation of all trackside assets (geometry, capabilities, properties, events, connection, functional relations) that are safety relevant or are used by EI. **[**awaiting approvals **]**

**SRP-4758 -** TOPO4 shall assure a very high data quality (assumed: 1 safety relevant data fault in 20 years). **[**awaiting approvals **]**

**SRP-4759 -** TOPO4 shall provide technologies to automatically acquire the topology data **[**awaiting approvals **]**

**SRP-3638 -** Requirements for trackside objects control (Object Controller, OC) **[**awaiting approvals **]**

**SRP-4761 -** OC shall allow an industrial migration process (fast, low cost) **[**

awaiting approvals **]**

**SRP-3698 -** OC must be able to connect two or more interlockings to the same trackside asset and to switch between them in a safe way **[** awaiting approvals **]**

**SRP-3699 -** OC must provide one interface to EI which fulfils the "open safety" ( SRP-3301)  requirements **[** awaiting approvals **]**

**SRP-3639 -** Requirements for safe control of human actions in the track (EI via GLAT Tablet): EI shall provide warning and Information functionality. **[** awaiting approvals **]**

### SRP-3640 - Requirements for Safe localisation of objects in the track (GLAT) [ awaiting approvals ]

**SRP-3735 -** GLAT shall provide a **g**eneric platform for **l**ocatable enddevices on which safe and unsafe **a**pps for **t**raffic control and management can be executed on the same enddevice. **[** awaiting approvals **]**

**SRP-3736 -** GLAT shall have an open interface to EI fulfilling the open safety requirements **[** awaiting approvals **]**

**SRP-3737 -** GLAT shall provide the functionality to EI to locate freely moving objects near to the track or on the track. **[** awaiting approvals **]**

**SRP-3738 -** GLAT shall provide server-functionality to register, supervise and locate all enddevices in realtime  **[** awaiting approvals **]**

**SRP-3739 -** GLAT shall notify EI if an registered enddevice is not locatable any more. **[** awaiting approvals **]**

**SRP-3740 -** GLAT is a safe system concerning the server functionality **[** awaiting approvals **]**

**SRP-3741 -** GLAT enddevices shall provide functionality for the safe display of information (actual, correct) and safe user input (double checked), that cannot be influenced by software on the enddevice in any way. **[** awaiting approvals **]**

**SRP-3742 -** GLAT enddevices shall safe provide localisation information to the server concerning the reliability of the precision of this information **[** awaiting approvals **]**

**SRP-3743 -** GLAT endevices shall allways provide the functionality to warn their users. **[** awaiting approvals **]**

**SRP-3744 -** GLAT enddevices shall be used as tablets, tags or portable systems e.g. for trackworker safety **[** awaiting approvals **]**

**SRP-3745 -** GLAT Tags shall be used as train enddevices **[** awaiting approvals **]**

**SRP-3746 -** GLAT Tags shall be useable for locating people **[** awaiting approvals **]**

**SRP-3747 -** GLAT Tablet shall be able to execute a safe MTC app (e.g. EI-MTC). This means, that safe user-input and user-output is supported by the tablet. **[** awaiting approvals **]**

**SRP-4813 -** GLAT enddevices shall have a localisation precision and safety that allow conventional train detection systems to akquire their exact lateral front position (1.5m precision) **[** awaiting approvals **]**

**SRP-4815 -** GLAT enddevices shall have a localisation precision and safety that allow the application of train enddevices, which deliver a longitudinal Position with speed dependend precision between 5-50m. **[** awaiting approvals **]**

**SRP-4876 -** GLAT enddevices shall have a localisation precision and safety that allow conventional train detection systems to akquire their exact vertical position (3.5m precision) **[** awaiting approvals **]**

**SRP-3752 -** GLAT enddevices shall have a localisation precision and safety that allows conventional train detection systems to be replaced by mobile devices **[** awaiting approvals **]**

**SRP-3753 -** GLAT enddevices shall have a precision that allows EI to identify, in which track a trackuser is located and if he would interfere with movements on that track **[** awaiting approvals **]**

**SRP-3641 - Requirements for Building and maintaining CCS assets [** awaiting approvals **]**

**SRP-3642 -** Requirements for Automated engineering and planing (AMP) **[** awaiting approvals **]**

**SRP-3707 -** AMP shall provide functionality to automate the engineering and planning process for building and replacing trackside assets as much as economically possible **[** awaiting approvals **]**

**SRP-4812 -** AMP shall provide functionality to automate the engineering and planning process for configering, comissioning and putting EI in operation as much as possible and economically reasonable **[** awaiting approvals **]**

**SRP-3643 -** Requirements for monitoring and diagnostic systems (DIAG) **[** awaiting approvals **]**

**SRP-4762 -** DIAG shall provide system diagnostic information for all SR40 systems **[** awaiting approvals **]**

**SRP-4763 -** DIAG shall provide functionality for a root cause analysis **[** awaiting approvals **]**

**SRP-3644 -** Requirements for remote maintenance (RM) **[** awaiting approvals **]**

**SRP-4764 -** RM shall provide a functionality to get fast access to the remote maintenance GUI of all SR40 systems **[** awaiting approvals **]**

**SRP-3748 - Requirements for the Transfer System (data exchange system) [** awaiting approvals **]**

**SRP-3767 - General functionality of the Transfer System [** awaiting approvals **]**

**SRP-3800 -** The transfer system must synchronize data objects with their functions, data and event-triggers/callbacks between different systems, as if these objects are identical. **[** awaiting approvals **]**

**SRP-3801 -** The transfer system must be able to handle the communication between safe systems in a safe way **[** awaiting approvals **]**

**SRP-3802 -** The transfer system shall be able to use different carriers to fulfil its function and to combine their capacity or use them as redundant carriers **[** awaiting approvals **]**

**SRP-3768 - Requirements concerning FRMCS (Future Rail Mobile Communication System) [** awaiting approvals **]**

**SRP-3803 -** FRMCS shall have the functionality, performance and the capacity to fulfil the needs of the SR40 components for mobile communication **[** awaiting approvals **]**

**SRP-3770 - Requirements for the onboard CCS equipment [** awaiting approvals **]**

**SRP-3637 -** Requirements for Train control onboard (onboard, ETCS OBU) and for the EI-RBC: Defined in the TSI CCS. **[**awaiting approvals **]**

**SRP-4760 - TSI CCS**

http://www.era.europa.eu/document-register/pages/ccs-tsi.aspx

## **SRP-3606 -** Non-functional requirements **[**awaiting approvals **]**

### **SRP-3558 -** Requirements for the program management **[**awaiting approvals **]**

**SRP-3556 - SR40 Compliance Requirements [**awaiting approvals **]**

**SRP-3555 -** Programm Management must be compliant to suisse laws, suisse regulations und company-internal rules of SBB. **[**awaiting approvals **]**

**SRP-3557 -** SR40 Programm and its projects must work compliant to the regulations in SRP-3154 - Regulative und normative Vorgaben, as long as a deviation is not decided by the responsible authority. **[**awaiting approvals **]**

**SRP-4808 - Requirements for the SR40 developement process [**awaiting approvals **]**

**SRP-4807 -** Components shall be developed like products for a open market **[**awaiting approvals **]**

**SRP-4811 -** Useful subsets of the SR40 Systems shall be useable as Independent applications **[**awaiting approvals **]**

**SRP-4810 -** All concepts will be published for public usage (public license with minimal limitations concerning the usage and the compliance to the defined open interfaces). **[**awaiting approvals **]**

**SRP-4806 -** The developement of third party products using SR40 concepts shall be as simple as possible. **[**awaiting approvals **]**

**SRP-3602 - LifeCycle optimisation: Architectural requirements [**awaiting approvals **]**

**SRP-3603 -** It shall be easy to Change or exchange software and hardware from different types or vendors in SR40 systems (FFFiS principle). **[**awaiting approvals **]**

**SRP-3708 -** In a subsystem of SR40 there shall be an hardware abstraction layer (HAL) between application software and Hardware (where aplicable) **[** awaiting approvals **]**

**SRP-3709 -** Hardware shall be connected to the HAL over open interfaces. For safe components these interfaces shall fulfil the open safety requirements. **[** awaiting approvals **]**

**SRP-3710 -** Hardware status and capabilities shall be represented by the HAL to the application  software as abstract description and API independent from technologies (capability profiles) **[** awaiting approvals **]**

**SRP-3716 -** If a hardware is replaced with a different hardware with the same capabilities the HAL shall assure that there is no need to change or configure the application software, even for safe applications **[** awaiting approvals **]**

**SRP-3717 -** As Addition to the HAL there should by a aggregation layer, that can interface with sensor fusion and actor fusion subsystems based on specific raw data. These Subsystems shall combine capabilities of different sensors or different actors to one virtual component with a combined capability **[** awaiting approvals **]**

**SRP-3714 - Handable independent components in the right size [** awaiting approvals **]**

**SRP-3715 -** The SR40 architecture shall be devided in small independent components with open interfaces. For safe components these interfaces shall fulfil the open safety requirements. **[** awaiting approvals **]**

**SRP-3718 -** Open interfaces: Open interfaces must not be defined in a way, that only certain products can be connected. **[** awaiting approvals **]**

**SRP-3719 -** Interfaces shall always be defined with an upward- and downward compatible mechanism (profile based protocol negotiation). **[** awaiting approvals **]**

**SRP-3720 -** Interfaces are always the first step in the definition of the architecture. Interface-definitions also define the functional scope of its communicating partners. **[** awaiting approvals **]**

    - **SRP-3721 -** Components shall have a size, that enables also smaller companies to provide products **[**awaiting approvals **]**

    - **SRP-3722 -** Interfaces shall have a structure and protocol that allows the easy exchange of components at runtime **[**awaiting approvals **]**

  - **SRP-3754 - Independent life cycles [**awaiting approvals **]**

    - **SRP-3755 -** The architecture shall provide a set of interfaces that allow the components to have independent life cycles **[**awaiting approvals **]**

    - **SRP-3756 -** The HAL of components shall generate the flexibility to have different life cycles for hardware and software **[**awaiting approvals **]**

  - **SRP-3773 - Regional splits, open system scaling [**awaiting approvals **]**

    - **SRP-3774 -** SR40 and its components must allow to split the system into instances responsible for a part of an topology working together as one system **[**awaiting approvals **]**

- **SRP-3607 - Performance and capacity requirements for the System [**awaiting approvals **]**

  - **SRP-3771 -** SR40 shall have the technical performance and technical capacity to handle a traffic density twice as high as on the SBB Network in 2017 **[**awaiting approvals **]**

  - **SRP-4809 -** SR40 shall be able to handle every type of usual railway traffic (high speed, main line, regional, metro, on demand), that is existing today **[**awaiting approvals **]**

  - **SRP-4740 -** The amount of users of the SR40 systems shall be possibly as high as necessary for the biggest existing railways. **[**awaiting approvals **]**

- **SRP-3608 - Compatibility and interoperabilty requirements [**awaiting approvals **]**

  - **SRP-3775 -** SR40 must be compliant to euopean interoperability standards (TSI) **[**awaiting approvals **]**

  - **SRP-3776 -** SR40 must be able to interface to surrounding foreign systems (other companies, other countries) **[**awaiting approvals **]**

  - **SRP-3777 -** SR40 must be upwards compatible to an extended functionality to plan, control and integrate multimodal traffic, in which every type of traffic follows a physical or electronic track **[** awaiting approvals **]**

### SRP-3609 - Portability Requirements (Adaptability, Installability, Replaceability) [ awaiting approvals ]

**SRP-4890 -** SR40 component shall be configurable in a way that they can be used in all typical types of railways with national requirements (mainline, regional, Metro) **[** awaiting approvals **]**

**SRP-4889 -** SR40 components shall be easy to install, following the idea of "plug&play" **[** awaiting approvals **]**

**SRP-4892 -** SR40 components shall be replaceable on runtinme **[** awaiting approvals **]**

**SRP-4891 -** SR40 component-interfaces shall be defined with a mechanism, that allows components, using an older special protocol version to communicated with components, that are using a newer version **[** awaiting approvals **]**

### SRP-3610 - Safety requirements. See: SR40 Safety Targets and SR40 Safety Rules for Safe Systems (SRSS) [ awaiting approvals ]

**SRP-5193 -** SR40 applications must fulfil the SR40 safety targets and the SR40 safety rules for safe systems. If a safety relevant design decision hast to be taken, that is not covered by these two requirement sets, the highest safety level has to be reached, that can be achieved in an economic and affordable way. **[** awaiting approvals **]**

### SRP-3611 - Availability requirements [ awaiting approvals ]

**SRP-3778 -** SR40 and its components shall fulfil all availability targets that can be achieved in an economic and affordable way. **[** awaiting approvals **]**

### SRP-3612 - Maintainability requirements [ awaiting approvals ]

**SRP-3779 -** SR40 and its components shall fulfil all maintainability targets that can be achieved in an economic and affordable way. **[** awaiting approvals **]**

**SRP-3780 -** SR40 components shall provide remote diagnostics, remote configuration and remote repair even if they are safe components. **[** awaiting approvals **]**

**SRP-3781 -** SR40 shall support the replacement on runtime where economically possible **[** awaiting approvals **]**

### **SRP-3613 - Security requirements [** awaiting approvals **]**

**SRP-3757 -** SR40 and its components shall provide the highest security level that can be achieved in an economic and affordable way. **[** awaiting approvals **]**

**SRP-4749 -** The interaction of safety and security processes and systems musst fullfil special high requirements, for example: **[** awaiting approvals **]**

**SRP-2121 -** The system shall store all information in such a way that only a defined group of employees can access the data. **[** awaiting approvals **]**

**SRP-2120 -** The security keys shall be stored securely. The private key should be generated and stored only on the hardware where they are used. **[** awaiting approvals **]**

**SRP-2122 -** High data privacy requirements for localization information of person related GLAT Tag. **[** awaiting approvals **]**

**SRP-2119 -** The system must ensure a very high level of integrity and authenticity for everything that is involved in the safety critical control of the outside world, such that an attacker cannot take over control of parts of the system. **[** awaiting approvals **]**

### **SRP-3614 - Reliability, availability and maintainability requirements (RAM) [** awaiting approvals **]**

**SRP-4741 -** At Minimum SR40 and ist components shall allow to fullfill the RAM requirements of today. **[** awaiting approvals **]**

### **SRP-3615 - Environmental and physical requirements [** awaiting approvals **]**

**SRP-3792 -** SR40 components must be as robust as necessary and defined in the use case Environment. **[** awaiting approvals **]**

### **SRP-3616 - Life cycle Management requirements [** awaiting approvals **]**

**SRP-3793 -** SR40 components shall provide functionality to support their life cycle management **[** awaiting approvals **]**

### **SRP-3617 - Usability requirements [** awaiting approvals **]**

**SRP-3783 -** MMI shall be self explaining **[** awaiting approvals **]**

**SRP-3784 -** MMI shall achieve high productivity **[** awaiting approvals **]**

**SRP-3788 -** MMI must be as robust as necessary in the use case enviroment **[** awaiting approvals **]**

**SRP-3789 -** MMI should have a positive style and design **[** awaiting approvals **]**

**SRP-3790 -** MMI should react in a short period or show pending processes **[** awaiting approvals **]**

**SRP-3618 - Migration requirements [** awaiting approvals **]**

**SRP-3723 -** The SR40 architecture and functionality shall allow the migration of large transport network segments in one step **[** awaiting approvals **]**

**SRP-3794 -** The SR40 architecture shall allow to split migrations and rollouts in industrial processes **[** awaiting approvals **]**

**SRP-3724 -** The SR40 architecture and its components shall allow**,** that single SR40 components are integrated in legacy architectures. Especially for TMS, EI, GLAT and ATO. **[** awaiting approvals **]**

**SRP-3619 - Obsolescence requirements [** awaiting approvals **]**

**SRP-3795 -** SR40 components shall be designed for a lifespan, where the index of LCC/lifespan has the lowest value **[** awaiting approvals **]**

**SRP-3796 -** SR40 components shall support diagnostic functionality for a prognosis of the end of life **[** awaiting approvals **]**

**SRP-3620 - Other non functional requirements [** awaiting approvals **]**

**SRP-5226 -** SR40 components shall fulfil "state of the art" requirement levels concerning
Privacy
LCC
Implementation
Supportability
Compliance
Capacity
Time, Performance, Throughput
Effectiveness
Accessability
Accountability, Monitoring, Diagnosis
Reusability
Resilience
Fault Tolerance

Adaptability and Extensability

Scaleability

Portability

Configuration Management

Testability and Tests

Backup and Recovery

Robustness and Stability

Self-Sufficiency

Form and Fit

Design

Environmental protection

EM Radiation and Robustness

Physical Protection and Robustness

Climate and Humidity Robustness **[** awaiting approvals **]**

## **SRP-3621 -** Requirements concerning business change **[** awaiting approvals **]**

**SRP-3797 -** Business change projects shall be divided into reasonable short steps and should start as early as economically reasonable **[** awaiting approvals **]**

**SRP-3798 -** Business change projects must not create instable production situations **[** awaiting approvals **]**

**SRP-3799 -** The implementation of new systems in business change projects is always executed with prepared business continuity measures, if something goes wrong **[** awaiting approvals **]**

## 3 Glossary

| Term | Abbrev. | Description |
|---|---|---|
| **Man Machine Interface** | MMI | Software: The layout and functionality of the user interface<br>Hardware: Displays, keyboards, switches, touchscreens, etc. |
| **Mobile Traffic Control Systems** | MTC | An MTC is a system, that controls safe movements over mobile end devices, that are locatable (Tablets, Tags, portable Systems). Its core functionality is the movement authorization and separation (server function), and on the mobile device the MMI for movement requests, authorization information, information about the movement status, warning and general information/location based services. |
| **Open safety** | Open safety | An interface fulfils the open safety requirements, when it is built in a way that allows to homologate (safety case) the communication partners separately without knowing each other. Normally this means a "small protocol" and a minimized number of status-combinations, and the requirement of a "full testability" (test vector, reference systems, isolated certification) of the component against the interface specification.<br>See also |