ERJU SYSTEM PILLAR

# Operational Vision CCS Part

# Operational Vision CCS Part

# 1 Document purpose and target group

This document was decided by the System Pillar Steeing Group in 2022.

This document sketches a compressed operational picture of the CCS and TMS/CM future. It is written for all readers. Technical background is not needed. A basic operational knowledge is being expected.

This vision is intended to be the starting point for the top-down discussion about the operational concept. It defines general directions and the ambitions for the future CCS and TMS/CM target systems as a discussion basis. It shall set the frame for more detailed discussions in the System Pillar, structured along the operational process areas.

Since the vision is touching several fundamental issues, a purely document-driven review process is not recommended. A collaborative discussion process, that will be initiated in the next step, will analyse this vision and the harmonisation process more in detail.

This operational vision was influenced (besides CBO, common business objectives) by the analysis of several future operational concepts or approaches of Shift2Rail (e.g., ATO, Moving Block, LinX4Rail), existing concept from initiatives (e.g., EULYNX, RCA, OCORA), ongoing enhancement discussions for the TSI CCS 2022 (e.g. for enhanced shunting and better support for ETCS Level 3 operations) and large railway programs (Target190 in NetworkRail, Digitale Schiene Deutschland in Deutsche Bahn, smartrail4.0 and succeeding projects in SBB, Hybrid Level 3 Concept). This document summarizes the major operational ideas behind them.

This document contains only considerations for CCS and TMS/CM.

Operational concepts touch all conceptual levels – from strategic to practical issues.

## 2 Purpose and structure of this operational vision document


Figure 1 OpCon derivation process

The CBO are generic targets, that were derived from several analysis documents in the sector for example in LinX4Rail, ERRAC, OCORA or RCA. In this document the CBO are translated into a compressed vision for CCS and TMS/CM from the operational perspective.

The operational concept describes three different conceptual areas (see also ISO 15288):

- CONOPS: Concept of operations,
  - Characteristics and requirements from business view
  - Major inter-company interactions on business level
  - Legal concepts and constraints
  - Shared sector and company structures (templates or standard services)
- CONUSE: Concept how to use the system
  - Concept for the production processes
  - Parameters, constraints, and rules of system usage
- CONEMP: Concept of employment
  - Asset management processes (plan, build, run, maintain, change, disinvest)

## 3 Operational Vision for CCS and TM/CM

On business level the vision is to make best CCS and TM/CM (traffic Management, capacity management) practices available as standardized operational processes, products, planning models, target systems, tender specifications, or configuration templates – ready to “download and use”. The idea is not “one fits all”, but “a set of strictly standardized configurations (scalability) fits all needs”, while every configuration is interoperable with each other and not designed with national or company specific features (“borderless”).

The intention is not to avoid every diversity or competition. These shall be focussed on the services and products where they support the competitiveness of the railway system. Analogy: Although there is a large variety of “cars” with different price/performance offers, there are “application categories” with standard functionalities (trucks, SUV, small cheap automobiles, mobile homes, etc.) and highly standardized components from the component industry market, that are used (standard tires, batteries, OPC-UA(OPC-UA: see OPC Unified Architecture – Wikipedia) based control systems, etc.). This standardisation does not mean that all SUV shall have the same price and quality; or that there is only one type of battery or one type of fuel for all types of cars. Standardisation shall focus on the right areas and shall allow a reasonable bandwidth of solutions per area.

In the same way the CCS and TM/CM application categories for the railway system types can be defined and standardized, based on agreed set of targets, requirements, and functionalities.

**standard components**
The operational vision for CCS and TM/CM is to change all operational processes on business level,

production level and asset management level towards a much stronger CCS and TMS/CM production based on such “standardized application categories” and standard components (subsystems).

**long-term evolution: modularisation**
This means a market change in terms of stronger industrialisation and specialized large-scale market services on the long run, depending on the long-term evolution of the rational modularisation. Railway asset management organisations will focus more on designing and procuring asset capacity instead of designing special systems or maintaining special installations.

**Competitiveness**
Overall, a very efficient process chain will allow to increase the competitiveness of the Railway system and to implement a faster improvement process and better evolvability.

# 4 CONUSE Vision for CCS and TM/CM

## 4.1 Traffic Management / Capacity Management

See corresponding chapter Operational Vision CMS_TMS Part

## 4.2 Traffic Control and Supervision

**Traffic CS shall offer an optimized and automized basic functionality to control and report any type of track usage**
The basic vision for Traffic Control and Supervision (Traffic CS) is that this control layer offers a very precise interface for the traffic management (e.g. detailed speeds, train characteristics, progress of processes). This preciseness allows to optimize all movements in relation to each other (capacity, speed, energy consumption), to reduce train ahead times, dwelling times, delay times, and unproductive waiting times of maintenance teams or construction sites. The operational state includes detailed information about all actors and systems in the production. The communication to all actors is digitized and because of this automatable.

**ATO for normal and degraded modes**
The second aspect of the basic operational vision is to highly automate Traffic CS (still allowing manual control) for normal and most of the degraded production situations, based on a scalable physical architecture and in collaboration with the Traffic Management process. Technical and operational interoperability - as needed for the SERA - is based on a simple compatibility management that supports an economic migration and mixed generations. Executing an operational plan coming from Traffic Management processes in short intervals in real-time shall be automated in all aspects, based on cooperation rules and procedures. This includes movement permissions for normal train movements, shunting, joining, splitting or other manoeuvres (supported by automated coupling), as well as granting possessions for construction sites, track access for maintenance teams, warning processes, or the change of a point position that a maintenance team needs. The automation shall decrease effort and duration for operation and deployment, and increase reliability, safety, and precision/capacity.

**Track user planning via Traffic Management process**
All track user (vehicles, or field forces: e.g., track workers, operational services in the field, etc.) requests, needed actions, permissions, or asset changes are requested to and planned via the Traffic Management process in an optimized and integrated way. They can also be requested by field force applications or TM terminals in or near the train (e.g., to initiate remote controlled train movements), to allow a completely automated process. Non-track-bound track users or mobile objects (like a locatable construction site boundary marking device, or a localized person) are seamlessly integrated into to the safety supervision process like normal trains to achieve a complete safety supervision.

**Safety assessment on run time**
The Traffic Control process implements a “safety assessment on run time” method to assure flexible and scalable configurations, flexible and efficient migrations (deployment and evolvability), line access by heterogenous train types with different capabilities, asset changes on run-time, different asset capabilities, and degraded modes with still available production capacity and automation. The method shall follow the approach to assess dynamically and in real-time the available reliable information about configuration, track usage and asset conditions before allowing any change of status, movement, or new track usage.

Example:

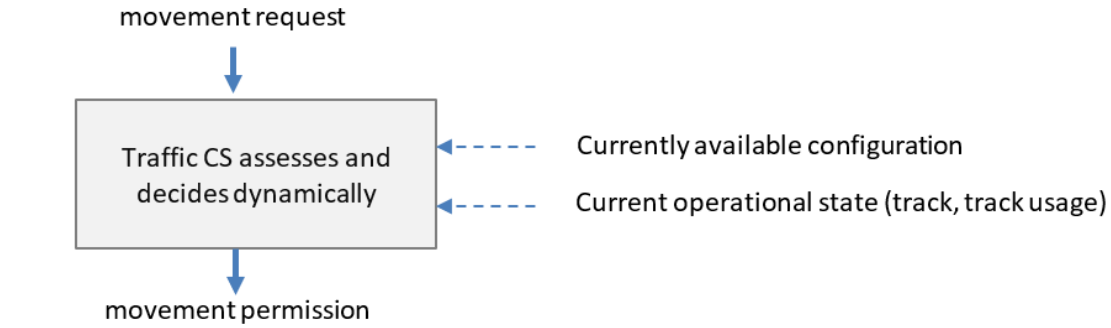


*Figure 2 Example: Dynamic safety assessment on runtime*

**Automation in degraded modes and system intervention**
One important improvement/requirement inside of this dynamic safety assessment is to allow some automation in degraded modes (if still possible) and to change infrastructures (or intervene into the system) under production in a safe way. Instead of working in an “on/off/verify/on” way, the Traffic CS shall assess on the basis of its available operational state information (assets, trains, etc.) what automation in degraded modes (“rich degraded modes”, e.g. automatic command for sweeping a defect point by moving on sight) or what system intervention (e.g. diagnosis test run in an component under production) is still safe. This increases availability and efficiency.

**Continuous supervision of railway production**
The safety, condition and availability supervision of the railway production is a continuous process for all types of track users (track-bound or non-track-bound) in the same way and includes static as well as configurable event pattern recognition for automatically triggering event-related mitigations or measures. All types of more and more available mobile, train-born, or fixed sensor information (also from outside of the CCS and TM/CM system) and data sources (like WIFI detection or mobile maintenance apps) are included dynamically into and combined in this supervision (like person counters for platforms or car detectors on crossings) to increase the reliability, robustness, availability, and precision of this supervision process.

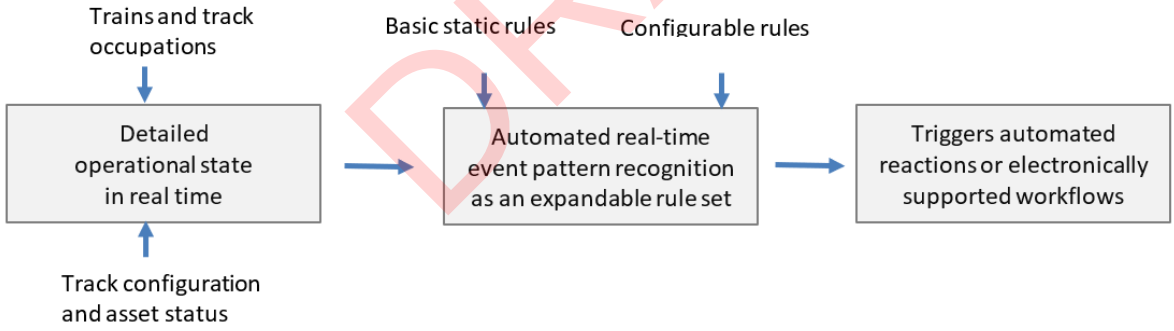


*Figure 3 Comprehensive event pattern recognition for safety, availability, and asset conditions*

Another important aspect of the improvement of the traffic control processes is the next evolution step for ETCS-based processes. The important next evolution step for ETCS is to tune the existing architecture to the performance and cost that it was designed for and like it is visible in some CBTC implementations (higher performance, less cost for trackside assets, simple deployment).

**Improved ETCS performance**
This includes for example precise braking and speed regime, complete supervision in all normal situations (like for shunting), fast and simple border transitions, fast change of direction, all types of movements (like propelling of yellow fleet trains) or fast start of mission.

**Optimizing track capacity**
The relevance of track occupancy information including safety margins shall be taken into account for optimizing track capacity.Traffic CS of today on mainline does not make the full use of the physical track

capacity in this way. Diffuse operational states (e.g., track position of a starting train) are reported and control optimisations do not take train capabilities into account.

**Stable and backwards compatible air gap interface**
This does not mean to significantly change the interoperability-related specifications for the air gap interface as defined in the TSI CCS. Here only some dedicated extensions will be needed in future for automation, higher performance, less migration effort, and more scalability (e.g., driverless ATO GoA 4, support for enhanced onboard localisation, coexistence of ETCS system versions on a line (to a limited extend), supporting degraded modes on lines without trackside train detection, etc.).

## 4.3 Train Control and Supervision

**Train CS shall offer all basic onboard functionalities for suboprocesses conercerning TM/CM, ATO and ATP (ETCS) happening in trains or train units**
This if the roof requirement for all standard capabilities that Train CS shall offer

**Train CS (CCS onboard) for mainline traffic today has a low grade of automation...**
Train CS (CCS onboard) for mainline traffic today has a low grade of automation and creates out of this higher operational cost and unnecessary capacity usage.
Missing integration into the train and insufficient technology quality leads to a lack of information about the train, that reduces the precision for trackside planning and control processes.

**ATO**
The operational vision for the Train CS (CCS onboard) contains fully automated (ATO) and interoperable (ETCS) train operations even for shunting or joining/splitting (digital automated coupling) processes.

**Driver advisory systems**
When train drivers are needed for the process, they are supported by assistance systems that support an optimal driving process concerning traffic flow and energy consumption.

**Optimizing track capacity**
The train protection processes onboard are tuned in a way that allows the optimal use of the physical capacity without blocking capacity too early or too much.

## 4.4 Field forces processes and trackworker safety

**Field Force Applications, Control and Supervision shall support a safe and performant trackusage (basif functionality) for objects, vehicles and persons which are not track-bound and which shall not create dangers for the traffick on track**
This is the roof requirement for all capabilities concerning Field Force applications. These include for exmaple trackworker safety systems, integration of non-trackbound vehicles into the safety logic, or production status information for operational people near the track.

**Reduce production impact**
The productivity of field forces, especially track workers, and the effort for preparing, starting, and stopping operations on the track or influencing trackside assets shall be automated to shorten the duration of maintenance windows (reduce production impact) and to increase the safety.

**Automated field force protection**
Persons, blocking devices or tagged obstacles on track shall be identified and protected automatically.

**Efficient and cheaper warning systems**
Efficient and cheaper warning systems (with very low number of wrong alarms) allow a rapid set up and end warning areas with high reliability and safety.

## 4.5 Trackside Assets Control and Supervision

**Trackside Asset CS allows to control a broad heterogenity of systems and technologies in a standardized way**
This is the roof requirement for all basic standard functionlities for Trackside Asset CS (currently for point-machines, crossings and trackside sensors).

### 4.6 Transversal Systems

**The Transversal Systems shall offer efficient and automated support to manage asset data, technical asset status information (for diagnostics), configurations of CCS systems, seurity, and integrated user interfaces**
This is the roof requirement for all basic functionalities of the transversal systems

### 4.7 CCS PRAMSS targets and production cost

**The quantitative targets for PRAMSS shall fulfil the needs of the System Pillar stakeholders, in a scalable releation to the cost they create**
PRAMSS targets shall be analysed and agreed together with the stakeholderes. Targets can, if needed and agreed concerning risk acceptance, have a bandwidth with a defined minimum. The bandwidth should relate to scalable but also agreed cost bandwidth.

## 5 CONEMP Vision for CCS and TM/CM

### 5.1 Reducing TCO of CCS and TM/CM(total cost of ownership)

Besides of supporting lower energy consumption, resilience, and sustainability with the right choice of technology, control processes and materials the reduction of the total cost of ownership (TCO) for CCS and TM/CM is the primary target.

**Reduced TCO**
Reducing TCO is directly driven by the customer perspective. It allows to generate lower transport prices or to afford more capacity or service. It is the primary factor for the railway system's competitiveness and urgently needed for it's the change towards SERA.

**Positive business case**
Positive business cases are a strong prerequisite for the operational and technical change and for the fast deployment of ERTMS. The economic advantage needs to be significant for any type of innovation, otherwise the railway system will not evolve. The investments needed for multi-modal transport chains will only be affordable if the TCO are reduced to the needed level.

**TCO Optimization**
The TCO are influenced by

1. The number of needed assets for CCS and TM/CM (effects also energy consumption and disturbances)
2. The grade of automation of processes in the life cycle (planning of infrastructures and vehicles, construction, configuration, maintenance, monitoring, updates, upgrades, add-ons, etc.)
3. The architecture quality e.g. concerning the "intelligence" of the traffic management and traffic control that reduce the need for physical assets
4. The development cost caused by heterogeneity, instability of requirements, and lack of specification quality
5. The needed specialist skills for special systems
6. The number of standby expert resources during the full lifecycle
7. The missing forward and backward compatibility or modularity of assets causing early replacements/changes and preventing selective component replacements
8. The integration cost for components increased by complex and diverse interface structures
9. Ineffective/inefficient safety assurance processes with a high amount of bureaucracy, control processes without impacts, missing modular homologation, and low maintainability of safety case documentation
10. The marketing, training, procurement, and distribution cost caused by a high variety of systems (coming from heterogenous requirements)
11. The unit prices for systems and their lifetime duration

**Unit prices**
The CONEMP vision is to significantly reduce all these cost factors. The last factor – the unit price – may increase (smart automation) when the other factors are reduced. Since unit prices make only a very small part in the TCO in most cases, this automation effect is acceptable.

## 5.2 Process design and requirements management on sector level

**Operational process harmonization**
The large business case of “reusability of nearly everything” is based on standardisation. Standardisation is based on harmonized requirements. To reach this goal, a large part of the requirements (change) management has to be done on sector level. Most of the requirements come from operational process design, which therefore needs also to be standardized in detail.

**Re-use**
Based on this, products, procurement documentation, education and know how, handbooks, rulebooks, integration methods, safety cases, test facilities, market services, etc. can be reused cross-company and cross-country. This reduction of effort, the simplification and homogenisation of skill needs is not only reducing the TCO in every aspect – it also allows the change of market towards specialized services for certain process areas that can work with high efficiency and at large scale. Also, the development and innovation, which no longer has to implement individual solutions for every customer, can afford higher investments in system quality and automation which again reduces the TCO by automating many life cycle processes.

**Upgradeability**
Homogenous requirements lead in the end to homogenous systems, and this is the basis for simple and efficient upgradeability. Upgradeability means to keep all systems up-to-date, to reduce the cost of heterogeneity, to have access to more market products, and much higher security. Upgradeability and updateability is one of the very first important steps of the architecture and process optimisation, based on modularity, automated tool chains, support systems for continuous process changes, and simplified integration methods.

This higher flexibility for extended CONEMP business models, which becomes possible with standardisation, is a potential which will be translated to new large-scale services and more market strength. Specialized component providers will be able to sell much higher volumes at lower price and better service. There will be RU and IM that decide to reduce their internal business scope to customer services and operating assets, while system services and the assets are mostly provided externally from the market (like it changed for data centres in the last 20 years). Other perhaps larger RU and IM may decide to take advantage of the standardisation to reduce the number of steps in the supply chain and the asset management process and integrate standard components inhouse for certain areas themselves. The market will decide, how the new potential is used.

## 5.3 Enhanced System Architecting and Integration processes for CCS and TM/CM

The architecture of today is the result of many decades of small component-wise transformations and patching new systems into the overall architecture. The paradigm of the past was often to change as little as possible the architecture in every step (more stability, focus short-term cost). Out of this, today’s CCS and TM/CM architecture (especially for main-line railways in Europe) is a patchwork of old and newer philosophies and features, sometimes hard to handle, inflexible, difficult to integrate and expensive to migrate and replace. High architectural dependencies lead to the need for “large and complete” asset replacements, with high project risks, very large budgets in short time periods and imbalanced asset age structures as a long-term consequence.
The patchwork of today includes several redundancies like between interlockings and RBC, between ATO and ETCS (ATP) related processes, or between interlockings, control systems and planning systems. Redundancies in control systems create additional effort in several life cycle processes concerning synchronisation, hazard management, additional interfaces, integration safety cases and functional compatibility.
This complexity also influences the cost for safety assurance in the life cycle. Around 50% of the CCS and TM/CM functionality (including game changers) is safety relevant today and the safe functionality is distributed to several dependent systems with different life cycles, which leads to expensive safety integration work in every change step of an infrastructure or vehicle.

**Simplified, modular architecture to avoid redundancies**
The basic vision of an enhanced architecting and integration process is based on a simplified, and modular architecture that simplifies and decouples the architecting and integration processes including decoupling homologation/authorisation/life cycle processes for trackside systems, trains, and trackside assets. The number of systems and the functional size of the systems is reduced and the functional volume for safety assurance is reduced. All functional redundancies are eliminated, and architecting can

focus on improving single components instead of handling large-architecture complexities and dependencies. Asset owners just chose from existing standard configurations and architectures.

**Improved change process and backwards compatibility**
After the migration from legacy to the target system, the evolution inside of the target system architecture versions will – because of architecture qualities like the reduced dependency structure and higher modularity, layered architecture, and smarter interfaces - allow an improved backwards compatibility, scalable and modular implementations, and a change process with much lower impacts.

**Decoupling of asset life cycle**
Technology and asset life cycles of components are completely decoupled which reduces the overall complexity for the architecting, integration, and asset management processes. Every technology can be designed, managed, procured, installed, and configured in an isolated and independent industrial process for a whole infrastructure or fleet. Integration and system compatibility is just a matter of automated compliance testing which is in some cases only done on run-time.

### 5.4 The vision concerning skill management

One of the todays largest hindering factors is the lack of available skilled resources for architecting, developing, integration and troubleshooting, as well as the high risk of losing the skill availability for older systems in the middle of the system life cycle.

**Reduced amount of skill needs**
The vision concerning skill management is addressing the reduced amount of skill needs by using more standard IT technologies and the creation of isolated specialist areas per smaller CCS and TM/CM architecture zone, that is scoped, interfaced, and specified by a standard architecture. Smarter components and advisory system demand less knowledge from users, maintainers, planers, or integrators.

**Scalability of skills**
Out of this the skill pool, training facilities and advisory systems can scale, and smaller specialization areas allow to enlarge the pool of available skills.

### 5.5 Infrastructure asset management

Traffic Management systems will be more and more cross-company integrated layer/solution with standard IT life cycle management, multi-service-oriented software structures and continuous development, deployment and integration (“DevOps”). Instead of large and company specific installations the market model changes in many areas to “Software as a service” (SaaS) and continuous service contracting. Complexity of system management is shifted from operators to specialized companies which are able to handle the system management.

Traffic CS today is a very expensive system architecture with many ten-thousands of assets per railway. Changing assets or onboard components needs years of planning and manual individual handcrafting, very high skills on the user side and creates high cost, although only a half of the architecture is containing safety relevant functionality.

The basic vision for the Traffic CS asset management processes is based on a system, that can operate every type of radio based ERTMS infrastructure and vehicle configuration mix with the best performance that is currently available with the available sensor and control configuration – even if it changes on run-time asset by asset.

**Reduction of trackside CCS assets**
The amount of trackside CCS assets is reduced by more than 50% (in the long-term just radio antenna, a strongly reduced number of balises and train detection sensors, and controller for points and crossings). Trackside control and safety systems are centralized to reduce maintenance, cost, and to simplify upgrades/updates.

**Simplified process for planning and installing CCS systems**
Safety cases or signalling planning processes for new installations become simple, just - component compliance tests, plug the assets, and operate.

**Selective on demand replacements**
Combined with an integrated and automated toolchain, upgradeable architectures in the trackside cheaper

migration, and selective replacements lead to fast and efficient industrial deployments and low total cost of ownership.

**Optimizing track capacity**
The ability to combine, mix and use all modern sensor technologies (scalability) even on the same line delivers a precise perception of the operational state and exact traffic flow. Combined with precise and dynamic control algorithms the traffic flow is tuned to the physical capacity limit.

**Mixed system versions**
Migration can make use of older system versions or very new versions (trackside and onboard) on the same line because the smart trackside control and safety logic can use on the basis of the currently available information mix and control features the optimal way of interaction and production.

**Independent asset life cycle**
Trackside assets are replaced with completely independent lifecycles and safety cases, which eliminates a dependency for 80% of the asset capital.

**Data acquisition**
Map, topology, and asset information is acquired automatically over multiple channels (running trains, measurement trains, satellite pictures, drones, etc.)

**Reduced special hardware**
The extended vision for Traffic CS asset management is built on the idea of moving more and more to ICT-like system landscapes and asset management principles to reduce TCO, increase availability, and automate/simplify asset management processes. Expensive special safe hardware is replaced by safe software container technologies and virtualisation to reduce the cost for the software life cycle, increase the availability, and simplify upgrades or network wide deployments. Hardware extensions or replacements are simpler because of standard communication busses and a standardisation of software<>hardware interfaces, which also make the use of centralized clouds possible.

**Data center deployment**
Traffic CS is an architecture based on small or big data centres with central management, and decentral independent device life cycles with plug & play features and industrial replacements under production. Software and hardware components of an open market are freely combinable on run-time. Reliable and redundant communication architectures based on freely combinable communication stacks (scalable) are used, to use any type of public or private carrier network or combination, inside of the constraints of interoperability. System construction and maintenance is supported by smart, automated, and learning management systems. Scalable market services for “Software as a Service” (SaaS), or “Traffic control interface as a service” become possible.

Overall, the TCO are reduced by independent life cycle optimisation, the specialisation and scale of asset management services, and by automation.

### 5.6 Asset management for the Train Control and supervision systems

Achieving interoperability for onboard systems today means large efforts in development, verification and authorisation, as well as national or even local specific features, compliance, tests and procedures or product versions are still needed. The CCS onboard is too expensive during its lifecycle for radio based ERTMS. High authorisation and integration cost, too many different requirements sets, and the missing modularity/upgradeability leads to unsound investments and high total cost of ownership.

The change to ICT-like asset management principles is in general the same as for infrastructure asset management. TCO reduction happens because of a fundamental change of the dependency structures, standard architectures and technologies, by the automation of life cycle processes and by the simplification of the architecture.

The basic CONEMP vision for Train CS is based on cheap, modular (interchangeable between suppliers, level of granularity to be defined in the System Pillar design process), upgradeable and precise radio based ERTMS/CM technologies, ATO GoA4/C-DAS, high bandwidth radio, automated joining/splitting (virtual coupling), and continuous high precision localisation.

**Data acquisition**
The CCS onboard delivers all needed information about the train and can control all functions needed for automatic train operations, automated shunting under full supervision, and remote train control for example for stabling trains.

**Remote upgrade**
The extended vision includes a higher maintainability with onboard platforms for different software products, that can be upgraded remotely, to ensure the train behaviour is always “state of the art” and with a high security protection.

**Driver Support Systems**
The onboard ICT provides all needed information for the driver to avoid special training for knowledge about routes or special procedures (e.g., when entering a shunting yard or using a terminal).

## 5.7 Simplified asset configuration management

**Simplified asset configuration management**
To reduce software effort (avoiding translating functionality), configuration effort and to simplify interfaces between CCS and TMS/CM systems the exchanged information about network-wide configurations (like the track topology or addresses of communication services) shall be standardized and the data acquisition and deployment shall follow a centralized approach to avoid redundant data creation or manual data transport. Configuration data shall be openly available for infrastructure and vehicle systems, or partly also for public data services.

## 5.8 Integrated diagnostic systems

**Standard diagnostic features**
To reduce the duration of troubleshooting and recovery processes the CCS and TMS/CM architecture shall introduce standard diagnostic features for every CCS and TMS/CM system which allow a centralized and fast diagnosis of root causes, an automated monitoring of the asset conditions and analytical functions for supporting continuous improvements process to foresee and avoid disturbances.

**Sharing of diagnostic information**
Diagnostic information shall be shared between involved participants in the maintenance and asset life cycle process.

## 5.9 Enhanced security management processes

**Enhanced Security Management**
The implementation of state-of-the-art security management processes is based on an architecture with multiple protections layers, enhanced authentication and authorisation methods, continuous monitoring of attacks or insufficient protection levels, a continuous improvement process and “security by design”.

**Security by Design**
Security by design means to integrate multiple protection mechanisms in every software or hardware function as well as every data item that can be attacked with relevant consequences.

## 5.10 Enhanced safety assurance process

**Enhanced Safety Assurance Process**
The enhancement and simplification of the safety assurance process plays a key role as a catalyst for the evolution and innovation of CCS. It is a big lifecycle cost driver and THE development obstacle today that hinders CCS to make use of all modern technologies “cross-sector”.

**Modular Safety**

- Because of a high architecture quality safe integration of components to a whole safe application is just done by a centralized (online) compliance test (certificate), that is done once (strategy “modular safety”)

**Risk assessment quality**

- The quality of validation/testing and practical risk assessment for components and “system of systems” reaches a quality level, that allows to simplify bureaucratic development processes of today

**Dynamic change of system configurations**

- Independent/redundant/stable safety monitoring systems and actor advisory systems allow a more dynamic change of systems and diversity of configurations and support a continuous improvement process.

Note: The role of ‘safety related activities’ within existing TM/CM systems and the role of these systems in further automation need further consideration. Also, the safety relevant impacts of higher grades of system automation need to be analyzed. This will be considered in the next phases of the System Pillar.