Refining Signalling Technology for Efficient ETCS Level 2 Operation

Efficient use of the European Train Control System (ETCS)

by
Name: Richard Kretzschmar
Institute: German Centre for Rail Transport Research at the Federal Railway Authority
Address: August-Bebel-Straße 10, 01219 Dresden, Germany

1 Advanced Protection System (APS)

1.1 Context

Replacing outdated interlocking technologies is a key challenge for the modernization and further development of railway control and signalling system. In view of the slow rollout of the European Train Control System (ETCS) in Germany, there is an urgent need for action to expedite the digitalization and automation of rail transport. The aim of the research project is to further develop the Advanced Protection System (APS), an innovative railway signalling technology that ensures safe train operations and maximise the potential of ETCS, which even results in a technological change.

Since 2017, efforts have been underway to develop an ETCS interlocking system, which led to the establishment of the Reference CCS Architecture (RCA) initiative. The idea of the Advanced Protection System (APS) was developed as part of this initiative to realise modern architectures for signalling technology for the use of ETCS Level 2 with train integrity and European standards of interfaces and elements within railway signalling systems (EULYNX) [SKO22; TRI24]. The currently incomplete documentation and specification necessitate further development of the system.

1.2 System structure

The APS is a train-orientated signalling technology that is specially designed for the use with ETCS at equipment Level 2 with Train Integrity Monitoring System (TIMS). The aim of APS is to combine the functions of the Interlocking (IXL) with those of the Radio Block Centre (RBC) in a central component and to authorise and monitor all ETCS vehicle movements taking place in the Area of Control. [SCHM19] The interaction of APS and ETCS Level 2 is shown in Figure 1.

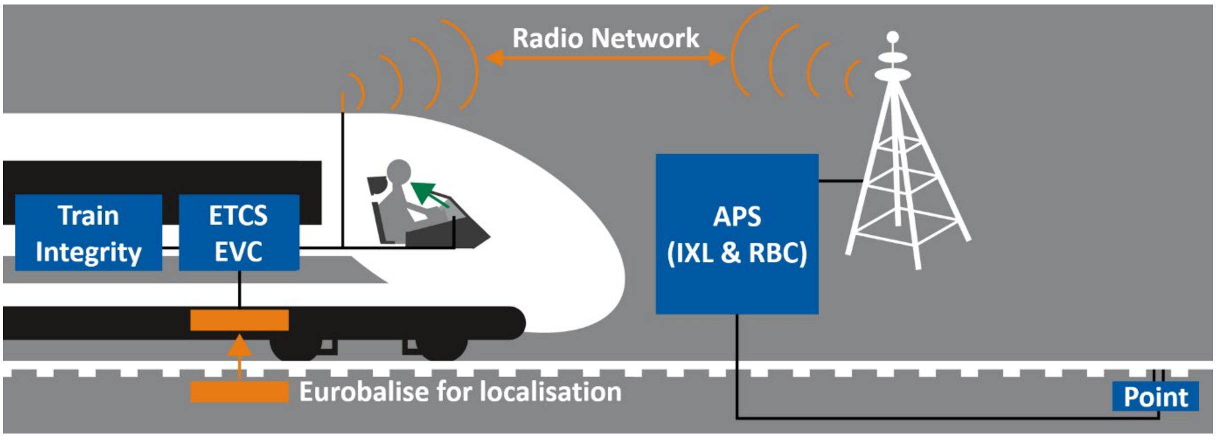

Figure 1: Train operation under APS with ETCS Level 2 and TIMS [TUD25]

Once the route elements have been set and locked, the APS can generate the secured route, the Movement Permission Area (MPA). In the intended regular operation in ETCS Full Supervision (FS) mode, the created MPA is the basis of the Movement Authority (MA), which is transmitted as a radio message via radio network to the ETCS vehicle. In the conventional ETCS Level 2 configuration, the RBC controls and manages the continuous radio connection to the vehicle, ensuring the transmission of all relevant information for vehicle movement. Consequently, the APS also handles the continuous data exchange with the ETCS vehicle.

The vehicle's European Vital Computer (EVC) processes all incoming radio messages from the APS and initiates the corresponding vehicle response. All relevant data for the execution of the vehicle movement under ETCS are shown to the train driver in the driver's cab display, allowing the trackside infrastructure to dispense with fixed signals.

Each ETCS vehicle is equipped with a Train Integrity Monitoring System (TIMS), which monitors whether a train is complete and intact, i.e., whether no wagon or vehicle part has been lost. The Eurobalises are static reference points in the track that have a unique ID and whose data content is read out by the ETCS vehicle when the train passes over them. The ETCS vehicles cyclically communicate information about the last passed Eurobalise and train integrity to the APS, enabling it to locate the vehicles within the track layout and update authorized train movements. As a result, conventional track vacancy detection systems can be dispensed.

1.3 System advantages

The APS offers advantages over the conventional system that make railway operations more efficient and economical. The transition from fixed block operation to moving block procedures increases capacity and ensures optimal utilization of the available infrastructure. At the same time, APS enables greater operational flexibility, as it is no longer necessary to differentiate between train and shunting movements. The APS is aimed at the consistent implementation of the target image ETCS Level 2 with TIMS in order to utilise its advantages. These include, for example, the reduction of trackside infrastructure by eliminating fixed light signals and track vacancy detection systems. [RCA22a; RCA22c]

As a result, time and cost savings can be achieved in the planning, construction, and maintenance of infrastructure. The reduced number of infrastructure elements also contributes to higher reliability of the overall system. In the long term, APS leads to significant cost reductions and sustainably improves the economic efficiency of the railway system. [SCHM19]

Although the APS is still in the concept phase, the RCA documentation already comprises several hundred pages [RCA22e]. The enormous complexity of ETCS, especially in combination with conventional interlocking technology, is one of the major challenges in the ETCS rollout and a significant factor in project delays. This paper takes up the basic ideas of the RCA on the subject of APS and expands on them in certain aspects. The necessary integration into the RCA, in terms of compatibility, is always taken into account. A key objective is to reduce complexity compared to the existing signalling technology and documentation. This is to be achieved through the use of new technologies and the development of innovative solutions, which may also go beyond existing regulations.

2 Methodology

The methodological approach of Model-Based Systems Engineering (MBSE) is used for the functional development of the Advance Protection System (APS). This methodology uses a structured and formalised approach for the development of complex systems. By integrating requirements, functions, architecture and behaviour, MBSE facilitates the design of a well-balanced system solution. Its application starts in the system conceptualization phase and can extend through subsequent engineering and lifecycle stages. [HAR15; SPA22]

In this paper, the application of the MBSE methodology is limited to analysing the system requirements, conceptualising the system functions and presenting the architectural design (see Figure 2). The choice of MBSE is based on its establishment and proven use in system development in the railway sector. The method is used, for example for the development of digital interlockings by the Deutsche Bahn (DB) [MUE21] and in the Reference CCS Architecture (RCA) for the specification of EULYNX and Moving Block [X2R5D10.2]. MBSE remains a key methodological component within the System Pillar of Europe's Rail Joint Undertaking [RIE24], focusing on the integration and harmonization of systems within the European railway network.

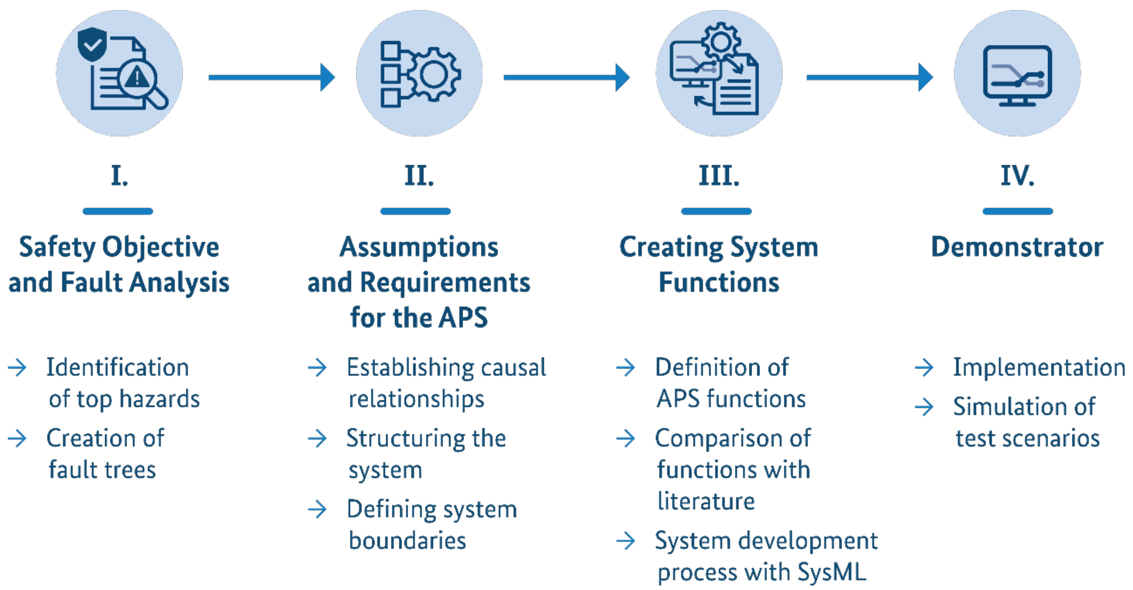

Figure 2: Methodological structure of the paper

The study begins with an analysis and listing of the protection objectives in railway traffic. This is followed by the creation of a qualitative fault analysis. The aim is to identify the main causes of faults and risks in the ETCS Level 2 TIMS target image and present them in a tree structure (see Figure 2 - I).

Based on the fault analysis, a quantitative requirements analysis is carried out, which records the safety-critical requirements for the APS and the necessary assumptions (e. g. for the environmental systems). The requirements (R) and assumptions (A) can be derived directly from the created tree structures, allowing to trace the causal chain (Figure 2 - Ⅱ).

In the next step, the safety-critical requirements are converted into APS functions and the system architecture is structured accordingly. The created functions (F) can be subdivided into further Subfunctions (SF) in terms of modularity and improved readability. To avoid creating the functional description of the system exclusively verbally, a formal and consistent representation is provided using Systems Modelling Language 1.6 (SysML)-Diagrams. The non-commercial, free software Papyrus is used for this purpose, which enables a consistent and clear representation of the target system. Papyrus can be used to model the system structure as well as the functional behaviour and to register and manage the system requirements in a structured manner (Figure 2 - Ⅲ).

This structured modelling forms the basis for the subsequent implementation in a demonstrator. The implementation takes place in the ETCS simulation environment of the German Centre for Rail Transport Research (DZSF). This simulation software offers a complete test environment for ETCS, in which railway tracks with ETCS equipment can be configured, operating scenarios simulated and then evaluated. The aim is to verify the functionality and practicability of the APS concept in this ETCS simulation environment and to prove it through test scenarios (Figure 2 - Ⅳ).

3 Potential hazards in the APS target system

In order to be able to define the protective functions of the APS, the central hazards of the railway system (so-called 'top hazards') has to be analysed and systematically listed. These top hazards are generally known in railway operations but have been restructured as part of this research. The identified top hazards lead to the main potential hazards in the desired ETCS Level 2 TIMS target image and are illustrated in Figure 3. The APS must reliably prevent the occurrence of these hazard potentials, which is why the system functions must be specifically designed to address them.

Figure 3: Top hazards in the railway system

The main potential hazards are dangerous operating situations in the system [CIC24]. A fault analysis is carried out for each of these operating situations in order to determine the underlying causes. This analysis follows a top-down approach. The main causal relationships that lead to the dangerous event are presented in a tree structure [X2R5D10.4; SCHW23].

All safety-related requirements that must be fulfilled independently by the APS are listed as (Requirements - R). However, the analysis shows that the APS cannot independently guarantee safe railway traffic under ETCS on the trackside. There are safety-critical needs that can only be fulfilled in cooperation with other subsystems or entirely by other subsystems and are therefore referred to as (Assumptions - A).

To illustrate the following example, four selected assumptions from a total of 17 general assumptions for a safe APS with ETCS Level 2 TIMS are highlighted. These were chosen to demonstrate their level of abstraction and specificity, as well as two of them are also shown in Figure 4.

(A1) All parts of the railway system are in proper condition and the structural integrity of all components is guaranteed.

(A2) The systems involved are correctly installed, configured and fulfil the required safety level. Data exchange between the involved systems is faultless.

(A7) Every ETCS vehicle movement in the APS area occurs only with properly functioning ETCS onboard equipment and a continuous radio connection to the APS.

(A8) Each ETCS vehicle movement is approved by the APS and only in exceptional cases it occurs under the sole responsibility of the train driver or the Automatic Train Operation.

In this paper, the fault analysis will be presented using the example of a potential flank collision. The analysis is pictured in Figure 4 and relates to regular operation with a granted Movement Authority (MA) in Full Supervision (FS) mode.

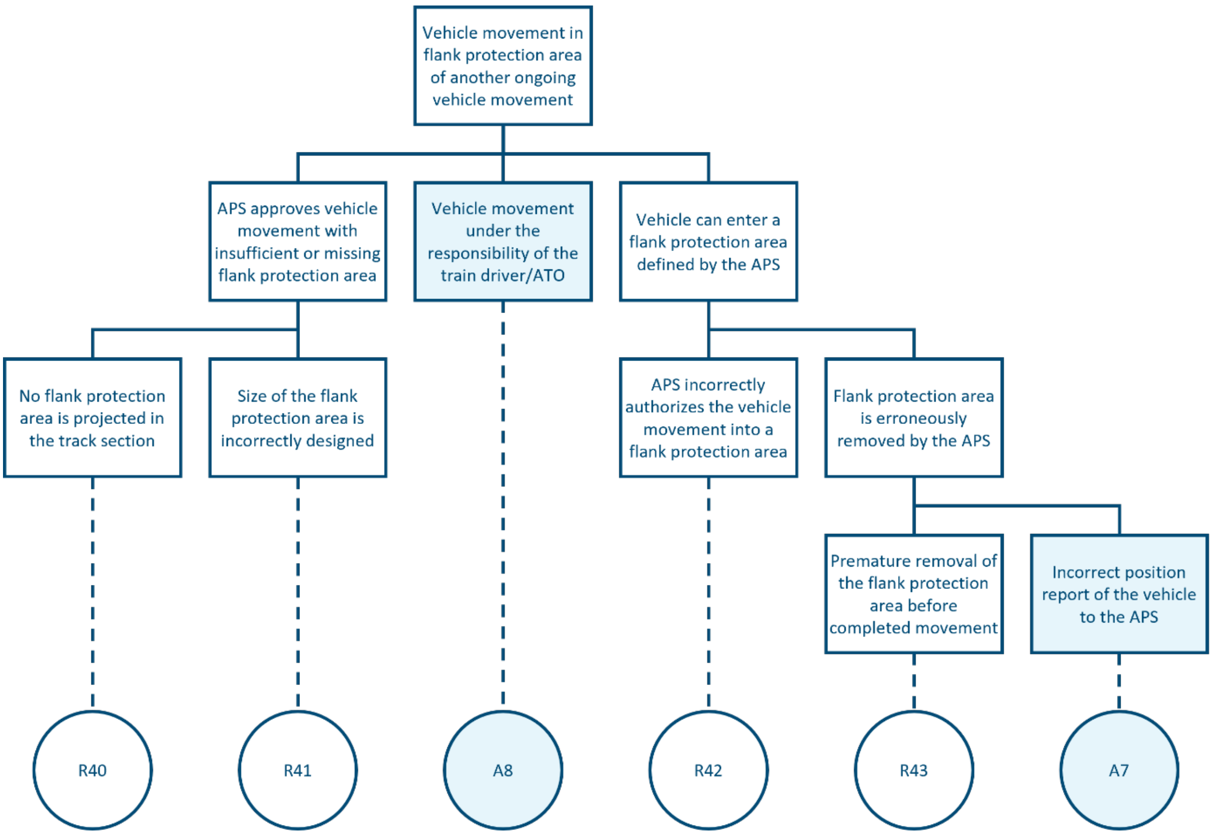

Figure 4: Fault tree structure for potential flank collision

The danger of a flank collision exists where infrastructure elements, such as points or crossings, can cause a vehicle to collide with another vehicle on the side and literally 'drive into the flank' (top level in the fault tree). Three scenarios are conceivable for this (second level in the fault tree). The first possible cause for a flank collision is the absence of a Flank

Protection Area on the non-traversed point branch or its incorrect size. The Flank Protection Area prevents a second vehicle from entering the same point via the second point branch. Two requirements can be derived:

(R40) APS must provide flank protection if there are merging or crossing routes in the requested movement area of the vehicle.

(R41) All flank protection areas must be implemented with the correct length.

In the second scenario, the APS creates a correct Flank Protection Area. In the first error case, the second ETCS vehicle will receive a Movement Authority (MA) in the secured Flank Protection Area of the first vehicle.

(R42) APS must never allow the covering of a movement permission area and a flank protection area.

A second error case would be the incorrect removal of the Flank Protection Area, although the relevant point has not been fully passed.

(R43) APS must never clear the Movement Permission Area behind the ETCS vehicle if it has not been passed by the Max Safe Rear End (MSRE) of the vehicle.

However, the untimely cancellation of the Flank Protection Area could also be triggered by an incorrect position report from the vehicle. This error cannot be prevented by the correct operation of the APS and must be ensured by the correct operation of the vehicle systems (A7).

In the third error scenario, it is considered that the driver or the Automatic Train Operation mistakenly moves the ETCS vehicle without APS-authorisation. A resulting flank collision cannot be ruled out by the APS alone either (A8).

4 System design of a demonstrator

4.1 APS functions

All ETCS vehicle movements under APS are executed and secured on the basis of defined areas. The APS basically distinguishes between four types of areas:

- Available Track Area (ATA)
- Movement Permission Area (MPA)
- Forbidden Track Area (FTA)
- Flank Protection Area (FPA)
- Restricted Track Area (RTA)

The APS can create, convert and resolve the areas based on rules. Using the example of potential flank collision, the necessary APS functions are examined in relation to the creation, management and clearance of an MPA in combination with an FPA. The requirements are the basis for the APS system functions, which has to be defined. The four APS functions (F) are intended to ensure the safe operation of Point 01 in Figure 5.

4.1.1 Authorisation of ETCS vehicle movement over a point

The ETCS vehicle movement under APS begins with the reservation of all necessary and free track sections from the head of the vehicle to the kilometre destination marker. Points along the route are controlled by the APS. Before the vehicle movement can be authorised, the APS checks the current position of the points. If necessary, a process to switch the point position is initiated. During this process, the point is unlocked in its position, moves according to the switching command, reaches the new end position and reports this back to the APS. When all movable track elements are in the requested end position, they are locked against switching. The next step is to define a Movement Permission Area (MPA) and a Flank Protection Area (FPA) for each point along the non-traversed branch, up to the limit marker. The MPA comprises the track area in front of the ETCS vehicle in which the vehicle is authorised to remain, can move safely and is protected against collisions and derailments.

(F400) The flank protection area for a ETCS vehicle movement is part of the respective MPA. (R40)

The MPA always represents the current ETCS vehicle position from Max Safe Front End (MSFE) to Max Safe Rear End (MSRE) as well. This ensures protection when the ETCS vehicle is stationary. (R40) states that the APS must provide flank protection when the vehicle is to move over a point. The APS ensures this by including an FPA for the unused point branch (up to the limit marker) in the MPA for the vehicle movement. The safe prevention of flank collisions is ensured by the fact that another MPA can by definition never cover another FPA. The created function (F400) ensures that the requirement for adequate flank protection (R40) is met.

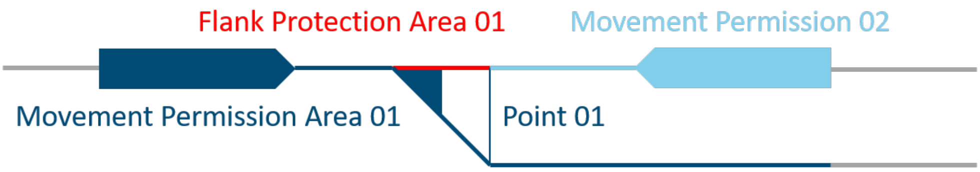

Figure 5: ETCS Vehicle movement is authorised by APS and protected against flank collision

4.1.2 Preventing flank collision

Figure 5 shows that another MPA 02 has been authorised by the APS up to the limit marker of Point 01. The APS is responsible for ensuring that the two vehicles cannot cause a flank collision. The following functions (F) and sub-functions (SF) are intended to ensure the correct implementation and operation of the FPA created in order to meet the requirements (R41) and (R42). The requirement (R41) demands the correct limits of the FPA so that two vehicles can pass each other in the area of a turnout without colliding.

(F410)	The topographical mapping of the track system in the control area enables the correct generation of the Flank Protection Areas.	(R41)
(SF411)	Design and dimensions of points (e. g. distance from the tip of the switch blade to the end of the switch (limit marker), length of the switch blade rail)	
(SF412)	Design and dimensions of crossing (e. g. distance from limit marker to limit marker)	

The requirement (R42) demands that a MPA must never cover an FPA, as otherwise there is an immediate risk of a flank collision.

(F420)	An area is limited by two reference markers, each marking a unique position on a track segment.	(R42)
(SF421)	An MPA and an FPA must not cover each other	
(SF422)	Two FPAs may cover each other	

4.1.3 Removing Movement Permission Area (MPA) behind ETCS vehicle

The APS must be able to remove the MPA of the track section behind the MSRE of the vehicle and allocate it for further operation (F430). The removal of the FPA is directly linked to the removal of the MPA in the area of point and other infrastructure elements. This is achieved by processing a valid position report with a train integrity message from the vehicle to the APS (SF 431), which allows the track section to be used by subsequent movements. Points and other infrastructure elements are released as a whole. The APS must therefore be able to reliably determine the vehicle position behind the point limit marker using the position report and the known vehicle length. Figure 6 shows that the first vehicle has completely passed the limit marker at Point 01 and the position report now sent can be used to release the point (SF 432).

(F430)	The MPA (and FPA if present) behind the MSRE of the ETCS vehicle can be removed with a valid position report	(R43)
(SF431)	Valid position report with train integrity confirmation	
(SF432)	Validation of the safe vehicle position behind the infrastructure element to release the existing area	

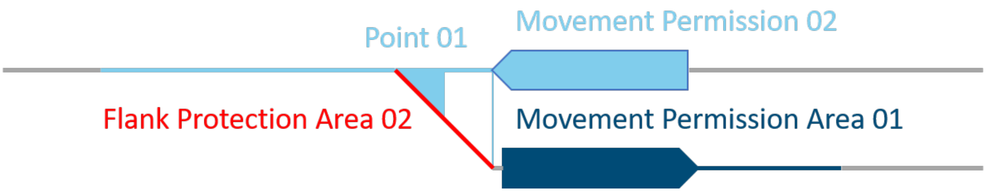

Figure 6: Remove flank protection area and assigne to new MPA

4.1.4 Subdivision of points

The Reference CCS Architecture (RCA) proposes an optimised use of movable track elements to reduce the occupancy time. The point blades (from the tip of the blades to the spring location) is defined as a Drive Protection Section (DPS) and is considered separately from the rest of the point (see Figure 7) [RCA22e; RCA22b]. As soon as the Max Safe Rear End (MSRE) of the ETCS vehicle has safely passed the DPS, the point can be unlocked and switch the end position.

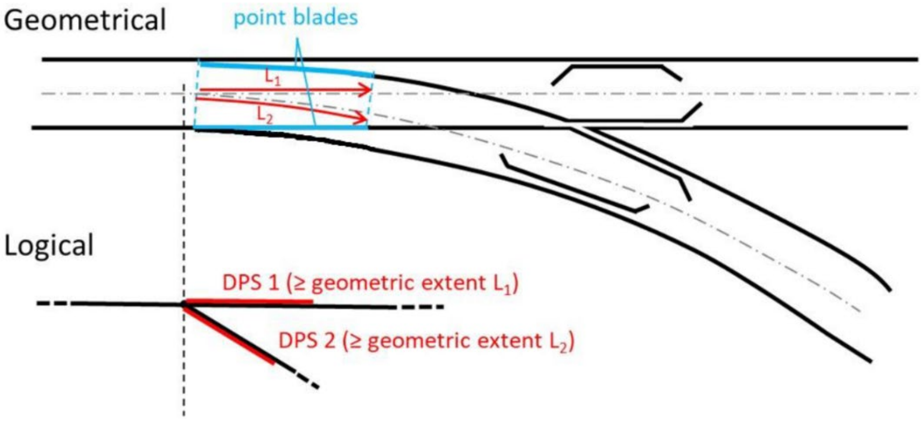

Figure 7: Drive Protection Section (DPS) of a single point [RCA22a]

The Allocation Section (AS) covers the area from the start of the point to the limit marker [RCA22e]. As soon as the MSRE of the ETCS vehicle has passed the Allocation Section (AS), which is pictured in Figure 8, the existing MPA and the existing Flank Protection Area (FPA) behind the ETCS vehicle can be removed and the point can be provided for another ETCS vehicle movement.

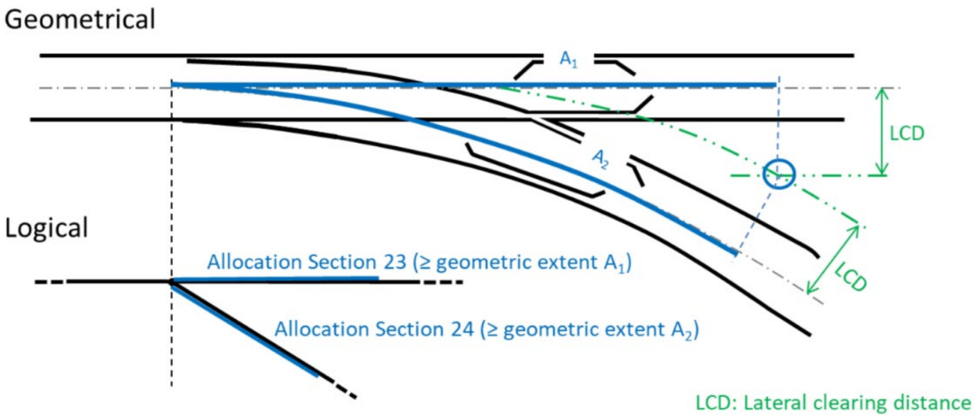

Figure 8: Allocation Section (AS) of a single point [RCA22a]

This technical control of the points in the signalling technology of the APS differs fundamentally from the classic points control in conventional interlocking system. In these, the points remain locked until the (partial) train route is completely removed and can only be changed afterwards. The APS is intended to enable faster departures from train stations, time savings when removing MPAs with several points and capacity gains in highly frequented traffic hubs. However, the basic prerequisite for this is that the APS has precise location data and short processing times. [RCA22a; RCA22b]

4.2 SysML-Diagrams

It is a crucial part of the further development of APS to model the target system consistently and comprehensibly. Following the methodological approach of MBSE presented in section “2 Methodology”, the target system is modelled using SysML 1.6. The example from section “4.1.1 Authorisation of ETCS vehicle movement over a point” and “4.1.2 Preventing flank collision” is used to illustrate the implementation of the necessary functionalities in a coherent “Activity Diagram”. Activity diagrams are particularly suitable for visualising workflows and processes within the system. The diagram describes the created interaction of the involved system components and the required sequence of activities to create the MPA in Figure 9.

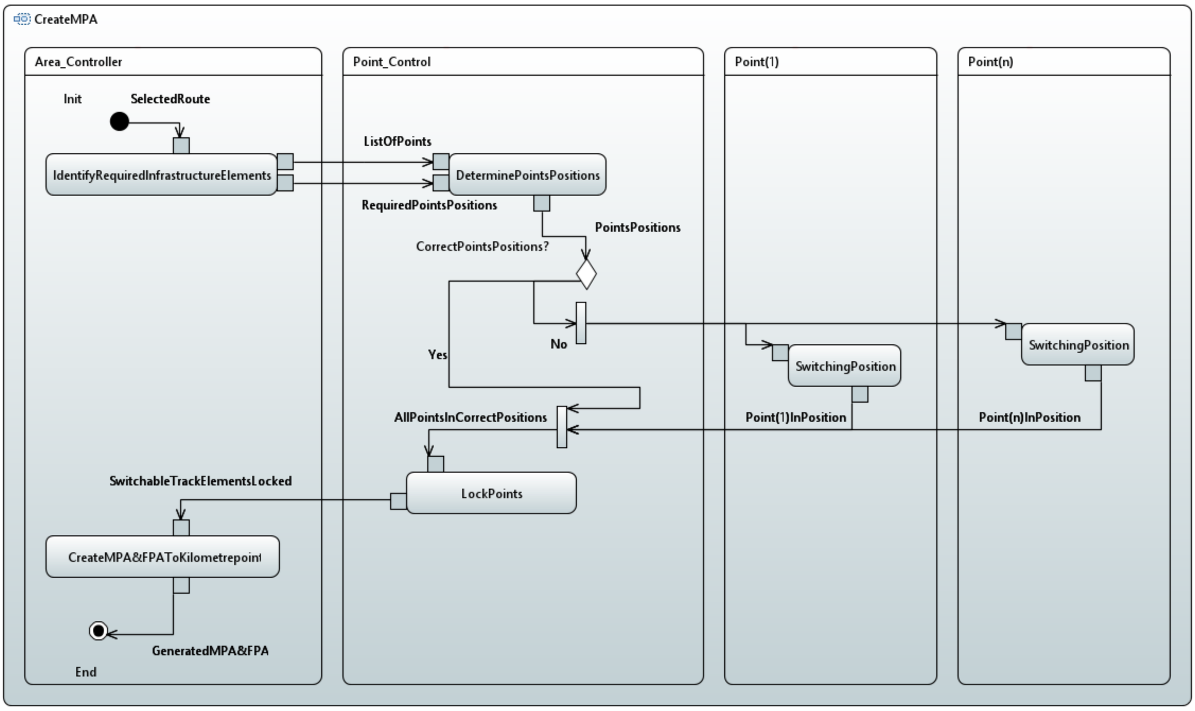

Figure 9: Activity Diagram (SysML 1.6) to create a Movement Permission Area for vehicle movement

The activity diagram describes a superordinate and abstracted level to provide an overview of the process. The actual and more detailed process steps are explained further in separate, subordinate diagrams. The creation of the MPA is triggered by a selected route for the ETCS vehicle movement. The Area Controller (see Figure 9) determines the required infrastructure elements to provide the route. The correct position of all movable track elements is a prerequisite for the successful execution of the vehicle movement. The

Point Control monitors the position of the points and can initiate the switching process if necessary. As soon as all points are in the required end position, they are locked in this position and are secured against switching. The feedback from the Point Control enables the Area Controller to convert the route into an MPA and create the associated FPA. The functions F400, F410, F420 and the associated sub-functions are implemented in the "CreateMPA&FPAToKilometrepoint" function. In the next step, the RBC Communication module converts the created MPA into a Movement Authority (MA) and sent it to the ETCS vehicle so that the vehicle can be started.

5 Conclusion et Perspectives

To implement the APS signalling technology with the presented functions and extensions, it is necessary to develop a suitable module structure. The draft for a coherent architecture is shown in Figure 10. The operator controls the APS with the User Interface, in which the operable track layout is displayed. A routing algorithm is implemented to determine the possible routes according to the operational situation. The safety logic is mainly implemented in the Area Management submodule and ensures safe control and safety during operation. With the help of the Point Control module, it is possible to control, lock and monitor the movable track elements in the Area of Control. Special focus is placed on the integration and compatibility of the APS with the existing system. Data exchange between infrastructure and the ETCS vehicle occurs exclusively via radio messages defined in the SUBSET-026-8 specification. The SUBSETs are the technical specification documents for ETCS that standardize system components or functions. The points are controlled via the specified Standard Communication Interface - Point (SCI-P) of the EULYNX specification.

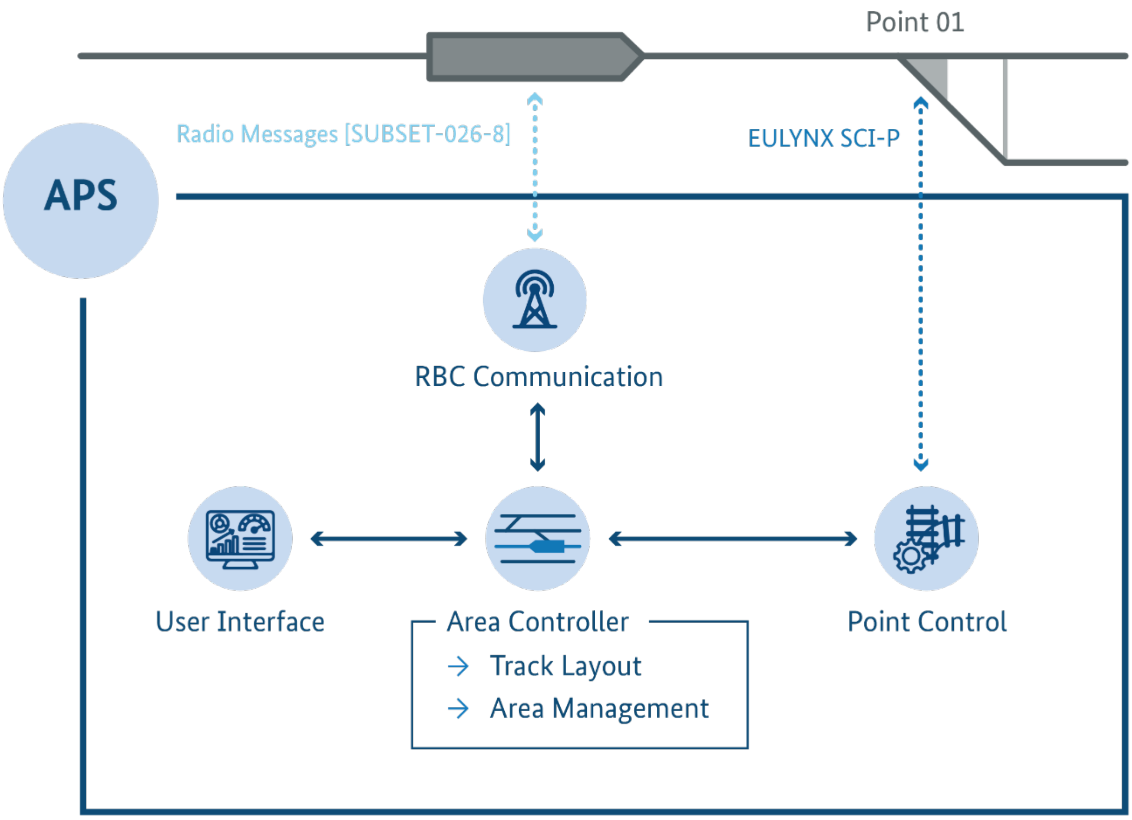

Figure 10: Draft for APS-Architecture

The aim of the research project is to realise an APS demonstrator and verify the functionality of the APS signalling technology. The functionalities will be implemented in the ETCS simulation environment of the German Centre for Rail Traffic Research (DZSF), whereby the functionality is verified by simulating test scenarios. Based on the analyses, the following test scenarios are initially conceivable:

1. Point-to-point movement of a ETCS vehicle on a track segment
2. Vehicle movement over a point
3. Prevent a collision at the end of the track
4. Prevent a head-on collision
5. Prevent a following collision while operating in moving block mode
6. Prevent a flank collision
7. Prevent a touching collision due to insufficient track clearance
8. Restricted vehicle movement by taking into account a Restricted Track Area (RTA)

The main contribution of this research project is the development of a technical concept for conducting regular vehicle movements under ETCS. This concept is formally documented using SysML-Diagrams. The functionality of APS with ETCS Level 2 TIMS should be validated through a demonstrator in the ETCS simulation environment.

References

[CIC24] Cichos, Moritz: Schutzziele für den Eisenbahnbetrieb: Methoden zum Aufstellen von Schutzzielen sowie deren Zweck, Definition und Anwendung. In: *DER EISENBAHNINGENIEUR* (2024).

[HAR15] Hart, Laura (2015): Introduction To Model-Based System Engineering (MBSE) and SysML: Presented at the Delaware Valley INCOSE Chapter Meeting.

[MUE21] Müller, Ralph: Digitale Stellwerke tragen die Digitalisierung der Bahn. In: *Eisenbahn Ingenieur Kompendium* (2021), S. 180–201.

[RCA22a] Kaufmann, Martin; Morman, Bettina; Schiffmann, Frank (2022): APS Concept. Version 1.0.

[RCA22b] Skowron, Frank (2022): APS Detailed concepts overview. Version 1.0.

[RCA22c] Kunde, Marius; Nicolaus, Phillipp; Kaufmann, Martin; Schiffmann, Frank (2022): APS Concept Operating State and APS Domain Objects. Version 1.0.

[RCA22e] Morman, Bettina; Schiffmann, Frank; Schneider, Philipp (2022): APS Concept Movement Permission. Version 1.0.

[RIE24] Ried, Werner: Harmoniously through Europe. In: *Deine Bahn* (2024).

[SCHM19] Schmidt, Steffen: APS – Advanced Protection System, die günstige Einführung von ETCS Level 2/3. In: *SIGNAL+DRAHT* (2019), 22-31.

[SCHW23] Schwencke, Daniel: Modellbasiertes Testen zeitbezogener LST-Anforderungen unter Berücksichtigung der RCA. In: *Eisenbahntechnische Rundschau (ETR)* (2023), 1+2, S. 31–37.

[SKO22] Skowron, Frank; Treydel, Roman: Blöcke waren gestern – Chancen einer zugzentrischen LST. In: *DER EISENBAHNINGENIEUR* (2022), S. 34–37.

[SPA22] Systems, Sparx (2022): Systems Engineering: User Guide Series. Version 16.0, S. 1–79.

[TRI24] Trinckauf, Jochen; Maschek, Ulrich; Kahl, Richard; Baumhacker, Sascha; Braun, Wolfgang; Brune, Lars et al.: ETCS in Deutschland. 2. Auflage, Leverkusen: GRT Global Rail Academy and Media GmbH, 2024.

[TUD25] Kunze, Michael: European Train Control System (ETCS). Vorlesungsskript. TU Dresden, Dresden. Professur für Verkehrssicherungstechnik, 2025.

[X2R5D10.2] Berglehner, Randolf; Rasheeq, Abdul; Auris, Felix; Schwencke, Daniel: X2R5 - Deliverable D10.2: Proposed extension of specification approach to meet needs of RCA. In: *X2Rail-5* (2023), S. 1–68.

[X2R5D10.4] Borälv, Arne; Schwencke, Daniel; Mejia, Fernando: X2Rail-5 Deliverable D10.4: Verification Report. In: *X2Rail-5* (2023), S. 1–41.

Figures

Figure 1: Train operation under APS with ETCS Level 2 and TIMS [TUD25]

Figure 2: Methodological structure of the paper

Figure 3: Top hazards in the railway system

Figure 4: Fault tree structure for potential flank collision

Figure 5: ETCS Vehicle movement is authorised by APS and protected against flank collision

Figure 6: Remove flank protection area and assigne to new MPA

Figure 7: Drive Protection Section (DPS) of a single point [RCA22a]

Figure 8: Allocation Section (AS) of a single point [RCA22a]

Figure 9: Activity Diagram (SysML 1.6) to create a Movement Permission Area for vehicle movement

Figure 10: Draft for APS-Architecture

List of abbreviations

A .... *Assumption*
APS .... *Advanced Protection System*
AS .... *Allocation Section*
ATA .... *Available Track Area*
CCS .... *Control Command and Signalling*
DPS .... *Drive Protection Section*
ETCS .... *European Train Control System*
F .... *Functions*
FPA .... *Flank Protection Area*
FTA .... *Forbidden Track Area*
MA .... *Movement Authority*
MBSE .... *Model-Based Systems Engineering*
MPA .... *Movement Permission Area*
MSFE .... *Max. Safe Front End*
MSRE .... *Max. Safe Rear End*
R .... *Requirements*
RBC .... *Radio Block Centre*
RCA .... *Reference CCS Architecture*
RTA .... *Restricted Track Area*
SF .... *Subfunctions*
SysML .... *Systems Modelling Language*
TIMS .... *Train Integrity Monitoring System*