DECISION OF THE SYSTEM PILLAR STEERING GROUP

approving for internal publication within EU-RAIL of the CCS/TMS diagnosis and configuration concepts to allow testing and validation and further development

N° 4/2024

THE SYSTEM PILLAR STEERING GROUP OF THE EUROPE'S RAIL JOINT UNDERTAKING, NOTES

- The Transverse CCS components (TCCS) domain is responsible for the standardisation of the CCS/ TMS data processes within the System Pillar, especially
  - CCS/TMS Data Model derived from ERA-ontology, and associated documents
  - Diagnosis
  - Configuration

  in close cooperation with System Pillar Tasks, Domains and Innovation Pillar projects, as far as concerned. TCCS serves the needs of data preparation, data configuration and data processes, especially supporting the standardisation of data communication interfaces of structural domains of the System Pillar.

- The status of the CCS/TMS data model is presented in Decision 3/2024.

- The work on diagnosis and configuration has progressed sufficiently far to inform the SP-STG on progress, and request approval to move to the next stage of development.

- The position on diagnosis is presented in Annex 1.

- The position on configuration is presented in Annex 2.

- The deliverables listed in the Annexes have received the necessary approvals within the System Pillar. Further details and full approval status overview can be obtained from the Publication Overview. Concerned Innovation Pillar projects have been regularly informed and consulted.

- In sum, the work within TCCS on diagnosis and configuration means there is a proposal for the current fragmented and decentralized processes on diagnosis and configuration to be centralized and connected, using also shared services of cybersecurity like a common reference time information. The benefit of the successful implementation of such an approach would be on both efficiency and quality:
  - Central configuration processes ensure coherence in data configuration (software updates). There is no more need for local updates, staying with incompatible versions of assets for considerable time.

- Digital registers for vehicles and infrastructure depend on the configuration process as it distributes central data to decentralized data consumers. The configuration process is only responsible for the distribution of the data, not for the data and its preparation itself.
  - Central diagnosis processes ensure implemented assets becoming the “single source of truth” for the asset inventory: Continuous monitoring enables a live asset inventory where each change of a spare part will automatically result in an immediate update of the asset inventory. This way, the request of the authorities to have always complete awareness of equipment locations and serial numbers in the field and on trains down to LRU (spare part) level can reliably be satisfied and constitutes a digital twin.
  - A generic equipment model facilitates the interoperability of design specific equipment models without imposing any specific design choice. The standardization of data points (data sensor sources) for the technical parameters – raw data as well as processed data – has been achieved for trackside assets and will reach further out to vehicles and additional infrastructure installations. The “need-to-know-principle” fosters the exchange of data for mutual benefit of data providers and consumers without imposing any specific governance.

- The maturity of the proposed diagnosis and configuration processes, allow for testing in order to further mature the specifications. The first reference implementation of the “single source of truth” approach of the diagnosis process will be shown on Innotrans 2024 in the DG MOVE/ERA/EU-RAIL booth. A number of projects has already indicated ready- and willingness to demonstrate the configuration process, e.g. moving block in R2DATO WP 45.

- Commercial projects that want to take up CCS innovations from EU-RAIL usually depend on the operability of the diagnosis and configuration processes as the prerequisite for implementation. Therefore, the operability of the processes shall be tested sufficiently in advance. This decision is supportive in this.

THE SYSTEM PILLAR STEERING GROUP OF THE EUROPE'S RAIL JOINT UNDERTAKING, AGREES

- on the specified design and the basic principles as draft concepts to be followed in the next specification steps.

- to publish on the EU-RAIL share point, and elsewhere, the CCS/TMS diagnosis and configuration documents as set out in the Annexes 1 and 2 for internal use and further testing and validation within EU-RAIL.

ANNEX 1 Diagnosis

- The general context for diagnosis within rail, is
  - Efficient diagnosis significantly contributes to the reliability, availability and maintainability of the railway system
  - Diagnosis is considered not safety relevant. Safety-relevant data is transmitted via Standard Communication Interface (SCI), non-safety relevant data via Standard Diagnostic Interface (SDI). Here we are concerned with the non-safety relevant data via the SDI.
  - Diagnostic data should follow the "need-to-know" principle as outlined in the document "TCCS SD2 Summary on General Diagnostic Concept". It clarifies that ingested data should be made available to every stakeholder that "needs to know" the data. Specifically:
    - The RU/IM would like to operate reliable and safe components.
    - The suppliers would like to deliver reliable and safe components. Along with the product a supplier/integrator should deliver algorithms that are able to predict the behavior of the product.
    - These needs are not conflicting per se and can be mutually satisfied by a sound standardization of sufficient amount of data points. Here, the diagnosis process has been designed to enable exchange of (standardized) diagnostic data points. The standardization of specific data points is out of scope of the current deliverables and is subject to specifications on sub-system level (e.g. Trackside Assets, see SP/EULYNX BL4R3).

- To support the development and harmonisation of approach to the future development of the CCS (and interface to TMS) systems based on radio-based ETCS-only deployment, it is favourable to have a standardised diagnosis approach in order to unleash the potential of predictive maintenance and optimisation of operations. Such an approach has been developed and should be further evolved in the frame of the EU Data Act and potentially contributing to EU Mobility Data Spaces.

- The diagnostic approach has been developed from top-down. Based on research experience from previous European projects, and from ongoing implementations in Innovation Pillar Flagship Projects. Especially it is compliant with the bottom-up developed standardization of data points published in the SP/EULYNX joint B4 R3.

- The CCS/TMS diagnosis concept is use case driven, which means each data input provider (data point) shall be justified from the perspective of
  - Operational forecast (TMS/CMS need), represented by the restriction model of the CCS/TMS Data Model
  - Condition based maintenance, supported by the equipment models of the suppliers, based on the generic equipment model as published by SP/EULYNX joint B4 R3.

- To achieve the sufficient level of harmonization national or supplier specific procedures are explicitly prevented. Thus, a generic equipment model for both train- and trackside has been developed.

- The decision is to validate the main design decisions on concept level, meaning that in the next specification steps this concept is considered as a constraint for the design
    - data categorization, focusing on semantics and metadata across the dimensions of Modeling Rule, Data Type, and Data Category
    - OPC-UA (Open Platform Communications Unified Architecture) is a data exchange standard widely used in industrial automation and communication. It is an Ethernet-based, service-oriented messaging specification that defines various transport, encoding, security, and data models for command, control, and data exchange. OPC UA is an independent standard, not tied to any specific system or manufacturer, and facilitates both PC-to-machine and machine-to-machine communication
    - Though not being a design decision, a first reference implementation, specifically highlighting the initial deployment of a Maintenance, Diagnostics and Monitoring (MDM) will be shown at Innotrans 2024
    - Allow and prepare for Condition-Based Maintenance (CBM) and operational optimisation
    - Data Access control, following the “need-to-know principle”
    - Build on the SP/EULYNX B4R3 published list of the standardized trackside data points, showcasing the railway sector’s commitment to standardization while also highlighting the challenges and motivation to progress further. This effort extends beyond just vehicles and trains, aiming for intelligent, comprehensive coverage of the Single EU Railway Area.
    - ambition to evolve through diagnostics and digital modeling towards a digital twin of the railway system and its subsystems. Once a digital twin is available, railway system operations can shift from a reactive approach to a proactive one.

- The content defined in this release shall not be considered as fully finalized but rather a developed draft ready for continuous improvement. This explicitly includes developments upcoming in the Task 5 Harmonised Diagnostics of the System Pillar to ensure overall coherence.

- Nevertheless, the level of development is deemed sufficient to enable EU-RAIL internal publication.

- The relevant documents are:
    - TCCS SD2 – Operational Analysis - Operational Epics
    - TCCS SD2 – Operational Analysis - Operational Analysis
    - TCCS SD2 – System Analysis – FRS - Generic Diagnostic Concept

- The documents explain the top-down approach for defining and specifying basic harmonised functionalities for a CCS integrated subsystem and standard interfaces/protocols and diagnostic data points to be collected from CCS systems (e.g. field components, CCS-On Board, …) and CCS-external systems (e.g. sensors, monitoring devices for tracks and train, …).

- The approval process that has been followed as described in the Publication Document.

To note:

- The diagnostic concept was presented at the SP-STG meeting 9, and further work requested in particular on the categorization of the data, and the preservation of modularity. The following document has been additionally produced in order to respond to the questions of the Steering Group:
  - TCCS SD2 - Summary on General Diagnostic Concept

- In summary, the concerns raised in the SP-STG about data categorization and ownership have been treated in the following way:
  - The standard data interface (SDI) as defined by EULYNX is introduced
  - SDI ensures the interoperability of diagnosis data towards a data collector, i.e. the Maintenance, Diagnosis and Monitoring (MDM) functionality
  - The diagnosis data transmitted via SDI results from standardized data points, i.e. sensors and further sources of diagnostic data
  - Whatever is the design choice of a sub-system, the mapping of its data points with those of the generic equipment model ensures the standardized syntax and semantics of those data points. Naturally, the generic equipment model provides more data points than the equipment model of the supplier, representing product behavior.
  - The standardization process of data points is use case driven according to the "need-to-know-principle". This principle fosters standardization on the basis of mutual benefit of stakeholders.
  - Based on the available diagnostic data, analytics can apply and evolve. At the begin of the lifecycle the supplier is in the best position to provide algorithms for prediction. Considering environmental data such as operational data and with learnings during the lifetime, the operator becomes better prepared in evolving algorithms and predict behaviour more precisely.

Annex 2 Configuration

- To support the development and harmonisation of approach to the future development of the CCS (and interface to TMS) systems based on radio-based ETCS-only deployment, it is necessary to have a standardised, centralised and industrialised configuration process. Otherwise, the configuration would need to be continued on local level with manual configuration (updates, uploads) of field elements, vehicles and interlockings. It would result in a period of incompatible configurations unless all interacting systems have been updated to the foreseen configuration. This process would need to be repeated for every bug-fixing, update or upgrade of functions. Hence, the digital railway system would be severely hampered by each configuration need, if not centrally and compatibly – thus standardised – organised.

- Configuration refers to the arrangement of settings, parameters, or components that define how a system, device, or software operates. It involves specifying how different parts interact, what resources they use, and the rules or instructions that govern their operation. Configurations can be applied to a wide range of systems, including computers, networks, applications, and even physical devices. The following is specifically important:
    - Configuration applies for safety-relevant and non-safety relevant data including software. It is one common process with additional steps only applicable for safety-relevant data.
    - Configuration is vital for the operability of the system and also for the safety, where required
    - Configuration forms a dependency tree where the number of dependency levels is not limited
    - Configuration process is manufacturer independent, applies both for train and trackside and encompasses suppliers, integrators and RU/IM
    - Safety: Configuration ensures that only correct and consistent validated software configurations are deployed and dependencies are managed
    - Optimal Performance: Proper configuration ensures that a system operates at peak efficiency. For example, configuring a network correctly can reduce latency and improve throughput, while software configuration can optimize resource usage.
    - Stability: Correct configurations help ensure that systems run reliably. Misconfigurations can lead to errors, crashes, or security vulnerabilities.
    - Security: Configuration enables fast patch management in case of detected vulnerabilities.
    - Scalability: In larger environments, proper configuration enables systems to scale effectively, whether it's a cloud infrastructure that can handle more traffic or a database system that can process a larger volume of queries.

- The significance of correct configuration includes:
    - Influence on Success or Failure: Proper configurations can mean the difference between success and failure of a system. Misconfigurations often lead to downtime, data loss, or security breaches.
    - Adaptability and Flexibility: Configurations allow systems to be flexible, adapting to new requirements without needing to rebuild or replace them.

    - Compliance and Governance: Configuration settings help ensure systems meet industry standards and regulatory requirements, which are important for avoiding fines or legal issues.
    - Long-Term Maintenance: A well-configured system is easier to maintain, troubleshoot, and update. This reduces operational costs and enhances the system's life span.

- In summary, configuration is crucial for ensuring a system functions correctly, safely, and efficiently. Decisions made during configuration have long-lasting impacts on performance, security, and usability, which are essential for the system's operational success.

- The CCS/TMS configuration concept has been developed from top-down following established configuration processes in distributed systems. Especially it builds upon and evolves further the bottom-up developed standardization of SMI published in the SP/ EULYNX joint B4 R3.

- It is explicitly prevented to include national or supplier specific procedures or guidelines.

- The content defined in this release shall not be considered as fully finalized but rather a developed draft ready for continuous improvement.

- Nevertheless, the level of development is deemed sufficient to enable ERJU internal publication.

- The relevant documents are:
    - TCCS SD3 - Operational Analysis (ORS) – Operational Epics
    - TCCS SD3 - System Analysis (FRS) – System Requirements
    - TCCS SD3 - Logical and Subsystem Architecture – Logical Concept

- Within the documents the main design decisions on concept level to support the key features of configuration are set out. These design decisions will be
    - Automated configuration (updates) over the network
    - Configure Systems of any size and complexity
    - Manage complexity by explicit dependency management
    - Use one management system for safe and non-safe configurations
    - End-to-End responsibility of suppliers and integrators
    - Manufacturer independent
    - For vehicles and trackside infrastructure
    - Process to organise suppliers, integrators and operators (RU/IM)

- Use Case examples include:
    - An area of control with five TPS, EAL and ATO-TS (which may collectively contain several 1000 field elements from different suppliers) needs a configuration update.
    - The ETCS vital computer and the radio system of a fleet of trains needs to be updated.
    - IT security patches for a lot of subsystems.

    - All ATO-TS in a country or in a corridor simultaneously need a configuration update.

- The TCCS configuration management work extends the work of the joint EU-RAIL SP/EULYNX B4R3, specifically the SMI interface for transmitting configuration items to trackside assets. In the EULYNX concept the safety is ensured by the interlocking via the SCI interface. This concept has been developed further:
    - Context in data preparation and data distribution is defined
    - Documents for data distribution, dependency management and safety attestation are standardized
    - For data distribution the SMI interface is needed only
    - Works for vehicles and infrastructure
    - Update only components that need an update
    - The concept is applicable for configuration updates of field elements, TPS, ATO-TS, EAL, TMS etc.
    - Communicating with the RU planning system and TMS an operator determines the best point in time for the configuration updates and expresses his "will" to start the update. When the interfaces to the RU planning system and TMS are specified further this process can be automated further.

- The approval process that has been followed is described in the Publication Document.