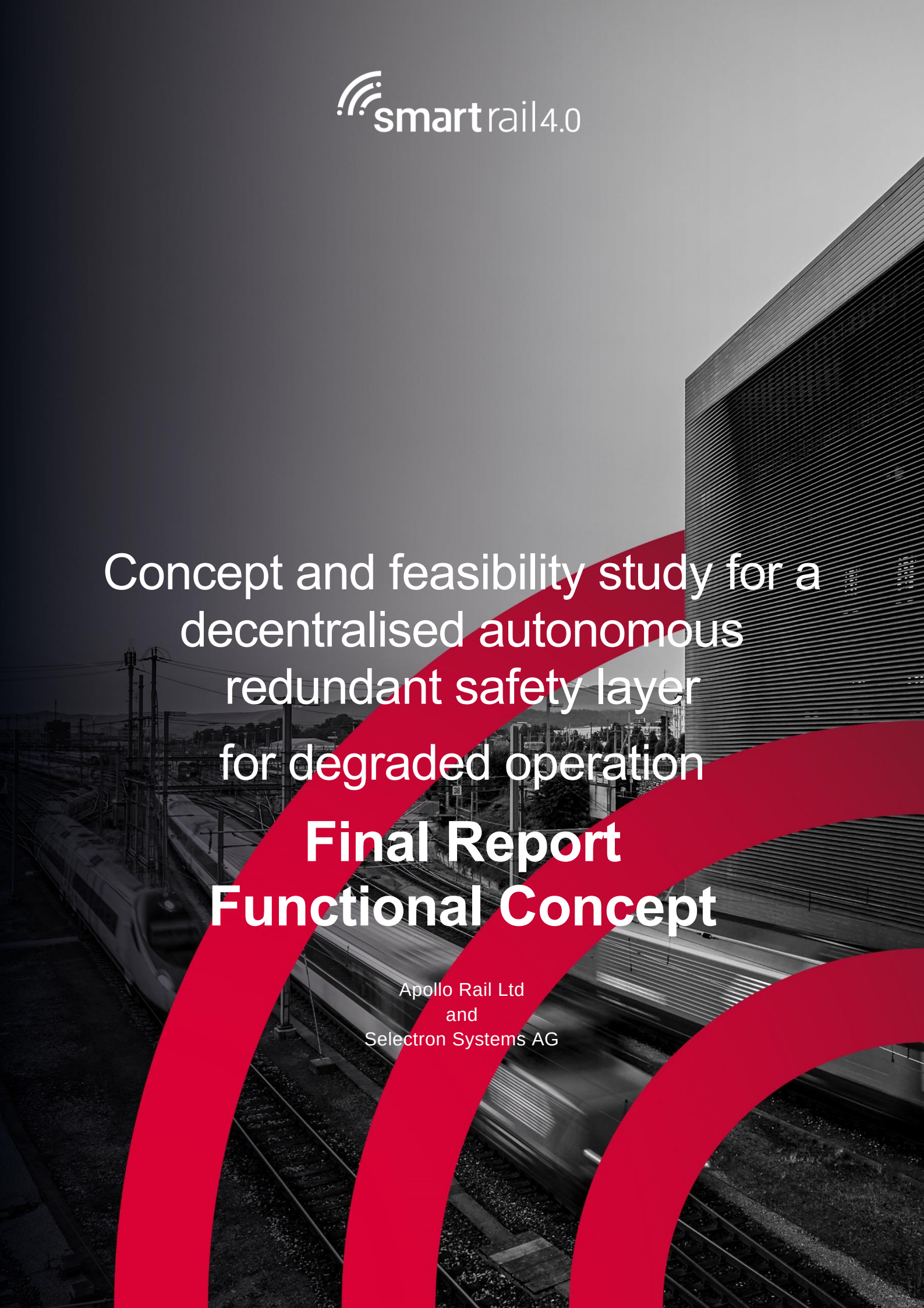


Concept and feasibility study for a decentralised autonomous redundant safety layer for degraded operation

Final Report
Functional Concept

Apollo Rail Ltd
and
Selectron Systems AG

Document Information

Title: Concept and feasibility study for a decentralised autonomous redundant safety layer for degraded operation, Final Report Functional Concept

Status: Issued

Version: 1

Date: 31st October 2019

Owner: Janina Bonjour

Authors: Apollo Rail Ltd: Adam Stead, Xavier Quayzin, Raphael Cavalcanti, Sam Bemment, Nick Barker
Selectron Systems AG: Beat Knuchel

Document History

Version	Date	Lead Author	Approved by	Modification Notes
1.0	31.10.2019	Adam Stead, CEO, Apollo Rail Ltd	Janina Bonjour, Project Manager MTC, SmartRail 4.0	First Issue

Executive Summary

Introduction

Apollo Rail Ltd and Selectron Systems AG have carried out a feasibility study on behalf of the SmartRail 4.0 (SR4.0) programme to consider whether a Redundant Safety Layer (RSL) can be added to the SR4.0 system architecture as a secondary train protection system for use in degraded scenarios.

The feasibility study has been directed to define an Autonomous Movement Supervision (AMS) system that is decentralised and therefore highly resilient to widespread system outages.

The idea for an AMS system is included within the Beta release of ERTMS Reference Control Architecture as an extension of the Vehicle Supervisor.

The study has been completed over 12 weeks through reviews of existing published SR4.0 documentation, interviews with SR4.0 analysts, managers, engineers, and directors, and also required the authors involved to invent novel concepts to create a feasible AMS solution suitable for introduction onto the SBB railway network.

The study has considered:

- **Operational Feasibility:** when a fallback system should be used, how it will be activated, and what improvement it will have on the train service during disruption
- **Technological Feasibility:** whether an AMS system can be conceived that would provide safety for train movements and control of trackside assets.
- **Integration Feasibility:** whether the AMS system can work within the SR4.0 architecture, dependencies on other systems, and modifications necessary to other systems to facilitate the AMS being deployed
- **Development and deployment Feasibility:** whether a system can be developed and trialled in line with the SR4.0 programme
- **Economic Feasibility:** if there is a business case based on estimated costs and benefits of the system. (N.B. available within the Business Case report complementing this study).

Each of these is summarised in the following sections.

The study concluded that AMS offers a practical and resilient alternative to provide a Redundant Safety Layer for ensuring safe movement of trains in degraded scenarios, and can also be used for resuming basic train services during extended outages of several hours or days at a time.

In addition, AMS provides an additional level of assurance for Business Continuity Management during national crisis when evacuation of populations from regions is vitally important.

Having an alternative safety system in place for these failures significantly de-risks the centralisation strategy of SR4.0.

The scalable, lightweight nature of the software-based decentralised AMS system means it can be developed and deployed at relatively low cost on top of existing SR4.0 solutions within the tight constraints of the available direct benefits. The business case analysis shows that the AMS has a positive long-term business case with a positive 2025 NPV for a horizon up to 2052 (15 years after the last commissioning).

The conclusion of this feasibility study is that development of AMS moves forward to the next stage of development through to proof-of-concept and test train fitment, with critical go/no-go gateways at each stage of the development, revalidating the business case, and with tight control of costs and risks to ensure the business case is not undermined by the narrow budget available for the development and through-life operation of AMS.

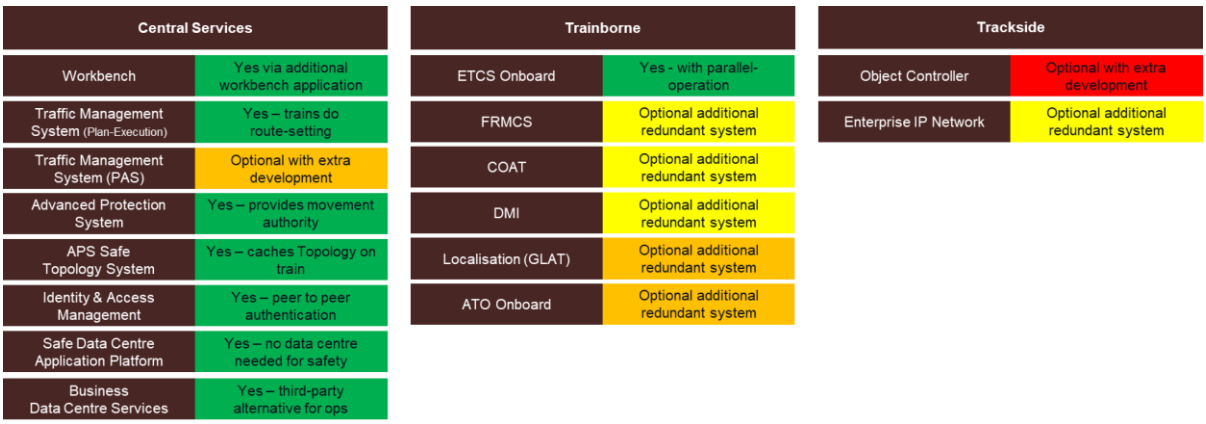
Operational Feasibility of a Redundant Safety Layer

The feasibility study has first considered whether it is necessary to consider a Redundant Safety Layer within the SR4.0 architecture and what failure modes it should address.

The primary function of the Redundant Safety Layer is to provide: **full signalling, control, and route-setting or "steering" (**DE: "*Signalisierung, Steuerung und Fahrstrassenbildung***")** to provide safe transportation of passengers to the nearest station in the event of the primary signalling & control system being unavailable. The Redundant Safety Layer should provide the necessary functionality to resume a basic train service until the primary system is restored.

The SR4.0 system design already features high levels of availability with resilience-by-design and redundancy in most systems with diverse technologies available. The resilience of these systems negates the need for an RSL to replicate their functionality and instead RSL can depend on those subsystems being available. Figure 1 identifies the subsystem failures that will be primarily addressed by RSL in Green. The primary benefit of providing an RSL is for failure with Central Services where the impact affects multiple trains.

FIGURE 1 SUBSYSTEM FAILURES MITIGATED BY RSL



Whilst Trackside Object Controller Failures and Trainborne Failures are expected to fail much more frequently, their failures can be mitigated through operating rules, there is no safety risk necessitating an RSL.

However, for operational resilience it is possible that an RSL could be introduced that also provides a fallback for trainborne system failures and trackside object controller failures through providing a parallel suite of hardware and software on train and trackside to mitigate failures with these elements.

Items depicted in Yellow, Orange and Red within Figure 1 represent objects that could optionally be replicated within the Redundant Safety Layer as a “lite” version for enhanced resilience of the system; Yellow being the least complex/expensive to replicate and red being the most complex/expensive.

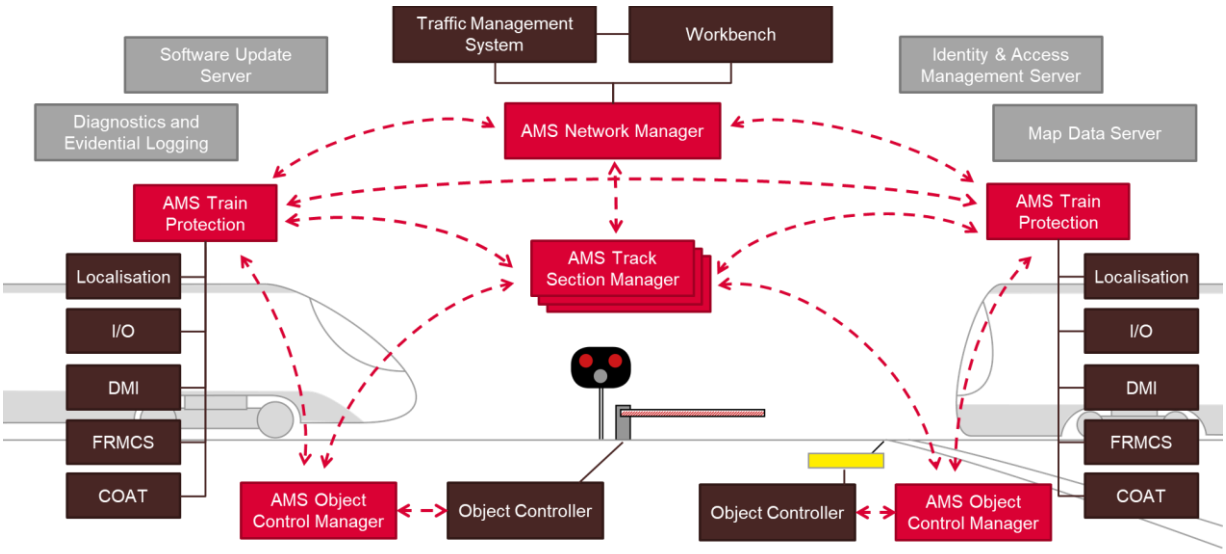
The study has concluded that an RSL is operationally feasible and will provide a reduction in disruption from primary system failures.

Technical feasibility of an Autonomous Movement Supervision system

An Autonomous Movement Supervision (AMS) system has been devised with a highly resilient architecture that enables continuous train protection when central systems have failed within the SR4.0 architecture.

The system uses peer-to-peer communication between trains so that each train understands the state of the railway around itself and can generate its own movement authority. Its general system architecture is shown in Figure 2.

FIGURE 2 AUTONOMOUS MOVEMENT SUPERVISION SYSTEM GENERAL SYSTEM ARCHITECTURE

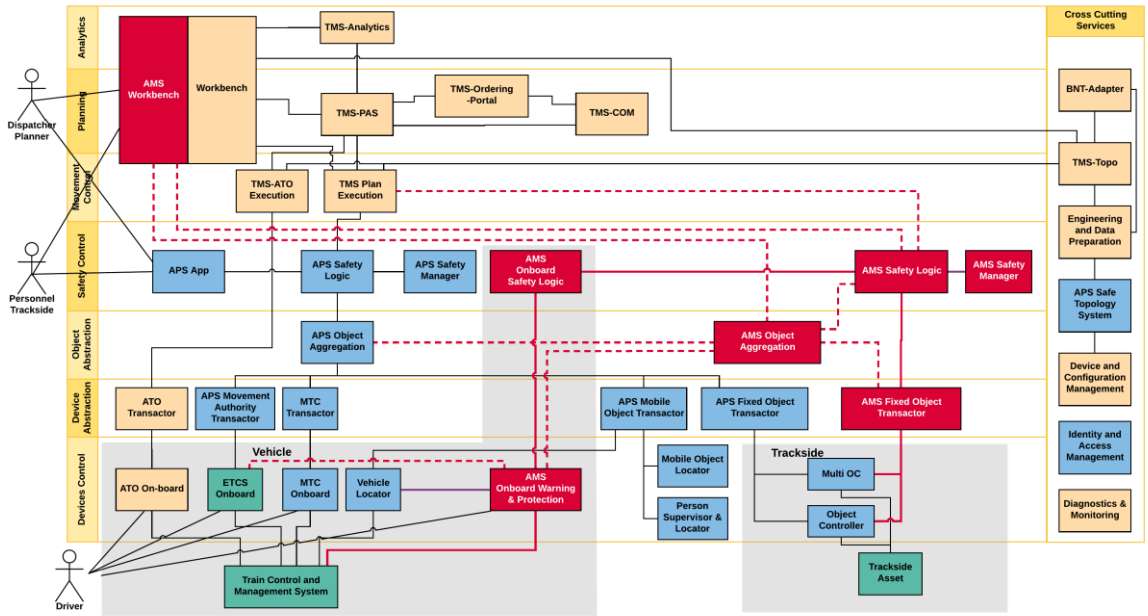


The feasibility study has concluded that an Autonomous Movement Supervision system can be developed and introduced to provide safe protection of trains in degraded scenarios, operating initially at on-sight speeds 40km/h and then up to a safe maximum speed (beyond line of sight) as determined by a detailed safety assessment. An Autonomous Movement Supervision system will fully satisfy the needs of a Redundant Safety Layer.

Integration feasibility with SR4.0 architecture

A high-level logical architecture is provided in Figure 3 that demonstrates the integration of AMS interfacing with SR4.0 subsystem on the train, central services, and object controllers.

FIGURE 3 - SR4.0 ARCHITECTURE WITH AMS SUBSYSTEMS & INTERFACES INCORPORATED



Using an Autonomous Movement Supervision system as a Redundant Safety Layer enables its implementation as software-only, integrated into existing hardware platforms with safety integrity.

The trainborne AMS Train Protection System will be deployed as software onto the COAT platform utilising other trainborne SR4.0 systems that have high-resilience and degraded operating capabilities.

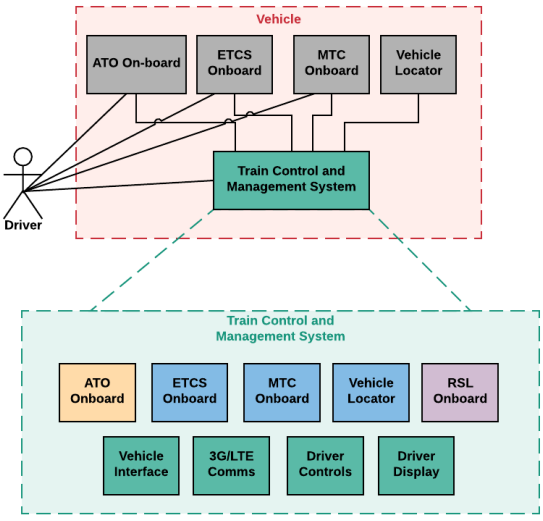
For trackside AMS services: the AMS Track Section Manager and AMS Object Control Manager services, the ideal decentralised architecture for maximum resilience would be to host the services within the Object Controller itself. However, the current strategy of SR4.0 (and the ERTMS Users Group, Reference Control Architecture – beta version) is to have no platform independence for Hardware and Software on the Object Controller and to use a tightly defined EULYNX protocol (RCA Interface 11) for communicating with the Object Controller – the Object Controller itself is envisaged to become embedded into the trackside asset providing direct electrical and mechanical control to the device.

As a result of this significant architectural constraint, AMS must retain some centralised services operating in the cloud, or a private data centre, to provide safe movement protection for trains. The feasibility study does not recommend deviating from this strategy.

The SR4.0 RAM team estimates that over 50% of all delay minutes and disruptions might be caused by trainborne subsystem failures on which the Redundant Safety Layer depends, such as COAT, Localisation, FRMCS, DMI, etc.

To provide additional resilience for these, a “lite” version of these components could be replicated within RSL at a lower safety integrity level, however this could significantly increase the cost of RSL and undermine its business case.

FIGURE 4 - FULLY ENABLED AMS RUNNING ON TCMS



An alternative approach could be to utilise similar subsystems which are present within a modern TCMS platform such as localisation, communications, driver interface, etc., combined with application virtualisation to allow RSL to operate as software deployed on the TCMS. Indeed, this might even be an option for the primary safety layer, e.g. ETCS onboard, to operate in a degraded mode.

Each SR4.0 subsystem has been reviewed as part of the feasibility study where AMS has dependencies. Additional functionality has been identified for most systems to facilitate handover to AMS and hand back to APS – in most cases this is minor (e.g. data feeds), and integration is considered feasible.

The integration of Object Controller to RSL is not fully understood. Two options are available for integration – the preferred option is to update the Object Controller interface protocol (EULYNX) to require Object Controllers to communicate with a Redundant Safety Layer as a backup system when it

detects its link to APS has failed. If it is not possible to introduce this functionality to the Object Controller then a Load Balancer (i.e. an automatic “Y-switch”) will be required to sit between the APS and Object Controller to fail over to AMS. This architectural constraint needs to be resolved also for the Object Controller to switch over to the backup APS - all other APS interfacing systems have a similar constraint and it is understood to be an open point within SR4.0.

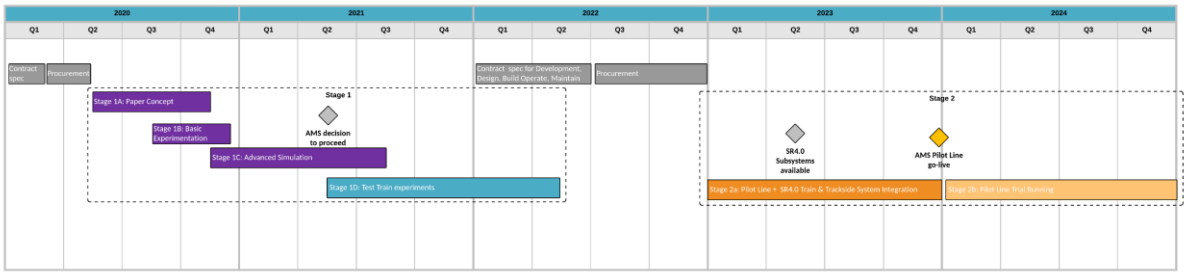
Development and Deployment Feasibility

The feasibility study has analysed the development effort required to realise the AMS system and integrate it into the SR4.0 wider systems, and then roll out across the whole SBB railway network.

AMS requires a phase of proving its concepts as a train control system which should be done as early as possible to validate the concepts before making strategic decisions to commit to deploy as a core component of SR4.0.

A two-year Development programme is proposed that develops a paper concept, a basic software proof-of-concept, then an advanced simulation for a whole region, and then installs onto a test train and test track to prove in cab with user feedback. This is envisaged to conclude in mid-2022, with an initial decision to proceed in mid-2021 once results from the region-wide simulation are available.

FIGURE 5 - AMS DEVELOPMENT ROADMAP



A further two-year development programme is envisaged to trial AMS on a pilot line, expected to be a branch line requiring interface with 6 trains and 20 track switches and/or level crossings. The pilot line is expected to utilise SR4.0 subsystems such as Localisation, COAT, and FRMCS as they become available however if these will not be available until later the planned start date for Stage 2 could be delayed without cost implications for suppliers – substitute technology might be available to allow progress to continue anyway. This phase will run throughout 2023 and 2024 with the first year for robust design and assurance, and the second for trial running on the pilot line to understand how the system works in operation.

Roll-out across the SBB network is envisaged with the first commissioning in 2027 through to 2037 concluding that it is feasible to develop a novel AMS system to integrate with the overall SR4.0 deployment programme.

Contractually, this feasibility study argues that the best model is to award:

- Concept and Pilot line to one solution provider which will develop, demonstrate, and standardise an AMS solution which will be type approved.
- Open competition for the regional deployment and as a result have multiple deployment suppliers implementing the standard solution trackside. For the on-board, the preferred solution is to include the integration of the on-board AMS software in the CCS on-board contract.

Benefits

The major benefit of an AMS-based RSL is the provision of an additional layer of resilience that mitigates or eliminates system-debilitating failures. This ensures that the railway can maintain a higher level of performance & safety in degraded scenarios and that emergency evacuations are speedy in catastrophic scenarios. Even taking into consideration that not all failures will be mitigated, and operational limitations might further limit this mitigation, the net benefit/cost avoidance of an AMS-based RSL is positive.

As a direct consequence of failure mitigation, the overall railway network will have higher levels of safety, reliability and availability, ultimately providing a better service to passengers and freight operators alike.

There are also a multitude of intangible benefits that arise from the presence of an AMS-based RLS. These could be the increased public confidence in the railway, the mitigation of other systems' failures, and the possibility of being deployed as a primary CCS system if there would be a catastrophic primary system failure. These benefits are more difficult to quantify and would only be realised in very rare situations but it is safe to say that equipping a modern railway with an AMS-based RSL is beneficial to all stakeholders.

The RSL can therefore increase the confidence in the ability of the railway to ensure compliance to the legal requirement on evacuation in case of nuclear accident by providing a resilient and independent system to run trains in the evacuation zone.

Risks

As with any solution at a low Technology Readiness Level (TRL), the risk profile is relatively high as there is a lot of development work to complete and many unknowns to work out. However, none of them seems insurmountable if the RSL supplier and the SR4.0 work collaboratively and openly. This is the behaviour that was observed during this feasibility and all issues and unknowns can be resolved efficiently.

Table of Contents

Glossary

Term	Abbrev.	Description
Advanced Protection System	APS	Group of components in the RCA interface architecture, aggregates approximately the function of today's interlockings.
Autonomous Movement Supervision	AMS	Decentralised train control and protection system proposed to provide a redundant safety layer.
CCS onboard application platform for trackside related functions	COAT	Shared computing platform for trainborne applications of mixed SIL levels to be deployed in parallel.
Command, Control & Signalling	CCS	The systems, which are ensuring the safe operation of the railways as e.g. the train control system or the interlocking.
Commercial Off-The-Shelf	COTS	Solutions that are non-specific to SR4.0 or rail that can be readily acquired without development.
Device & Configuration Management	DCM	Providing management of software configuration and application data across all SR4.0 systems.
Driver Machine Interface	DMI	The interface to enable direct communication between the on-board equipment and the driver
European Vital Computer	EVC	The European Vital Computer is the heart of local computing capabilities in the driving vehicle. It is connected with external data communication, internal controls to speed regulation of the loco, location sensors and all cab devices of the driver.
Fixed Object Transactor	FOT	RSL element that allows communication between object controllers (fixed assets) and other RSL sub-systems
Future Railway Mobile Communication System	FRMCS	FRMCS has the objective to become the worldwide standard, conforming to European regulation as well as responding to the needs and obligations of rail organisations outside of Europe. As such, the UIC FRMCS project duly associates non-European members and is a first concrete application of UIC strategy to build a Global Rail Traffic Management System for the whole rail industry.
Global Navigation Satellite System	GNSS	Global Navigation Satellite System refers to a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers. The receivers then use this data to determine location.
Global system for mobile communication - Railway	GSM-R	GSM-R is an international wireless communications standard for railway communication and applications.

Term	Abbrev.	Description
Grade of Automation	GoA	Levels 0 to 4 defined by UITP – key levels are GoA2 with a driver but only for emergencies and door operation, GoA3 for driverless operation but still with an attendant for emergencies, and GoA4 for no on-train staff.
Identity and Access Management	IAM	AM is, in computer security, the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons".
Level Crossing	LX	A level crossing is an intersection where a railway line crosses a road or path at the same level
Manoeuvre Train Control	MTC	SR4.0 signalling & control system for network areas deprived of ETCS and designed for special manoeuvres such as shunting, joining, splitting, etc.
Network Manager	NM	An AMS subsystem for coordinating network-wide factors such as Usage Restriction Areas and providing an AMS Workbench to the dispatcher.
Object Control Manager	OCM	An AMS subsystem for enabling trains to interface with Object Controllers, providing safety verification and movement permission to trains.
Object Controller	OC	Device Control component in the RCA interface architecture. The different OC component types and their interfaces are defined in EULYNX to enable interlockings do communicate with trackside assets such as level crossings and track switches.
Peer-to-Peer	P2P	Communication method where individual systems/objects exchange information directly with each other w/o the need of a mediating central server e.g. device to device, train to OC, train to train, TMS to OC, etc.
Rail Safe Transport Application	RaSTA	It is a network protocol especially designed to meet the requirements of railway applications, but that can be also used in other areas with similar requirements.
Redundant Safety Layer	RSL	Fallback signalling, command, control & communication system compatible with SR4.0 for degraded operation.
Reference Control Architecture	RCA	RCA is an initiative by the members of EUG and EULYNX to define a harmonized architecture for the future railway CCS, with the main goal to substantially increase the performance/TCO ratio of CCS in comparison with today’s implementations.

Term	Abbrev.	Description
Reliability, Availability, Maintainability (and Safety)	RAM(S)	RAMS constitutes the key element of the assessment in the rail industry today. For rail system operator, RAMS means a safe, reliable, high-quality service and lower operating and maintenance costs. For the rail system provider, RAMS is representing a high-quality system and product.
Research and Development	R&D	Research and Development refers to the work a business conducts for the innovation, introduction and improvement of its products and procedures. It is a series of investigative activities to improve existing products and procedures or to lead to the development of new products and procedures.
Safety Integrity Level x	SIL x	Safety Integrity Level is defined as a relative level of risk reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a safety instrumented function. (x = 1, 2, 3, 4)
SmartRail 4.0	SR4.0	Digital transformation programme to improve affordability and performance of train control and safety systems.
Technical Specification for Interoperability	TSI	The Technical Specification for Interoperability are specifications drafted by the European Railway Agency and adopted in a Decision by the European Commission, to ensure the interoperability of the trans-European rail system.
Technology Readiness Level	TRL	A measure of assessing the maturity of a novel technology being developed and tested.
Track Section Manager	TSM	An AMS subsystem that governs a length of track between two points / buffer stops (an edge on the topology) to ensure that trains can discover each other on the network.
Traffic Management System	TMS	Traffic Management Systems provide permanent control across the network, automatically sets routes for trains and logs train movements as well as detects and solves potential conflicts.
Train Protection System	TPS	An AMS trainborne subsystem for wayfinding, route-setting, generating a movement authority and applying the emergency brakes on the train.
Usage Restriction Area	URA	A hazard on the railway through which trains should not be operated, or be operated only at a reduced speed.

1 Introduction

1.1 Objectives of this feasibility study

SmartRail 4.0 (SR4.0) is harnessing digitalisation and the potential of new technologies to increase capacity and safety, making more efficient use of railway infrastructure, saving costs, and maintaining the railway's competitiveness in the longer term.

One of the core ways that SR4.0 will achieve these objectives is through the elimination of traditional infrastructure-based signalling systems, instead relying on trains to report their position via the European Train Control System (ETCS) protocol to centralised Advanced Protection Systems which generate movement authorities for trains and control trackside assets such as Switches and Level Crossings. The SR4.0 strategy aligns with the Reference Control Architecture (RCA) work being undertaken by the ERTMS Users Group – currently in Beta release version.[1]

Traditional infrastructure-based signalling systems are quite resilient to failures, where the failure of one track-circuit for train detection, or failure of a signal aspect, or even interlocking failure impacts only the area where that failure has occurred. With traditional systems, services on the rest of the network can continue unabated with degraded operation only being required in the vicinity of the affected asset.

With a centralised data-driven signalling system there is a much greater impact of failures which could now affect an entire region or the whole network through a single outage.

Whilst SR4.0 systems are being designed for very-high availability and low-likelihood of failure, there will still be risks of systematic failures through issues such as software bugs, incorrect configuration, cyber-attacks, black-outs, and other failures that are difficult to predict.

Normally system failures can be mitigated through providing additional redundant backup systems ready to take over in such scenarios, sometimes programmed and designed completely independently to eliminate the risk of common-mode failures, but the economic cost of providing additional redundancy of the primary system might outweigh its benefits given that it is likely to be used in such rare scenarios.

The aim of this feasibility study was to explore whether it is cost-effective and technologically feasible to provide a redundant safety system to provide a robust secondary method to keep passenger and freight trains moving safely in situations where standard signalling is not fully functional, that will be fully compatible with the SR4.0 and RCA architecture (up to GoA2 but with cognisance also for future GoA4 operation.)

[1] https://eulynx.eu/index.php/documents2/rca/rca-beta

The study provides a holistic view of the advantages, disadvantages as well as potential costs and economic benefits of providing a Redundant Safety Layer, while also highlighting opportunities & risks of the technology when compared to current and proposed future alternative solutions.

1.2 Methodology of the study

The feasibility study has drawn on published materials from the SR4.0 programme available on the SR4.0 website (www.smartrail40.ch), the Reference CCS Architecture (RCA) Alpha and Beta publications available on the ERTMS Users Group website (www.ertms.be) and other publicly available information about the SBB railway network.

Additionally, the authors have interviewed leaders across the SR4.0 programme to clarify the feasibility of the ideas contained within this study to confirm that what is proposed aligns with the direction of the wider SR4.0 programme.

In Section 2, the problem space for a Redundant Safety Layer (RSL) is explored considering what its key features should be, when it needs to be activated, what failure modes it addresses and how it will be used to resume safe movement of trains.

Section 3 introduces the concept for an AMS system that can provide the functionality required to satisfy the purpose of providing a Redundant Safety Layer.

In Section 4, the integration of the AMS system with the SR4.0 architecture is described.

Section 5 considers the activities required and commercial methods for procuring, developing and supporting the AMS system.

Section 6 concludes and provides recommendations and next steps for developing AMS further.

1.3 About the authors

The feasibility study has been developed in collaboration between Apollo Rail Ltd (“Apollo”) and Selectron Systems AG (“Selectron”) under the supervision of Janina Bonjour within the SR4.0 programme.

Selectron is a Swiss company based in Lyss and a member of the Knorr-Bremse Group with over 60 years of experience in electronics and programming – as well as over 30 years' activity in the rail-vehicle sector.

Selectron have a wealth of experience in system solutions for automation in rail vehicles (TCMS) and specialise in control, network, and communication technology. Their products (systems, components, and applications) are built to be in accordance with the highest Safety Integrity Level (SIL) safety standards.

Apollo are a UK-based start-up company who formed in 2017 with an innovative concept for train signalling & protection with a decentralised train-based architecture whereby trains autonomously generate their own movement authorities without any centralised supervision.

Apollo were selected to undertake this feasibility study as their architectural approach provided an attractive method of solving the SR4.0 challenge of providing a Redundant Safety Layer.

Whilst Apollo's existing intellectual property and know-how has formed the inspiration and basis for this work, the further development of this solution is not constrained to using Apollo's technology and Apollo maintains no intellectual property constraints on the exploitation of these concepts by any third-party.

1.4 Swiss Railway Network context

The feasibility study is prepared in the context of the SBB national railway network for which the following key characteristics have been identified to frame the study:

- **High-density network** with the highest number of trains per km per day in Europe.
- **Mixed-traffic network** consisting of multi-modal freight, high-speed, commuter, rural and mountain railways.
- **Complex network** with very long tunnels, cog railways, spiral loops, and more miles of railway per square km than any other country in Europe.
- **Punctual** providing a reliable service consistently with 90% of trains arriving within 3 minutes of their scheduled arrival time.
- **International** with cross-border services from France, Germany, Italy, Austria and beyond.
- **Dependable** providing a vital public service that can be relied upon by passengers and freight users and which underpins the economy and transport network of Switzerland.

The feasibility study will be cognisant of these key features whilst defining a solution to provide a Redundant Safety Layer.

2 Redundant Safety Layer Needs Analysis

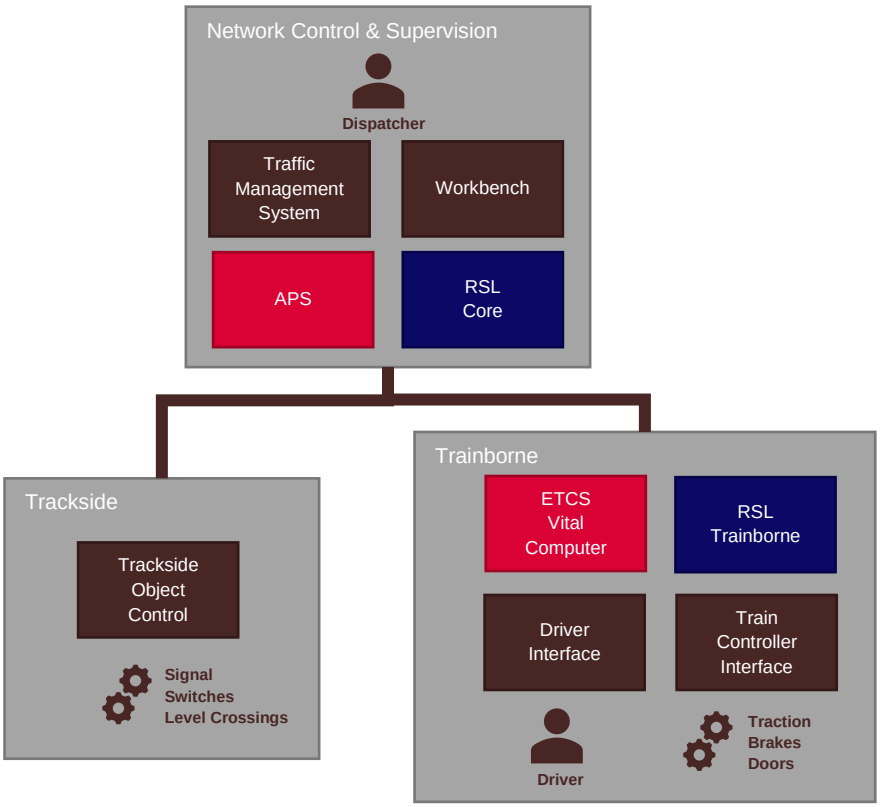
Operational Feasibility of a Redundant Safety Layer

The Redundant Safety Layer (RSL) is to provide an alternative method of protecting train movements, suitable for use on the SBB railway network in conjunction with SR4.0 primary command, control and signalling systems.

This section of the study considers when an RSL would need to be used and how it should be used.

Figure 6 Illustrates at a high level how an RSL is expected to sit alongside the primary safety layer (the Advanced Protection System and ETCS European Vital Computer onboard trains).

FIGURE 6 - RSL ALONGSIDE THE PRIMARY SAFETY ARCHITECTURE



2.1 Key features of a Redundant Safety Layer

The primary function of the Redundant Safety Layer is to provide: **full signalling, control, and route-setting or "steering" (**DE: "*Signalisierung, Steuerung und Fahrstrassenbildung*"**)** to fully substitute primary signalling & control systems.

Based on discussions with SR4.0 project leaders and system architects, it was determined that the primary objectives of RSL should be to ensure safe transportation of passengers to the nearest safe

point of exit from the railway in the event of the primary signalling & control system being unavailable for any reason.

In degraded operation, capacity and journey-time have been specifically excluded as objectives for the system and so use of drivers to verify the state of the network is permissible with the speed limited to 40km/h for on-sight movements.

These requirements encompass failure modes that involve a multitude of SR4.0 primary systems ranging from central services, trainborne signalling & trackside equipment, communications, power and data centres.

In support of these primary goals the Redundant Safety Layer must also provide the following key functionality that exists with the primary CCS system to enable the railway to be managed effectively:

- **Network state monitoring** – accurately report the current state of all objects on the network (or region), their position and other necessary variables to enable efficient operation and supervision of train movements.
- **Alternative planning & timetabling** – grant dispatchers the possibility to alter timetables, manage Usage Restriction Areas & transmit manual train movement instructions.

Additionally, four key characteristics that the RSL solution should achieve to be effective:

- **Adaptable** – a software-based system to allow for flexible and inexpensive adaptation to the SR4.0 architecture as it evolves.
- **Affordable** – the system should complement existing investments in train control such that the redundant layer is a marginal increase in cost.
- **Autonomous** – the system should operate with minimum human involvement as in a future automated network there may be insufficient personnel in control centres to provide manual movement instructions to all trains within a region.
- **Available** – the system should not be vulnerable to the same failures modes as the primary safety layer and support degraded operation even in the most severe system-wide failures.

2.2 Failure scenarios and RSL coverage

Most of the subsystems within SR4.0 are proposed with levels of resilience and redundancy and there are very few common modes of failure that would cause a widespread outage by design – however there remains a likelihood of unexpected systemic failures such as misconfiguration, data corruption, or cyber-attack, which could have system-wide impact making whole areas, regions or the whole network unusable.

For RSL to provide additional levels of resilience to the overall network, it must not be subjected to the same failure modes as the primary SR4.0 components. A fallback system should therefore rely on alternative systems, hardware, software and cloud storage capabilities that are distinct or disconnected from their analogous SR4.0 primary systems.

However, across SR4.0, systems are being designed with diversity and redundancy from the outset and can continue to provide a degraded functionality for the primary safety systems.

For instance, the Localisation solution could be implemented as a combination of technologies such as GPS, Eurobalise reader, Tachometer, Doppler Radar, etc., and continue to provide a degraded level of functionality even with a failure of one of the components. With such diversity, the Redundant Safety Layer needn't be activated because the primary system can still be operated in a degraded mode.

RSL should try to make use of the existing designed-in resilience and redundancy in SR4.0 systems to provide functionality required for the Redundant Safety Layer even in a degraded scenario.

Alternatively, RSL could be developed as a fully independent system whereby it is self-contained so that it could provide full supervision in any combination of multiple simultaneous total failures/unavailability of the primary system components. For instance, the train-borne Redundant Safety Layer could include its own Localisation using a duplicate GPS sensor and Inertial Measurement System.

If a "lite" platform is developed for backup operation for RSL, then it might also be possible to utilise this to provide additional redundancy to the primary safety layer in the first instance before activating the Redundant Safety Layer, i.e. making the backup localisation system including GPS and Inertial Measurement System also available to the ETCS Train-borne Vital Computer.

The feasibility study examines each failure mode and proposes how RSL should mitigate for the failure mode.

2.2.1 Central Services Failure Use-cases

Failure of central services in SR4.0 are expected to be extremely rare, which means that any RSL should provide an extra level of resilience but without the cost or project execution complexities of replicating the entire SR4.0 architecture.

Based on current analyses, the central service most prone to failure would be the workbench, where RSL would need to provide an alternative workbench to allow dispatchers emergency network planning and dispatching capabilities, while allowing trains and OC's to continue operating under RSL.

TABLE 1 - RSL APPLICATION SCENARIOS FOR CENTRAL SERVICE FAILURES

Primary system	Use-case description	Failure mode description	Estimated likelihood of primary system failure occurring	RSL additional resilience suggestion
Workbench	Emergency planning & MA generation in event of central Workbench is required to bring passengers to safety	Central workbench goes offline	Low	RSL Workbench application that runs in control centres and autonomous control for trains to move without control centre command

Primary system	Use-case description	Failure mode description	Estimated likelihood of primary system failure occurring	RSL additional resilience suggestion
Traffic Management System (Plan-Execution)	Trains that are stranded or in running between stations need to be able to derive MA during a temporary TMS outage	TMS goes offline for a prolonged period due to business data centre outage or other cause	Low	Manual and autonomous route-setting should be possible for trains to work without centralised steering or route setting
Advanced Protection System	Upon an APS outage, trains need to safely reach the closest safe point of passenger egress thanks to an automated RSL	Central datacentres, that house APS, are temporarily unavailable (power outage in region where datacentre located)	Very low	Trains in affected region derive movement permission based on known network status and negotiate arrival at "safe harbour"
APS Safe Topology System	Safe topology system goes offline, but trains and OC's require snapshot of topology to enable safe degraded operation & hazard avoidance	Same as above	Very low	Latest topological data stored locally on trains and on OC
Identity & Access Management	Alternative form of authentication of trains & OC's is required to ensure safe movements & "legal" objects are on the network in case main IAM system fails	External datacentre that performs IAM is temporarily offline	Very low	Alternative certificate-based peer-to-peer authentication between trains & OC's running in parallel to standard IAM processes becomes active (rather than passive)
Safety Critical Data Centre Services	If datacentres fall victim to DDoS or similar attack, a non-datacentre-based logic system is needed to ensure trains & passengers reach a safe exit point promptly	DDoS attack provokes major disruption of datacentres and increases latencies to inoperable levels	Very low	Peer-to-peer communication and embedded safety logic allow RSL independence from any centralised datacentres or similar structures
Business Data Centre Services	In the event of significant downtime from the business datacentres, ensuring that basic network planning & management is still functional	Like above but affects all business data centre-hosted services (TMS, Workbench, etc.)	Very low	Peer-to-peer communication and embedded safety logic allow RSL independence from any centralised datacentres or similar structures

Recommendation 1. RSL should incorporate functionality that mitigates against failures to supporting services to the APS, such as Topological data server, Identify & Access Management servers, and Data Centre Services; each of these currently could be a single-point failure mode to the APS system.

2.2.2 Trainborne Subsystems failure Use-cases

Table 2 illustrates the trainborne use-cases that would be catered to by an RSL. As most onboard systems and sub-systems have embedded redundancy or use application-specific hardware, a cost-effective RSL should provide redundancy for elements with the lowest degree of embedded redundancy and strive to run on existing onboard hardware. Given these characteristics, a functional RSL would, at the very least, provide a fallback to the primary onboard ETCS system.

TABLE 2 - RSL APPLICATION SCENARIOS FOR TRAINBORNE SYSTEM FAILURES

Primary system	Use-case description	Failure mode description	Estimated likelihood of primary system failure occurring	RSL additional resilience suggestion
ETCS Onboard	Fallback onboard signalling & control system takes over from primary system when ETCS onboard fails	ETCS onboard becomes non-functional, emits conflicting or non-safe instruction to train driver	Medium	Alternative system running onboard and supervising train movement across network in "passive" mode
FRMCS Onboard	Optional additional redundant system in case of failure	Out of scope in current state of feasibility study	Low	Out of scope in current state of feasibility study
COAT Platform	Optional additional redundant system in case of failure	Out of scope in current state of feasibility study	Low	Out of scope in current state of feasibility study
DMI	Optional additional redundant system in case of failure	Out of scope in current state of feasibility study	Low	Out of scope in current state of feasibility study
Localisation/GLAT	Optional additional redundant system in case of failure	Out of scope in current state of feasibility study	Low	Out of scope in current state of feasibility study
ATO Onboard	Optional additional redundant system in case of failure	Out of scope in current state of feasibility study	Low	Out of scope in current state of feasibility study

Recommendation 2. RSL should be utilised when multiple trains in a region fail simultaneously due to systematic issues such as misconfiguration of the ETCS logic or a failed software update (e.g. a new version of GSM-R corrupting telegrams to/from trains).

For a single train failure, the dispatcher is able to provide verbal instructions to the train driver for him/her to operate the train from block marker board to the next block marker board and so on until reaching the nearest station for passengers to alight. RSL could support these movements by enabling the driver to continue without the need for verbal authority however if RSL is only activated on a single train then there are likely to be synchronisation issues between the primary CCS safety layer and RSL introducing complex safety hazards which could be difficult to fully model and predict.

Alternatively, MTC, a SR4.0 system that aims to provide signalling & control in network areas deprived of ETCS and specially designed for special manoeuvres such as shunting, joining, splitting, etc., operating on a “Lite” hardware platform could provide mitigation for all single-train failures without the need for RSL Hybrid mode.

2.2.3 Trackside system failure use-cases

The RSL use-cases & failure modes for trackside equipment can be seen in Table 3.

TABLE 3 - RSL APPLICATION SCENARIOS FOR TRACKSIDE SYSTEM FAILURES

Primary system	Use-case description	Failure mode description	Estimated likelihood of primary system failure occurring	RSL additional resilience suggestion
Object Controller	None - OC required for RSL to interface with assets	N/A	N/A	N/A
Fixed Comms Network	Optional additional redundant system in case of failure	Out of scope in current state of feasibility study	Low	Out of scope in current state of feasibility study
FRMCS Trackside	Optional additional redundant system in case of failure	Out of scope in current state of feasibility study	Low	Out of scope in current state of feasibility study
Train Detection Systems (Track Circuits / Axle Counters)	Interlocking needs up-to-date segment/block occupancy information always to grant/reject movement permission	Track circuit fails & is unable to report whether track segment/block is free or occupied, bringing traffic in affected region to a standstill	Medium	Alternative system that allows sector occupancy, train length and movement permission to be determined consistently, precisely and in real-time
Track Switches	None - APS will operate trains through/to failed track switch	N/A	N/A	N/A
Level Crossings	None - APS will operate trains up to failed LX	N/A	N/A	N/A
Eurobalises	None - Localisation/GLAT and TOPO will accommodate Eurobalise failure	N/A	N/A	N/A

Primary system	Use-case description	Failure mode description	Estimated likelihood of primary system failure occurring	RSL additional resilience suggestion
Signals	None – There will only be a very low number of signals left on smartrail4.0 network	Out of scope in current state of feasibility study	Medium	N/A

All trackside systems have one of the following characteristics that results in it being out of scope for RSL:

1. **Inherent redundancy** - systems such as FRMCS will have in-built redundancy, allowing switching to different communication technologies and backup router if main fails;
2. **External functional redundancy** – Eurobalise functionality is replaced by combination of GLAT and TOPO systems, which themselves already have redundancy at the central services level;
3. **Component w/ mechanical or electrical interface** – functionality of failed track switches & level crossings requires a secondary mechanical/electrical/hydraulic system that physically replaces the failed component;
4. **Operational mitigations** – accepting a trackside asset in its failed state and generating movement authorities for trains at degraded speed; or
5. **Asset depreciated in SR4.0 architecture –** Train Detection Systems and Signals are expected to be largely eliminated through the introduction of SR4.0 systems.

For **Trackside safety layer** failures, each object is largely discrete and as such trains can be verbally instructed through the failed object in its detected state. The Object Controller is closely coupled to the object which it controls and is the only way of interfacing with the object. The only way to provide resilience for this via RSL is to replicate its functionality with a duplicate object controller which isn't a scalable solution since it would be very expensive and require deep integration into the trackside asset electrical and mechanical interfaces.

Recommendation 3. If the planned reliability/availability of the Object Controller has such a high potential impact on the railway that it necessitates a redundant Object Controller, then a "Lite" version of the Object Controller should be considered that interfaces via the primary CCS safety layer rather than instructing all trains to use RSL for a specific area. This would be done to mitigate against the risk of synchronisation issues occurring between the primary CCS safety layer and RSL.

2.2.4 Summary of RSL failure modes to be addressed

Table 4 contains an analysis of the subsystems of SR4.0 comprising the functionality of the primary CCS safety layer and making recommendations about whether the subsystem functionality should be replicated within RSL.

The Red-Amber-Green colour-coding in Table 4 provides a visual indicator of cost/complexity/ease where Red is the bad/negative, and green indicates good/positive. The determination of the classification is on a qualitative basis based on the professional experience of the authors.

Blue elements in Table 4 are optional where a fully-independent RSL system could provide additional resilience as a “lite” version with lower performance or availability levels but sufficient for degraded operation. The feasibility for these elements is not considered within the scope of this study because the functionality of these elements is in essence a simplified version of what is already being delivered by existing SR4.0 feasibility studies.

Recommendation 4. If a fully independent RSL system is preferred, then each existing SR4.0 subsystem project should be extended to consider a “lite” version of its solution for degraded operation that could be incorporated into RSL.

TABLE 4 - SUBSYSTEM FAILURES COVERED BY RSL

Subsystem	Diverse components[2]	Complexity to replicate[3]	To be included in RSL?
Network Control & Supervision			
Dispatcher Workbench	No	Low – workbench alternatives widely available	Yes – low complexity
APS	Partial – core SIL4 software should be diversely programmed to avoid systematic s but can still fail with common-mode, high-impact failures.	High – logic rules needed for junctions and level crossings, but it is core scope to provide alternative method of generating movement permission	Yes – core scope
Safe Topology (TOPO4) System	Partial – core SIL4 software should be diversely programmed to avoid systematic errors but can still fail with common-mode, high-impact failures.	Low – database can be cached on trains	Yes – low complexity
Identity & Access Management	No – likely to share configuration and algorithms	Low – secondary authentication & encryption system can operate with lesser integrity for RSL using COTS methods	Yes – low complexity
Safety Critical Data Centre	No – likely each datacentre shares configuration tools for launching and managing instances	Low – create fallback data centre to support RSL safety functions	Yes – low complexity
Trainborne			
ETCS Onboard	Partial – core SIL4 software should be diversely programmed to avoid systematic errors but can still fail with common-mode, high-impact failures. If only a single train has failed, the driver can operate under verbal instruction from the dispatcher.	High – new solution required but it is core scope to provide alternative method of generating movement permission	Yes – core scope but only worthwhile for multiple-train failures.
COAT Platform	No – likely to include shared configuration and operating system layers that could fail.	Low – alternative computing hardware readily available	Optional – subject to COAT planned availability.
DMI	Partial – could, in theory, utilise an alternative DMI screen in the cab during degraded modes.	Low – alternative DMI hardware readily available	Optional – subject to DMI planned availability.
Localisation	Partial – could include GNSS, Doppler Radar, Tacho, Eurobalise etc. but can still fail with common-mode failures.	Medium – no COTS localisation systems exist but most signalling suppliers have a solution available and it would be possible to replicate topological algorithms.	Optional – subject to planned availability of Localisation.

[2] Supporting continued / degraded operation of primary CCS system
[3] Complexity of adding additional resilience in RSL through duplicating the components – complexity typically implies cost also

Subsystem	Diverse components[2]	Complexity to replicate[3]	To be included in RSL?
Trackside			
Object Controller	No – trackside PLC controlling specific objects. When failed, trains will be given verbal authority to pass the failed object at degraded speed.	High – required to interface to all types of trackside equipment	No – likely to be cost-prohibitive for a fully duplicated system and can be mitigated through operational rules – safety functions but not considered primary CCS layer.
Fixed Train Detection (track circuits / axle counters)	Partial – could fall back to based localisation however this may be unavailable and hence the inclusion of track-circuits and axle counters in an area. Theoretically possible for driver to validate location but this should be in localisation scope.	Medium – would include in Localisation system if replicated.	Optional – subject to planned availability of Localisation and Fixed Train Detection.
Non-safety options for RSL to consider			
Fixed Communications Network	Yes – expected to be decentralised architecture with diverse routes for communications.	Low – alternative using COTS modem for radio-based communications.	Optional – subject to Fixed Comms planned availability.
FRMCS Radio Network	Yes – expected to include multiple bearers / radio networks	Low – alternative using COTS modem for radio-based communications.	Optional – subject to FRMCS planned availability
FRMCS Onboard	Partial – could include LTE, 5G, Satcom, GSM-R etc. but can still fail with common-mode failures with no way for driver to contact control centre.	Low – alternative train-to-wayside modem readily available	Optional – subject to FRMCS Onboard planned availability.
ATO	No – expected to be SIL2 and therefore single compute platform, but with GoA2/3 a driver will be available to provide diversity.	High – all functionality would need to be deployed into RSL.	Optional - outside of scope of this study – not safety layer.
Traffic Management System	Partial – could fall back to manual train movement optimisation using dispatcher skills and experience.	High – optimisation algorithms complex to implement but autonomous decentralised optimisation is theoretically possible	Optional - outside of scope of this study – not safety layer
Business Critical Data Centre	No – likely each datacentre shares configuration tools for launching and managing instances	Low – create fallback data centre to support RSL non-safety functions (via commercial cloud provider)	Optional - if required for TMS – easy to include

2.3 Operations and Control concept

The following key principles underpin the Operations and Control Concept:

- The look, feel and functionality of RSL should be as closely-related to the primary CCS system as practicable, such that there is no ambiguity for users (drivers, dispatchers, etc.) as to how the system should be operated and how the system will respond to instructions.
- It should be obvious to users that they are using RSL rather than the primary CCS system so that no one expects a higher degree of safety supervision than that available – this could be through visual distinctions such as changes to colour scheme, bordering of the display, or a periodic visual and audible reminder.
- The system should operate with minimum human involvement as in a future automated network there may be insufficient personnel in control centres to provide manual movement instructions to all trains within a region.
- RSL shall limit the speed to 40km/h which is today's speed limit for on-sight operation until the route is proven clear. This speed enables the driver to intervene if a hazard is observed on the track ahead such as rocks on the track or another train. After the route is proven clear, a safe maximum beyond-line-of-sight speed can be adopted suitable for the RSL system.

2.3.1 Operating modes for fallback system

To satisfy these failure scenarios, RSL shall have three distinct operating modes described in Table 5.

TABLE 5 - RSL OPERATING MODES

Operating Mode	RSL Standby	RSL Hybrid	RSL Active
Scenarios	All primary systems working normally or functioning correctly in degraded mode.	Trainborne systems' failure	Central systems or trackside communications failure
Scope of Control for RSL	None	RSL is activated on single train; other trains continue to use Primary Safety Layer (ETCS)	RSL is activated on all trains and trackside objects in defined area or region
Safety Actor	APS responsible for safety logic. Movement permission from APS.	APS responsible for safety logic. Movement permission from APS Object Aggregator is transmitted to trains using RSL in lieu of ETCS	Trains determine their own movement permission and generate control request to trackside objects.

RSL Standby mode will allow RSL sub-systems to track the movement & state of objects on the network and thus monitor the state of the network at any given time. While in this mode, the RSL system will not

actively engage with the other SR4.0 sub-systems, it will rather be “listening” to state changes and recording them. This is necessary so that, in the event of a primary system failure within a region of the railway or a track segment, RSL is quickly able to determine which primary systems have failed, become the active signalling & control system in the affected region, know which new potential hazards might be present on the network and what movements would be deemed safe/unsafe for each specific train affected by the failure.

RSL Hybrid mode is engaged when a trainborne primary system failure occurs. RSL is then used to provide full signalling & control over the specific train’s movement and generating safe movement permission. All other trains and objects continue to use the primary safety layer.

RSL Active mode used when a primary system failure (central services or trackside communications) occurs and a segment or region of the network are no longer functional. Under this mode, RSL takes full responsibility for signalling & control. The system is thus capable of generating movement permission for emergency and special movements to all trains in the affected region via its components, effectively substituting the failed primary CCS system. All objects and trains should be able to automatically detect a failure of APS. Each driver will be required to switch RSL to Active mode for the train – albeit with the system primed and initialised ready to be activated by the driver. Each object controller should fail-over to communicate to the RSL layer automatically upon detecting a failure. The dispatcher shall provide the final authority for the use of RSL via the workbench – the RSL system should be designed so that it shall not generate any movement authorities or change the state of trackside objects without the dispatcher having given authorisation for use of RSL.

Note on RSL Hybrid mode vs MTC

Whilst RSL Hybrid mode is feasible to achieve and meets the need of providing a backup safety layer for a failed trainborne ETCS, there is another project in SR4.0 that has the same objective; the MTC project for Manoeuvre Train Control.

The MTC project provides movement permission functionality for slow speed manoeuvres such as shunting and coupling and construction sites where ETCS today does not accommodate these scenarios

Whilst MTC exists as a trainborne system alongside ETCS trainborne, MTC will communicate directly with the APS and so it would eliminate the benefit of having an RSL Hybrid solution. However, the ultimate aim of MTC is to include its functionality within the formal ETCS Specification in future updates to the Technical Standard for Interoperability. If that is achieved, then MTC will not be available when ETCS trainborne isn’t, and a need for an RSL Hybrid solution could arise; MTC might also be determined as unsuitable to use as an RSL necessitating the introduction of RSL Hybrid mode.

The report will continue to reference the integration of an RSL Hybrid mode, but greater emphasis will be given to RSL Active mode where all trains and objects in an area are under the control of RSL.

2.3.2 Activating RSL

It shall not be possible for a backup system (RSL) to override the primary system unless it is designed to the same level of safety integrity as it could put the system into an unsafe state – particularly it also opens up a new system vulnerability for cyber-attack.

If the trainborne system fails it will apply the emergency brake on the train, or if the central services fail all trains will brake to the end of their movement permission. The control of the brakes by ETCS onboard Vital Computer needs to be overridden to activate RSL and the control of the Trackside Asset needs to be overridden – this should not be possible from RSL itself. Instead the primary Object Controller or ETCS Vital Computer shall activate RSL when entering a failed state where it can no longer function or communicate with the APS. The train shall be stopped, and trackside asset locked in state before the safety responsibility is relinquished from the primary CCS systems.

The dispatcher or driver shall also have a capability to manually activate RSL for trains and trackside assets when the primary CCS system has not failed gracefully handing over to RSL. This shall always be in accordance to national operating regulations.

The following key steps of RSL activation are described:

1. When ETCS on the train has entered a failed state or is unable to communicate with the APS, RSL shall be automatically initialised on the train (or manually initialised if required to comply with ETCS operating principles):
    a. On initialisation RSL shall exit Standby mode and enter Hybrid mode. If RSL can contact the APS, then RSL will provide a movement permission for the driver using information from the APS.
    b. If the Hybrid mode cannot contact the APS, then RSL on the train will enter Active mode to become the safety actor responsible for generating a movement permission.

    The Driver shall not be required to re-enter any configuration data such as train length, mass or braking performance – the configuration of the train within the ETCS trainborne systems shall be mirrored in the RSL trainborne systems to mitigate against any human error for data entry, learning lessons from ETCS train configuration incidents on SBB in 2019[4].
2. RSL Core Services shall be in constant contact with the APS to know if it has failed. RSL Core Services shall be able to operate in the Hybrid mode for only specific trains, whilst maintain all other Standby mode functionality in readiness for engaging Active mode. Active mode shall be engaged automatically upon detecting a failure of the APS.
3. Object Controllers shall be constantly checking that their link to the APS is active. If the connection is lost to all redundant APS, then the Object Controller shall establish communications with RSL Core systems. *This ensures that in the event of a cyber-attack on*

[4] https://www.derbund.ch/panorama/vermischtes/sbb-entdecken-fehler-bei-der-zugsicherung/story/31639286

RSL when not active, it cannot impact on the operation of the SIL4 system; the OC itself isolates the RSL at all times other than when APS has failed.

2.3.3 Ensuring the activation of RSL does not cause unsafe scenarios to arise

Of fundamental importance to the safety integrity of the system are the handover arrangements from primary signalling system to AMS, and, later, the resumption of operations with the primary signalling system.

Recommendation 5. RSL shall only become the safety actor responsible for generating movement authorities for trains if the train has detected the APS has failed AND the RSL Core Services have detected the APS has failed.

Recommendation 6. RSL control areas must be aligned to APS control areas so that there is no possibility of mixed safety responsibility for an area.

Object Controllers shall only change state if the RSL Core Services and trains have all detected that the APS has entered a failed state. As such it is not possible for RSL to become the safety actor whilst the APS is available.

The primary hazard associated with activation is that switches change state whilst a train is approaching or over them, or that a level crossing opens whilst a train is approaching. The initialisation of RSL for Object Controllers must carefully consider the state of the railway prior to making any change of state to a trackside object.

The safety-critical loop controlling points and level crossings is generally engineered to SIL4 standard. The addition of AMS cannot interfere with the safety integrity of the primary signalling system. An Object Controller will not know why it was commanded to change state by the APS and therefore has no knowledge whether a train is approaching.

If the OC loses communication with the APS but is then subsequently commanded by RSL to change state when a train is approaching, it could cause a major derailment with serious consequences. To mitigate this the RSL interface to Object Controllers should not be activated by the OC logic until a timeout has expired. The timeout shall be defined such that all trains will have come to a stand following the cancellation of their movement permission from the primary CCS system. This timeout must be aligned with the national configuration parameters within ETCS as this is not a characteristic defined within the TSI. This timeout is essential to ensures that a SIL4 system does not enter into an unsafe state after a movement permission has been given to a train confirming it is clear to pass over the track switch or level crossing.

Once the timeout has expired a train might come to a stand over a track switch or level crossing. With a failed APS, the RSL will have no reliable knowledge of why the track switch was set and for which train it was set. Additionally, if RSL fails to initialise correctly on the train, the dispatcher and RSL Core

will have no visibility of the train stopped over the track switch and therefore there is risk the track switch could move under a train whilst it is stopped for another approaching train. A low speed derailment could occur when the train next moves.

If the driver is aware that the train has stopped over a track switch or level crossing, the driver must not move until RSL is active on the train or without the dispatcher manually controlling the track switch to allow the train to move safely.

2.3.4 Reverting to full ETCS-based interlocking

Handing back from RSL to APS needs detailed consideration for how the APS initialises and how the EVC systems initialise. The following considerations should be made in the design of these systems:

- When the APS system is being restored, the dispatcher must revoke authorisation for all trains to use RSL to avoid any complexity risks from multiple safety systems operating in parallel in the same control area.
- When EVC on a train regains connection to the APS it shall refrain from applying the emergency brakes if RSL is in Hybrid or Active mode until the EVC is fully initialised and a movement permission has been received from the APS. This is to ensure that there are no further delays caused whilst waiting for EVC to initialise and no further discomfort caused to passengers through emergency braking.
- Objects shall not be commanded to change state by APS until all trains in the control area are initialised within the APS such that Switches do not change state ahead of a train that has commanded the switch using RSL.
- Trains might have entered the control area during outage of the APS so their locations may be unknown. RSL shall include an Object Aggregator function that can handover data to the APS or dispatcher to better understand the state of the railway. The process for this must be considered in detail during the definition of both the APS system and RSL system.

Recommendation 7. The hand back from RSL to EVC requires a functional change to onboard EVC to avoid hard emergency braking when the primary systems come back online - this should be considered under future TSI updates.

Recommendation 8. Operating procedures for the initialisation of ETCS and APS, when restoring service after use of RSL, must be based on a comprehensive safety risk assessment based on thorough modelling of all potential scenarios.

2.3.5 Operating and Controlling unfitted trains and usage restriction areas

Construction trains, steam trains, cross-border trains, or trains with failed RSL systems present a hazard to other RSL trains. Their location will not be known within the RSL system when it initialises.

Unfitted trains must be manually registered as Usage Restriction Areas within the Dispatcher Workbench, providing a safety 'bubble' or 'block' within which the unfitted train can move and then given verbal movement authorities. This is required to ensure that correct movement authorities can be generated by RSL for fitted trains. This requirement for trains without ETCS fitted is also expected for the APS.

Similarly, maintenance worksites, livestock, rock-fall, flooding, etc., are some of the many dangers that might result in temporary speed restrictions being placed on an area of the railway network, or a total blockage of that area. These dangers will need to be known by RSL to ensure that correct movement authorities can be generated.

Recommendation 9. RSL, in standby mode, should maintain a synchronised copy of the URA register contained within the primary Dispatcher Workbench or Traffic Management System to improve the validity of its movement authorities upon initialisation.

This recommendation is based on lessons learned from an incident in the UK on the Cambrian line with loss of temporary speed restrictions within the ERTMS system after the system was restored.[5]

An on-sight speed restriction (understood to be 40km/h) should be implemented so the driver can mitigate hazards. Once the routes are proven clear of any hazardous unfitted trains, the speed limit can be lifted to a safe maximum suitable for RSL operation.

The volume of unfitted trains operating on the network, in particular international services (such as from Deutsche Bahn and SNCF), will present a significant operational workload challenge on dispatchers to provide movement authorities to all of these trains using verbal instructions. Evacuation of trains via verbal instruction can take 2 to 3 hours for 2 to 3 trains on a small track section.

Each day in Switzerland there are usually 42 passenger trains from other countries (SNCF TGV: 15, DB ICE4: 20, ETR610 TrenItalia: 7). The study has assumed that each train spends 4 hours within Switzerland and that passenger services are spread evenly from 09:00 to 18:00 represented in Table 6.

TABLE 6 ASSUMED PROFILE OF INTERNATIONAL PASSENGER SERVICES IN SWITZERLAND

Hour	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00
Trains	6	12	18	24	24	24	24	18	12	6

There are potentially up to 24 international services from other countries operating on the network at any time. Sharing this load between 5 regional control centres results in only 5 trains per region requiring

[5] Rail Accident Investigation: Interim Report Loss of speed restrictions on the Cambrian line 20 October 2017 https://assets.publishing.service.go.uk/media/5bc871d5e5274a0956564a41/IR012018_181018_Cambrian_TSRs.pdf

verbal instruction in degraded modes; this could be a reasonable workload for any control centre to accommodate.

Freight services have been assumed to be between 30 and 40 non-Swiss freight trains at any time based on percentages from a Swiss Government Report in 2017[6]. The study has assumed that each international freight train spends 6 hours operating within the Swiss Railway Network and that they are spread evenly throughout the day and night. As such a maximum of 10 trains are likely to be operating on the network at any one time which the study has assumed could reasonably be accommodated within any control centre with potentially only 2 operating in each region.

[6] https://www.newsd.admin.ch/newsd/message/attachments/50147.pdf

3 Autonomous Movement Supervision system concept

Technological feasibility of an Autonomous Movement Supervision system

An Autonomous Movement Supervision (AMS) system is introduced within the RCA Architecture Overview (Beta), without further definition beyond that which is in the quote below:

> ""AMS: Autonomous movement supervision": Diversely implemented fall-back functionality that provides a basic safety with the minimal use of other functions (e.g. only train2train coordination and direct access to OC or trackside assets). AMS could also be a completely isolated function."

This feasibility study expands on the concept in order to satisfy the functional needs of an RSL by providing a decentralised solution that can add resilience to the SR4.0 architecture for scenarios described in Section 2.

AMS is a Communications-Based Train Control system with a radically different architecture to traditional systems; a decentralised system with unique characteristics described in Table 7 below.

TABLE 7 - DECENTRALISED VS CENTRALISED CBTC SYSTEMS

Centralised CBTC system	Decentralised CBTC system
Trains and Objects respond to instructions they are given from a central control system. The state and status of object must be transmitted to a central system before and instruction can be transmitted back; the control-loop has a radio network in the middle.	Decentralised decision making where safe decisions are made at the edge of the system – directly on the objects that are affected by the decision. Information can be quickly acted upon with the control loop constrained to the train or object itself.
Central servers need to be expanded to handle additional trains running on a network and additional regions or track sections being added.	Scalable architecture where each object comes with the computing capability to serve its own needs and no need to expand central servers.
Synchronous control - If a link to the central system is lost or data hasn't been updated in a timely manner, or commands haven't been acknowledged by remote systems, then trains will stop.	Asynchronous control where all objects take decisions in a timeframe that suits their needs with no 'real-time' control between objects to mitigate the problems with lossy communications; information is deemed to be 'out-of-date' as soon as it is sent and trains and objects must accommodate this by design.

The AMS concept is specifically conceived to meet the needs of providing a highly-resilient solution for remote/rural railway networks with poor connectivity and poor quality infrastructure, whilst also providing high-capacity throughput in urban environments and high-speed operation on intercity routes.

A decentralised architecture for safe control of trains and junctions significantly reduces the likelihood of total unavailability of the railway network provoked by major outages affecting centralised systems as individual AMS components are unlikely to be affected by a common-mode failure; failures of AMS itself would be localised only to a very specific area or specific train.

3.1 Introduction to Autonomous Movement Supervision

The concept for AMS uses a peer-to-peer approach whereby trains communicate directly with other trains, and directly with objects on the railway.

AMS uses an asynchronous model requiring monitoring of telegram sequencing to ensure safe operation, in other words, to ensure that the position status received is the most up-to-date and not superseded by an old position report that took longer to arrive at the recipient.

AMS has four key subsystems:

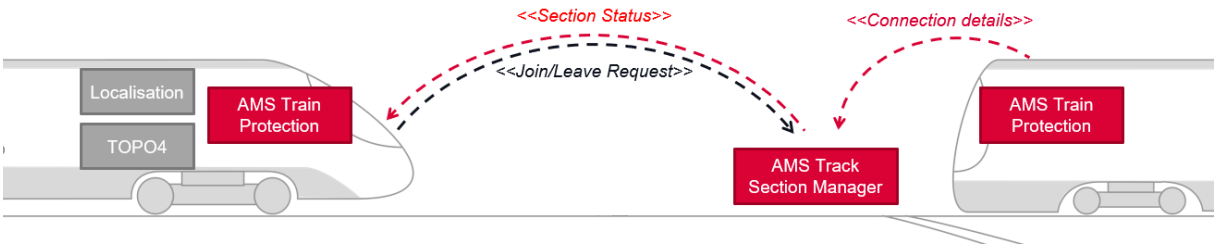
AMS Train Protection System *Trainborne System*	**AMS Track Section Manager** *Trackside system*
A trainborne system setting a route for the train and generating its movement permission. The Trainborne Protection system will sound warnings to the driver and apply the Emergency Brakes where necessary.	Providing management of which trains are permitted to enter a track section with any speed restrictions, hazards, and providing a register of trains in the section such that a train can find out which other trains are in its vicinity.
AMS Object Control Manager *Trackside System*	**AMS Network Management System** *Datacentre Service*
Receiving requests from trains and responding through changing the direction of switches or opening and closing level crossings. The AMS Object Control Manager authorises only specific trains to be responsible for control of the asset and informs them when it is safe to extend their movement permission.	Providing a means for a dispatcher to govern the railway network – adding hazards and danger-areas to the network to protect trains from external factors such as rock-fall or flooding, or construction sites, or vehicles or animals on the railway.

To better illustrate the workings of AMS and its sub-systems, an explanation of the basic concepts of generating a movement permission using the AMS subsystems is provided below.

1. **Wayfinding**
    a. A train receives details of its next destination from the timetable, Traffic Management System or Dispatcher – depending on whichever is available.
    b. The train detects its own location, reconciles it with topological data cached on board the train.
    c. The train then computes a wayfinding route through the network to get to its destination.

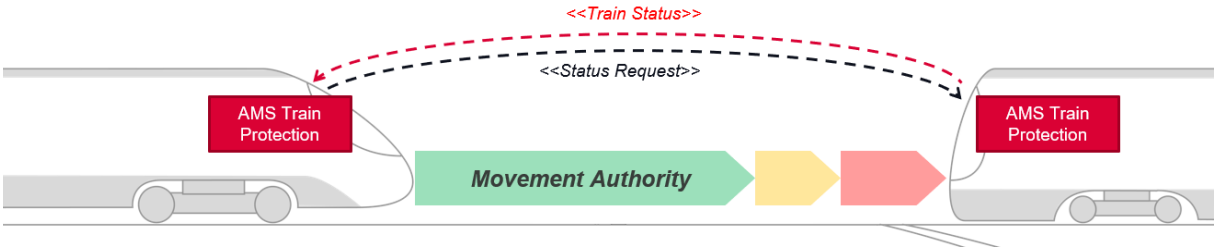
2. **Maintaining Safe Separation from the train ahead**
    a. The train learns about the state of the rail network in its vicinity thanks to direct communication with other Trains and AMS Track Section Managers.
    b. The AMS Track Section Manager is responsible for a section of track between two sets of points (an edge between two nodes on the topology data) and holds a register of all trains within a section of track; like an axle counter counts axles – the Track Section Manager records train IDs within a track section.
    c. A train sends a request to the AMS Track Section Manager to join the track section and receives back a list of authorised trains in the section. If the train itself is included in the list, then it has permission to extend its movement permission into that section of track.

FIGURE 7 - AMS TRAIN PROTECTION ENGAGES DIRECTLY WITH AMS TRACK SECTION MANAGER



    d. The AMS Track Section Manager includes an addressing register (much like a dynamic Domain Name System server) holding an IP address list for all the trains in the section. This is to facilitate peer-to-peer communication in a dynamic connectivity environment.
    e. The train uses the list of trains to determine which train is directly ahead and requests the location of that train directly from it. Once its location is received, the train extends its movement permission up to the rear of the train ahead.

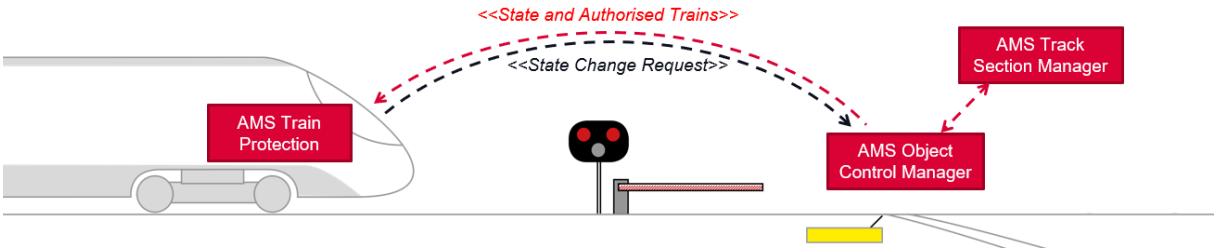
FIGURE 8 - TRAIN-TO-TRAIN COMMUNICATION ENSURES AUTONOMOUS GENERATION OF MOVEMENT PERMISSION



3. **Controlling trackside assets for clearing the route ahead and steering**
    a. When a train wants to pass through a Switch or Level Crossing it sends a request to the AMS Object Control Manager for the change of state and authorisation.
    b. The AMS Object Control Manager publishes back the ID of the train in control and its state.

c. Once the state is valid for the requested movement and the train is identified as being in control, the train extends its movement permission over the switch or level crossing.
d. Once the train completes the movement, it relinquishes control of the object.

FIGURE 9 - TRAINS APPROACHING SWITCHES & LX ENGAGE DIRECTLY WITH OC TO CHANGE STATE OF SWITCH/LX



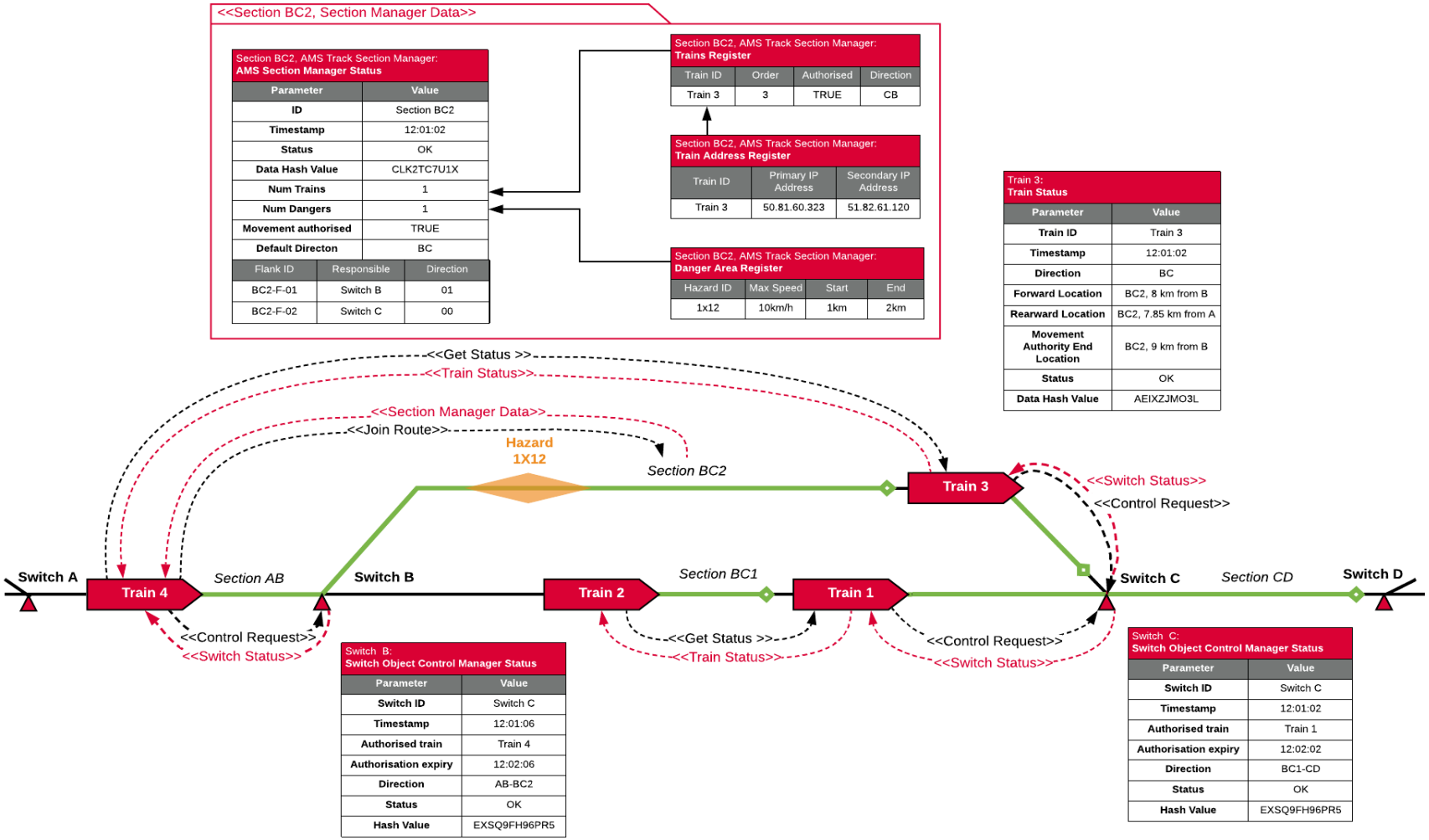
4. Managing dynamic hazards safely in total outage of centralised systems

a. On initialisation of the Autonomous Movement Supervision system, the trains and Track Section Manager might not know if there are hazards or Usage Restriction Areas on the railway.
b. Speed is automatically restricted for all trains within a Track Section until the section has been proven clear by a full transit of a train through a section.
c. The Autonomous Movement Supervision system thus restores service after a total outage of centralised information systems.

These basic rules and principles when combined permit fully moving-block, bi-directional operation with no theoretical limits other than the physical infrastructure itself. An example of how these rules manifest together for emergent capacity, safety, and performance is included in Figure 10, where each train's movement permission is generated based on its understanding of the state of the railway network as far as the route is clear ahead.

In this example, as Train 4 on track section AB, approaches the track section BC2, its **AMS Train Protection System** will have requested to the **AMS Object Control Manager** to take control of Switch B, changing its position if needed, and will send a join request to the **AMS Track Section Manager** for section BC2. Train 4 will query the **AMS Track Section Manager** to receive an update of any hazards on its requested track segments (e.g. Hazard 1X12). Train 4 will then check the Trains Register within the **AMS Track Section Manager** to determine which train is ahead and how to communicate with it (i.e. Train 3 in direct segment BC2). Train 4 will then query Train 3 to determine its location. With all this information in hand, Train 4 can derive its movement permission autonomously, knowing that its movements will be safe.

FIGURE 10 - EXAMPLE OF AMS SYSTEMS ON AN RSL ACTIVE TRACK SEGMENT



3.2 Basic concepts to ensure safe movement

A decentralised Autonomous Movement Supervision system differs from a traditional interlocking in that there is no central authority reserving infrastructure for the movement of trains. With this being the case, many of the basic safety concepts for APS and ETCS are quite different for AMS.

Table 8 Includes a summary of how RCA has defined its safety logic concepts, contrasted with how AMS achieves the same safety logic. All conditions are satisfied through an alternative architectural approach.

TABLE 8 - COMPARISON OF RCA BASIC CONCEPTS OF THE SAFETY LOGIC

RCA Safety Logic Core Concept	RCA Safety Logic Description	AMS equivalency for safety logic
Utilisation Permission	A utilisation permission is a permission to utilise a geometric area of the network topology under defined utilisation conditions. There are two types, Movement Permission and Usage Restriction Area / Usage restriction area.	The AMS Object Control Manager shall generate a utilisation permission for a specific train following a control request from the train.
Utilisation Condition	A utilisation condition defines how a certain geometric area may be used (e.g. maximum speed, allowed driving direction, allowed train type).	The AMS Train Protection System uses its copy of Topology data to generate a speed profile ahead for the train and its limit of safe movement.
Usage restriction area	It is possible to set a Usage Restriction Area over a certain part of topology (e.g. track segment). A Usage Restriction Area request is typically submitted due to an exceptional situation (e.g. landslide, maintenance work, etc.). This request may be submitted by the traffic management system but also by the safety manager APS-SM (watch dog). A Usage Restriction Area and a movement permission may overlap under certain conditions (e.g. construction vehicle must enter in a construction site).	The AMS Network Management System is used by the Traffic Management System or Dispatcher to add Usage Restrictions to the network. This data is transmitted to AMS Track Section Managers so that trains can be aware of hazards and adjust its own movement permission accordingly.

RCA Safety Logic Core Concept	RCA Safety Logic Description	AMS equivalency for safety logic
Movement Permission	A movement permission is an authorisation to move in a specific direction for a specific distance according to a given speed profile. This includes data on track-conditions as known today in ERTMS/ETCS. The movement permission is requested by the traffic management system and verified by the APSSL. After verification the movement permission is sent to the moving object (e.g. Movement permission in ETCS). The moving object must always stay inside its movement permission. Movement permissions may overlap under certain conditions (e.g. joining).	The AMS Track Section Manager grants permission to trains to enter a track section and travel in a specific direction including data on track-conditions known. The AMS Train Protection System queries other trains in its vicinity to learn about their locations and generate a movement permission for itself. The AMS Train Protection System ensures that the train always stays inside its movement permission. Movement permissions shall never overlap. If two trains are travelling towards each other head-on a train will request the AMS Track Section Manager places a usage restriction on the section of track in which it is operating.
Safe Distance	The safe distance (in time and space) between two consecutive utilisation permissions is needed for safety reasons. To ensure these safe distances, Risk Buffers will be set at the boundary of the utilisation permissions (e.g. movement permission).	A train shall not let its stopping distance be in excess of the distance to a train or hazard ahead and shall add a suitable risk buffer based on the calculated accuracy of sensor data, environmental conditions and speed of the train.

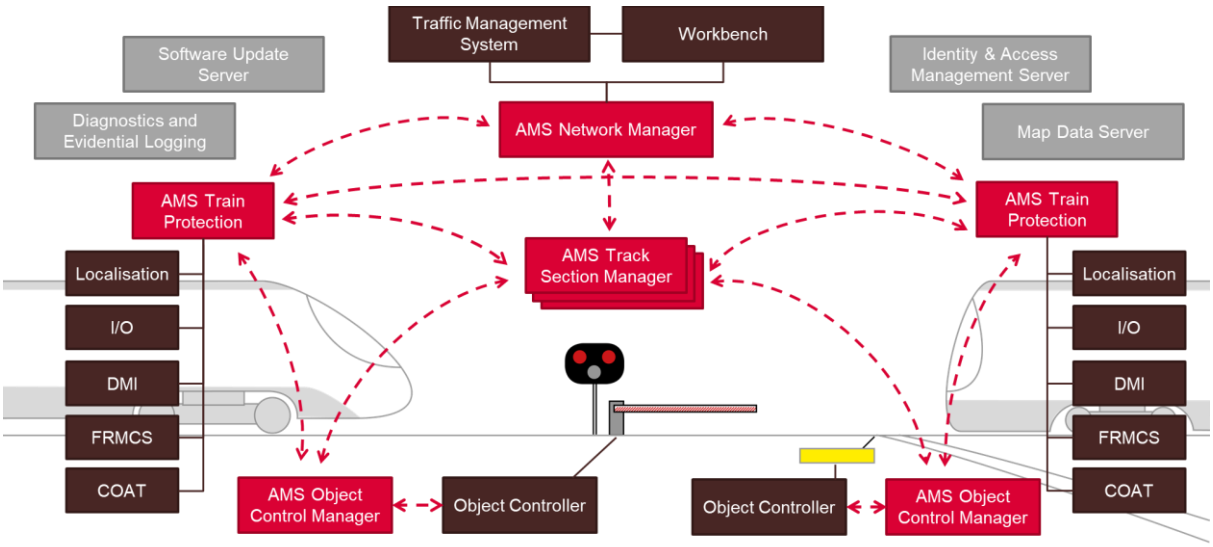
Source: RCA - Architecture Overview (RCA.Doc.2 version Beta.1). EUG and EULYNX Partners. (Document from 26/8/2019) https://eulynx.eu/index.php/documents2/rca/rca-beta/227-rca-architecture-overview/file

3.3 High-Level System Functionality

Figure 11 shows the key components of the AMS system and its wider interfacing components. The physical hosting of each of these key components has a few options available and these are introduced below.

A comprehensive description of key system functionalities for each subsystem is included within Appendix D, supported by Appendix E which describes a decentralised interlocking approach for enabling complex junction control from simple logic controllers interacting through cascading flank protection methods.

FIGURE 11 - ARCHITECTURE FOR AMS SYSTEM AND WIDER INTERFACES



AMS Network Manager

AMS Network Manager is a centralised service providing safety-related functionality which would necessitate a server running the service somewhere; this could be cloud-hosted, or on a third-party or AMS supplier data centre, or on the SBB Business data centre infrastructure. A desktop application and/or web-based application will be required to be deployed into the Control Centres to connect to the AMS Network Management System.

AMS Track Section Manager and AMS Object Control Manager

The AMS Track Section Manager and AMS Object Control Manager are software-based micro webservices that could be physically located in a variety of architectural locations, whether in the cloud, a private datacentre, on lineside computing equipment, or on the Object Controller itself.

These applications are all safety critical. They require a communications gateway to the Object Controller and wider AMS systems but otherwise these services could run in any location; (it is even potentially possible that they could be hosted on a train that operates as the “Master” controller for that track section and set of objects – shutting down the service as the train exits the section so that another train can initialise it as the “master”).

AMS Train Protection System

The AMS Train Protection System is envisaged as a software-based application that can be executed on any general computing platform suitable for safety-critical applications (SIL2/SIL4 suitable). The compute platform would require interfaces to train inputs and outputs, driver displays, localisation sensors, communications systems, and hardware-based encryption for attestation and authentication.

Additional services necessary for AMS functionality

An AMS system requires additional information, data and services to correctly function. These are:

Service name	Description	Rationale
Addressing Service	A central system that provides connection details to other central services and Object Controllers by listing their IP addresses and other connectivity details; analogous to a Domain Name System server for internet traffic.	When switching between connectivity types or using diverse communication routes or setting up new instances of central processes, connectivity details will change. A service is required to help trains and other controllers discover to which system they can connect to.
Authentication Service	A central service that is responsible for signing certificates used for authentication by trains, objects and AMS subsystems. The service shall also be responsible for issuing new certificates to trains. The authentication service shall also include a Certificate Revocation service.	Authentication is required to enable cyber-security and integrity of messages between AMS systems and interfaces. New certificates will need to be issued to trains whenever equipment is modified or replaced during maintenance. Any faulty or quarantined components should have their certificate revoked until repaired.
Communications subsystem	A trainborne subsystem that provides radio-based communications to the internet and trackside fixed networks.	The AMS Train Protection System needs to communicate with other AMS subsystems to understand the state of the network and control trackside to generate a safe movement permission.
Compute management service	A central service that manages the cloud/hosted applications deploying them to servers. A compute management service helps spread these services over a variety of servers	Many micro webservices are required to support AMS operation on a network – this is required for the resilience of the system. The Compute Management Service will also be necessary to provision new microservices in line with topology updates.
Data Aggregator and Message Broker	A central service that provides a snapshot of the state of the railway and shares data from one subsystem to others that require it – e.g. providing train location to customer information services.	Trains and Objects would become overwhelmed with status requests if all third-party systems had to request the state directly from them – a Data Aggregator will have more resilience and capacity to accommodate a wide number of connections for non-SIL needs.
Driver Interface	A shared driver display (touchscreen or with buttons) that enables the driver to interact with AMS when activated.	AMS would otherwise need to have a specific display integrated into each train's cab for the sole purpose of AMS (impractical when using AMS as a backup system only).
Evidential data recording	A service running on all AMS systems that records all inputs and outputs and key decision factors. A Central logging service will aggregate all data periodically to be used for deeper investigation and prognostics.	As a safety-critical system it is essential that the system can be demonstrably safe to facilitate robust investigations and liability if an accident occurs.

Service name	Description	Rationale
Information Link Service	A central service that publishes sanitised data into the public domain for information services and connected applications.	Not all data from within the AMS system should be made available to the public – especially for trains carrying sensitive materials such as nuclear waste.
Localisation subsystem	A trainborne subsystem that uses a variety of sensors to locate the train on the topological map of the network.	The MS Train Protection System needs to know where it is to generate a movement permission.
Map data service	A central information service that trains use to update their own cached version of map data, provide in a 'node-edge' topological vector model. Map data might be pre-cached on the train for future infrastructure changes.	The AMS Train Protection System requires map data to generate its own movement permission including distances, curve radii, maximum segment speeds, temporary speed restrictions, tunnels, non-passable hazards, etc.
Object Controller	A trackside system that enables a trackside asset to be commanded via the EULYNX protocol.	The AMS system would be very complex if designed to communicate with all possible trackside systems electrical or mechanical interfaces.
Safety Manager	Analogous to APS Safeguard, the Safety Manager shall act as an independent verifier of correct functionality of the system with the capability to stop trains, suspend object control, and stop all trains within a region if unsafe behaviour is detected. The Safety Manager should also include a level of cyber-security and intrusion monitoring. The Safety Manager monitors all inputs and outputs and is capable to send an emergency stop instruction to all AMS services.	The Safety Manager is required to provide additional safety resilience to protect against any systematic errors within the safety-critical AMS system – these might include: Overlapping movement authorities between trains, track switch movements within a movement permission, level crossings opening within a movement permission, trains exceeding usage constraints or violating Usage Restriction Areas.
Service Manager	A central service used by system administrators and technicians to monitor and manage the AMS system.	The AMS system will require a capability to have configuration changes applied, to restore services after failures, or expand services to incorporate new regions and additional trains.
Software update service	A central service shall be provided for the train to ensure it is running the correct version of software. The software shall be securely signed and contain a new root certificate for all subsystems such that they cannot communicate with old software versions.	As a software-based system deployed to all trains, it is impractical to manually update software on all trains at once during depot hours and moving physical copies of safety-critical software via CD, USB, or laptop introduces its own security risks.

Service name	Description	Rationale
Train Configuration data	A trainborne data set used to setup how the AMS Train Protection System makes safe interventions applying the emergency brakes.	If AMS does not have accurate information, it must default to a standards-based scientifically calculated worst-possible default braking curve which could impact capacity and performance.
Train Control Interface	A system that enables AMS to command application of the emergency brakes of the train.	AMS would otherwise need to be designed to interface with each train's specific electrical/control systems.

3.4 Additions to AMS for RSL Hybrid mode for SR4.0

Special AMS functionality must be introduced to AMS to facilitate an RSL Hybrid mode capability, i.e. parts of a controlled region are under AMS and others are running under the primary ETCS-based safety layer. Since this mode presents a unique set of potential risks, the following sequence of actions/interactions is suggested to ensure safe RSL Hybrid movements:

i. For a train in RSL Hybrid mode, the dispatcher must authorise the use of Hybrid mode in the AMS Network Manager, specifying which train can use it and defining an area for its use.
ii. The AMS Data Aggregator receives the movement permission (including distance and speed profile) from the APS Object Aggregator. The AMS Data Aggregator passes the movement permission to the train.
iii. The train publishes its status and location to the AMS Data Aggregator as normal. The AMS Data Aggregator publishes the train status and location to the APS Object Aggregator as normal.
iv. When RSL Hybrid Mode is activated on the train, the train checks with the AMS if it is authorised for use. The AMS Train Protection System uses the localisation data to monitor the train's movement and provides a warning if the train is encroaching on the limit of its movement permission, applying the emergency brakes if required.

3.5 Why AMS is the best approach for meeting the needs of RSL

For the purposes of this study, the adequacy of an AMS as an alternative CCS system will only be evaluated in its use as an RSL. It should be highlighted that an AMS can be deployed as a primary signalling & control system, as its elements & architecture allow for full CCS functionality at normal line speeds just as well as in degraded operation. This capability, coupled with its inherent safety, reliability, resiliency and system performance, place AMS as an ideal system to meet all the needs of an RSL.

AMS will be safe

AMS shall be designed such that the system adopts a safe state under any failure conditions and when identifying hazard mitigations, a technical mitigation which eliminates the potential risk will be preferred to one which controls it, which will in turn be preferred to an operational mitigation.

At the core of AMS' safety approach is the concept of safety through simplicity, the AMS system shall always propose the simplest solutions for its architecture, functions and safety logic by:

- **Limiting complexity** - using modular design and restricted system states.
- **Partitioning the system** – establishing well-defined interfaces to make sub-systems easily testable, maintainable, and upgradable.
- **Eliminating shared failure modes** – being run on non-centralised systems distinct from core primary systems eliminates the potential of shared failure modes.
- **Eliminating single points-of-attack or -failure** – AMS' decentralised architecture makes it less prone to cyber-attacks that would more easily take down centralised systems.

By having simplicity and safety embedded in its decentralised design, AMS will achieve high levels of system safety whilst reducing development and assurance costs associated with centralised safety systems.

AMS will be dependable/reliable

The AMS system is designed for high reliability and availability as well as for ease of maintenance through:

- **Design and testing for harsher environments** than the standard operating environment
- **Minimising novelty** by using proven technologies (fewer 'teething' issues)
- **Modular design** to ensure short MTTR (Mean-Time-To-Repair) via replaceable components
- **Eliminating hardware** that would result in common cause and dormant failures
- **Prioritising meaningful alarms** and alerts
- **Intelligent monitoring** and Built-In Test to ensure efficient and quick diagnostic

Other than the design elements mentioned above, AMS' stand-by mode will include constant logging and monitoring of performance. This data will be reviewed periodically to identify failures and degradation of performances, allowing them to be fixed at the earliest opportunity and providing potential insight into the workings of other systems.

As a result of the design elements above, AMS systems will offer higher levels of reliability & availability when compared to centralised RSL alternatives.

AMS will be resilient

Like any safety layer, a fallback system also requires a high degree of resilience to ensure that in the event of a sub-system failure, a secondary or tertiary system will provide the required functionality while the primary system can be recovered quickly.

AMS' decentralised architecture already equips it with a high degree of resilience, where single points of failure are nearly completely eliminated. As an example, AMS' simple software-heavy/hardware-light architecture allows it to generate new instances of software on other elements of hardware if a software process freezes or becomes unresponsive unexpectedly.

The hardware elements necessary for AMS to run are also highly resilient. Most AMS hardware is foreseen to be of SIL2 or higher grade, thus being of an extremely high resilience. In the event that hardware of a lower safety integrity level fails or if data transmission were to fail, AMS' design allows it to be equipped with alternative systems such as safe tablets for in-cab visualisation, other localisation systems, mobile modems, etc.

Similarly, to safety and reliability, the decentralised, software-based architecture of AMS arms it with a much higher grade of resilience when compared to an equivalent centralised fallback system.

AMS will meet the needs for capacity and performance

A fallback system should guarantee a minimum capacity and allow for a minimum level of system performance measured as the number of recovered trains per hour in situations of primary safety layer failure. In these two categories, AMS excels in providing higher capacity and higher performance than centralised fallback systems thanks to:

- **AMS' original design as a primary CCS system** - AMS safely handles more objects in a safer manner at lower line speeds e.g. RSL linespeed, when compared to block-based systems.
- **Autonomous safety logic & route-setting** – trains and trackside objects negotiate movement authorities autonomously with each other, ensuring safe movements & reducing the reliance on human intervention.

As a result of these two qualities, AMS would very likely allow for a network to achieve higher levels of performance in degraded scenarios when compared to an equivalent centralised fallback system.

Other areas where AMS fulfils RSL goals:

Additional to the areas mentioned above, there are other criteria which an RSL system must fulfil for it to be an effective fallback system. As can be seen in Table 9 below, AMS clearly fulfils all of the additional goals required for an effective RSL system.

TABLE 9 - HOW AMS COMPLIES WITH/ACHIEVES ALL RSL FUNCTIONS & GOALS

RSL Function or Goal	Criterion fulfilment level by AMS	AMS sub-systems/characteristics fulfilling RSL function/goal
Provide full signalling, control, and route-setting or "steering" capability	Complete	AMS can be deployed as a primary decentralised CBTC CCS system across a region or an entire network
Monitor state of the network	Complete	AMS services are envisaged to continuously receive state change information from central services and provide updates to other systems when primary safety layer fails
Enable alternative planning & timetabling	Complete	AMS provides dispatchers fully functional alternative interface for viewing & executing short-term planning & timetabling in the event of a primary workbench failure
Be highly adaptable	Complete	Decentralised, software-based architecture can be modified and swiftly adapted to meet current & rising operational conditions/constraints
Be affordable	Complete	Software-based architecture allows AMS to scale from small to large field applications with only minimal changes to CCS hardware
Be autonomous	Complete	AMS grants trains and objects autonomy over safety logic and movement, thus limiting the need for human interaction

3.5.1 Known areas of potential performance impact on AMS

As is the case with any system that has not yet been fully implemented, there will be areas of unknown performance. At this early stage, some factors were identified as potentially affecting system performance but after initial analysis, none of them seem to jeopardise the use of AMS as an effective RSL. Table 10 summarizes the results of the preliminary analysis.

TABLE 10 - PRELIMINARY ANALYSIS OF FACTORS AFFECTING AMS PERFORMANCE

Identified factor/trigger	Qualitative performance impact as fallback system	Rationale vs. alternative system	Qualitative performance impact as primary system	Rationale vs. alternative system
Driver & dispatcher acknowledgement time (potentially 3 minutes)	Medium to Medium High	Initiating AMS from a standstill when primary system is out will allow faster overall network recovery	Neutral	If AMS is primary system, boot up of onboard computers will load all AMS relevant software

Multiple AMS activations in same track section	Medium to Medium High	Request to activate AMS must be done individually for each affected train but mitigates visual driving via voice command	Neutral	AMS would already be active as primary
Communications latency (if unusually high)	Neutral	With reduced line speeds, higher latencies do not affect performance or capacity	Low to Medium	High latency could limit the operational linespeed, thus impacting total system capacity negatively
Compute cycle time of AMS subsystems	Neutral	With reduced line speeds, higher latencies do not affect performance or capacity	Low to Medium	Compute delay could limit the operational linespeed and result in conflicting information thus impacting total system capacity negatively
“Shadow/blackout/patchy” comms regions	Neutral	With reduced line speeds, comms would be able to establish secondary or tertiary backup in timely fashion	Low to Medium	If backup comms is not able to establish stable connection, linespeed might have to be limited, thus impacting capacity negatively

3.5.2 Why AMS fulfils all RSL criteria and is the ideal RSL system

Based on the characteristics described above, one can conclude that a decentralised CCS system such as AMS is an ideal fallback safety layer. Its highly flexible, intelligent & decentralised architecture grants it great adaptability and affordability while not sacrificing safety or availability. Moreover, its embedded, autonomous safety logic greatly simplifies interlocking, while also establishing the basic conditions for use in GoA3/GoA4 operation in the future. Despite some areas of uncertain performance, AMS clearly fulfils all the necessary criteria of a safe, cost-effective and reliable RSL.

4 Integrating AMS into SR4.0

Integration feasibility for AMS into the SR4.0 architecture

The AMS system to provide RSL has been designed to integrate with the planned architecture of SR4.0.

Many of the specific functionalities and interfaces remain somewhat undefined within SR4.0.

The integration of AMS into SR4.0 considers only the general technological possibility for integration. These ideas have been based on feedback on concepts during interviews with respective project technical leaders across the SR4.0 programme. The feasibility study has ensured that the data and the functionalities on which AMS depends are planned to be available as the SR4.0 programme advances. For full integration, work will be required to each of these interfacing systems to establish the interfaces.

Within this section, firstly, the general system architecture is described, and then more specific functional integration and dependencies are defined such as for the Data Centre Hosted Systems, the SR4.0 COAT platform, and SR4.0 Object Controllers.

4.1 Functional System Architecture

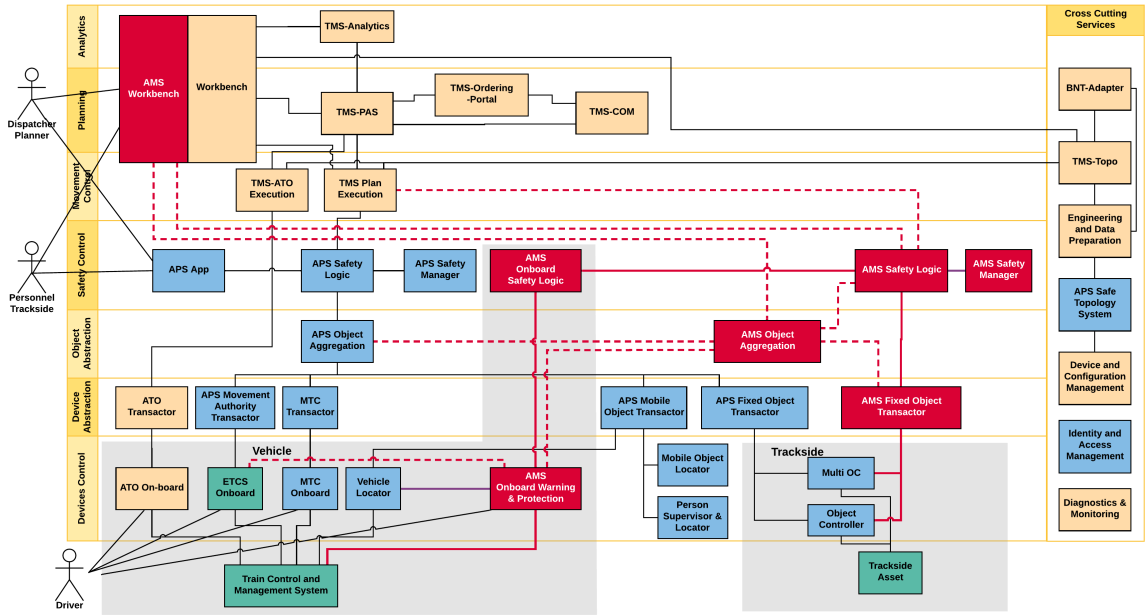
The AMS system for providing RSL extends the Reference Control Architecture through providing equivalent systems at each layer:

- The ***Analytics***, ***Planning*** and ***Movement Control*** layer is extended by an AMS Workbench to be able to provide movement instructions to trains with AMS and to control trackside objects with AMS.
- The ***Safety Control*** layer includes the AMS Safety Logic and AMS Safety Manager to ensure that control of trackside objects and authorisations to trains are made safely. An additional Safety Manager service may be required to achieve higher Safety Integrity Levels and acceptance of the Redundant Safety Layer.
- The ***Object Abstraction*** layer with the AMS Data Aggregators records the state of all vehicles and objects across the network to be used by AMS systems and Interfacing systems.
- The ***Device Abstraction*** layer provides translating state demand into commands that are compatible with trackside objects via the AMS Fixed Object Transactor.
- The ***Device Control*** layer provides direct control of trains and objects – trains will have an AMS Trainborne system however there will be no modification to trackside object controllers.

Uniquely to an AMS system compared to the SR4.0 architecture, the AMS trainborne system also includes Safety Control as it is a decentralised system.

A high-level functional architecture identifies the integrations and interfaces with the SR4.0 architecture, each of which will be introduced within this section of the report. This can be seen in Figure 12.

FIGURE 12 – CURRENT SR4.0 ARCHITECTURE WITH RSL SUBSYSTEMS & INTERFACES INCORPORATED



A large version of Figure 12 is included in Appendix A.

The RSL Object Aggregation service is a key service to provide RSL in RSL Hybrid mode, however an API might be available from the APS layer to be queried directly by RSL Trainborne systems which might eliminate the need for this component. However, it will be required to support the AMS Workbench and connection to TMS anyway.

4.2 Subsystem Interfaces and Dependencies

4.2.1 Central Services

Advanced Protection System (APS)

Functionality on which AMS depends:

For RSL Active mode there are no functional dependencies.

For RSL Hybrid mode the APS needs to provide full safety logic and object aggregation as RSL will provide only a proxy-alternative for ETCS Movement Authorities.

Additional functionality required:

For RSL Active mode the APS system is required to provide a health status available that will notify the RSL that it is failed. It is expected that this will be provided via a RaSTA protocol connection which provides a health heartbeat every 300ms. Alternatively, this health status could be provided as a feed from the Central Diagnostics & Monitoring system.

For RSL Hybrid mode, the APS Object Aggregation needs to provide a movement permission for the train with failed a trainborne subsystem. This information needs to be available to the AMS Data Aggregator service for specific trains operating in RSL Hybrid mode.

For RSL Hybrid mode, the APS Object Aggregation needs to know if a train has RSL Hybrid active so that it does not see a train move without an active EVC and thus might otherwise force a shutdown for unsafe behaviour.

For RSL Hybrid mode, the APS Object Aggregation needs to know the location of the train. This can be provided by the AMS Data Aggregator service however it only needs to know this for the train that is operating in RSL Hybrid mode so it must be a subscription or query for the state of that specific train.

For handing back from RSL Active to APS as the safety actor, the APS must not generate a movement permission for a train that overlaps an Object that is still under the supervision of RSL in order to prevent points being moved under or against a train in motion that generated a movement permission by AMS. The status of the safety actor for an Object shall be provided via the AMS Data Aggregator for incorporation to APS Object Aggregation. The Object Controller will also have this requirement to provide an additional layer of protection against this safety hazard.

Traffic Management System (TMS)

Functionality on which AMS depends

The AMS system relies upon trains determining their own movement permission – to achieve this they need to know their destination, calling points and intermediate timing points from the Traffic Management System.

Real-time planning updates from TMS should be made available as a feed or API for the trains to query or subscribe to for understanding all the intermediate timing points on their journeys. *N.B. The TMS is not required to request a route for the train as route-setting is done by the train itself.*

The Traffic Management System must include which train is to serve which timetabled service so that the train can automatically retrieve the correct data – otherwise the driver must manually specify which train service the train is operating.

The Usage Restriction Area Management functionality of the TMS Plan Execution service must provide a feed to the AMS Data Aggregator such that the AMS system on initialisation does not route trains through track workers, flooding, livestock, landslide and other immediate hazards on the railway. (see 4.2.2 for more information).

Additional functionality required

If the Traffic Management System data is not available, then as a fallback the Workbench and Driver should have a capability to manually enter journey information.

For the Traffic Management System to continue to function effectively, the TMS must be capable of receiving train state and status from the AMS Data Aggregator.

To ensure that there are no traffic-jams or gridlock at junctions on the railway network, the AMS Object Control Manager should be able to receive a list that includes the order of trains to arrive at the junction so that the AMS Object Control Manager can permit or deny control requests from different trains.

Recommendation 10. If TMS is not able to include functionality for prioritisation of trains through junctions then additional scope should be added to AMS to include peer-to-peer negotiation, and development of autonomous train-based bottleneck optimisation algorithms as part of AMS.

Workbench

Functionality on which AMS depends

For RSL Hybrid the primary workbench should have the ability to instruct the APS that a train is using RSL Hybrid mode.

Additional functionality required

The dispatcher workbench will require a graphical user interface – this could be accessed via a web browser or dedicated application but will require human factors integration for the dispatcher desk and operating rules.

Single sign-on to the AMS Workbench, using cached session tokens, could mitigate against the risk of users forgetting their password and mitigate against IT login system failure.

A simulator and training will be required for dispatchers to understand how to use the AMS system and maintain their competencies.

Identity & Access Management

Functionality on which AMS depends

Each subsystem within SR4.0 is expected to use Public Key Infrastructure (PKI) for certificate-based authentication. Root Certificates are expected to be issued to all subsystems during installation/commissioning signed by a Root Certificate Authority used by all SR4.0 systems with Intermediate Certificate Signing Authorities used for layered protection of the Root Certificate Authority Server.

AMS expects to use these same processes for certificate-based authentication with interfacing systems within the SR4.0 architecture, and AMS will require its own signed certificates for its trainborne applications together with access to the Root Certificate to verify the authenticity of interfacing systems.

Additional functionality required

It is possible that during a failure of the APS system or safe data centre, that the Identity & Access Management Services are also unavailable. RSL should include a redundant Certificate Revocation List

that trains and objects can utilise to verify that all trains and objects and other central services remain authorised and trusted.

The dispatcher workbench shall have the capability to isolate trains and systems that are felt to have a security breach such that damage to the wider network can be contained.

Datacentres

Functionality on which AMS depends

AMS has central services that are expected to run in secure data centres. These could be the safety datacentres, or business-critical datacentres alongside TMS with lower SIL level, or a third-party hosted data centre.

SR4.0 Data Centres could provide power, backup power, physical security, networking, internet connectivity, cooling, fire protection, etc. The precise dependencies should be determined during detailed design.

Additional functionality required:

Only additional server capacity and performance monitoring is required to facilitate co-location of AMS servers.

TOPO4 and Data & Configuration Management

Functionality on which AMS depends

AMS uses topological data to generate safe movement authorities based on track distances, curvatures, gradients, clearances, etc.

The safe decision logic for complex junction interlocking is expected to also be part of the TOPO4 data. The data used in AMS is expected to be the same source as APS.

AMS will depend on being able to query the topological database in a way that facilitates its own safety logic and the topological data will need to include all necessary features for trains to generate a movement permission and control level crossings and points. At this stage it isn't expected that any data beyond that which is already required for APS is needed for AMS.

Additional functionality required:

AMS generates movement authorities on board the train itself as a decentralised system so it requires accurate and valid topological data – even when APS is unavailable. Topological data is expected to be digitally signed by the Identity & Access Management service, with a limited validity such that the data can be cached on board the train and verified.

AMS is one of several trainborne systems that depend on valid topological data so a service should be implemented on COAT that provides the caching function to make this data available to AMS such that each subsystem doesn't need to make its own cache of the TOPO4 data.

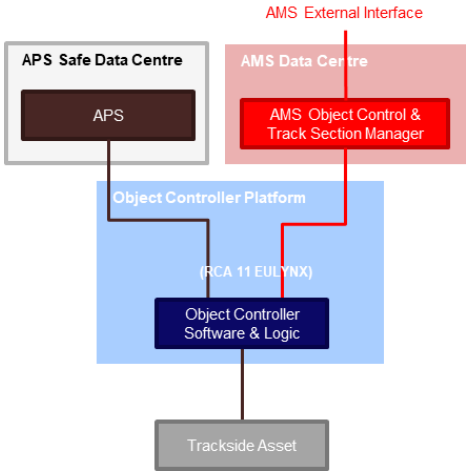
The Data & Configuration Management Service is expected to hold the true and correct versions of software and data configuration for all services, trains, objects, etc. As such it will need to also accommodate RSL data for deployment onto trains. Any third party hosted AMS services will need to interface with the SR4.0 Configuration & Data Management services.

4.2.2 Trackside Integration

Object Controller

Functionality on which AMS depends:

The feasibility study has not been able to get visibility of RCA Interface 11 (EULYNX) which will be the only interface for communicating with all Object Controllers however it is expected that AMS will need to utilise most of what is defined for RCA Interface 11 (EULYNX) for communicating with Object Controllers. AMS will do this by emulating the functionality of the APS Fixed Object Transactor. It is expected that APS will use RaSTA protocol to monitor the status of the APS connection.



An alternative architecture is offered in section 4.7 whereby the Object Controller can also host some central services of AMS for a fully decentralised system.

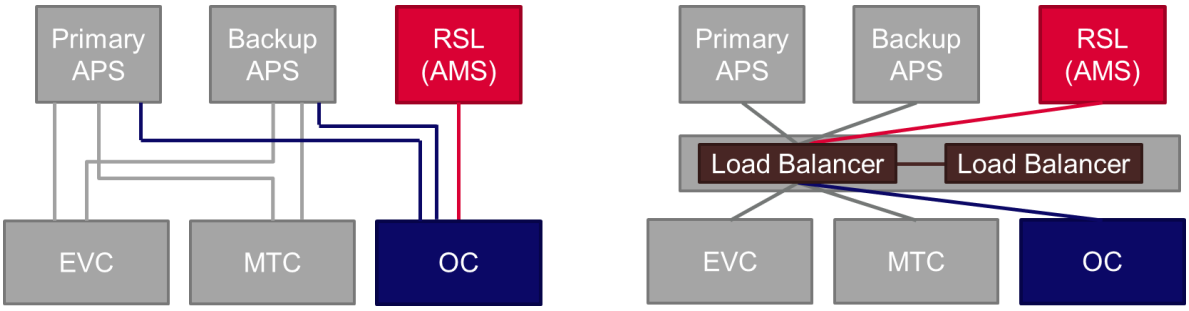
Additional functionality required:

The Object Controller must have the capability to communicate with multiple destinations: primary APS, secondary APS, and fallback safety layer. The Object Controller must only communicate with RSL when it has detected that ALL redundant APSs have failed. This connection could be facilitated in two ways represented in Figure 13:

- **Load Balancers between Object Controller and APS/RSL** (i.e. an automatic “Y-switch”) to enable automatic switching from primary to backups – however load balancers also need redundant architecture to avoid becoming another single-point of failure and handover from one Load Balancer to the other needs to be carefully considered. OC might have no means to know if it is communicating with APS or RSL to govern safe handover of safety authority.
- **Hard-coded IP Addresses** of Primary APS, Secondary APS and AMS Object Control Manager hard-coded into the Object Controller during commissioning. This approach makes it more difficult to achieve a resilient architecture for communication via multiple internet gateways and could mean that OCs need to be reconfigured during some configuration changes to APS/RSL, however it does eliminate the need for any other single points of failure. It might not be possible under the current EULYNX specification to achieve this.

Recommendation 11. This open point affects not only RSL but also TMS and MTC and any other services dependent on APS. This open point should be confirmed as soon as possible to inform designs for all service dependencies.

FIGURE 13 - ARCHITECTURE OPTIONS FOR HOW OC CONNECTS TO APS AND RSL (AMS)



AMS shall remain in control of the object until it authorises its own release – the APS shall be prohibited from demanding the state change of an object in case a train is approaching under AMS movement permission.

The Object Controller must "know" the state of the object that it controls so that if the APS link fails, and therefore the "demand" communication is no longer available, the existing response of "confirmed" includes an actual state such that AMS can understand the state of the railway.

Recommendation 12. The secondary safety layer communication link is crucial for RSL to interface with Object Controllers – it is a significant risk to the technical feasibility due to the standardisation efforts of EULYNX group outside of SR4.0. This should be incorporated into the SR40 OC programme scope as a matter of high importance.

Multi Object Controller

Functionality on which AMS depends:

The distributed Object Control architecture depends on RSL Object Control Safety Logic negotiating between each microservice (or rather, "automata") to provide safe interlocking of complex junctions. Within a Multi OC arrangement RSL must have the ability to address commands to specific Object Controllers contained within a Multi OC implementation.

Additional functionality required:

None required.

Trackside workers localisation and warning system

The scope for mobile personnel and vehicles providing localisation into APS has not been defined yet and as such this integration is hypothetical. Warning systems will not function correctly when APS is in a failed state but themselves should fail safe to warn vehicles and track workers that they are no longer under protection. Integration of these systems into AMS is not considered and would require further feasibility and development.

Functionality on which AMS depends:

No integration.

Additional functionality required:

Trackside workers localisation and warning system has no integration itself. AMS instead must integrate via TMS to retrieve data about trackside workers. AMS will accommodate mobile workers or vehicles as Usage Restriction Areas so that AMS trains cannot extend their movement permission into an area where trackside workers are located. The Usage Restriction Area will need to be manually removed by the dispatcher once he or she confirms that the mobile workers and vehicles are no longer on the railway.

4.2.3 Trainborne Integration

CCS onboard application platform for trackside related functions (COAT)

Functionality on which AMS depends:

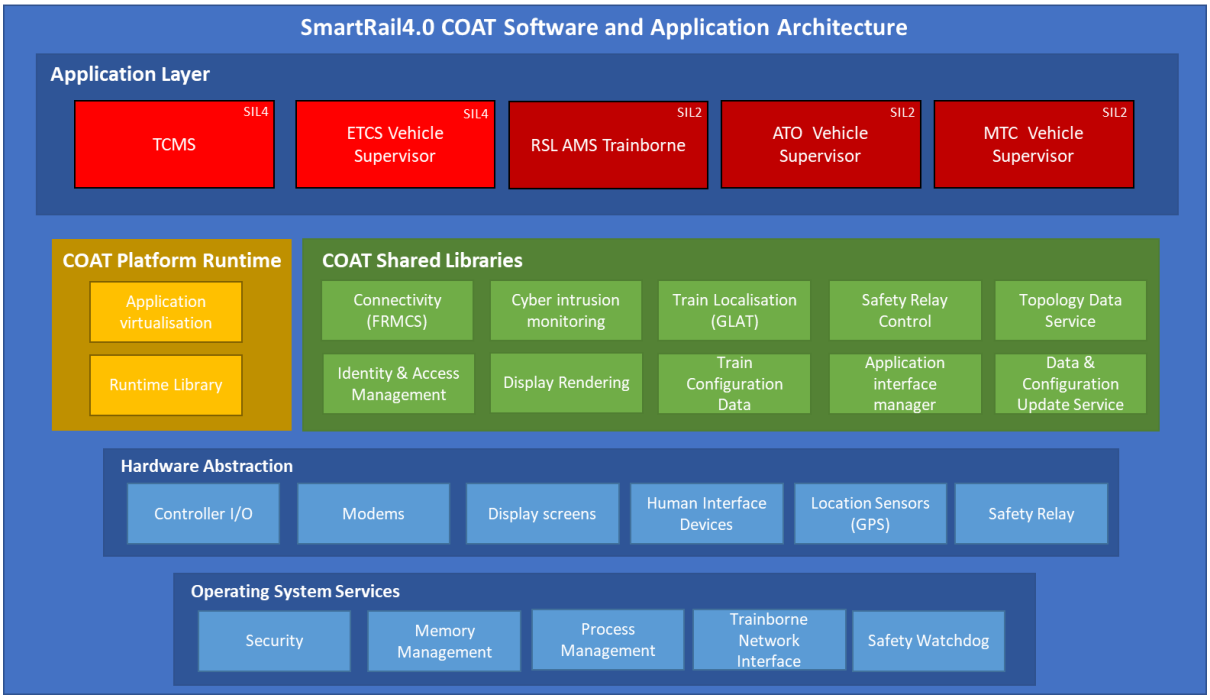
The COAT platform on board trains is still early in its definition - so the dependencies outlined in this feasibility study are supposing a COAT platform that includes the following key capabilities:

- Application Layer – where multiple applications of different SIL levels can be executed in parallel
- Platform Runtime Layer – for managing and containerising applications.
- Share Libraries Layer – for providing common services that are used by multiple applications and to enable interfacing with COAT platform hardware
- Hardware Abstraction Layer – for AMS Train Protection software to interface with peripheral subsystem controllers (TCMS), localisation sensors (GLAT), DMI, emergency brake, communications (FRMCS), and driver inputs, etc.
- Operating System Services Layer – for ensuring that applications and services execute in a safe and secure manner.

Additional functionality required:

It is assumed within COAT that the following services in Figure 14 are available for use by AMS to enable it to interface with all other SR4.0 trainborne services:

FIGURE 14 - COAT ARCHITECTURE AS UNDERSTOOD FOR FEASIBILITY STUDY



There are several COAT libraries which might not be envisaged under the current COAT strategy however if they could be made available the integration of AMS and other future systems will be more straightforward. These include:

- Topology Data Service – caching map data on the train and checking for new data periodically. The service should also include a method to verify the cached data is current before it is made accessible to other applications.
- Train Configuration Data – so that train lengths and wheel diameters don't need to be input into multiple systems (ETCS and RSL).
- Data & Configuration Update Service – for over-the-air trainborne software updates
- Identity & Access Management – so that each application can securely connect to remote SR4.0 services.

AMS also depends upon a method for applications to exchange data with each other. AMS must be able to understand the reasons for a failed ETCS Vehicle Supervisor so that AMS can seamlessly initialise when ETCS Vehicle Supervisor has entered a failed state.

COAT should also include a method for multiple applications to interface with Emergency Brake relay/controls and Traction Brake Isolate relay/controls. These relays/controls must be able to be overridden from one application to another when switching between ETCS control, MTC control, and AMS control.

Localisation / Generic Location Aware Toolbox (GLAT)

Functionality on which AMS depends:

AMS depends upon knowing where the train is on a node-vector map of the railway infrastructure – not simply its latitude and longitude or relative distance travelled. It is expected that this is provided as an output from the Trainborne Localisation system reconciled with TOPO4 data providing:

- Vector on which the train is on (between points A and B)
- Direction of travel (from A to B or B to A)
- Speed in metres per second along vector (A to B)
- Gradient
- Location precision (degree of error)
- Location confidence (sensors available and in agreement of location / SIL suitability level)
- Train Integrity status (including from end of train devices)

Additional functionality required:

It is not known fully what information will be provided by localisation as it is still in its definition stage undertaking technology trials. The following data would be preferable if included within Localisation:

- Rearward location of unit
- Rearward location of train when coupled
- Rearward location based on End-of-Train device (freight)

The following use-cases should be defined and understood by Localisation that AMS can confidently utilise the Localisation data:

- Localisation on cold start in depot/yard
- Localisation after reboot trackside
- Localisation on cold start outstabled in stations/sidings
- Localisation after plausibility error
- Localisation during implausible sensor data (Wheel slip/slide)
- Localisation with a single failed sensor
- Localisation at night
- Localisation in poor weather (snow / floods / fog / storm)

Additionally, to improve performance, the last location data shall be stored in Non-volatile memory for improved time to fix following reset.

Localisation should also include a redundant service on the COAT platform otherwise it risks becoming a common-mode failure risk for trainborne ETCS and RSL if it should fail.

Recommendation 13. A potential opportunity for improving localisation is if the trainborne localisation system knows what direction the junction is set in when the train passes over the junction. This

information would allow the train to quickly confirm which track it is on without the need for balises. This can be achieved via a feed from the central APS Object Aggregator or AMS Data Aggregator or could be introduced as a function from Trainborne AMS Train Protection system into the localisation system.

Recommendation 14. A further opportunity for localisation could be using the driver to validate which track the train is on when there's ambiguity – particularly after a plausibility error or restart of the system. On the DMI, the driver could be presented with a visual depiction of the track layout for the area they are in to be able to manually inform the localisation system which specific track the train is on.

Recommendation 15. To mitigate the risk of invalid map data further, SR4.0 Localisation project could consider introducing a mitigation against changes to topological data such that the first train to pass through a construction site, after it is handed back into operation, could feature a track geometry measurement system or forward-facing camera that is used to validate that the topology is correct.

Future Railway Mobile Communication System (**FRMCS)**

Functionality on which AMS depends:

The FRMCS concept, which abstracts the Application Layer from other OSI model layers, allows for solutions such as AMS to utilise whatever comms bearer networks are available.

FRMCS is expected to include multiple modems using different communications bearers and technologies such as LTE, 5G, Satcom and GSM-R – switching between appropriate bearers and applying appropriate Quality-of-Service management for different applications.

FRMCS is expected to run on COAT as a software-based router so that it can apply QoS to different applications without the need for separate physical network adapters to an external router.

FRMCS is expected to interface with lineside telecoms networks to demand appropriate QoS from their services.

Additional functionality required:

FRMCS should also include a redundant router on the COAT platform otherwise it risks becoming a common-mode failure risk for trainborne ETCS and RSL if it should fail.

Manoeuvre Train Control (MTC)

Functionality on which AMS depends:

Manoeuvre Train Control is expected to introduce a system to support additional train control use-cases that are not currently provided for under ETCS. It will achieve this through a separate in-cab system, either running on COAT or a "lite" hardware platform akin to a Tablet PC or iPad.

It is possible that if MTC is implemented on a “lite” hardware platform then RSL could integrate onto that platform as a standalone safety system for when all primary systems fail.

Additional functionality required:

No consideration has been made in AMS for how MTC could continue to operate using data from AMS. MTC is expected to receive authority directly from APS.

Recommendation 16. The use-cases that MTC addresses must therefore also be addressed within AMS or within degraded operating procedures.

EVC Vehicle Supervisor

Functionality on which AMS depends:

AMS should require the ETCS-based Vehicle Supervisor to be set to ETCS Level 0 to facilitate its activation using an AMS DMI and warning system.

Additional functionality required:

Alternatively the AMS could be utilised in ETCS Level NTC whereby the AMS gives a warning or EB command to the ETCS NTC interface – how this works via software on COAT as a generic interface to an ETCS onboard application requires further study in conjunction with EVC suppliers; this integration could be complex and require rework to existing suppliers onboard systems so it is not the preferred strategy for AMS at this stage.

ATO

Functionality on which AMS depends:

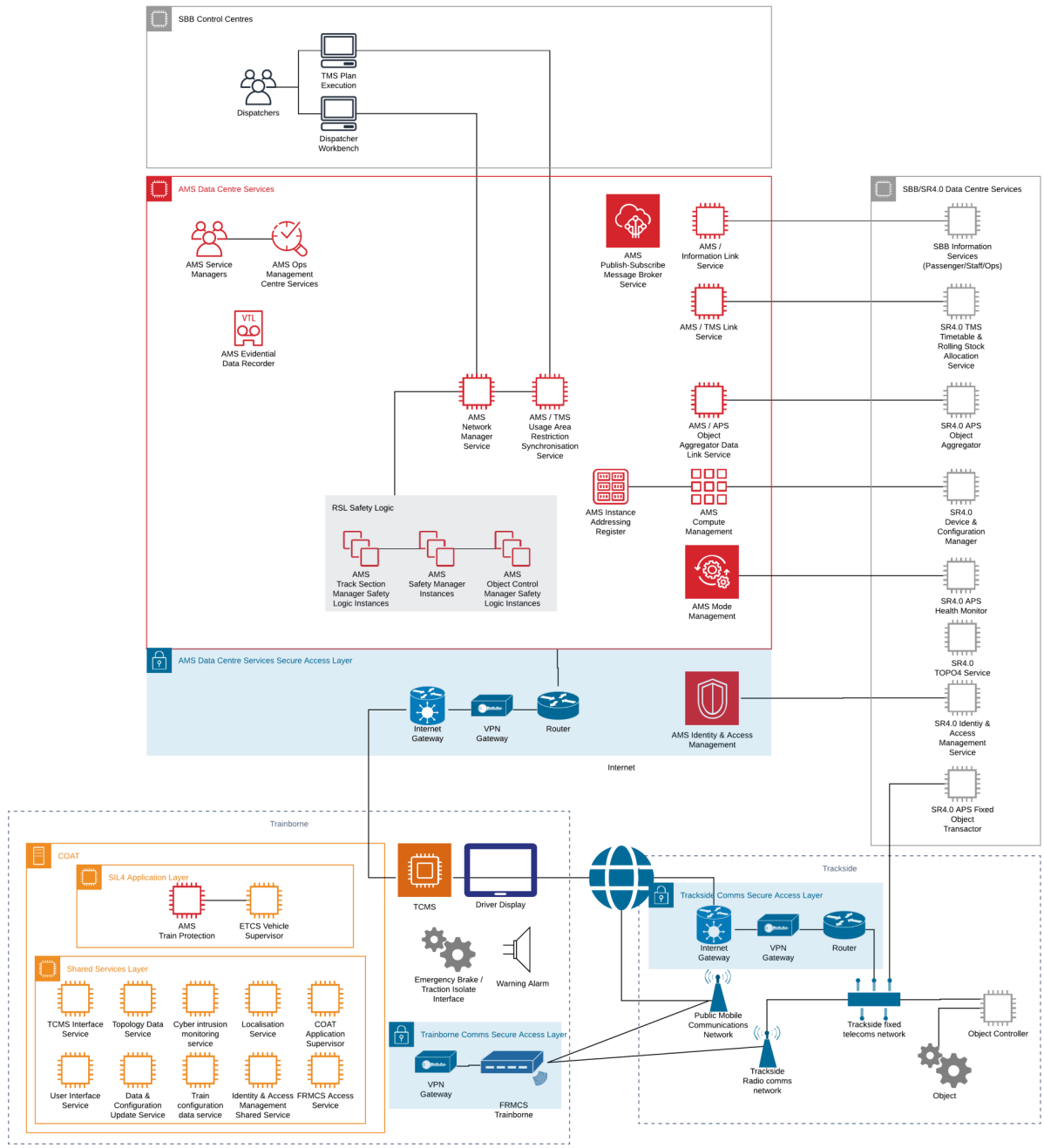
There is no integration envisaged between AMS and ATO however for GoA4 operation AMS provides a viable fallback solution so that GoA4 trains can continue to operate with an APS failure. Fallback ATO GoA4 functionality could also be incorporated into AMS if required with integration to traction, brakes and door controls.

4.3 Physical System Architecture

Using AMS for RSL enables its implementation as software-only, deployed upon existing SR4.0 components. However due to the architectural constraints of the OC platform within RCA and SR4.0, some safety-critical central computing services also need to be provided.

It is expected that the central computing services for AMS will be implemented using COTS servers suitable for safety-critical applications. These could be hosted in the SR4.0 Enterprise Data Centre which hosts the Traffic Management System for diversity, or a third-party location.

FIGURE 15 AMS PHYSICAL SYSTEM ARCHITECTURE



A large version of Figure 15 *is included in Appendix A.*

4.4 Cybersecurity Integration

AMS can use the same cybersecurity principles, connectivity, and assurance methods adopted for the primary signalling system, adopting the same identity & access management, hardware-based authentication, proactive intrusion detection and monitoring.

All system interfaces will be tightly governed and controlled within the overall SmartRail4.0 architecture.

The greatest vulnerability is unauthorised access to services running cloud processes in a shared processing environment and potentially compromising system states within memory. AMS shall encrypt its memory space and use containerised CPU processes to mitigate the risk of low-level interference with the system.

The integration of AMS into SmartRail 4.0 is designed such that it does not open any new vulnerabilities into the central services, object controllers, or trainborne systems, by ensuring that the primary CCS systems are responsible for activating the AMS system during failure – not the other way around.

A further risk arises from if/when the central identity management servers are unavailable – the certificate revocation list might be unavailable so trains and objects are not able to verify that a rogue train or object has been isolated on the network.

Recommendation 17. The next phase of the project should consider web-of-trust decentralised models for certificate revocation – or provide a backup certification revocation list server.

4.5 Handover between control areas

As the train reaches the end of an RSL area, the RSL will generate a movement permission up to the boundary and return to Standby mode. The driver must then activate the EVC again to gain a new movement permission from the APS for the next region.

It is expected that there is an overlap area for APS control of trains so that there is no requirement for the driver to request verbal authorisation from the dispatcher to drive on-sight into the new region.

If RSL is activated in multiple regions, and RSL is distributed with one RSL system per region (not necessarily required as it is designed to be a scalable central architecture) a train will simply cease transmitting its state to one AMS Data Aggregator service and begin transmitting to the next as it is generating its own movement permission.

4.6 Ad-hoc lineside communications network variant

If the AMS Safety Logic could be deployed onto a flexible trackside computing platform, it is quite possible that AMS could be implemented with a totally independent peer-to-peer radio network to operate without any connection at all to any central services or without base stations.

Two examples of peer-to-peer radio systems for providing collision warning systems include:

- Secondary warning system which provides a radio-based Train Collision Avoidance system using 400MHz band with secure frequency from 1km to 33km.
- Train Collision Avoidance System with range up to 2500ft

These systems are only designed to supplement existing safety systems and do not provide any control of points or level crossings, or dealing with unfitted trains, or hazards, or routing of trains through the network to their destination. Nevertheless, their communications bearers provide for an interesting

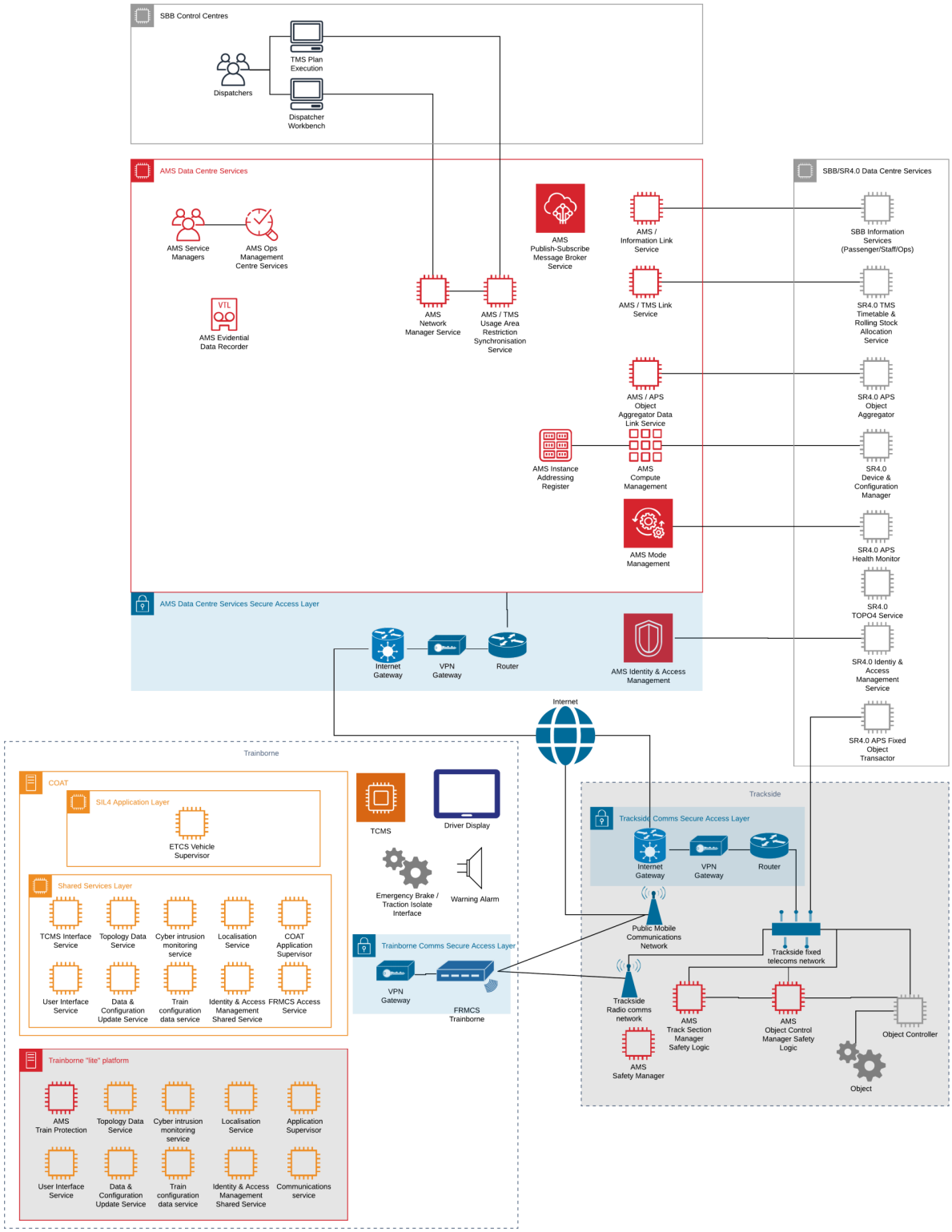
method to provide additional resilience to FRMCS to facilitate peer-to-peer data exchange between fitted trains.

4.7 Fully duplicated architecture with RSL for total CCS resilience

Trainborne and trackside considerations for a fully independent decentralised architecture are considered herein and costs for these parallel platforms are considered within the business case (available as a separate report) as an option to be considered for inclusion in the SR4.0 programme.

An alternative physical architecture for a fully duplicated and decentralised AMS system is shown in Figure 16 with additions to trainborne and trackside systems, and components removed from central services:

FIGURE 16 ALTERNATIVE PHYSICAL ARCHITECTURE WITH FULLY REDUNDANT PLATFORMS FOR TRAINBORNE AND OC FOR DECENTRALISED AMS

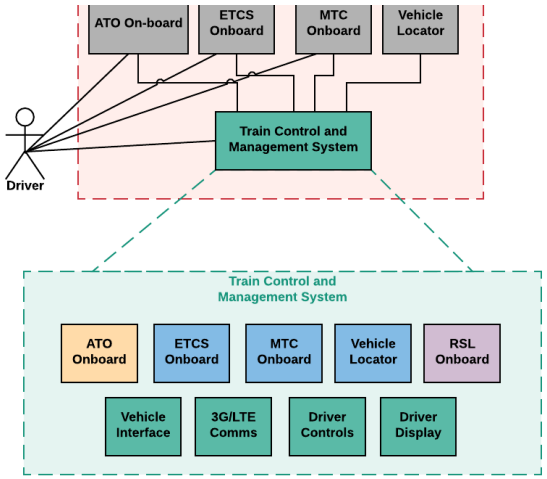


A large version of Figure 16 *is included in Appendix C.*

Trainborne considerations

It is anticipated, based on experiences of existing ERTMS-fitted railways, and verified by SR4.0 estimates, that 50% of all delay minutes and disruptions might be caused by trainborne subsystem failures on which the Redundant Safety Layer depends, such as COAT, Localisation, FRMCS, DMI, etc.

FIGURE 17 RSL AND PRIMARY BACKUPS DEPLOYED ONTO TCMS PLATFORM



To provide additional resilience for these, a “lite” version of these components could be replicated within RSL at a lower safety integrity level, however this could significantly increase the cost of RSL and undermine its business case. If such a system is to be provided for MTC however, it could provide an economical way of achieving this resilience once MTC is absorbed into the normal ETCS standard and is then a redundant in-cab platform available for use by RSL.

An alternative approach for providing a trainborne “lite” platform could be to utilise similar subsystems which are present within a modern TCMS platform such as localisation, communications, driver interface, etc., combined with application virtualisation to allow RSL to operate as software deployed on the TCMS. This could even be an option for the primary safety layer, e.g. ETCS onboard, to operate in a degraded mode.

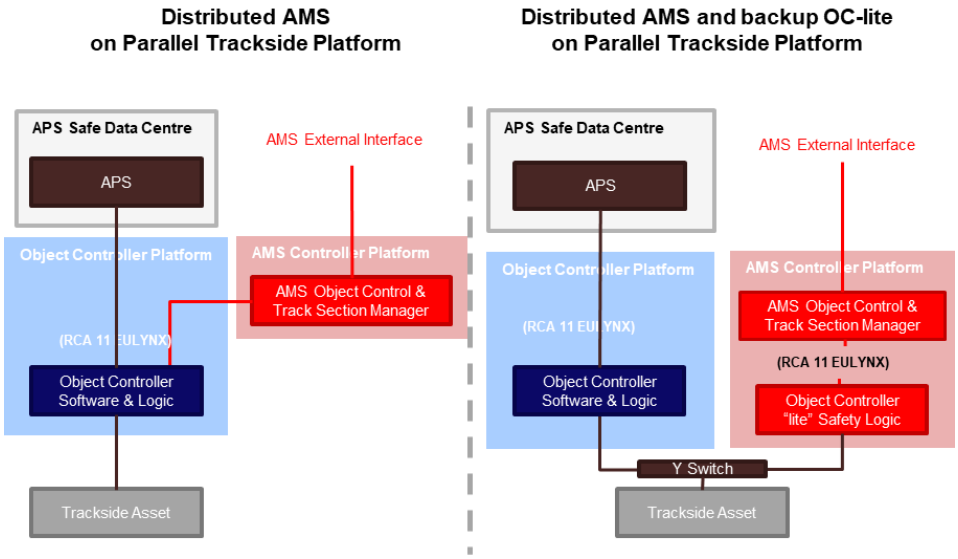
Trackside Object Control architectural considerations

Object Controllers are likely to be responsible for a significant proportion of CCS system failures due to the quantity of controllers to be deployed in the field.

The Object Controller functionality could be replicated onto a “lite” parallel system that also provides a computing platform providing resilience for OC failures. Additionally, this parallel platform could host AMS decentralised safety logic – eliminating the need for data centres for safety logic and retaining them only for operational efficiency for supporting the dispatcher workbench.

AMS on a parallel trackside platform could either interface with the existing Object Controller via RCA Interface 11 (EULYNX) or have a direct interface with the trackside asset, replicating all of the Object Controller logic within the “lite” platform with a Y-switch to provide the selection from primary system to backup. These two options are shown in Figure 18.

FIGURE 18 PARALLEL TRACKSIDE PLATFORMS ARCHITECTURE OPTIONS FOR RSL SERVICES

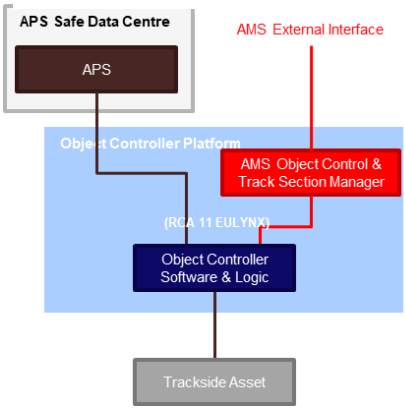


In the first Parallel Trackside Platform option, AMS functionality is external and hosted in the cabinet, transmitting commands to the Primary OC, which remains directly and solely connected to the object. This option has distributed processing (greater resilience) and still requires some additional capability within the Primary OC which would need to be specified but requires more equipment lineside (therefore potentially higher installation cost) and does not mitigate against OC failures itself.

The second Parallel Trackside Platform option duplicates the full functionality of the Primary OC lineside, and cuts into the safety-critical signalling loop between the Primary OC and trackside asset. This would be the most invasive fitment. For existing switches, this could be achieved, for example, with a simple latching relay. However, two key design issues exist with this approach. Firstly, the number of lineside objects (lights, barriers, object detection, sirens) to switch between controller in a typical level crossing implementation may render this approach impractical. Secondly, it is envisioned that in future, switch machine manufacturers will sell switch and OC as a 'matched pair' - no interface between the two is defined in OC specifications. Between the OC and AMS Object Control Manager, it would therefore be difficult to cut into this circuit to provide alternate means of actuation unless this interface was specified and standardised at procurement time, or a requirement was placed on the manufacturer to provide functionality within the switch machine for control by two independent OC's.

The Object Controller itself is presently outside of the scope of SR4.0 – only its interface is being specified under the EULYNX standardisation group which includes enhancements for extra envisaged functionality. However, the Object Controller itself is expected to be a proprietary platform with proprietary applications such that it is commercially and technically complex to integrate its functionality into a backup parallel system – as such, the study has decided that the primary method of interfacing with OC shall be RCA Interface 11 only.

FIGURE 19 DECENTRALISED RSL ON OC PLATFORM



The RCA Beta release includes a chapter on Platform Independence which quotes the following; this position cements the strategy not to incorporate AMS functionality into Object Controllers.

> "The object-controllers (with interface to "the real world") are likely to be physically more distributed than most other RCA components and probably don't benefit from a Platform Independence. I.e. OC are likely to be procured as "systems", including SW and HW."[7]

An idealised option for providing a truly decentralised system was initially envisaged as part of this feasibility study, whereby all RSL Central Services (Track Section Manager and Object Control Manager) could be hosted on Object Controller platforms in parallel to the Object Controller Safety Logic (see Figure 19). This would significantly improve the resilience of the RSL system by allowing continuous operation when all central services have failed – even AMS Central Services. This architectural approach is the preferred option when implementing AMS as a primary signalling system.

To implement AMS within the OC platform as an additional application would necessitate collaboration with OC equipment suppliers (Siemens, Thales, etc.) for them to adapt their systems to host multiple virtual applications, or to define precisely the AMS logic that must be integrated into their systems, and provide an additional non-EULYNX interface protocol specifically for AMS. Commercially this would result in OC equipment suppliers producing SR4.0 specific solutions reducing the cost efficiencies expected through collaboration across all EULYNX partners. Additionally, re-homologation of the OC might be required whenever there is an update to AMS logic making maintenance and support impractical.

The OC integration strategy that is being considered in the business case in this feasibility study considers the two options of Centralised AMS OCM services, hosted within a data centre, or on a parallel OC platform, both options communicating with the OC via RCA Interface 11 (EULYNX) only.

[7] Section 3, Page 7, "Where is platform independence applicable in RCA?" https://eulynx.eu/index.php/documents2/rca/rca-beta/238-rca-chapter-platform-independence/file

Recommendation 18. SR4.0 could consider engaging OC suppliers to embrace the flexible platform-independent computing platform strategy as being explored for COAT on trainborne, where multiple trackside applications could be satisfied via the same hardware running a variety of software from different suppliers, such as additional diagnostics capabilities for condition monitoring of assets, advancements in Level Crossing Obstacle detection with Radar/Lidar, 5G connectivity deployment, and future innovations not yet conceived.

5 Development Roadmap for AMS Introduction

Strategy for realising an AMS system within the SR4.0 programme

The AMS solution is a novel complex software-based system, but it is not complicated and its strategy for realisation is straightforward.

AMS is made up of basic components that follow simple rules. When these basic components are combined a huge amount of complexity emerges – but not in a bad way – in a way that creates possibilities for capacity, performance and resilience of the railway network. Just as a chess game has a few simple rules for each piece, but there are more ways the game can be played than there are atoms in the universe. (See Shannon Number[8])

Traditional command and control systems are much more complex through their central decision-making systems that need to consider all possible states of the railway network on each processing cycle. The available computing time and the complexity of designing such a logic system limits the potential of such centralised systems to realise the true capacity and performance of the railway infrastructure.

The guiding philosophy for AMS as a decentralised system is to enable order to emerge from chaos[9]. Its basic components use simple rules make its strategy for realisation rather more straightforward.

Integration with the wider SR4.0 programme and interfacing systems adds complexity. The strategy for realising the AMS system for RSL functionality is separated into these two tracts to mitigate the risk of integration until the novel concepts of AMS are proven.

5.1 Solution Development Roadmap

AMS has novel concepts for which the solution requirements cannot be fully understood until some development occurs. An iterative development roadmap is proposed which matures the understanding of AMS at each stage de-risking the investment and risk of unexpected change at later stages. The stages of development recommended are inspired by Technology Readiness Levels[10] widely used for managing innovation, these are:

- Stage 0: Concept Feasibility Study
- Stage 1: Proof of Concept
    - 1A: Paper Concept
    - 1B: Basic Experimentation
    - 1C Advanced Simulation

[8]See more information at https://en.wikipedia.org/wiki/Shannon_number
[9] For inspiration on concepts of emergence see: HOLLAND J. H. 1998. Emergence: From Chaos to Order. Addison-Wesley, Redwood City, CA.
[10]See more information at https://en.wikipedia.org/wiki/Technology_readiness_level

    - 1D Test Train Experiments
- Stage 2: Pilot Line
    - 2A: Pilot Line deployment and SR4.0 subsystem integration
    - 2B: Trial Running
- Stage 3: First Deployment

The iterative approach first addresses the most novel concepts of the system – through experimental development the approach understands any system risks that might necessitate a change of architecture, principles, or operating modes. Once the novelty risk is reduced, formal design and development will commence in Stage 2 and 3 which will involve formally defining and developing the system for full assurance in line with CENELEC EN50126.

A description of each stage is included in Table 11. The total duration of development is expected to be 5 years to prove the system in trial running on a pilot line. A staggered delivery approach is proposed in Figure 20 incorporating procurement activity to support the development.s

The following key systems and interfaces will need to be defined, and subsequently refined, throughout the project until stable definitions can be finalised during the initial deployment. Key systems include:

- Dispatcher Workbench
- AMS Network Manager
- AMS Track Section Manager
- AMS Switch Object Control Manager
- AMS Level Crossing Object Control Manager
- AMS Train Protection System - Trainborne Protection and Warning System

The timescales for the wider SR4.0 programme development are not available however the study has assumed that no subsystems will be available in stable form until Summer 2023 therefore the development strategy focuses on developing AMS concepts only until the SR4.0 subsystems become available enabling AMS development to be progressed in readiness for when the wider SR4.0 system and technologies mature and reach a state of readiness for integration.

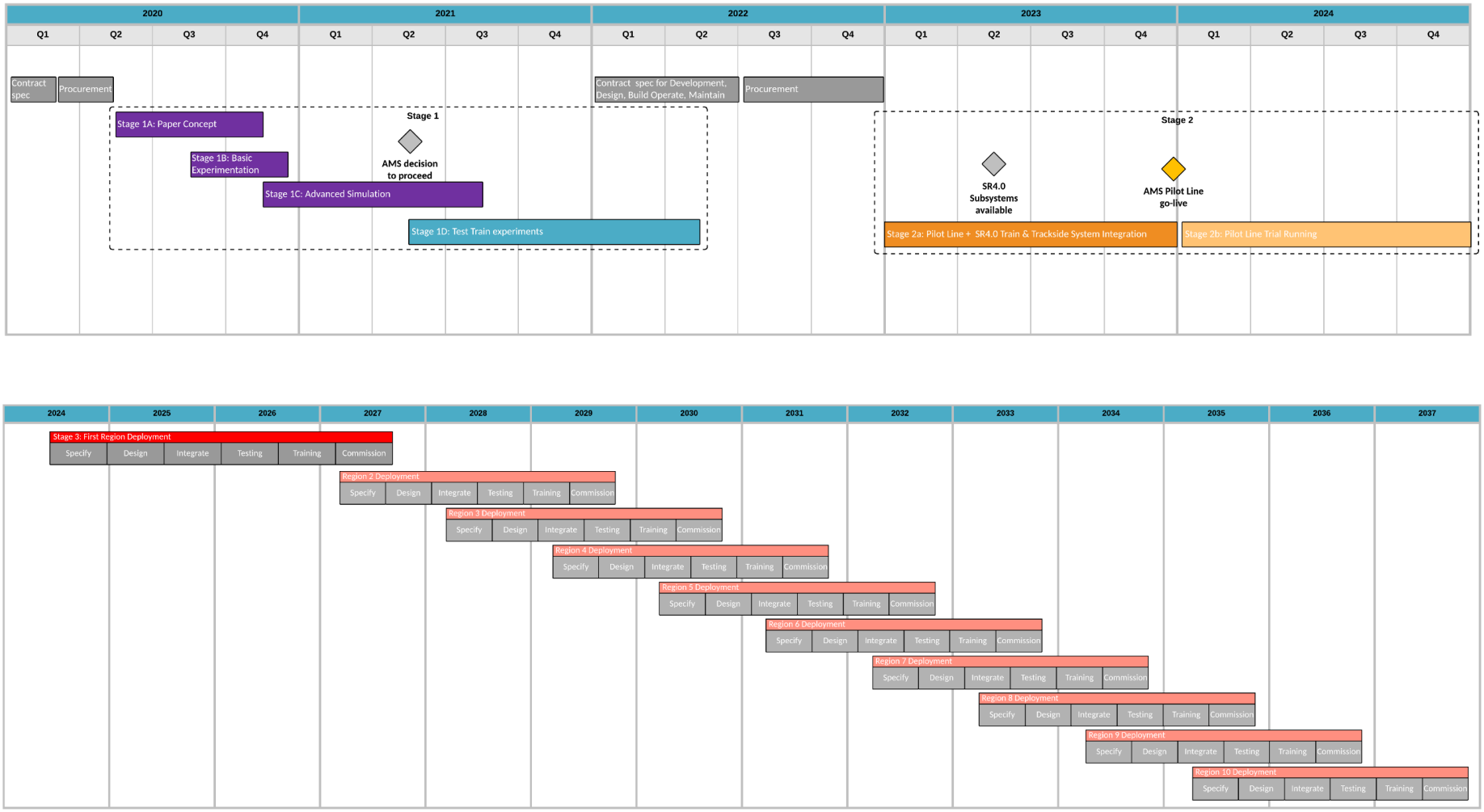
Initial integration with SR4.0 will happen during the Pilot Line deployment with the expectation that AMS will be implemented using platform subsystems from the SR4.0 programme including: COAT, FRMCS, and Localisation.

In parallel to Pilot Line deployment, AMS will finalise its interfaces into wider SR4.0 services including APS, Dispatcher Workbench, Information Services, TOPO4, Data & Configuration Management, Identity and Access Management, etc. Initial entry into service is envisaged for 2027 alongside the first segment enabled with SR4.0 systems.

TABLE 11 DEVELOPMENT STAGES

Stage	0	1A	1B	1C	1D	2	3
Title	Concept Feasibility Study	Paper concept	Basic experimentation	Advanced simulation	Test Train experiments	Pilot Line AMS overlay using SR4.0 subsystems	First deployment and full SR4.0 Integration
Location	Office	Office	Lab	Lab	Test Track	Pilot Line	Region
Description	Examining the business case and technical feasibility to determine whether to invest	Formalised system through detailed software description and detailed use-cases	To simulate key functionality and characteristics	Using robust software design and detailed simulation	Using illustrative hardware platforms to show system working on a test-track	First integration built on SR4.0 platforms & services but not integrated	First deployment as a redundant safety layer for fallback on APS.
Key risk addressed	Mitigates risks of unknown benefits of the system	Mitigates risks of unknown needs of the system	Mitigates risk of novel emergent behaviours	Mitigates risk of inadequate system performance	Mitigates the risk of train and infrastructure compatibility	Mitigates the risk of operational challenges in practice	Operational handover from APS to RSL through test activations
Duration (months)	3	6	4	9	12	12	18
Equivalent TRL	1	2	3	4	5 / 6	7	8 / 9

FIGURE 20 STAGGERED DEVELOPMENT ROADMAP FOR PILOT LINE VALIDATION WITHIN 5 YEARS



5.2 Solution Development Activities

5.2.1 Stage 1

The key activities for Stage 1 are represented in Figure 21. Because the AMS system relies heavily on emergent system behaviour once components are combined, it is recommended that design and experimentation progress simultaneously through agile development methods to quickly validate concepts. This will involve

1. Defining the expected behaviour of the subsystem
2. Modelling the expected behaviour
3. Developing an experiment to prove or achieve the expected behaviour
4. Executing simulations
5. Repeat above applying new understanding

A general system design will be available at the end of Stage 1 to inform the pilot line specification.

To gain greater stakeholder confidence in the solution, a test track experiment is envisaged with AMS operating on an isolated part of the railway network that is not in passenger service and isolated from other train services not involved in the test.

The safety review at this stage is enough to confirm the principles for test track operation. No software will be developed with any SIL rating although it will be designed robustly for subsequent quality and assurance to achieve SIL ratings at later development stages (if required).

5.2.2 Stage 2: Pilot Line

The key activities for Stage 2 are:

- Refining the system functionality and behaviour based on understanding from Phase 1.
- Software Quality Assurance towards SIL certification.
- Integration with SR4.0 subsystems (including prototype systems where necessary) including COAT, FRMCS, Localisation, Object Controllers).
- Design for trackside and trainborne deployment.
- Installation, Testing and Commissioning of trackside and trainborne systems.
- Generic Application Safety Cases for AMS system for Pilot Line.
- Specific Application Safety Cases for Pilot Line deployment.
- Development of manuals and training materials.
- Training pilot drivers and dispatchers.
- Homologation of the AMS system.
- Type approval of AMS trackside and on-board.
- Development of AMS training simulator for trainborne and control.

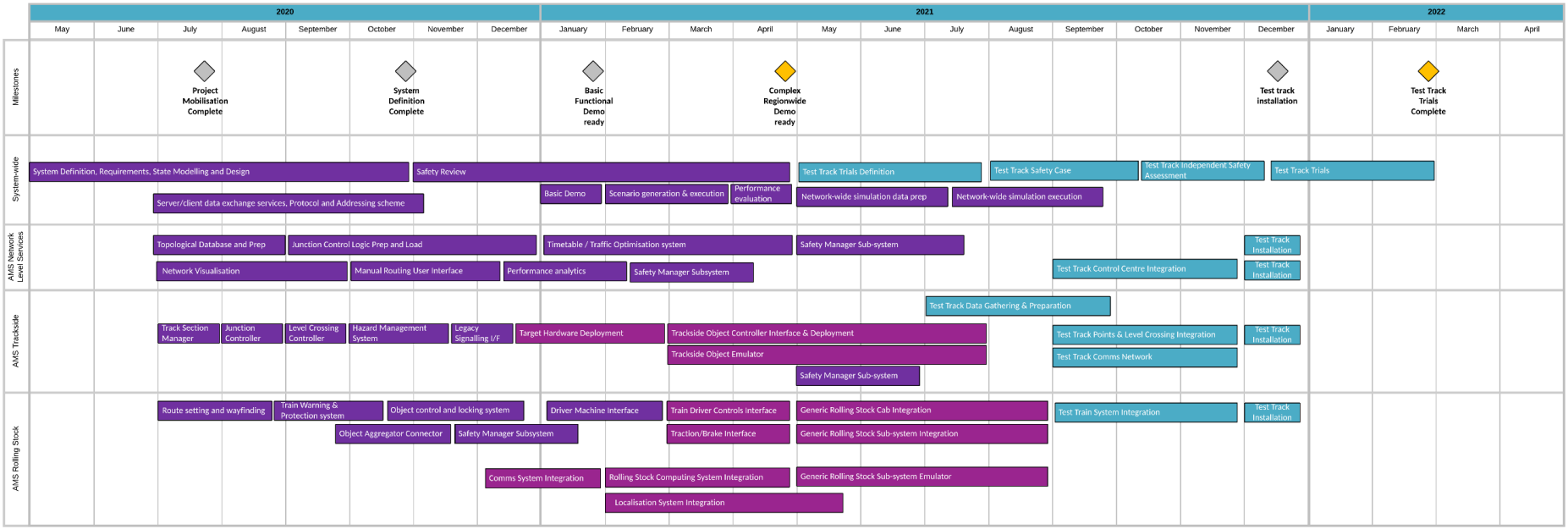
At the end of Stage 2, AMS will be fully understood, standardised, and ready for scaling across the SBB network.

5.2.3 Stage 3: Deployment across all regions

The key activities for Stage 3 are:

- Integration with all SR4.0 systems and services and legacy systems necessary for operational service (e.g. APS, TMS, Passenger Information, etc.).
- Design for trackside and trainborne deployment.
- Installation, Testing and Commissioning of trackside and trainborne systems.
- Specific Application Safety Cases for 1st deployment.
- Training all region drivers and dispatchers.
- Establishing support team including training
- Evaluation of operational performance and system performance.
- Stress-testing of AMS services.
- Trials of operational activation and system resilience.

FIGURE 21 STAGE 1 AMS DEVELOPMENT ACTIVITIES



5.3 Operation, Maintenance and Support Concept

Traditionally a railway safety-critical software system is procured as a hardware-based solution without on-going long-term support that can be self-maintained and serviced. Software-based systems require whole-life support due to the specialist skills and knowledge needed to define, design, build and assure software-based safety-critical systems.

The following key tasks are required to support the system throughout its life via a service contract which should be aligned with the current best practices used by the IT industry for data centre and cloud-based systems:

- Updates for core software for security patches, bug fixes, performance and stability improvements
- Root certificate access management for authentication
- Proactive monitoring to ensure the platform is operating in a stable state and not approaching the limits of the resources available to the software:
    - Power Supply voltage and current levels,
    - Processor usage,
    - Memory usage,
    - Storage utilisation,
    - Temperatures of components and platform,
    - Network Traffic for packet loss,
    - Virus and Threat detection,
    - Process monitoring to ensure availability for the software.
- Operating system updates for security, bugs, performance and stability improvements
- RSL Operational Capability Monitoring
- Defect Reporting and Corrective Action management
- Telephone Support & Site Attendance
- Technical Investigation
- Continuation of Homologation
- Technical Authority retention for supporting future change
- Obsolescence Management

The above activities apply not only to the core AMS services but also to the trainborne components and trackside controllers.

Additionally, the data centre facility(s) in which the software is operating should have adequate maintenance plans in place covering Climate control, Power Supply, Fire protection, Physical Security, Cyber security, Internet connectivity, etc.

Whether these activities are carried out by the AMS system supplier, or whether the solution is hosted and managed by SBB, will need to be determined during the next stage of the project however the

activities need to be done regardless and responsible parties should be clearly identified for supporting the system throughout its lifecycle.

5.4 AMS Safety assurance approach

5.4.1 Safety Integrity Level

The RSL will comply with the techniques and measures prescribed by EN50128:2011 for a SIL2 software, even if the subsequent safety analysis demonstrates that a SIL2 isn't required. Having a SIL2 software doesn't solve everything as a SIL level guarantees a low Tolerable Functional Failure Rate (TFFR), in the order of 10^{-7} failure per hour for SIL2 but doesn't exclude the occurrence of a failure.

5.4.2 Safety assurance process

The RSL project will comply with the SR40 safety documents (safety plan[11], safety policy[12] and subsequent documents) and requirements allocated to the project.

The following CENELEC standards are used to define the required safety assurance activities and deliverables across the lifecycle of the RSL project:

- EN 50126-1 (2017), Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
- EN 50126-2 (2017), Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
- EN 50128 (2011), Railway applications - Telecommunications, Signalling and Data Processing Systems - Railway Control Software and surveillance systems
- EN 50129 (2018), Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.
- EN 50159 (2010), Railway applications - Telecommunications, Signalling and data processing systems - Security relevant Communication in transmission systems.

The following deliverables will be produced as a minimum:

- Safety plan
- System Definition
- Risk Assessments: Interface Hazard Analysis (IHA), Functional Failure Analysis (FFA), OSHA…
- Hazard Record
- Safety Requirement Specification
- Safety Related Application Conditions
- Safety requirement validation plan
- Safety requirement validation report

[11] Safety Plan - SmartRail 4.0 version 1.0 (Anlage FQT_07)
[12] SR40 Safety policy version 1.0 (Anlage FQT_14)

- Safety Cases
- Independent Safety Assessment (ISA) Plan and Report (if required)

The RSL is not required to be compliant to the Technical Specification for Interoperability (TSI). However, it might use Interoperability Constituents in its architecture.

5.4.3 Safety targets and requirements

In cooperation with the SR4.0 programme safety team the Tolerable Hazard Rate (THR) and safety requirements will be defined and the RSL will have to comply with.

A balance between RSL operational speed and safety requirements will be sought. This will be done by using the THR, the RSL operational scenarios, and potential consequences of accident at various speeds. The project will allocate the THR to the RSL functions for several potential RSL speeds.

Until these safety requirements are specified, the RSL team will use the CSM design targets to carry out early SIL determination. At this stage and as the RSL is not in constant use nor used at line-speed, it is assumed that the RSL will not be implementing function more than SIL2. The only function that might carry a higher SIL level is the segregation and transition between primary signalling and RSL.

Whatever the outcome of the safety analysis, the RSL software and system will apply the techniques and measures specified for SIL2 functions in the CENELEC standards. This will ensure some flexibility if the use of the RSL is extended in the future. However, SIL2 ISA certification might not be included.

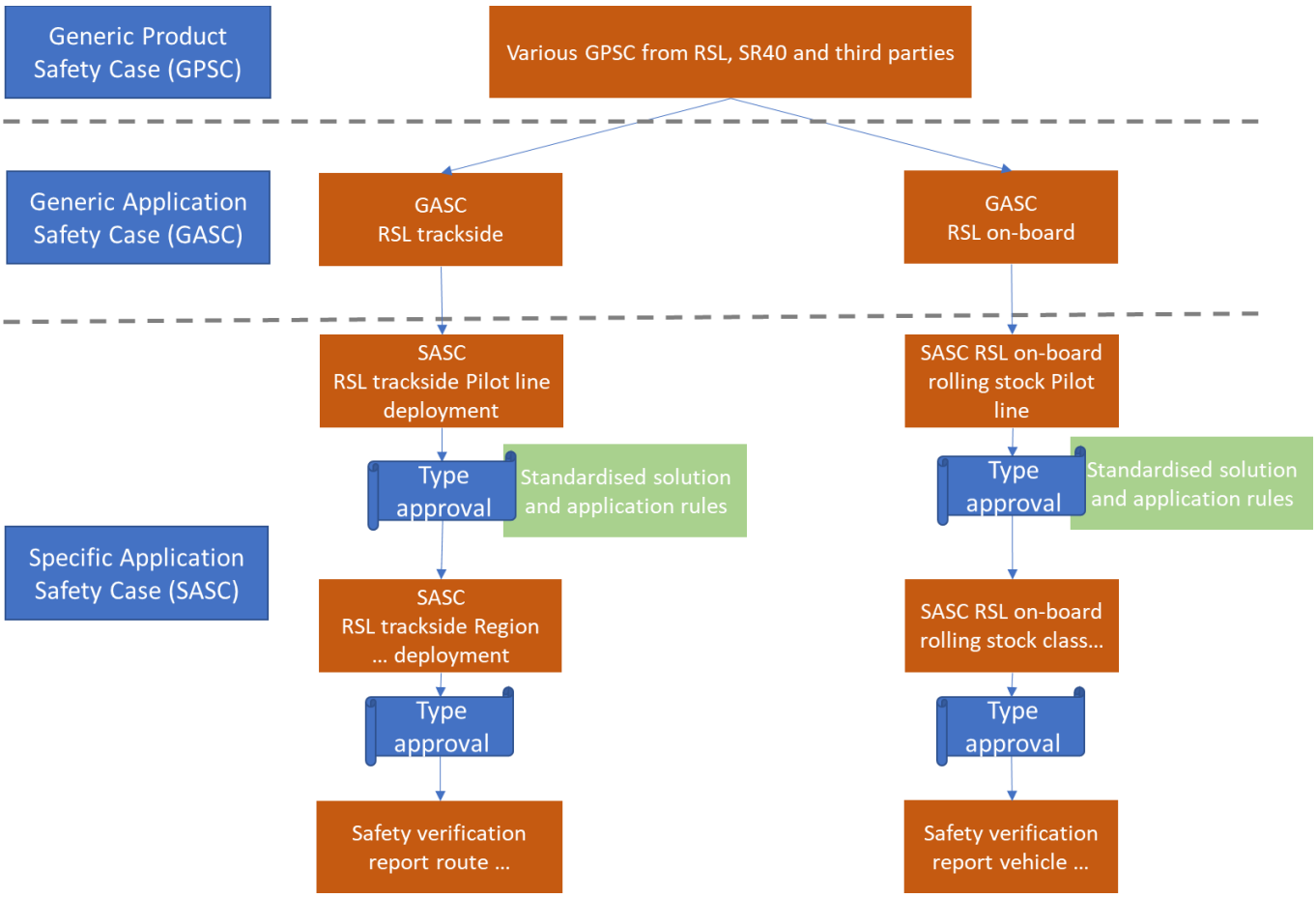
5.4.4 Safety cases

The safety cases will be divided between generic products, generic application and specific applications as defined in EN 50129.

The figure below provides the safety cases architecture for the implementation of the RSL. Following Federal Office of Transport (FOT)[13] guidelines, type approval will also be sought to reduce the amount of certification required.

[13] Bundesamt für Verkehr - BAV

FIGURE 8 – SAFETY CASES ARCHITECTURE AND TYPE APPROVALS



Generic Product Safety Cases (GPSC) will be available for some of the components of RSL from SR4.0 or from third-party for bought in components. A smaller number of GPSC might be produced by the RSL team.

Two Generic Application Safety Cases (GASC) will be produced: one for trackside and one for on-board. The integration of the on-board with trackside will be covered by the trackside GASC.

Specific applications safety cases (SASC) will also be divided between trackside and on-board. The SASC will be focused on the configuration of the system for the specific application, the closure of the Safety Related Application Conditions (SRACs) identified at generic application level and ensuring that all stakeholders, but mainly the operator, can operate and maintain the system safely.

For the Pilot line trackside, a SASC will be produced. This SASC – RSL trackside Pilot Line deployment will be the basis for the RSL trackside type approval. For each regional deployment, a SASC might be produced at region level in order to get the regional solution to be type approved and then a safety verification report for each route will ensure that the application complies with the scope of the type approval. This might not be required, if the regional implementation fully comply with the type approved RSL solution, only safety verification reports will be produced.

For Pilot line on-board RSL, a SASC will be produced and will support type approval of the RSL on-board. Then for each rolling stock class, the First in Class (FiC) implementation will be covered by a SASC – RSL on-board – rolling stock class… which will be used to obtain type approval for the RSL on-board for this rolling stock class. For each train within the class, safety verification report will be used. But for a different rolling stock class, a new SASC will be produced and a new type approval sought.

5.5 Application Lifecycle

The SBB AMS solution will be a novel system – a first-generation solution.

Even if AMS is successfully implemented on the SBB network it is likely that any supplier would use their experience developing the system to make significant changes on future deployments in other countries – the second-generation solutions.

The AMS solution procured by SR4.0 could be unattractive for suppliers to support longer-term once their focus is on new customers and markets; responsiveness to SBB could suffer despite Service Level Agreements.

The AMS system should be procured for an installed lifecycle of 20 years, with an initial enhancement update after 3 years once SBB has some experience of using the AMS to include any necessary changes.

A mid-life update is then expected after 10 years to improve any performance challenges and eliminate any obsolescence risks in the system.

Decommissioning (if and when required) simply requires disabling the AMS systems however additional costs will be required to reconfigure TMS, APS, and OC etc., so that they do not communicate with the existing AMS system and instead communicate with its replacement system.

5.6 Review of existing solutions and Intellectual Property

It is not appropriate for the authors of the report to comment on competitors' technology within this feasibility study.

Recommendation 19. A thorough market review should be undertaken of traditional suppliers and potential market disruptors to understand technologies available on the market and in development.

Full development of the system might not be required by SR4.0 as companies might already have technology that could be adapted to suit the needs of AMS.

- **Peer-to-peer radio warning systems:** existing solutions such as train collision avoidance system and secondary warning systems today don't have capability for trackside object control and incorporating Usage Restriction Areas - but these systems could be extended to include such capabilities.

- **Decentralised / Distributed CBTC systems:** these are not necessarily designed for scalability to national network coverage but could be rearchitected to become scalable.
- **Tram control systems:** might not be resilient enough or scalable enough for nationwide deployment but could be re-engineered to add resilience and assurance.

Existing intellectual property such as patents can be a barrier to innovation if a supplier is appointed who doesn't have the ability to licence or exploit any necessary patents required for an AMS solution. A supplier might discover part way through that their solution is not feasible, blocked by existing patents.

Recommendation 20. SR4.0 should undertake a worldwide intellectual property search to de-risk procurement by understanding Intellectual Property rights that might hinder or constrain the development of AMS.

6 Conclusion

6.1 Feasibility Assessment

Over 12 weeks this feasibility study has reviewed existing published SR4.0 documentation, held interviews with 25 SR4.0 team members including analysts, managers, engineers, and directors.

The study has considered:

- **Operational Feasibility:** when a fallback system should be used, how it will be activated, and what improvement it will have on the train service during disruption
- **Technological Feasibility:** whether an AMS system can be conceived that would provide safety for train movements and control of trackside assets.
- **Integration Feasibility:** whether the AMS system can work within the SR4.0 architecture, dependencies on other systems, and modifications necessary to other systems to facilitate the AMS being deployed
- **Development and deployment Feasibility:** whether a system can be developed and trialled in line with the SR4.0 programme
- **Economic Feasibility:** if there is a business case based on estimated costs and benefits of the system.

The following feasibility conclusions are made based on the findings of each part of the study:

6.1.1 Operational Feasibility of a Redundant Safety Layer

The feasibility study has first considered whether it is necessary to consider a Redundant Safety Layer within the SR4.0 architecture and what failure modes it should address.

The SR4.0 system design already features high levels of availability with resilience-by-design and redundancy in most systems with diverse technologies available: e.g. Localisation utilising GPS, Balise, Tacho, Doppler etc., and FRMCS using LTE, GSM-R, Satcom, etc. The resilience of these systems negates the need for an RSL to replicate their functionality and instead RSL can depend on those subsystems being available.

Whilst Trackside Object Controller Failures and Trainborne Failures are expected to fail much more frequently, their failures can be mitigated through operating rules; a single failed train can be instructed verbally to drive on-sight without automatic train protection and trackside assets will continue to be used in their failed state or trains will be re-routed around them; there is no safety risk necessitating an RSL.

However, for operational resilience it is possible that an RSL could be introduced that also provides a fallback for trainborne system failures and trackside object controller failures through providing a parallel suite of hardware and software on train and trackside to mitigate failures with these elements.

Consideration has been given to the automatic activation of RSL when the APS has failed and this is accommodated within the trainborne systems, central systems, and object controllers however it will require change to the primary system functions to enable the failover to RSL.

The study has concluded that an RSL is operationally feasible and will provide a reduction in disruption from primary system failures; its focus should be on providing a resilient fallback system for failure of the central safety-critical systems and its enablers within the SR4.0 architecture: the APS, Safe Datacentre, Enterprise IP network and Application Platform, and TMS (Plan-Execution) functions .

6.1.2 Technical feasibility of an Autonomous Movement Supervision system

An Autonomous Movement Supervision (AMS) system has been devised with a highly resilient architecture that enables continuous train protection when central systems have failed within the SR4.0 architecture.

The feasibility study has concluded that an Autonomous Movement Supervision system can be developed and introduced to provide safe protection of trains in degraded scenarios, operating initially at on-sight speeds 40km/h and then up to a safe maximum speed (beyond line of sight) as determined by a detailed safety assessment. An Autonomous Movement Supervision system will fully satisfy the needs of a Redundant Safety Layer.

In addition to the feasibility study, the authors have previously simulated many of the basic concepts in earlier development prototypes which share enough similarities with the AMS concepts that the authors are confident of the feasibility of the system design.

6.1.3 Integration feasibility with SR4.0 architecture

Each SR4.0 subsystem has been reviewed as part of the feasibility study where AMS has dependencies. Additional functionality has been identified for most systems to facilitate handover to AMS and hand back to APS – in most cases this is minor (e.g. data feeds), and integration is considered feasible.

However, the full integration is feasible if, and only if, the Object Controller interface protocol (EULYNX) can be developed further to require Object Controllers to communicate with a Redundant Safety Layer as a backup system when it detects its link to APS has failed. If it is not possible to introduce this functionality to the Object Controller then an additional component, an automatic “Y-switch”, will be required to sit between the APS and Object Controller to fail over to AMS – a change to the SR4.0 architecture. This is necessary for any RSL solution that mitigates APS failures – not just for AMS.

6.1.4 Development and Deployment Feasibility

The feasibility study has analysed the development effort required to realise the AMS system and integrate it into the SR4.0 wider systems, and then roll out across the whole SBB railway network.

AMS is a highly novel system based on new concepts not used before in train control for a large-scale mainline railway (although analogous technologies exist and similar concepts have been explored by several companies and academic institutions).

AMS requires a phase of proving its concepts as a train control system which should be done as early as possible to validate the concepts before making strategic decisions to commit to deploy as a core component of SR4.0.

A two-year Development programme is proposed that develops a paper concept, a basic software proof-of-concept, then an advanced simulation for a whole region, and then installs onto a test train and test track to prove in cab with user feedback. This is envisaged to conclude in mid-2022, with an initial decision to proceed in mid-2021 once results from the region-wide simulation are available.

A further two-year development programme is envisaged to trial AMS on a pilot line, expected to be a branch line with 6 trains and 20 track switches and/or level crossings to interface with. The pilot line is expected to utilise SR4.0 subsystems such as Localisation, COAT, and FRMCS as they become available. This phase will run throughout 2023 and 2024 with the first year for robust design and assurance, and the second for trial running on the pilot line to understand how the system works in operation.

Roll-out across the SBB network is envisaged with the first commissioning in 2027 through to 2037 concluding that it is feasible to develop a novel AMS system to integrate with the overall SR4.0 deployment programme.

6.2 Next steps

The conclusion of this feasibility study is that development of AMS moves forward to the next stage of development through to proof-of-concept and test train fitment, with critical go/no-go gateways at each stage of the development, revalidating the business case, and with tight control of costs and risks to ensure the business case is not undermined by the narrow budget available for the development and through-life operation of AMS.

Progress can be made irrespective of whether OC connects directly to AMS or via a load balancer however this uncertainty should be resolved as a high priority to ensure that a solution is available for AMS (and secondary APS) to use.

SR4.0 should immediately commence a specification for the development of AMS and undertake a supplier selection process to choose a development partner to work with them to develop AMS through to test train fitment in order to commence development from Spring 2020.

6.3 Risks

As with any solution at a low TRL, the risk profile is relatively high as there’s a lot more work to do and many unknowns to work out. However, none of them seems unsurmountable if the RSL supplier and the SR4.0 work collaboratively and openly. This is the behaviour that was observed during this feasibility and the study concludes that all issues and unknowns can be resolved efficiently.

6.4 Summary of recommendations

Recommendation 1. RSL should incorporate functionality that mitigates against failures to supporting services to the APS, such as Topological data server, Identify & Access Management servers, and Data Centre Services; each of these currently could be a single-point failure mode to the APS system.

Recommendation 2. RSL should be utilised when multiple trains in a region fail simultaneously due to systematic issues such as misconfiguration of the ETCS logic or a failed software update (e.g. a new version of GSM-R corrupting telegrams to/from trains).

Recommendation 3. If the planned reliability/availability of the Object Controller has such a high potential impact on the railway that it necessitates a redundant Object Controller, then a “Lite” version of the Object Controller should be considered that interfaces via the primary CCS safety layer rather than instructing all trains to use RSL for a specific area. This would be done to mitigate against the risk of synchronisation issues occurring between the primary CCS safety layer and RSL.

Recommendation 4. If a fully independent RSL system is preferred, then each existing SR4.0 subsystem project should be extended to consider a “lite” version of its solution for degraded operation that could be incorporated into RSL.

Recommendation 5. RSL shall only become the safety actor responsible for generating movement authorities for trains if the train has detected the APS has failed AND the RSL Core Services have detected the APS has failed.

Recommendation 6. RSL control areas must be aligned to APS control areas so that there is no possibility of mixed safety responsibility for an area.

Recommendation 7. The hand back from RSL to EVC requires a functional change to onboard EVC to avoid hard emergency braking when the primary systems come back online - this should be considered under future TSI updates.

Recommendation 8. Operating procedures for the initialisation of ETCS and APS, when restoring service after use of RSL, must be based on a comprehensive safety risk assessment based on thorough modelling of all potential scenarios.

Recommendation 9. RSL, in standby mode, should maintain a synchronised copy of the URA register contained within the primary Dispatcher Workbench or Traffic Management System to improve the validity of its movement authorities upon initialisation.

Recommendation 10. If TMS is not able to include functionality for prioritisation of trains through junctions then additional scope should be added to AMS to include peer-to-peer negotiation, and development of autonomous train-based bottleneck optimisation algorithms as part of AMS.

Recommendation 11. This open point affects not only RSL but also TMS and MTC and any other services dependent on APS. This open point should be confirmed as soon as possible to inform designs for all service dependencies.

Recommendation 12. The secondary safety layer communication link is crucial for RSL to interface with Object Controllers – it is a significant risk to the technical feasibility due to the standardisation efforts of

EULYNX group outside of SR4.0. This should be incorporated into the SR40 OC programme scope as a matter of high importance.

Recommendation 13. A potential opportunity for improving localisation is if the trainborne localisation system knows what direction the junction is set in when the train passes over the junction. This information would allow the train to quickly confirm which track it is on without the need for balises. This can be achieved via a feed from the central APS Object Aggregator or AMS Data Aggregator or could be introduced as a function from Trainborne AMS Train Protection system into the localisation system.

Recommendation 14. A further opportunity for localisation could be using the driver to validate which track the train is on when there's ambiguity – particularly after a plausibility error or restart of the system. On the DMI, the driver could be presented with a visual depiction of the track layout for the area they are in to be able to manually inform the localisation system which specific track the train is on.

Recommendation 15. To mitigate the risk of invalid map data further, SR4.0 Localisation project could consider introducing a mitigation against changes to topological data such that the first train to pass through a construction site, after it is handed back into operation, could feature a track geometry measurement system or forward-facing camera that is used to validate that the topology is correct.

Recommendation 16. The use-cases that MTC addresses must therefore also be addressed within AMS or within degraded operating procedures.

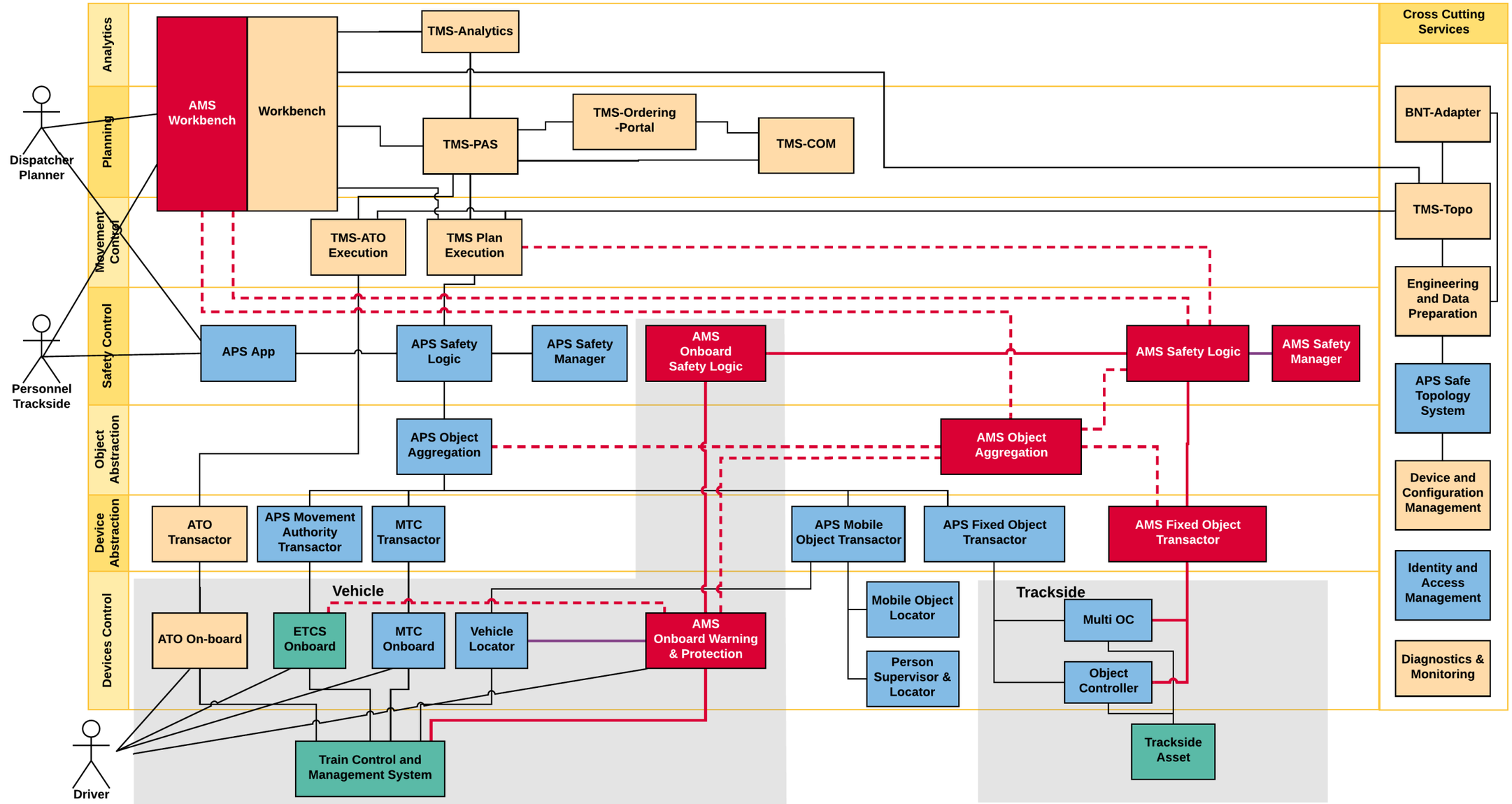
Recommendation 17. The next phase of the project should consider web-of-trust decentralised models for certificate revocation – or provide a backup certification revocation list server.

Recommendation 18. SR4.0 could consider engaging OC suppliers to embrace the flexible platform-independent computing platform strategy as being explored for COAT on trainborne, where multiple trackside applications could be satisfied via the same hardware running a variety of software from different suppliers, such as additional diagnostics capabilities for condition monitoring of assets, advancements in Level Crossing Obstacle detection with Radar/Lidar, 5G connectivity deployment, and future innovations not yet conceived.

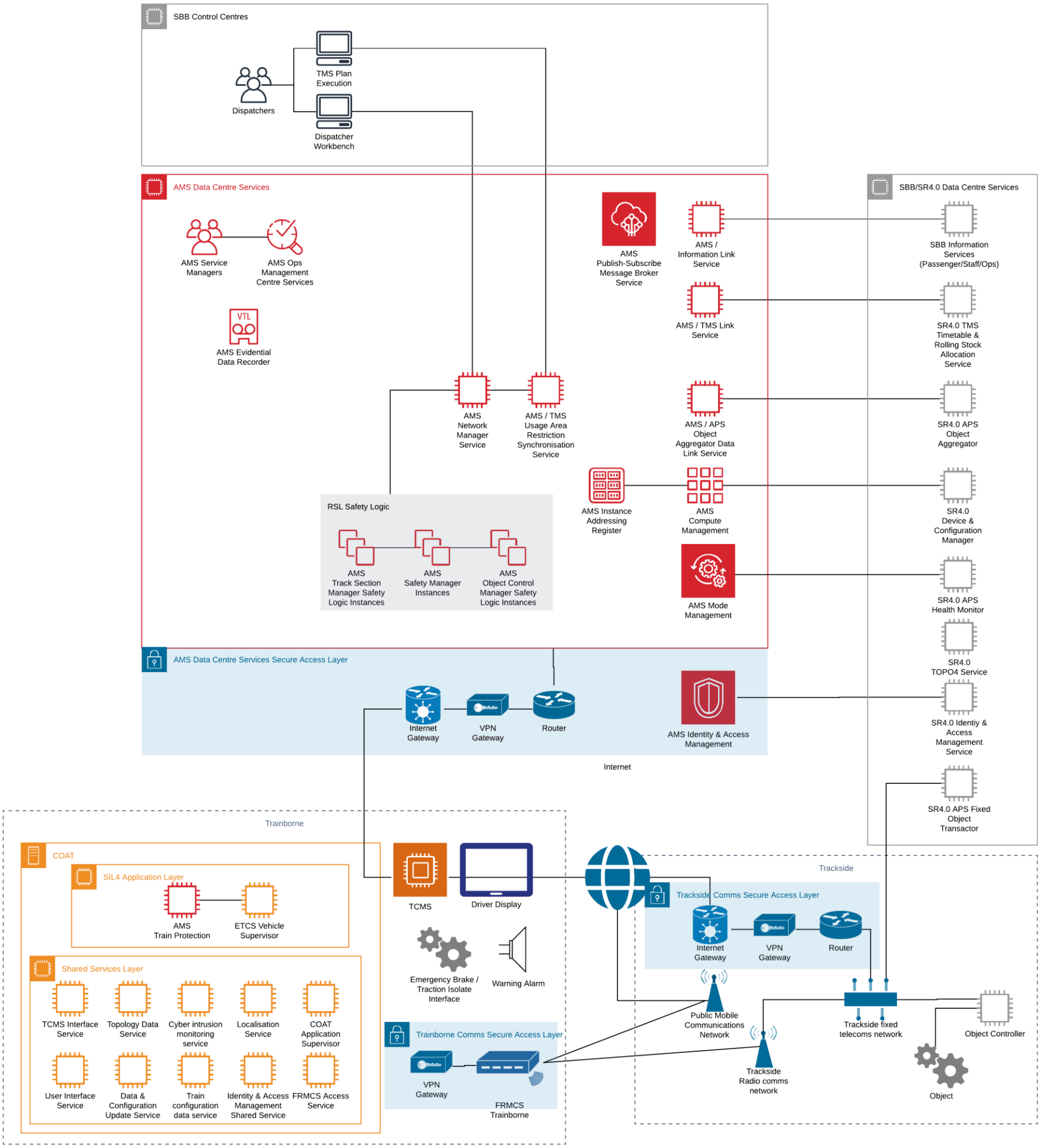
Recommendation 19. A thorough market review should be undertaken of traditional suppliers and potential market disruptors to understand technologies available on the market and in development.

Recommendation 20. SR4.0 should undertake a worldwide intellectual property search to de-risk procurement by understanding Intellectual Property rights that might hinder or constrain the development of AMS.

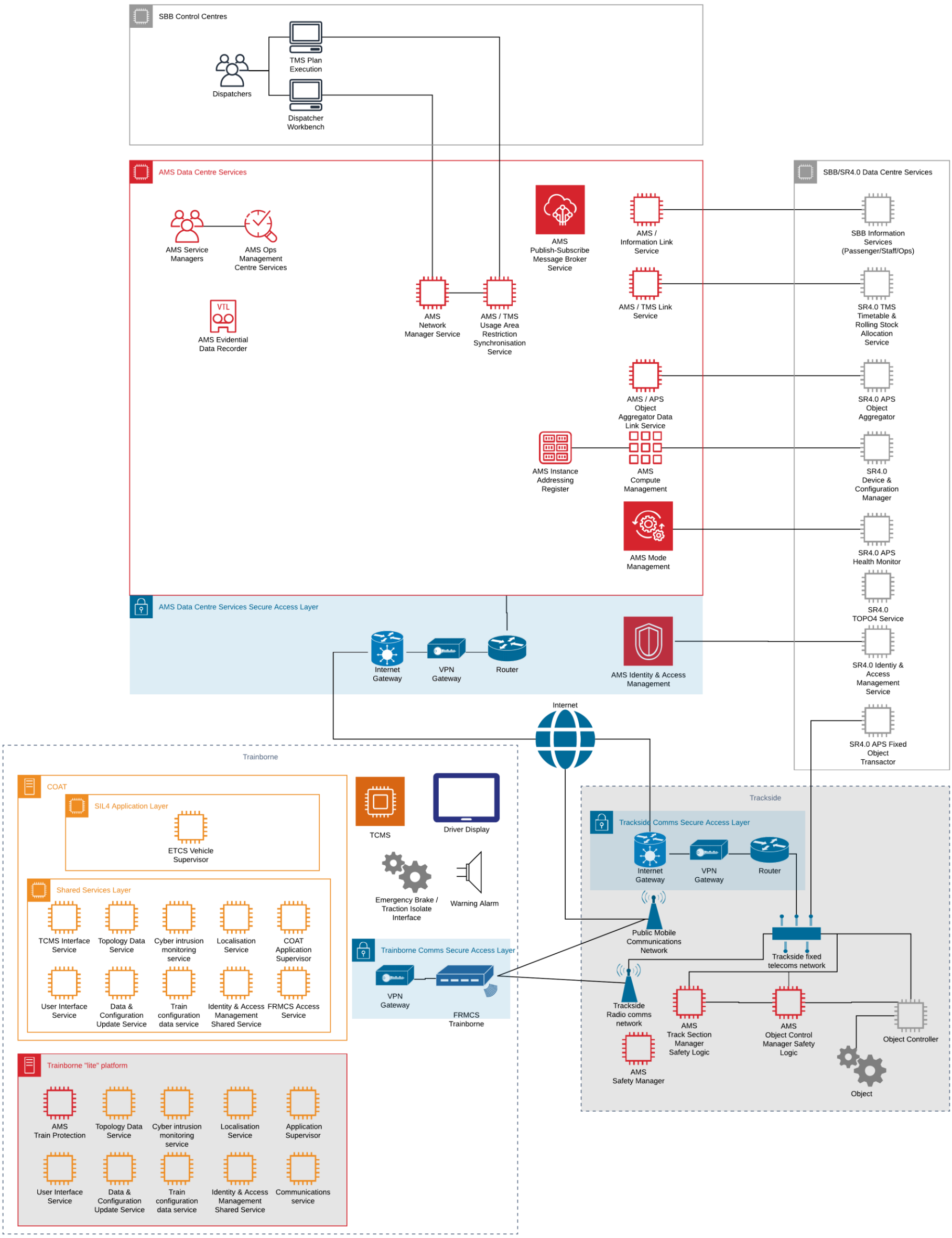
Appendix A. AMS Functional System Architecture



Appendix B. AMS Physical System Architecture



Appendix C. Decentralised independent AMS Physical System Architecture



Appendix D. AMS Key System Functionality

AMS functionality relies on data exchange between subsystems – between train and trackside objects, between train and network control, and between network control and trackside objects. Each system depends on robust input data – trusting the other party – to take safe decisions.

Functionality, such as setting the switches in the required direction for a train, depends on a request from an AMS Train Protection System to an AMS Trackside Object Manager for a direction to be set, and a timely response back to the AMS Train Protection System confirming that the direction has been set and the train is authorised. However, each subsystem itself is discrete and takes safe decisions based on input data received.

The Key System Functionality described in this section focuses on specific subsystems and the functionality that each performs – with the system boundary around each subsystem – such that each subsystem could be developed from this with formal interface specifications between subsystems.

In this section the following AMS functions are described:

1. AMS Network Manager
    a. Providing an AMS Workbench
    b. Dispatching trains
    c. Dispatching unfitted trains
    d. Manual control of trackside objects and track sections
    e. Managing Usage Restriction Areas on the Network
    f. Stopping all trains on the network
2. AMS Track Section Management
    a. Accepting/Removing a train on a track section
    b. Modifying a train on a track section
    c. Adding/Removing a Usage Restriction Area on a track section
    d. Proving a track section clear on initialisation
3. AMS Train Protection System
    a. Wayfinding to a destination
    b. Joining/leaving a track section
    c. Requesting control of trackside assets
    d. Generating a movement permission
    e. Governing safe movement
    f. Responding to information requests from other trains
4. AMS Object Control Manager
    a. Responding to information requests
    b. Controlling Track Switches
    c. Controlling Level Crossings
    d. Controlling other trackside assets

5. Additional services required to support AMS operation

Using these basic functions, that can be easily developed and verified, the system behaviour emerges that provides for safe and efficient operation. Table 12 illustrates via a RACI matrix how cross-cutting functions are via interacting subsystems of AMS.

TABLE 12 - AMS KEY FUNCTIONS FOR SYSTEM-LEVEL BEHAVIOUR (RACI MATRIX: R=RESPONSIBLE, C=CONSULTED, I=INFORMED)

AMS Function	Description	Train Protection System	Track Section Manager	Object Control Manager	Network Manager	Other interfaces
Generating a route for a train	AMS shall determine which route should be taken by trains to reach their destination.	R			C	C: TMS, Localisation, TOPO4
Permitting access to tracks	AMS shall govern which trains are permitted into a section and any usage restrictions in force.	I	R		C	
Control trackside objects	AMS shall command the change of state of track switches and level crossings to facilitate the safe movement of trains.	I	C	R	I	C: Object Controller
Manage Usage Restriction Areas	AMS shall have the capability to record the limits of Usage Restriction Areas on the railway network to ensure trains do not collide with hazards on the line.	I	C	I	R	
Generate movement permission	AMS shall generate a movement permission and speed limit profile for a train either using the status of the route set for the train from the primary signalling interlocking, or if unavailable, using the locations of other trains and hazards, and state of track switches and level crossings.	R	C	C	I	C: Other AMS Train Protection Systems

AMS Network Management System

a. Providing an AMS Workbench

i. The dispatcher will require a graphical user interface to enable the dispatcher to direct trains on the network and apply Usage Restriction Areas onto the network when TMS Plan Execution system has failed.

ii. It is feasible that this could be accessed via a web-browser so that it can be managed and maintained as a service without the need to maintain systems on-premises and accessed from any location.

iii. A touch-enabled interface could allow for continued workbench functionality with total IT failure or control centre failure.

iv. The AMS Workbench will require the functionality to define the area in which RSL is authorised for use so that trains can automatically activate the RSL quickly on failure of the APS – otherwise the driver might need to contact the dispatcher for verbal authorisation to activate RSL.

v. Usage Restriction Area management is a critical element of the envisaged AMS Workbench system for when TMS Plan Execution is unavailable. Dispatchers and drivers alike need to have means by which they can report or edit a hazard. When new hazards are detected, included or edited in the topological data, it is important that its type (passable, passable w/ speed restriction, non-passable), its approximate location and an estimate of the duration of the hazard be provided.

vi. Similarly, dispatchers also require the ability to manage unfitted trains, such as international services from Germany or France, via a graphical user interface.

b. Dispatching trains

i. Normally a train will directly monitor the Traffic Management System or timetable system for updates to its service pattern, but if these systems are not available, or the move is out-of-norm, a dispatcher might send a manual instruction to a train.

ii. A dispatcher using a Work Bench, provided by the Network Management system shall have the capability to inform the route that the train should take – but will not ‘steer’ or ‘set routes’ for trains in the traditional sense; the steering of trains is undertaken by trains themselves.

iii. The dispatcher shall specify which train needs to be at which destinations (or intermediate timing points) and the order which the train should arrive at the destinations; the destination may be at specific stations, platforms, yard, depot, siding or any other location on the railway network.

iv. The dispatcher might also specify the time at which the train should arrive at the destination.

v. To inform this the dispatcher should have visibility of where all the trains are on the railway network and their destinations to be able to check for conflicts in routes.

vi. The dispatcher should be able to direct a train on a track layout overview by selecting an ‘origin’ and ‘destination’, or by constructing a timetable diagram or creating a specific list of calling-points.

vii. The Network Management System shall post the information directly to the train, which will acknowledge it has received the information.

c. Dispatching unfitted trains

i. Trains that do not have an AMS system are a particular danger within AMS because they have no protection of their own, and if fitted trains do not know they exist then a collision could occur.
ii. A dispatcher shall have the ability to define an unfitted train operating on a map of the network.
iii. The dispatcher shall specify the start location and end location of the area in which the unfitted train is operating (a safe bubble or block around the train).
iv. The unfitted train shall be verbally authorised through the rail network with the Network Management System providing a formal record of the areas in which the unfitted train is operating.
v. The dispatcher shall update the start location and end location of the area as the unfitted train progresses through the railway network.
vi. It shall not be possible to update the end location for the train over a trackside object (track switch or level crossing) without the dispatcher having manual control of the trackside object and it being locked in the correct state.

d. Manual control of trackside objects and track sections

i. Normally a train will directly communicate with the AMS Object Control Manager to change its state in advance of the train arriving.
ii. For unfitted trains and in unusual scenarios a dispatcher will need to manually take control of a trackside object. This functionality shall be available within the Work Bench.
iii. The dispatcher shall be able to take responsibility for a trackside object and select its target state. This control request is issued from the AMS Network Management system to the Object Control Manager which confirms back that the dispatcher is responsible and confirms the state of the trackside object.
iv. Normally the AMS Object Control Manager and Track Section Manager will function correctly receiving correct information to and from trains, however unforeseen situations may arise where a reset is necessary (e.g. AMS Train Protection System fails on a train when it is leaving a track section so it never notifies the Track Section Manager that is leaving, and never relinquishes control of a trackside object after its movement has completed).
v. A dispatcher shall be able to reset or override the data within the AMS Object Control Manager and AMS Track Section Manager after verbal confirmation with train drivers and/or trackside maintenance teams. The override decision shall be formally recorded within the Network Management System and should also include a second level of independent authorisation from another logged-in user, a responsible manager, as very dangerous incidents could arise if this is done incorrectly.

e. Managing Usage Restriction Areas on the Network

i. A dispatcher might be informed about hazards from members of the public, train drivers, maintainers and emergency services. The dispatcher needs to be able to pass this information to trains in the vicinity.

ii. The dispatcher will use a visual track layout of the network to add the Usage Restriction Area to the network specifying its start location(s) and end locations(s) (N.B. This might involve multiple tracks and junctions).

iii. The dispatcher will also specify whether there are any usage restrictions associated with the Usage Restriction Area. The default option shall be that the Usage Restriction Area is impassable. The dispatcher might specify a reduced speed limit or a weight limit or gauging restriction for a train.

iv. The AMS Network Manager will post the information to the relevant AMS Track Section Manager(s) and AMS Object Control Manager(s) such that the information is available for trains to query.

v. The AMS Network Manager shall be capable of integration into third-party dynamic data sources about Usage Restriction Areas such as legacy signalling systems, overlaid/interfacing APS systems, and Traffic Management Systems.

f. Stopping all trains on the network

i. In an extreme emergency such as a train derailment, a dispatcher might want to send an emergency stop message to all trains. A dispatcher shall have the capability to trigger an emergency stop for a whole region or sub-region (area) of the network.

ii. Once initiated, the AMS Network Manager shall post this message directly to all trains on the network and also post the command to the AMS Track Section Manager to inhibit all movement on the track section.

AMS Track Section Manager

a. Accepting/Removing a train on a track section

i. The AMS Track Section Manager governs all the trains within a section of track. A track section is defined in AMS as an ‘edge’ or ‘vector’ (continuous length of track) between two nodes (typically Track Switches).

ii. The AMS Track Section Manager records all trains within a section of track, so that trains can find out which other trains are in the vicinity by querying the AMS Track Section Manager.

iii. The AMS Track Section Manager shall listen for requests from a train to join or leave the track section.

iv. Upon receiving a join request from a train to join the track section, including the Train ID, characteristics, desired direction, and IP addresses for the train. The AMS Track Section Manager verifies the characteristics against any permanent usage restrictions by the Track Section Manager.

v. Additionally, the join request from a train includes the map data version that it holds for that section of the track. The AMS Track Section Manager also has the map data version providing an additional method to verify that the train has the correct map data for that section if the map data server is unavailable.

vi. If accepted, the AMS Track Section Manager adds the Train ID to a register of trains in that section; the register is an ordered list with the train added at top or bottom of the list depending on which end of the track section it enters from. The Train ID is given the status of 'Authorised' and its direction is also added to the register based on the direction of travel that the train enters the track section.

vii. When a train is added to position 1 in the register, all other trains in the register shall have their position incremented.

viii. If the direction of travel of a train is opposing another train (head-on collision risk), the Track Section Manager must send a request to the opposing train (with the ID of the joining train) to accept this action – the Train must acknowledge the request before the joining train is authorised onto the route. N.B. the trains will from that point on negotiate directly with each other to ensure movement authorities are safe and do not overlap.

ix. If a train wishes to reverse or change direction within a track section, the Track Section Manager must make the same request as above.

x. In addition to the Trains Register, a Train Address Register holds the IP address(es) of each train in the section so that each train has a reference table with which to query how to communicate with other trains. The Train IP addresses for the joining train are added to the Train Address Register.

xi. When the Track Section Register receives a request from a train to update its IP addresses, it makes the relevant amendments to the Train Address Register.

xii. Upon receiving a leave request for a train, including its location, the Track Section Manager verifies that the train has left the track section and then the train ID is removed from the Trains Register and Train Address Register.

b. Modifying a train on a track section

i. When coupling AMS-fitted trains on a route, the Track Section Manager must merge two entries in the Train Register. When a request is received from one train, indicating a request to couple, that train's authorisation is revoked in the Trains Register. When the second adjacent train sends a request to couple (verified by including location within the request), within a configured time period (e.g. 5 minutes) the leading unit is kept and the trailing unit records are removed and authorisation to the train is restored.

ii. When uncoupling AMS-fitted trains on a route, the Track Section Manager must create two entries in the Trains Register where previously there was only one. When a request is received from one train, indicating a request to uncouple, that train's authorisation is revoked in the Trains Register. Once the second adjacent train (verified by including location within the request) sends an uncouple request, within a configured time period (e.g. 5 minutes) a new record is created for the previously trailing unit and then authorisation to both trains is restored.

iii. When uncoupling or coupling from unfitted trains, the dispatcher must create a Usage Restriction Area around the unfitted trains through operational rules.

c. Adding/Removing a Usage Restriction Area on a track section

i. An AMS Track Section Manager will receive from the AMS Network Manger a request to add a Usage Restriction Area onto the Track Section.

ii. The AMS Track Section Manager maintains a Usage Restriction Area Register to which the Usage Restriction Area is added, including any usage restrictions and its start and end location.

iii. When the Usage Restriction Area is no longer required, the AMS Track Section Manager will receive a request from the AMS Network Manager after which it will be removed.

d. Proving a track section clear of dangers

iv. Upon initialisation, the AMS Track Section Manager does not know if there are already trains in that section of track, or any hazards. The AMS Track Section Manager shall apply a blanket usage restriction to the track section limiting the speed of trains in the section to a safe "on-sight" speed (typically 40km/h) such that the driver can react to any hazards.

v. Once a train has travelled from one end of the track section to the other it is deemed to be proven clear of hazards – the driver is required to notify the dispatcher of any hazards encountered on the railway. The usage restriction is then eliminated.

AMS Train Protection System

a. Wayfinding to a destination

i. A train using AMS needs to know where to generate a movement permission to – this may be to the next station or an intermediate timing point on the network. There are several mechanisms the train can use to do this – the following options are given in order of priority where the first element should take precedence over other system inputs:

1. Driver manual destination input via DMI
2. Receiving a manual routing instruction from the dispatcher via the AMS Network Manager system
3. Subscribing to routing information from the Traffic Management System
4. Subscribing to timetable updates from customer information systems – the timetable data for a full service day should be cached on the train so that with outages of central services the train can continue to generate movement authorities for itself.

ii. The train shall use its current location, reconciled against the topology information cached on board the train, and from that starting point will search for a valid route to the destination through the railway network using the topology data stored on board the train.

iii. The train will query the AMS Track Section Managers and AMS Object Control Managers for its entire future journey path to ensure they are healthy and available with no usage restrictions that would prevent the train from utilising the route. If there are any outages on the train's path the wayfinding algorithms will re-run to find a better route.

iv. The wayfinding algorithms are not deemed safety-critical and may require very recursive search algorithms to find the most optimum path through a complex network.

v. This wayfinding approach does not take account for any congestion, grid-lock, or head-on conflicting movements that might result from inefficient pathing – this optimisation should be done by the dispatcher or Traffic Management System when generating the route for the train.

vi. The final wayfinding step is validation of the wayfinding path against the topological data – this activity is safety-critical but is simply a check that one track is connected to the next through a the correct sets of track switches that can be set in the right direction. The validation shall also include cross-checking train configuration against any usage restrictions of the route or topographical features that might inhibit its safe operation, e.g. axle load, train length, max. curve radius, gauge and other dimensions. The validated wayfinding path is then used by other safety-critical activities on the AMS Train Protection System.

b. Joining/leaving a track section

i. A train must send a request to an AMS Track Section Manager to be permitted to utilise that section of track. When there are no other trains between the train and the new track section, and the Track Switch at the entry to the track section is set in the correct direction for the train, then the request to join the track section will be sent by the train.

ii. The AMS Track Section Manager will respond to the train acknowledging the request. The train then queries the status of the AMS Track Section Manager to retrieve the Trains Register for the track section.

iii. If the train is included on the Trains Register for the track section it wants to join, and if the train is in the track register as “authorised” to use the track section, then train will deem itself as having joined the track section.

iv. The train will retry the join request to a Track Section Manager until it is permitted.

v. The train will maintain its own register of which Track Sections the train is currently assigned to and query those Track Section Managers periodically for the Trains Register for that track section.

vi. Once the train has travelled through a track section it will send a request to leave that track section to the Track Section Manager. Once the train’s ID has been removed from the Trains Register for that Track Section it removes the Track Section from its own register.

c. Requesting control of trackside assets

i. The train queries the topology data to discover whether there are any level crossings or track switches or crossings that the train is approaching.

ii. When a train approaches a Switch or Level Crossing, and there are no other trains between it and the Switch or Level Crossing, it sends a control request to the respective AMS Object Control Manager. The request shall include the desired state and expected arrival time at the Switch or Level Crossing.

iii. When the request is acknowledged by the AMS Object Control Manager, the train repeatedly queries the AMS Object Control Manager for its status. The train is checking to see if the Object Control Manager identifies that it is in control of the object, and that the object is set in the requested state, and the train is authorised to cross.

iv. A control request will timeout after a configured period after which the train should retry its request if the control request has not succeeded.

v. The train will maintain its own register of which AMS Object Control Managers the train is currently in control of and query those AMS Object Control Managers periodically for its status.

vi. Once the train has travelled through a trackside asset controlled by an Object Controller, it will send a request to relinquish control from the AMS Object Control Manager. Once the status for the Object indicates that the train is no longer in control, the train removes the Object from its own register.

d. Generating a movement permission

i. To generate a movement permission the train needs to understand the state of the railway network ahead. It does this by the following means:
    a. The train queries the AMS Track Section Manager to understand if there is a train or Usage Restriction Area ahead of it on the track section.
    b. If there is a train ahead within the track section, the train sends a status request to that train to receive its location and direction of travel.
    c. The train queries the topology data to identify if there are any level crossings between it and the train ahead. If there are, the train queries the status of the level crossing from the AMS Object Control Manager. If the train is identified as being in control of the Level Crossing, and it is the closed state, and it indicates that the train is authorised to proceed, then the train may extend its movement permission over the Level Crossing.
    d. If there are no other trains between the train and the end of the track section, the train queries the status of the track switch or crossover from the AMS Object Control Manager. If the train is identified as being in control of the junction, and it is set in the state required for the train path, and it indicates that the train is authorised to proceed, then the train may extend its movement permission over junction.
    e. If the movement permission can be extended over the junction, the train searches the next Track Section for the train or Usage Restriction Area ahead in that section, as in b, and then repeats c, d, and e, until it finds an impassable junction, level crossing, train or Usage Restriction Area on its path – the movement permission should not exceed the distance that the train would travel in 5 minutes to limit the levels of recursion required in generating the movement permission.

ii. The train shall generate its movement permission to a distance to the closest impassable junction, level crossing, train or Usage Restriction Area on its path

iii. A train may receive a request from a Track Section Manager to permit a facing train movement. The train will acknowledge this request and place a limit on the maximum distance that a movement permission can be generated – the limit will be the midpoint of the distance to the train ahead – the facing train will have the same limit ensuring that trains approach each other with decreasing speeds.

iv. The train's dynamic & static characteristics are evaluated against the route characteristics for a train's path (taken from cached topological data). A speed profile is generated up to the limit of

the movement permission considering characteristics such as acceleration and braking curves, maximum speed, position, track curvature, gradient, permanent speed restrictions, etc. The speed profile shall also incorporate any usage restriction areas received from the AMS Track Section manager.

e. Governing safe movement

i. To apply warnings and appropriate emergency braking, a train must reliably and precisely determine its location and speed at any given time via a suite of relative and absolute onboard sensors.

ii. The speed profile and movement permission should be presented to the driver of the train on a graphical user interface that permits him or her to apply an appropriate driving technique to keep the train within the limits of the speed profile and to not exceed the movement permission.

iii. To mitigate any human factors risks the following considerations should be made in the design of the graphical user interface:
   - Similarity to standard ETCS DMI displays (including variables shown)
   - Clear indication that it is an AMS providing a safety layer, rather than ETCS.
   - Clear visual indication of train's current movement permission limits & any relevant hazards
   - Visible and audible warnings capability
   - Allow driver inputs to amend destinations, acknowledge warnings and requests, etc.
   - Have alternative, visibly distinct visualisations for special movements e.g. coupling/uncoupling and shunting

iv. A warning alert will be presented to the driver when the train is tending towards exceeding its speed profile or movement permission.

v. When the AMS Train Protection System detects that the train is going to exceed either its speed profile or movement permission without intervention then the AMS Train Protection system automatically applies the emergency brakes.

f. Responding to status requests from other trains

i. When a AMS Train Protection system receives a status request from another train, object or network manager, it shall respond with data including, but not limited to, its ID, direction of travel, speed, worst-case forward and rearward locations, train integrity status.

ii. In addition the train might provide an extended status in order to facilitate future innovations in peer-to-peer traffic management and optimisation that includes: passenger numbers, freight quantity and priority level, minutes lateness, destination and arrival time, computed train path.

iii. All status information shall be periodically published to a central information system for access by a wide range of interfacing services such as Traffic Management Systems and Customer Information Systems.

AMS Object Control Manager

A decentralised AMS system requires a train to be able to ascertain that a chosen/proposed route is safe – this is of particular importance where tracks converge or cross over, or at a level crossing where trains interact with road vehicles. To do this an AMS Object Control Manager needs to mediate between trains that might want to use a track switch or level crossing at the same time to ensure there is no conflict, and also to ensure that the Object remains in a steady state until the train movement has completed.

The following functionality describes how the AMS Object Control Manager interacts with trains, other AMS Object Control Managers, and Trackside Asset Object Controller to make state changes to trackside assets which enable the safe movement of trains.

a. Responding to status requests

i. The AMS Object Control Manager shall respond in a timely fashion to requests for information about the state of assets under control.
ii. For level crossings, these requests shall include, but are not limited to, crossing state, minimum virtual strike-in time, list of trains with permission to cross, list of dispatchers holding manual requests, fault state.
iii. For switches, these requests shall include, but are not limited to, switch state (normal, reverse, in-transition, failed), switch reservation (unreserved or reserved), and if reserved, the single train with permission to utilise the switch, or dispatcher who has commanded the switch reserved. For other trackside assets, the responses shall include such information as is timely and relevant to the requesting entity.
iv. For other assets, these requests will vary depending upon the type of asset under control.

b. Controlling Track Switches

i. At no point should the AMS Object Control Manager be able to move the switch unless AMS is activated.
ii. The AMS Object Control Manager shall accept requests from dispatchers, or trains on approach, to change the position of and reserve those switches.
iii. If the switch is already reserved by another train or dispatcher, the AMS Object Control Manager shall reject the request for use outright and immediately.
iv. The AMS Object Control Manager shall perform some basic processing, using data related to its flank area direction states obtained from the AMS Track Section Manager, to accept or reject a request for state change and reservation.
v. If a request for state change is rejected, it shall be communicated to the train outright and immediately.
vi. If a request for a state change is accepted, the associated Trackside Asset Object Controller shall be instructed to change the switch position.

vii. Upon confirming the switch position is changed, the AMS Object Control Manager should change the published switch state. It should also set the reservation state to “reserved”, and publish the reserving train or dispatcher ID.

viii. If the Trackside Asset Object Controller is unable to change the switch to the requested position, the AMS Object Control Manager should reject the request.

ix. If a switch is unable to change position, it should try to drive back to its original position. If it is unable to reach its original position, it should immediately report failed, and wait for intervention and reset from a Dispatcher or maintainer. If it can reach its original position, it should indicate that (whilst it is in a locked and detected position) it was unable to reach the last commanded position.

x. The Trackside Asset Object Controller and AMS Object Control Manager should have some capability to monitor and publish if switches are in a functional or failed state. If the Trackside Asset Object Controller reports that the switch is in a failed state, this information should be published by the AMS Object Control Manager. A failure, in this sense, means an inability to reach the detection state required, within the required time after a position change request is issued.

xi. If the AMS Object Control Manager is informed that a train with a reservation on the switch has vacated the switch, or that a dispatcher has released a switch, it shall remove the train’s ID from the published permissions and set the switch state to unreserved.

xii. If a node is unreserved, the AMS Object Control Manager shall query the flank area direction state of its associated edges (AMS Track Section Managers) continuously. If the flank area direction states are observed to change to a more restrictive combination than the previous states, the switch shall be commanded to move to eliminate this, to ensure locked edges are always in correspondence. If changing switch position would not allow the elimination of out-of-correspondence states, or it would create other out-of-correspondence states, the switch should immediately flag this inconsistency for the attention of a Dispatcher.

c. Controlling Level Crossings

i. The AMS Object Control Manager shall accept requests from trains on approach to pass level crossings, which will either require a change of crossing state from barriers raised to lowered, or a requirement to keep the barriers lowered. The request shall include the predicted arrival time of the train.

ii. Upon receiving such requests, the AMS Object Control Manager should evaluate the predicted arrival time of the train, alongside that of other trains requesting the crossing (which may be on different lines) in order to decide whether, and when, to lower the barriers. This decision is based upon minimum barrier open and closed times for the crossing type under control.

iii. The AMS Object Control Manager shall reject the request to use the level crossing if it’s too far into the future to require immediate attention.

iv. The AMS Object Control Manager shall accept requests from dispatchers to manually close the barriers. When accepted, the barriers should be closed immediately, and the dispatchers ID placed in the list of entities in control of the crossing.

v. The AMS Object Control Manager shall accept requests from dispatchers to release control of the barriers. Upon accepting a request, the barriers are not directly raised, but the dispatchers ID is removed from the list of entities in control of the crossing.
vi. When the barriers are lowered, the AMS Object Control Manager shall publish this information, alongside a list of trains granted permission to pass the crossing, and dispatchers with requests on the crossing.
vii. After receiving confirmation from each train with permission to pass the crossing that its rear is clear of the crossing and it has relinquished control, the AMS Object Control Manager shall remove that trains identification from the authorised users list.
viii. Only upon receiving confirmation from all trains with permission to pass the crossing that their rear is clear of said crossing and ensuring the permission list is free of dispatcher requests for crossing close, the AMS Object Control Manager shall command the Trackside Asset Object Controller to raise the barriers and publish the crossing state as open.
ix. The controller shall provide means for a dispatcher to manually remove trains from the permission list to prevent errors based upon communications or positioning failure, whereby trains fail to release crossings blocking the road for extended periods, which may create a safety issue as road users became impatient. As this list is safety critical, removal of a train should have multi-stage authentication, suggested to consist of at least two dispatchers and the driver of the train concerned.

d. Controlling other trackside assets

Note: it is not proposed to control lineside assets other than switches and level crossings as part of this AMS implementation; other assets are considered out of scope for a fallback solution. However, if required, generic control of other lineside assets could be affected, and the general requirements can be distilled into three key points:

i. The controller shall receive a request from an external entity – typically a train or dispatcher - to change state or to reserve use.
ii. The controller shall perform some internal processing to discern whether the request is in correspondence with the logical rules for the asset in question.
iii. The controller shall reply either in the positive or negative as to the state change request, in as timely a fashion required for that asset. Where exclusive use is reserved, this should be maintained until such a time as a further request is received to release the asset.

Appendix E. Decentralised interlocking for trackside objects

Overview

In contrast to a traditional, centralised interlocking safety architecture, AMS devolves control and safety integrity to trains and lineside asset controllers. As described in previous section, under AMS, trains self-issue MA's based upon rich information about the local network and traffic, rather than be issued a 'dumb' MA by a central processor.

The same principle is extended to lineside assets. Under AMS, the AMS Object Control Managers relating to lineside assets hold their own authority to issue a 'safe state', and by consequence, to grant trains permission to pass.

With AMS trains interact *directly* with lineside assets such as points and level crossings to secure passage along a route defined by the AMS Train Protection wayfinding algorithm. Trains hold information on the location of such assets, obtained from the topology data cached on the train. Thus, the AMS Train Protection system on the train knows if a request is necessary and when to make that request. The permission granted to use a lineside asset - exclusive to the requesting train only - is independent of any other trains which may be concurrently using or requesting the same asset, and independent of other assets in the local or wider network.

The lineside assets are directly controlled by the Trackside Asset Object Controller which interacts with its paired AMS Object Control Manager service, and through this, the AMS Track Section Manager, trains and dispatchers. The software-based AMS services for object control could be hosted in a variety of potential locations – in the cloud, in a safe data centre, on a parallel trackside platform, or on the Trackside Asset Object Controller platform itself.

In simple cases, level crossings and turnouts do not need to rely on any interlocking or interact with the wider network. For more complex cases, for example most junctions involving more than a single switch, interaction between assets is limited to immediate geographic neighbours only, and safety is assured through cascade requests to adjacent assets. Decisions on whether to allow a train control of an asset are solely the responsibility of the AMS Object Control Manager, which base this decision upon data from the (virtualised or real) object controllers and the AMS Track Section Manager. This decentralisation of safety authority helps to ensure resilience and robustness in the event of failure – only the local object(s) will be affected rather than the whole region. The AMS Object Control Manager is responsible for safety conformity over individual trackside assts, which carry out different, but simple, processes depending on each request and the type of asset under control.

Of fundamental importance to the safety integrity of the system are the handover arrangements from primary signalling system to AMS, and, later, the resumption of operations with the primary signalling system. This is discussed elsewhere (2.3.4), noting the additional provision and controls which must be

in place for lineside assets so that set 'routes' are not dropped at handover leading to the potential for switches or LX to change state in front of trains.

Level Crossing (LX) Trackside Asset Control

This study recognises there are many types/classes of LX in use, and that future controller implementations may deviate from current practice. For the purposes of establishing feasibility and operational parameters, LX operation under AMS will be considered in three separate categories termed: *Passive, Non-interlocked and Interlocked.*

A. ***Passive -*** *Crossings such as user-worked, or telephone-for-permission, which do not have powered barriers, lights or sirens and instead rely upon a pedestrian/vehicle user ensuring the track is clear before crossing. This category includes crossings with single pedestrian warning light operated by track circuit.*

No changes are proposed to the operation of purely passive crossings under AMS. Drivers will still obey whistle-board instructions in the vicinity of all crossings – and this may also be automated linked to AMS. The public will be unaware whether trains are running under primary or AMS signalling. Dispatchers can respond as normal to telephone-for-permission crossings by observing the location of trains on the AMS Workbench in the control centre. The locations of such crossings are stored in the topology data which would also enable the application of crossing-specific speed limits. This category includes crossings which have warning lights to pedestrians which are activated by track circuit block occupation. Such crossings are designed to fail in a manner which indicates a greater danger than may be present; i.e. the system is designed to give the impression traffic may be approaching in the event of a fault or failure. As a primary signalling system, AMS may create a Virtual AMS Object Control Manager dedicated to passive level crossings which would allow the dispatcher to virtually mark the crossing as in use so that trains don't extend their movement authority over the asset – despite there being no physical lineside object control.

B. ***Non-interlocked -*** *Crossings with 'active' components (barriers, active warning lights, sirens) which are not interlocked with the wider signalling system, and may provide some local indication to the driver (e.g. remote indicator light), or those operating on drive-on-sight principles in order to ensure that the barriers are lowered and crossing clear.*

Non-interlocked crossings lend themselves to the same approach as Passive crossings. Their operation does not directly influence or interact with the wider system. Drivers are accustomed to their site-unique operation, which would continue as normal in the event of a central interlocking outage. The locations of such crossings are stored in the topology data which would also enable the application of crossing-specific speed limits.

For non-interlocked crossings, though not required, it may be desirable to retrofit crossings with AMS Object Control Managers and Trackside Asset Object Controllers as an enhanced safety overlay in order to ensure and/or confirm a crossing trigger. The choice of which crossings may be made based upon operational sensitivity, or blanket fitment to simplify driver interaction. These crossings may

operate in a fully interlocked manner as per type C, described below. Though inconvenient for the road-using public, the safety implications of a false-trigger of lights and barriers are minimal, meaning the AMS triggering device may escape the more stringent safety requirements of interlocked crossings in this case. For example, the trigger could be as simple as a relay-split parallel circuit to the treadle output in the control cabinet, with crossing position confirmation derived from the remote indicator lamp output.

Drivers will need to be made aware which crossings are of the non-interlocked type, and either instructed to use them as normal, or to rely on AMS for MA. This information should be displayed in real-time on the DMI for the avoidance of any doubt.

C. ***Interlocked -*** *Crossings with 'active' components (barriers, lights, sirens) which in primary signalling are interlocked with protecting signals and the wider signalling system, whereby trains are prevented from using the crossing by restrictive aspects or withheld MA's until such a time as the barriers are proven lowered and/or crossing proven clear of obstruction.*

Fully interlocked crossings require the greatest adaptations for use with AMS.

The topology data provides trains with information about level crossings they are approaching, and which of those crossings are AMS-enabled. Trains are prevented from self-issuing a movement authority across an AMS-enabled level crossing, without the level crossing AMS OC publishing that it is set safe for passage for that train. At a suitable time on approach, trains directly request the level crossing AMS controller for permission to use the level crossing. The OC processor is subscribed to the train's updates, therefore receiving its location, length and current speed.

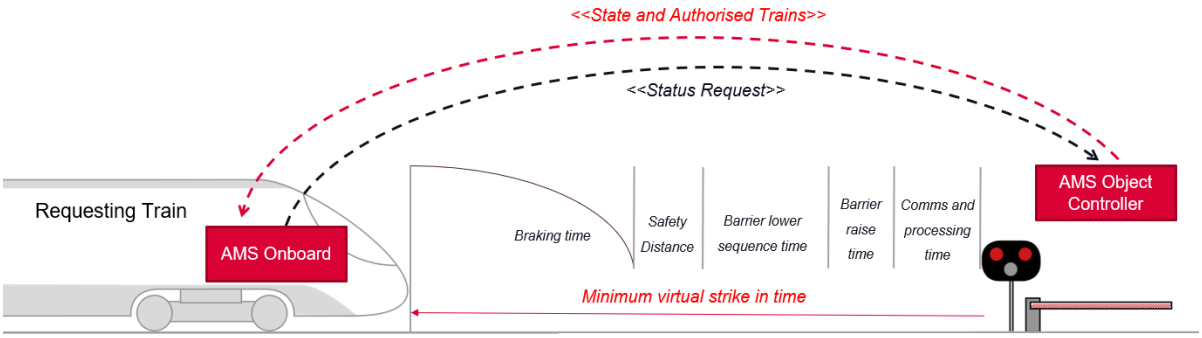
Subject to some simple decision-making logic in the AMS OC Interface (detailed below), the barrier sequence is initiated and confirmed completed. Ideally, barrier close and proving is completed just as the theoretical 'safety distance' in front of the train touches the crossing, but never before. At this point, the AMS Object Control Manager updates state that the crossing is OK to pass, also publishing a list of the train(s) with authority to pass. The train on approach is then able to self-issue an MA over the crossing. After vacating the crossing, and with a suitable allowance for position uncertainty, the train relinquishes it's request to the crossing and, subject to some more checks, the crossing's AMS Object Control Manager triggers a barrier raise as appropriate.

The example in the previous paragraph only considers a single train. Some further processing is required by the controller as it will need to cater for simultaneous, or overlapping, requests for multiple trains. This is firstly to prevent the barriers being raised for a very short time between flighted trains (and open to abuse by the road-using public) , and secondly because for multi-track crossings, the OC needs to take into account arrival and clearance times for trains passing on all tracks. AMS offers the advantage, through software, of doing away with the traditional fixed strike-in distance, offering a safety and efficiency enhancement over traditional interlocking systems. The controller, having subscribed to the relevant trains, can choose the optimum time to lower the barriers. To allow the controller to process requests in this way, a virtual 'strike-in' time-to-arrival needs to be set. This is the distance (or rather, time) away from the crossing at which the train must make a request. As a minimum to prevent

unnecessary braking, this time must allow for minimum headway (including safety distance), barrier lower time, barrier raise time, plus communications and processing time. In practice, to avoid inappropriately short barrier raise times, it should be significantly longer than this, but not so long that the LX controller is dealing with an unreasonable number of requests simultaneously. A practical solution may be to set the virtual strike-in to 2-3x the minimum time, as illustrated in Figure 22. The minimum virtual strike-in time could be unique to each crossing to allow for local conditions and will be published by that crossing.

A 'special', but common case is closely geographically coupled LX, where perhaps a single controller could perform the logic for more than one barrier set, with a group permission published, and trains treating the grouped crossings as a single entity.

FIGURE 22 - MINIMUM AND PRACTICAL VIRTUAL STRIKE-IN TIMES AT TYPICAL MULTI-TRACK LEVEL CROSSING



Drivers need to be made aware of which crossings are fully integrated with AMS, in order to ignore related lineside signals which in some failure cases may be showing restrictive aspects, and instead use AMS indications. This information, alongside the crossing state and object detection state, should be displayed in real-time on the DMI for the avoidance of doubt.

Track Switch Asset Control

Unlike level crossings, which have a simple go/no-go state, switches have two additional complications for control under primary or the proposed AMS architecture: that of routing traffic, and that of having an 'indeterminate' state whilst they change position, during which time the track is considered unsafe to traffic.

In operation under centralised signalling systems, safety protection against incorrectly set, or unsafe switches, conflicting moves, collisions and turnout speed restrictions is combined and provided by a central interlocking. This interlocking is a function of the infrastructure and is centralised or semi-distributed. Its parameters, such as routes through junctions, are fixed during project design and relatively inflexible to upgrade or adaptation.

The same level of protection must be provided under an AMS system, which may lead the reader to believe a system as expensive and complex as the existing interlocking is required. However, in this respect, the AMS architecture offers one huge advantage over traditional interlocking systems and

principles: that protection from inter-train collision and turnout speed restriction is entirely dealt with by the AMS trains themselves. This separates out the traditional interlocking roles, and instead of an all-encompassing system, the Trackside Asset Object Controllers and AMS Object Control Managers, need only provide safety protection against unsafe (undetected or incorrectly set) switches and conflicting moves.

The solution adopted is logically simple, scalable, and flexible and will be described in detail after some key definitions:

1. Each switch has a physical Trackside Asset Object Controller which is responsible for the command, move, lock, detection of the physical switch elements (as per existing practice). The Trackside Asset Object Controller accepts periodic requests for switch movement (either Normal/Reverse/Manual/Reset), and constantly publishes switch state, which can be any one of:
    i. Detected Normal - *The command has been received to place the switch in the normal lay, the lock is engaged, and the detection indicates both switch blades lay normal.*
    ii. Detected Reverse - *The command has been received to place the switch in the reverse lay, the lock is engaged, and the detection indicates both switch blades lay reverse.*
    iii. In Transition- *The switch is moving between positions and consequently there is no detection.*
    iv. Not Enabled – *AMS mode is not active so the Trackside Asset Object Controller has no authority to move the switch.*
    v. No Command – *The* Trackside *Asset Object Controller has not yet received a commanded position (only ever seen after handover or reset before an initial position command is received).*
    vi. Failed - *The switch has a failure and is locked out until manual reset by dispatcher or maintenance.*
2. The physical length of a switch is from switch rail toes to the conflict point, (or conflict point to conflict point), and the data related to conflict points is stored in the topology data, which the train has access to, in order to prevent conflict with trains on adjacent lines. However, the topological information is not relevant to the switch AMS Object Control Manager.
3. All switch AMS Object Control Manager have at least three tracks emanating, (emanating tracks referred to herein as ‘edges’). For simplicity within the AMS Object Control Manager, diamonds, switch diamonds, slips and tandem switches are treated as two back-to-back switches (and therefore two nodes), even if the physical track features overlap. Flat crossings are treated as virtual objects without physical trackside assets, but still governed by an AMS Object Control Manager with 4 edges (described later). Scissor crossings are treated as four switches with a central crossing, to make 5 nodes in total.
4. Each edge connecting to the node has a “Flank protection area” defined within the topology data. The “flank protection area” has a direction property that is managed within the Track Section Manager under the control of an AMS Object Control Manager. The AMS Object Control

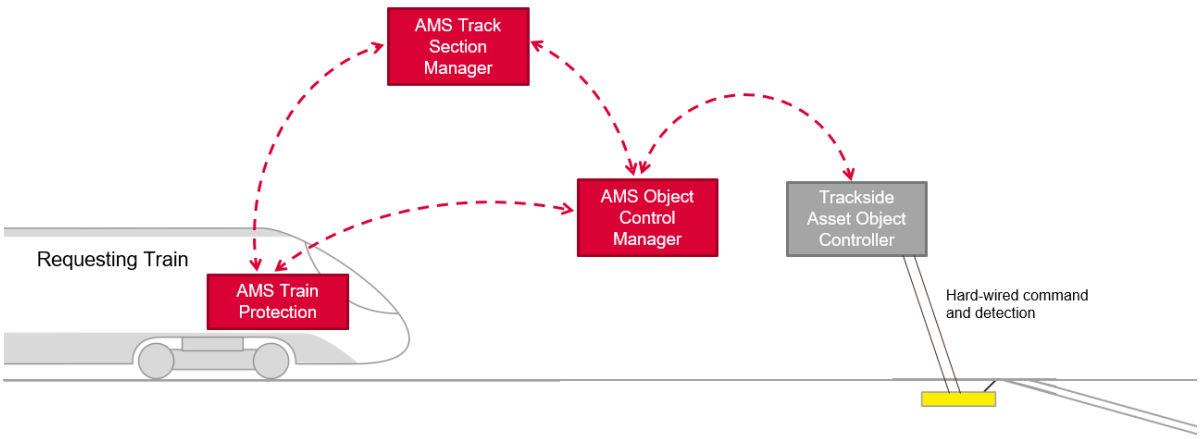
Manager configures a direction setting that inhibits trains from entering the flank protection area to ensure that an overrunning train (exceeding its movement authority) does not collide with an oncoming train. The flank protection area direction parameter can have four possible states. In binary terms, used as shorthand later, these direction states could be described as 00, 01, 10 and 11. A train can be permitted to move towards a 1, but never towards a 0.

i. Movement inhibited (00): No train may access, or self-issue an MA over inhibited track.
ii. Movement permitted in the up-km-direction, down-inhibited (01): Trains can self-issue an MA in the specified direction only.
iii. Movement permitted in the down-km direction, up-inhibited (10): Trains can self-issue an MA in the specified direction only.
iv. Bi-directional movement permitted (11): Trains can self-issue an MA in either direction.

5. Each Trackside Asset Object Controller is paired with an associated AMS Object Control Manager, which is a software service responsible for interacting exclusively with it. Requests to move the switch must go through the AMS Object Control Manager; the switch will only accept requests from this channel.
6. Each AMS Object Control Manager has three published state variables. The first is the physical, detected and locked, switch position, which can be 'normal', 'reverse', or 'failed'. The second indicates whether a switch has issued permission for a train to pass. If it has, it is considered 'reserved', otherwise it is 'unreserved'. A reserved state cannot be set without the corresponding train or dispatcher ID for which the switch has been reserved, also being published. A failed switch is reserved and sets the ID to 'FAILED'.

The relationship between AMS Object Control Manager and Trackside Asset Object Controller is shown in Figure 23. As the AMS Object Control Manager is a software service, it could be hosted in any location – even on the physical object controller itself.

FIGURE 23 - RELATIONSHIP BETWEEN THE ELEMENTS OF SWITCH CONTROL



The Trackside Asset Object Controller has a hardware interface with the switch machine and communicates via the AMS Object Control Manager.

The interface between the Trackside Asset Object Controller and switch is as per current practice, with command signal wires and logic provided for detection of the position of both switch blades, lock, and further supplementary detection, where required.

Everything downstream of the Trackside Asset Object Controller, i.e. the safety critical switch actuation, locking and detection loop, will remain unchanged from existing. The only entity with authority to command a Trackside Asset Object Controller is its associated AMS Object Control Manager.

There are no decisions taken by the Trackside Asset Object Controller related to track occupation, flank protection area direction state or trains on approach; these are all abstracted to a higher level as with existing interlocking practice.

The AMS Object Control Manager is a software service which provides the 'public face' of the switch. The AMS Object Control Manager requests the status of adjacent Track Section Managers for information regarding the edges connecting to the switch to establish the locked/unlocked state of those flank protection areas.

The AMS Object Control Manager receives commands to change switch position, and requests to reserve a switch from external actors (trains, dispatchers), either of which can only be carried out after a series of logical checks are complete. These logical rules, the same for every switch, form the safety and protection system for junctions when running under AMS. In isolation, they appear simple, but when combined together their effect is to create a cascade of protection which prevents conflicting moves, and automatically deploys, for example, flank protection, without such protection being expressly written into the route tables for every route through a junction. The rules are as follows:

1. At any time, if a switch has not been reserved by a train, the switch is considered unreserved. Only an unreserved switch can be requested to change position by a train or operator. Reserved switches should never be requested to move and will not move if commanded. This control prevents switches moving in front of, or under, trains.
2. A switch can only be reserved by a single train at a time. However, a single train can request position change and reservation from multiple switches at a time. This control prevents conflicts leading to head-on or side-on collisions.
3. If a switch is reserved, it remains reserved and locked until the train or operator which reserved the switch relinquishes control. This control prevents other trains taking control of switches when in use, or shortly due to be in use.
4. In either position, the AMS Object Control Manager transposes the flank protection area direction state from the approaching edge to departing edge and sets the other edge flank protection area to 'movement inhibited'. For example, a switch with 01 on approach would set the departure edge flank protection area to 01, and the other edge to 00. Transposition of flank protection area direction state allows the train permission to navigate the junction; setting the other edge to 00 prevents routes being set which would trail the switch.

5. A switch can only change position if this does not place its flank protection areas on edges into conflict with those set by reserved adjacent nodes. Conflict, in this sense, is transposing a more limiting edge direction state over an existing. For example, an up-km-direction movement permitted, down-km-direction inhibited (01) track section can lead to another 01 section, or a bi-di (11) track section, but not an inhibited (00) track section or a 10 section. This control prevents accidental moves into inhibited track sections for a given direction of movement.
6. If an unreserved switch experiences a change of edge flank direction state which conflicts with its current position, it should automatically move to a position to eliminate this conflict. If it cannot fully eliminate the conflict (i.e. if either position would place it into conflict), it will move to the position of least conflict and alert the dispatcher. This is an unlikely scenario but one indicative of potential gridlock without human intervention. This control brings about, by consequence, flank protection by ensuring that switches in flank must change position to prevent access to inhibited edge flanks, but as those switches remain unreserved, they may be used concurrently by other traffic.
7. To allow reservation, the AMS Object Control Manager must first ensure that control authority for that switch has been delegated to AMS. This control prevents trains self-granting MA's over switches not yet under the command of AMS – for instance it may be the case that there were problems handing over certain assets at a junction.
8. If a switch is reported failed during a direct request by train or dispatcher, the facing edge flank retains its edge flank direction state, and other edge flanks are set to 11, the least restrictive state. If a switch is reported failed as part of a non-reserved move (I.e. under rule 6), the locked edge change which triggered the move is allowed to remain, and the other edges are set to 11. The switch is set to reserved and sets the permitted ID to 'Failed'. This control effectively blocks the switch if it is in an unsafe state, as no train can then be issued permission to pass. Setting edge states to 11 after failure may seem counter intuitive, but the switch is already blocked by the first control. Granting the other flank protection areas a 11 state enables other switches in the vicinity to still be operated normally.

One other construct is required to allow the flexibility to apply this solution to every junction: the virtual object. A virtual object is a software construct which behaves as per a real switch yet forgoes any actual moving parts.

Virtual objects allow certain track layouts to function as intended by governing access to an area where two or more tracks cross over each other without any physical switches. Virtual objects have their own AMS Object Control Manager, but do not require a trackside object controller. For the sake of this study, it can be assumed that the virtual object 'behaves perfectly' and conforms with every request instantly.

The distance from a switch at which point the train must request switch operation and/or reservation is of prime importance for correct junction operation. Too close to the switch, and the route may not be set in time, leading to the train being forced to brake on approach, having a knock-on effect to following traffic. Too far from the switch and the junction may be blocked to other traffic for a period long enough to cause delays to conflicting traffic or a gridlock scenario.

It typically takes between 2-7 seconds to command actuate, lock and detect a switch. For optimum operation, an AMS Object Control Manager should publish a reservation at least 7 seconds prior the movement authority of the requesting train touching the flank protection area ahead of the switch toes to prevent unnecessary braking on approach. Figure 24 gives an illustration of the optimal request time.

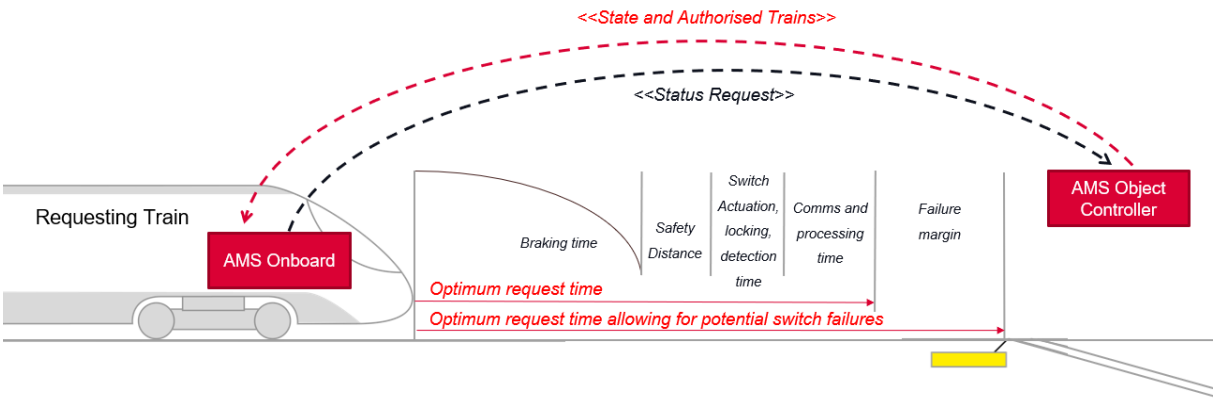
The train must endeavour to release reservation upon switches in its wake as soon as it is confirmed that they are vacated. If these timing rules are observed, it is anticipated (though not formally modelled or proven) that the capacity of most junctions could be significantly enhanced.

Also, of note: In some scenarios, such as due to local power supply constraints, it is important to ensure that multiple switches do not operate simultaneously. Traditional wired relay-relay interlockings sometimes include time-delay relays for this reason. However, AMS Object Control Managers using a fixed request time solve this problem by design as requests to change state will cascade through the junction as the train advances, with each switch commanded to change state a few seconds apart. This is possible as deconfliction and routing is abstracted to the non- safety critical AMS wayfinding service ahead of time.

Devolving control in this way clearly has many advantages, but there is one potential disadvantage to note related to switch failures. With traditional route-based interlocking, a train is not cleared to enter a route through a junction until every required switch is locked and detected as required. A switch failure therefore reveals itself when the train is some distance from the junction, leaving open the possibility of re-routing. With the AMS fully distributed system, switches are requested individually, meaning a switch failure would not reveal itself until the switch in question was commanded to move failed to get detection, and subsequently set movement inhibit (00) to the exit tracks. In extremis, this could leave a train standing across a junction, with exit tracks inhibited, blocking conflicting moves. A policy to overcome this drawback is needed. The simple solution is twofold:

1. To add an additional margin to the request time, which would be unique to the complexity of each junction, called the ‘failure margin’, which is equivalent to the time it would take the train to traverse the junction.
2. To prevent trains self-issuing an MA across a junction until the last node in that junction has issued a reserved state for the train, i.e. ‘don’t get in unless you know you can get out’. This would cost some capacity when compared to the optimised case - though it is anticipated (though not formally modelled or proven) that the capacity of most junctions would still be enhanced - but would serve mitigate against switch failures cascading to junction blockages.

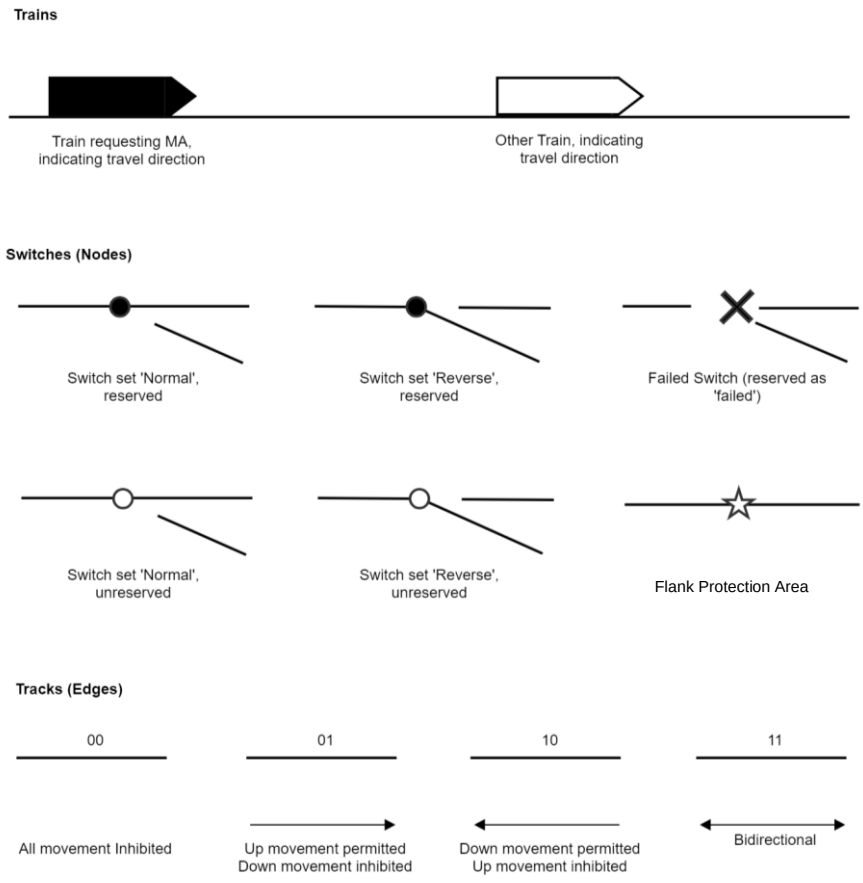
FIGURE 24 - OPTIMAL AND PRACTICAL REQUEST TIME FOR RESERVING SWITCHES BY AN APPROACHING TRAIN



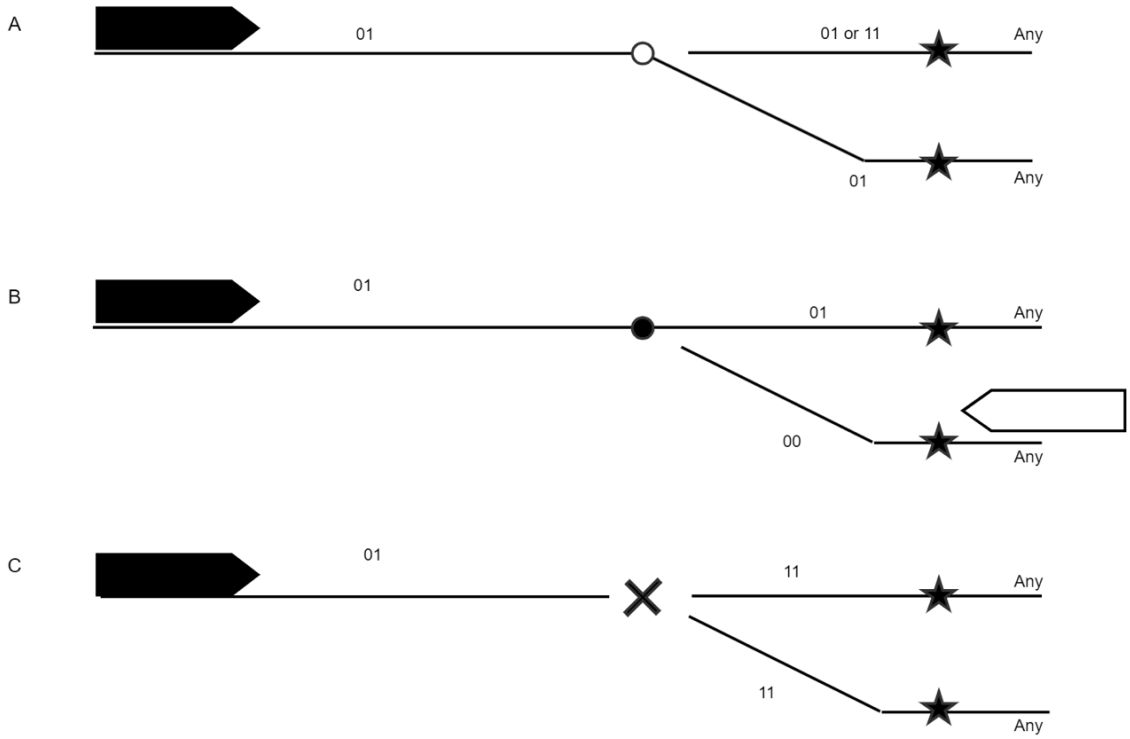
Switch and junction command and operation – worked examples

There follow several worked examples of how AMS switch control would work in practice. A key to the shorthand adopted for these examples is shown in Figure 25.

FIGURE 25 - KEY TO WORKED JUNCTION EXAMPLES

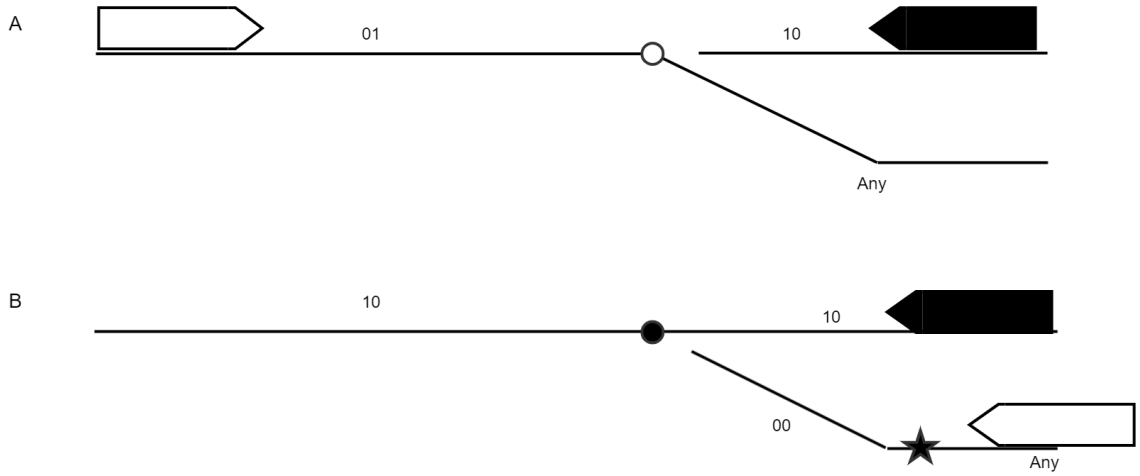


Simple facing switch



The first example is a simple facing switch. In diagram A, the requesting train approaches from the left and wishes to exit the ‘Normal’ Track. The switch is unreserved but set incorrectly. In B, the request is accepted, the switch changes position and is reserved for the requesting train. As part of this move, the direction of the ‘exit’ track is set to replicate the movement of the approaching train, and the alternate track to ‘00’ though in this case, this does not provide additional protection as no flank settings are required. Flank Protection Areas are required on the exit to the switch to allow conflicting traffic to approach and wait (otherwise the edge flank direction state would be copied to the next node, over a track section which may host a train). If, during actuation, the switch fails, the requesting train will fail to get a reservation, and cannot pass the switch – nor can any other train. The exit tracks are set to 11 to provide greatest flexibility in the wider network.

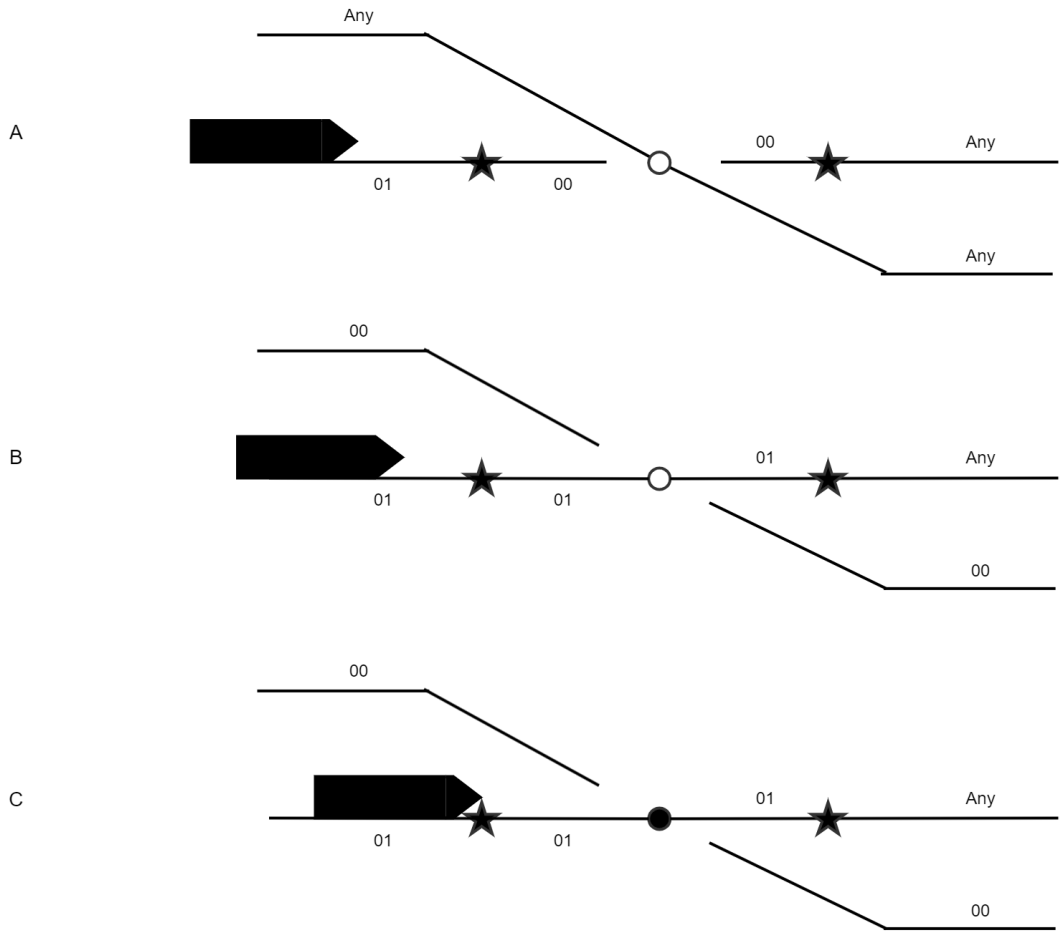
Simple Trailing switch



In A, the switch is unreserved, but the edge state on exit is locked due to the presence of the second train, this direction conflicts, therefore the request is denied by the AMS Object Control Manager, thus preventing setting a route which could lead to a collision.

In B, the train requesting MA has successfully had the switch set Normal and reserved for its move. The edge state on approach, 10, is replicated onto the exit track. The merging reverse track has its edge state set and locked to 00. If the switch allows two lines to merge, an edge flank protection area will be required to allow a second train to wait for clearance, as shown. The train cannot enter the flank protection area as the reverse edge state is locked to 00 thus preventing a move from less to more constrained track. Only once the first train clears and releases the crossing will the switch be unreserved, at which time the waiting second train can reserve both the edge flank protection area and the switch after calling it reverse.

Fixed crossing

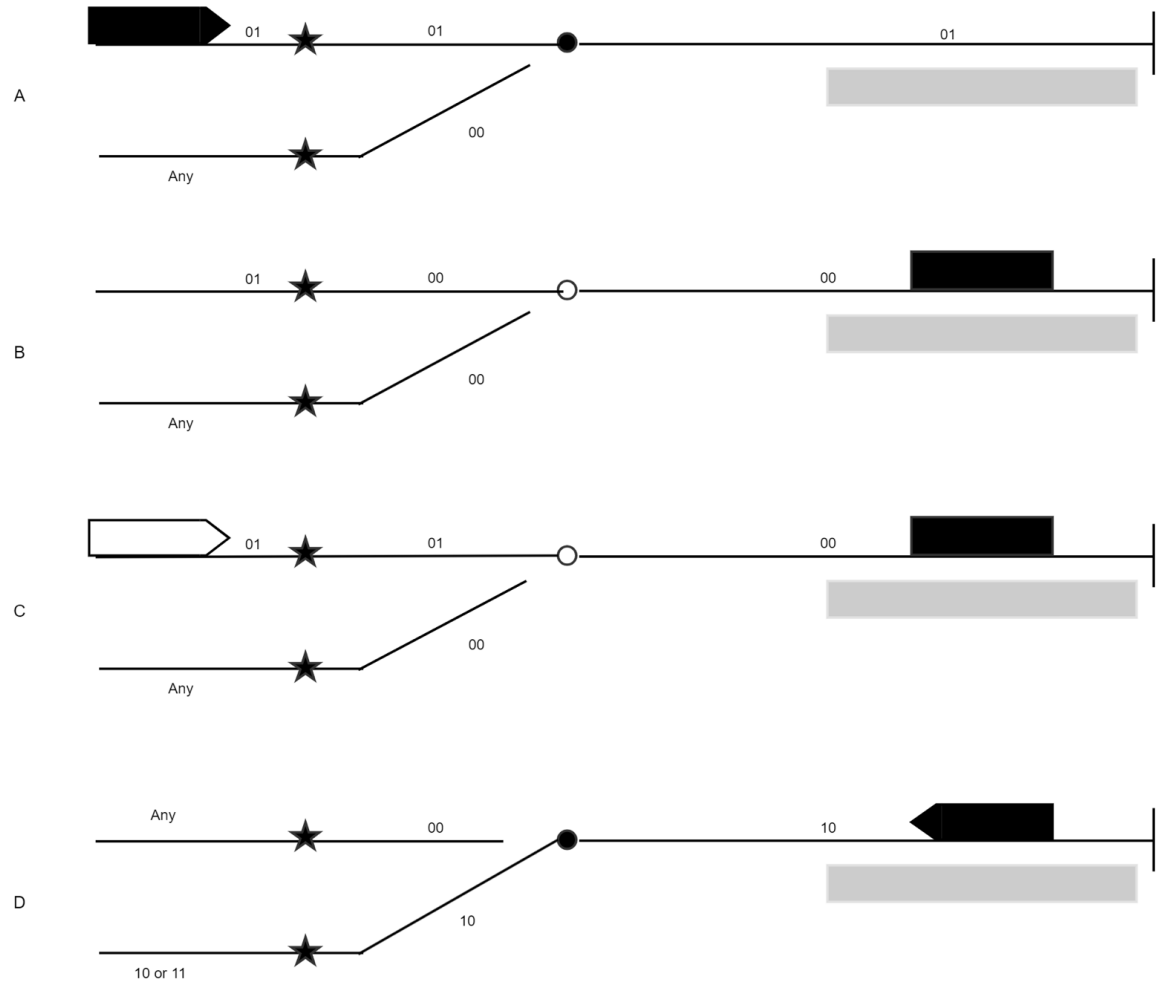


A fixed crossing is treated as a virtual object with 4 edges. The virtual object acts like an instantaneous, and perfectly reliable switch. For a flat crossing placed in plain line, and not near other switches, edge flank protection areas will be required to allow operation. Near other switches or crossings, the need for these would be negated.

In A, a train approaches a flat crossing which is set incorrectly but unreserved. The train must first request passage over the virtual object in its path. The exit track is set to 00, but both the edge flank protection area and crossing are unreserved, so this edge is free to be changed to 01 as the reservation over the virtual object is granted. At this point (shown in B) the AMS Object Control Manager for the crossing node sees a change of edge flank protection area state on approach and changes its edge flank protection area states to be in correspondence, as per rule 6. Note the train has not yet reserved the crossing.

In C, the train has reserved the crossing and is cleared to cross. Note conflicting moves are prevented by the reservation, NOT the movement inhibit 00's on the opposite track, which provide secondary protection only. Only after the train clears the second edge flank protection area is the track released for trains to request following or conflicting moves.

Terminal platform



A single terminal platform is a special case where trains must enter and then change direction to exit, often exiting down a different line as depicted in A.

A special rule is used within Object Control Managers for a ‘dead-end’ such as a terminating platform. The control of a switch will not be released by the AMS train until it has completed its exit manoeuvre.

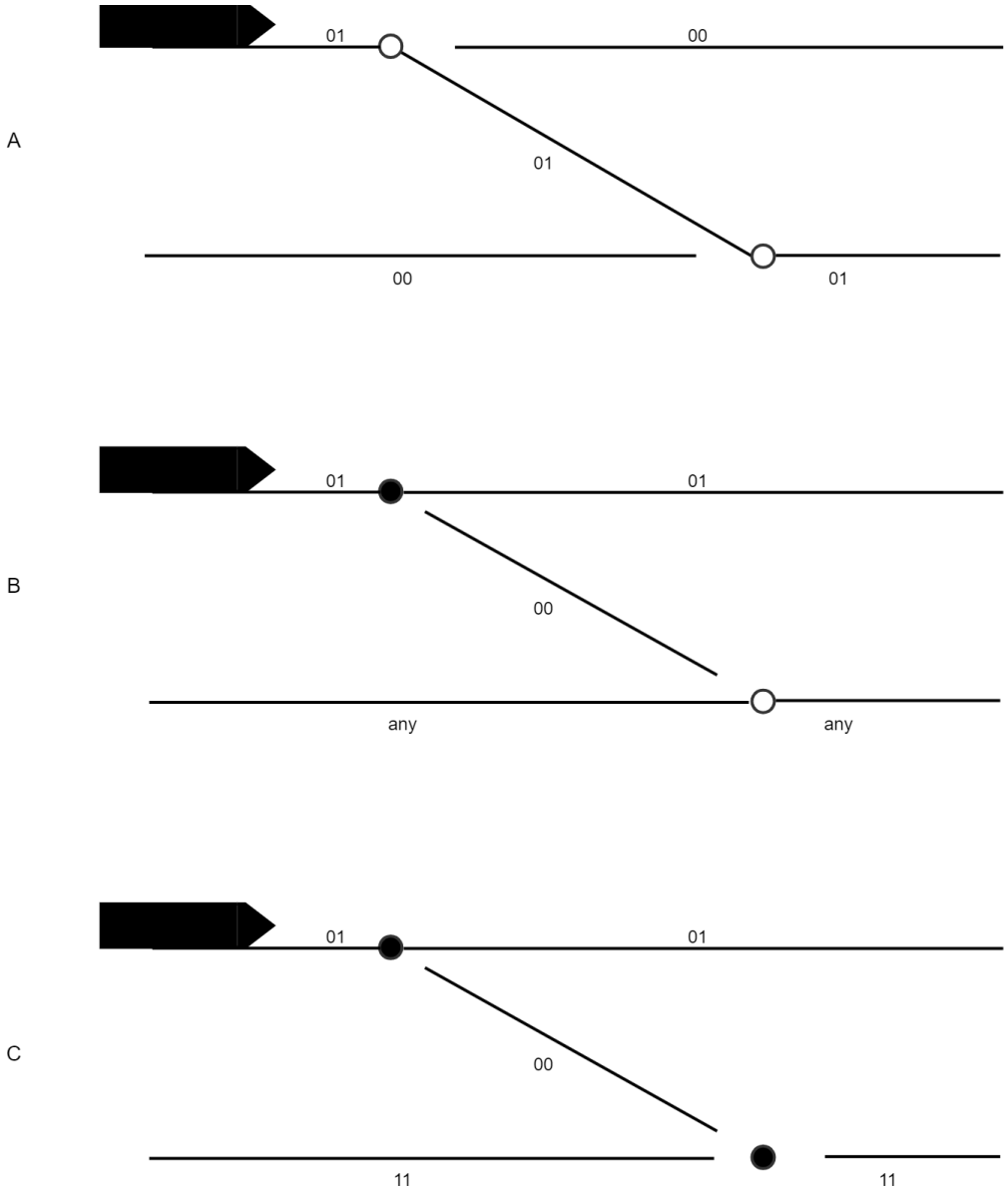
In B, this train has accessed the platform but immediately after the train passes over the trackside asset, it sends the Object Control Manager an inhibit request preventing all flanks from being occupied and retains control of the Object.

In C, an error with the wayfinding or timetabling algorithms has occurred, and a second train arrives to take the same platform berth. It requests reservation of the first edge flank protection area, for which the node requests to swap the next, unlocked, track section to 01. The AMS Object Control Manager in the switch recognises this edge change, and that the edge is locked, and recognises that there is no position the switch can move to in order to avoid conflicts, therefore the Dispatcher is alerted to deal with the situation, as per rule 6. Should the second train try to reserve the switch, the locked 00 flank

protection area state on exit will prevent reservation being granted, and prevent a gridlock scenario with the second train blocking the first into the platform.

In D, the berthed train is ready to commence its next journey, and requests the Track Section Manager for permission to begin moving by setting the track to 10 – the equivalent of an ‘off indicator’ in traditional signalling. The request is granted. The switch sees the change in edge flank protection area state, but this places it into conflict with edge flank protection areas, so it does not move. The train requests a change of state and reservation of the switch, which are both granted, and the train is free to depart.

Facing crossover



A facing crossover offers a good illustration of the power of edge flank protection area directions to provide passive protection. In A, a train approaches a facing crossover with the goal of continuing straight ahead. The crossover is still set from a previous move. The train requests the reservation of the switch in its path in normal. As none of the switch exit flank directions are locked, the switch complies.

The switches exit edges are set to 01, for the normal route, and 00 for the turnout route. The second switch sees the change of edge state, and, following rule 6, looks to set itself to a non-conflicting position on the locked route. This means moving normal to present a 00 to the reverse route, which it promptly does, thus providing flank protection. The result of this is shown in B. Crucially, the requesting train has called 2 switches to move despite only directly requesting and reserving one.

In C, the second switch failed during the move to align edge flank direction states. According to rule 8, the edge flank direction state change which caused the move can stand, and the other edges have been set to 11. The failed switch is still protected as it is reserved 'Failed', but the move by the train requesting MA can complete.

More complex layouts and further examples

Flank areas would generally be placed at the entry and exit to junction work such that direction state restrictions from a junction are not transposed long distances up and down the network, allowing for greater flexibility in operation.

The feasibility study has also considered additional junction types including: Single Slip Diamond, Square Crossing, Tandem, Trap Points, Double Junction, Ladder and Scissors. The analysis carried out confirms that the flank-direction control method within AMS allows for a simple, scalable approach to complex junction interlocking without the need for complex control tables.

Full validation of all feasible complex junction layouts in all scenarios shall be simulated during the next development stage to demonstrate the safety of the emergent system behaviour.

Other Signalling Equipment Trackside Asset Control

Whilst noting that the specifications of Object Controllers for use in certain future control concepts includes the ability to control additional signalling equipment, no further interface with this equipment is proposed as part of AMS. It can be envisioned how items such as signal heads, platform edge doors, tilt authority beacons or derailers could be controlled in the same manner as above. However, the purpose of this AMS implementation must be borne in mind: to enable passengers to alight from trains in the event of a central control failure. Trains will travel at low speed (negating tilt authority) and will autonomously derive their own MA (negating fixed signal heads). Platform edge doors can be operated manually at stations but could be interface with via AMS too. Conceptually, derailers could be operated in the same manner as switches, but as they generally protect exits to depots and sidings it is not proposed to integrate them with AMS.

Appendix F. List of References, Works Cited and Interviewees

SR4.0 Documents Supplied

#	SR4.0 Documents Referenced
1	SysArchitecture_System_Architecture_Description.pdf
2	System_Structure_Layer_20190517.png
3	ES_Innenanlagen_40_outputs_General_Concept_ETCS_Interlocking.pdf
4	Safety-critical Applications in Data Center in the Railway System SBB.pdf
5	STech2018_Sitges_Barcelona_vRS.pdf
6	Integrierter_ZwischenberichtTechPocGLAT_v1.2_web (Intermediate TechPoc GLAT Report)
7	DTU_Summit_presentationCaimi_20180531_V
8	Reference_Architecture_TMS_for_RCA.pdf
9	Anlage FQT_07 - Safety Plan SR40.pdf
10	Anlage FQT_14 - Safety Policy.pdf

Works Cited

1. https://eulynx.eu/index.php/documents2/rca/rca-beta

2. https://www.derbund.ch/panorama/vermischtes/sbb-entdecken-fehler-bei-der-zugsicherung/story/31639286
3. Rail Accident Investigation: Interim Report Loss of speed restrictions on the Cambrian line October 2017 https://assets.publishing.service.go.uk/media/5bc871d5e5274a0956564a41/IR012018_181018_Cambrian_TSRs.pdf
4. https://www.newsd.admin.ch/newsd/message/attachments/50147.pdf

5. https://eulynx.eu/index.php/documents2/rca/rca-beta/227-rca-architecture-overview/file

6. Section 3, Page 7, “Where is platform independence applicable in RCA?” https://eulynx.eu/index.php/documents2/rca/rca-beta/238-rca-chapter-platform-independence/file

7. See more information at https://en.wikipedia.org/wiki/Shannon_number
8. For inspiration on concepts of emergence see: HOLLAND J. H. 1998. Emergence: From Chaos to Order. Addison-Wesley, Redwood City, CA.
9. [1]See more information at https://en.wikipedia.org/wiki/Technology_readiness_level

10. Safety Plan - SmartRail 4.0 version 1.0 (Anlage FQT_07)
11. SR40 Safety policy version 1.0 (Anlage FQT_14)
12. Bundesamt für Verkehr - BAV
13. https://www.nccgroup.trust/uk/about-us/newsroom-and-events/press-releases/2019/july/heathrow-express-guarantees-cloud-continuity-for-mobile-ticketing-application-with-ncc-groups-escrow-as-a-service/

14. References for data centre outages were all taken via a search for articles including the word “outages” on the Data Centre Dynamics website: https://www.datacenterdynamics.com/news/?page=1&term=outages

15. Leitfaden Schutz kritischer Infrastrukturen - https://www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/ski/leitfaden/_jcr_content/contentPar/tabs/items/downloads/tabPar/downloadlist/downloadItems/74_1460990690209.download/20181217_Leitfaden_SKI_de.pdf
16. Leitfaden Schutz kritischer Infrastrukturen - Umsetzungshilfe - https://www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/ski/leitfaden/_jcr_content/contentPar/tabs/items/downloads/tabPar/downloadlist/downloadItems/141_1534504827295.download/20181217_Umsetzungshilfe_Leitfaden_SKI_de.pdf

17. Katastrophen und Notlagen Schweiz 2015 - https://www.babs.admin.ch/content/babs-internet/de/publikservice/downloads/gefrisiken/_jcr_content/contentPar/accordion/accordionItems/risiko_und_gefahrena/accordionPar/downloadlist_copy/downloadItems/121_1461071584193.download/knsbroschuere2015de.pdf
18. 732.33 - Verordnung über den Notfallschutz in der Umgebung von Kernanlagen (Notfallschutzverordnung, NFSV) vom 14. November 2018 (Stand am 1. Januar 2019)- https://www.admin.ch/opc/de/classified-compilation/20161603/201901010000/732.33.pdf

List of Interviewees

Interviewee	Department/Team
Steffen Schmidt	Program Manager ETCS interlocking
Janina Bonjour	Project Manager for MTC
David Grabowski	Head of Safety for SR4.0
Sebastian Ohrendorf-Weiss	Project Manager for Localisation (GLAT)
Markus Kuhn	Lead System Architect SR4.0
David Steiner	Business Architect MTC
Adrian Wildermuth	ETCS Interlocking Solutions Architect
Andreas Strahm	Trackside Object Controller Solution Architect
Olaf Zanger	Principal Cyber Security Lead
Christian Tobler	Control Center Manager
Markus Burri	Project Manager Datacentre strategy
Nicole Grundmann	Project Manager Topology data
Inna Höhener	Project Manager Topology data & EDP
Albert Ledermann	COAT Platform
Robert Badertscher	Project Manager Connectivity
Martin Zehnder	Project Manager OC Platform
Cirillo Ghielmetti	COAT Platform
Marcus Steiger	RAM Team
Tom Melchior	RAM Team
Pascal Gasser	RAM Team
Rafael Cueni	Business Case
Olaf Böggering	Business Continuity Team