RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

IPM Position Paper

Preliminary Issue

Document id: RCA.Doc.75

Table of contents

List of Figures

List of Tables

Version history

Version	Date	Author	Description
0.1	30.09.2022	David Schulz, Martin Kaiser, Martin Kemkemer, Tom Erzmann	Initial version

1 Introduction

1.1 Release information

Basic document information:

RCA-Document Number: 75
Document Name: IPM Position Paper
Cenelec Phase: 1
Version: 0.1
RCA Baseline set: BL1R0
Approval date: 30-09-2022

1.2 Imprint

Publisher:

RCA (an initiative of the ERTMS Users Group and EULYNX Consortium)

Support and Feedback:
For feedback, or if you have trouble accessing the material, please contact rca@eulynx.eu.

1.3 Disclaimer

This issue is a preliminary version of this document. The content of this document reflects the current ongoing specification work of RCA. Formal requirements management and change management will be introduced in future iterations. The content may be unfinished, will likely contain errors and can be changed without prior notice.

1.4 Purpose of this document

This document is a position paper to introduce the concept of Incident Prevention and Management (IPM) in RCA/OCORA. Coming from the current approach of the RCA/OCORA architecture this position paper describes the rationale for an additional group of subsystems related to IPM on trackside and on-board and its intended functionality enabling railway operation up to GoA4. Finally, a clear delimitation of the scope between IPM and RCA/OCORA subsystems shall be conducted.

1.5 Use of this document

The IPM position paper shall be used as a general description that helps to understand the basic intentions behind the IPM principles. It will be used for communication and onboarding events, for discussions about product development strategies, or to describe the business expectations for feasibility studies or for the design of prototype projects within Europe's Rail System Pillar and Innovation Pillar.

1.6 Target group

The target group for this document are asset manager, system architects, designer of operational processes, system engineers and industry representatives.

1.7 Related documents

Reference ID	Document Title	Source ID	Version
[1]	RCA Terms and Abstract Concepts	RCA.Doc.14	0.4 30.09.2022
[2]	RCA Architecture Poster	RCA.Doc.40	1.0 30.09.2022
[3]	A.P.M. business strategy and targets	RCA.Doc.50	0.6 30.09.2022
[4]	APS Concept	RCA.Doc.51	1.0 30.09.2022
[5]	DIRECTIVE (EU) 2016/798 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on railway safety	32016L0798	23.10.2020
[6]	RCA System Definition	RCA.Doc.35	0.4 30.09.2022
[7]	ERTMS/ATO Glossary	EUG Reference: 13E154	1.11 24.02.2022

1.8 Terms and abbreviations

1.8.1 Common terms and abbreviations

Term	Definition
Area of Control (AoC)	The Area of Control (AoC) is a special subclass of Track Area to define the common topologically limited area of control of the subsystems (the system borders). *Refer to RCA Terms and Abstract Concepts [1]*
Accident	An unwanted or unintended sudden event or a specific chain of such events which have harmful consequences; accidents are divided into the following categories: collisions; derailments; level crossing accidents; accidents to persons involving rolling stock in motion; fires and others. *Refer to Directive (EU) 2016/798 [5]*
ATO on-board (ATO-OB)	The subsystem and set of automated non-safety-related driver functions, depending on the grade of automation. *Refer to ERTMS/ATO Glossary [7]*
CCS	Control, command, and signalling
Digitalisierung Bahnsystem (DBS)	DBS is a core part of Digitale Schiene Deutschland (DSD / Digital Rail) railway sector initiative initiated by Deutsche Bahn. The Digitalisierung Bahnsystem (DBS) program aims to increase capacity, reliability, and efficiency of the railway system by using the opportunities of new technologies and concepts in the context of digitalization.
Emergency Control Centre (ECC)	Emergency Control Centre (ECC) represents an entity that carries out non-automated emergency functions which require human actions.
Field Element	Field element is a railway fixed equipment on/or adjacent to track e.g., light signal, point, level crossing. *Refer to RCA Terms and Abstract Concepts [1]*
IPM	Incident Prevention and Management
Map Data	Map Data contains a very detailed microscopic digital representation of the railway network that contains all information necessary for planning and performing railway operations, such as infrastructure characteristics, location and details of Field Elements, etc. The Map Data remain unchanged until the next provisioning of Map Data. *Refer to RCA Terms and Abstract Concepts [1]*
Movement Authority (MA)	Permission for a train unit to run to a specific location within the constraints of the infrastructure and supervision of speed. *Refer to RCA Terms and Abstract Concepts [1]*

Term	Definition
Movement Permission (MP)	A Movement Permission (MP) is an authorisation for a particular Trackbound Movable Object to move in a defined direction, with a defined maximum speed profile, along a defined path (a Linear Contiguous Track Area) on the track network represented as so-called Movement Permission Extent plus safety margins (Risk Path(s) and Risk Buffer). A Movement Permission includes all conditions under which the movement of the Movable Object can be performed safely. A Movement Permission always refers to exactly one Movable Object. *Refer to RCA Terms and Abstract Concepts [1]*
Operating State	The Operating State is the logical real-time representation of the actual state of the physical railway system in the Area of Control. *Refer to RCA Terms and Abstract Concepts [1]*
Operations Manager	The Operations Manager represents a person responsible for the railway operation of the system in a given geographic area. This person is part of the Infrastructure Management entity. The Operations Manager supervises the normal operation performed automatically by Planning System and manages specific actions that cannot be executed automatically. *Refer to RCA System Definition [6]*
Person Supervisor and Locator (PSL)	PSL provides additionally to Mobile Object Locator (MOL) warnings and protection from approaching movable objects. *Refer to RCA Architecture Poster [2]*
Serious accident	Any train collision or derailment of trains resulting in the death of at least one person or serious injuries to five or more persons or extensive damage to rolling stock, the infrastructure or the environment, and any other accident with the same consequences which has an obvious impact on railway safety regulation or the management of safety; 'extensive damage' means damage that can be immediately assessed by the investigating body to cost at least EUR 2 million in total. *Refer to Directive (EU) 2016/798 [5]*
Train Control Management System (TCMS)	Train Control Management System (TCMS) represents the on-board subsystems which are not part of ATO system, with which an interaction is necessary in order to perform automatic railway operations.

Term	Definition
Usage Restriction Area (URA)	A Usage Restriction Area (URA) limits or constrains movements on an area described by an overlapping free but not necessarily connected set of track edge sections. Usage Restriction Areas can be created according to an operational plan (e.g. for enabling construction works) or in response to an Incident (e.g. as a mitigation measure). Various limitations are possible for Usage Restriction Areas e.g. speed reduction or full track closure. Under certain conditions, a Movement Permission may overlap a Usage Restriction Area (e.g. construction vehicle must enter a construction site). Usage Restriction Areas can overlap, for example when multiple construction sites overlap or specific limitations apply to the same location. *Refer to RCA Terms and Abstract Concepts [1]*
Warning Area	A Warning Area is described by a TrackArea in which Authorised Trackside Person must be protected while performing trackside works. The Warning Area is related to a collective Warning Subsystem (light and sound) and/or an individual Warning Subsystem (light, sound, and vibration). These warning subsystems are activated when a Movement Permission is intersecting with the Warning Area AND the Trackbound Movable Object of the Movement Permission is approaching a defined entry point. These devices are deactivated when the (rear end of) the Trackbound Movable Object has left a defined exit point. *Refer to RCA Terms and Abstract Concepts [1]*

1.8.2 Ontology of terms in context of IPM

Within this document the term "**Deviation**" is used based on the ontology shown below to summarise specific undesirable events occurring in the system. Deviation is defined as an unwanted railway event. This includes types of events such as:

Deviation	**Threshold exceedance**	Quantity that has its value outside the required boundary
	Obstacle	An object which is, or might be in the future, within the intended extent of the motion of one train unit and its kinematic envelope. This definition excludes objects that are considered to pose no risk (safety and service quality) to train operations (e. g. newspapers, plastic bag, small bird).
	Failure (of an item)	Loss of ability to perform as required
	Reduced performance	An error by a physical component or system which does not meet the system's reliability requirements which will lead to restrictions and/or change request/command. Reduced Performance may have an impact to operational performance, operational planning and/or maintenance planning within the system.
	Deliberate act	Deliberate Act by humans intended to harm and injure, damage equipment and infrastructure, disrupt operations or compromise safety as well as the reputation in terms of the integrity of infrastructure and perception of safety and security of passengers and staff likewise.

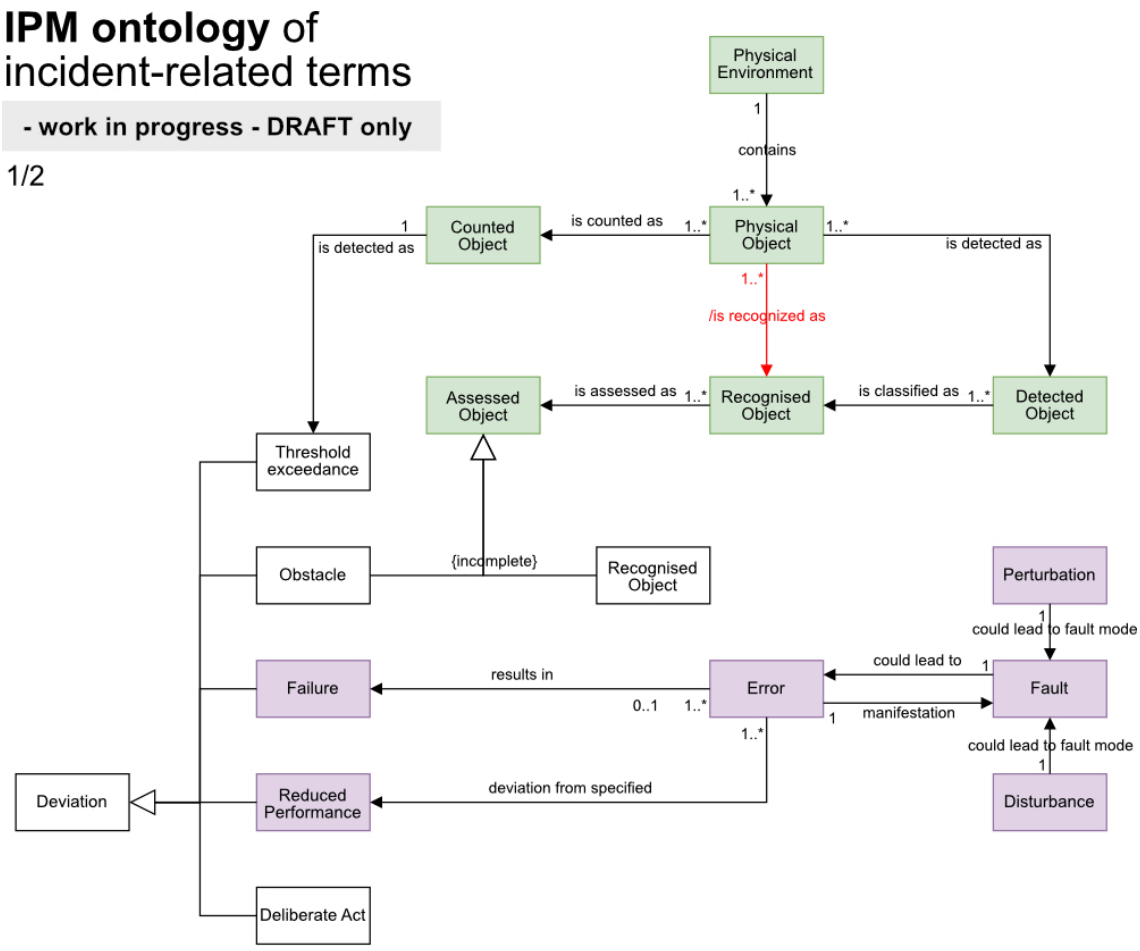

Figure 1: IPM ontology of incident-related terms 1/2

A deviation in this regard can lead depending on its nature to a safety incident/accident, service quality incident or a security incident as depicted in the part of the ontology below. (Refer to Figure 2) An **"Incident"** is defined as any occurrence, other than an accident or serious accident, affecting the safety or quality of railway operations. Incidents and accidents can finally result in a **"Feared Event"** which is defined as a deviation that causes a loss.

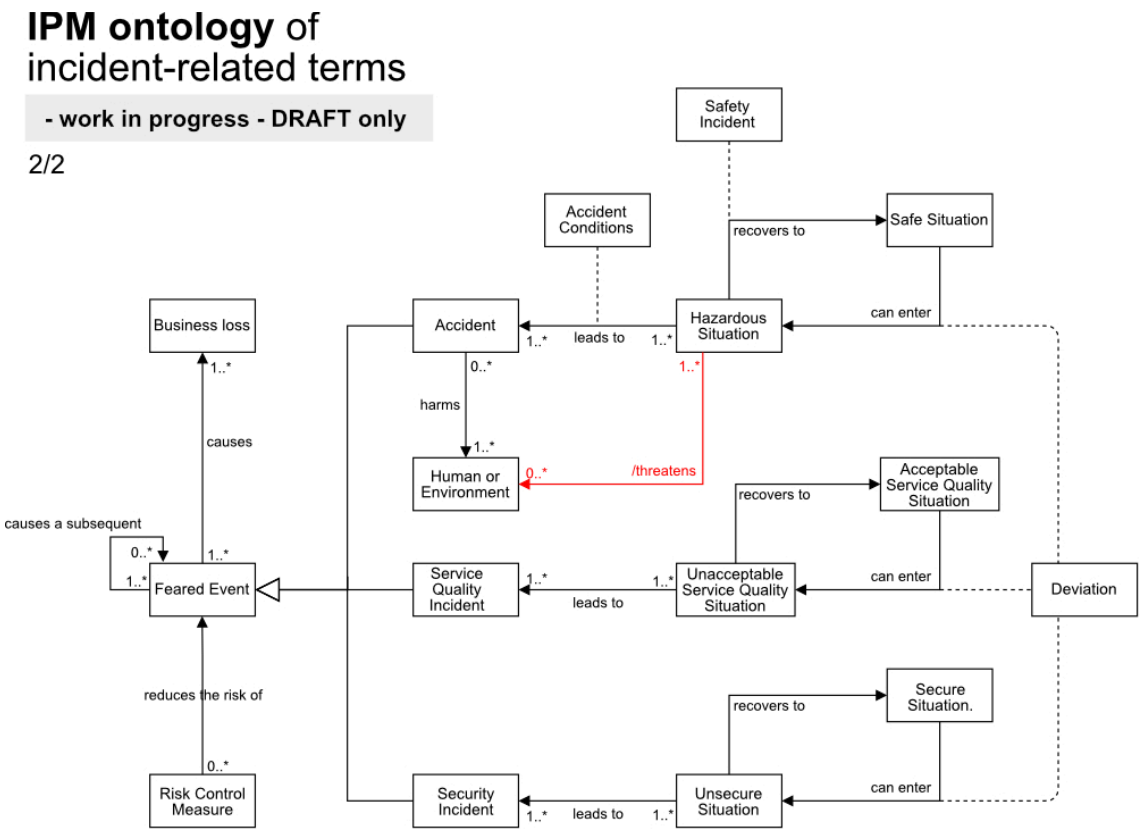

Figure 2: IPM ontology of incident-related terms 2/2

Safety	**Safety incident**	A deviation or near-miss, of internal or external causes, that is likely to lead to some negative consequences (except human harm) and could have compromised safety.
	Hazardous situation	Condition that could lead to an accident.
	Accident	An unintended event or series of events that results in potential loss of life, loss of health or loss of environmental integrity.
Service-Quality	**Unacceptable service quality situation**	Condition that could lead to a service quality incident
	Service quality incident	A deviation, of internal or external causes, that is likely to prevent the system from achieving its anticipated performance (reliability, availability and maintainability) without any compromise on safety.
Security	**Unsecure situation**	Condition that could lead to a security incident
	Security incident	A deviation, which is human intended, that is likely to harm and injure, damage equipment and infrastructure, disrupt operations or compromise safety as well as the reputation in terms of the integrity of infrastructure and perception of safety and security of passengers and staff likewise.

2 Incident Prevention and Management (IPM) as a conceptual proposal to complement the RCA/OCORA architecture

2.1 Current approach of A.P.M. and IPM in RCA/OCORA

The core of the reference CCS trackside architecture is constituted by three groups of subsystems resp. subsystem - "Advanced Protection System" (APS), "Plan Execution" (PE) and "Map Data Management" (MAP). All three together as a concept are called "A.P.M.". [3]

The Traffic Management System (TMS) plans and decides "when is what to do". The Traffic Management System (TMS) continuously re-plans the timetable and decides about measures to optimise the flow of traffic on the network for any planning horizon (short to long-term) and for any type of track usage. TMS is typically a large IT system landscape, which delivers a production plan. To implement the production plan, TMS will generate individual "Operational Plans" for each planned capacity object and will send these "Operational Plans" via SCI-OP (Operational Plan Interface) to subsystem PE (traffic control) and subsystem "ATO Execution" (train control) for execution.

Subsystem PE in turn determines specific requests (e.g. required state of Field Element, the required extent of Movement Permission) based on the "Operational Plan". PE sends these requests to APS via SCI-CMD (Command Interface) just in time for execution. As a gatekeeper APS, based on its geometric safety logic, ensures that every request leads to a safe Operating State and thus to safe railway operation and will reject the requested command otherwise. In addition, the subsystem Safety Manager (SM) as part of APS, monitors the Operating State continuously and reacts with a suitable safety reaction, if an immediate threat to the railway system occurs, e.g. due to spontaneous event in the "real world".

According to the A.P.M concept [3] APS itself is only usable in conjunction with PE since the functionality split and scope is different compared to today's interlockings. To keep the "SIL4-related functionality" as small as possible APS only contains the minimal necessary functions to assure a safe railway operation on the network (in the Area of Control). Additional "traffic control and supervision" functionality shall be allocated to subsystem PE and to subsystem Incident Prevention and Management as proposed in this concept. (Refer to chapter 2.3)

The current overview of RCA/OCORA Subsystem Architecture (track side) [2] depicts the A.P.M. related components and their allocation to layers reflecting the functional separation. (Refer to Figure 3)

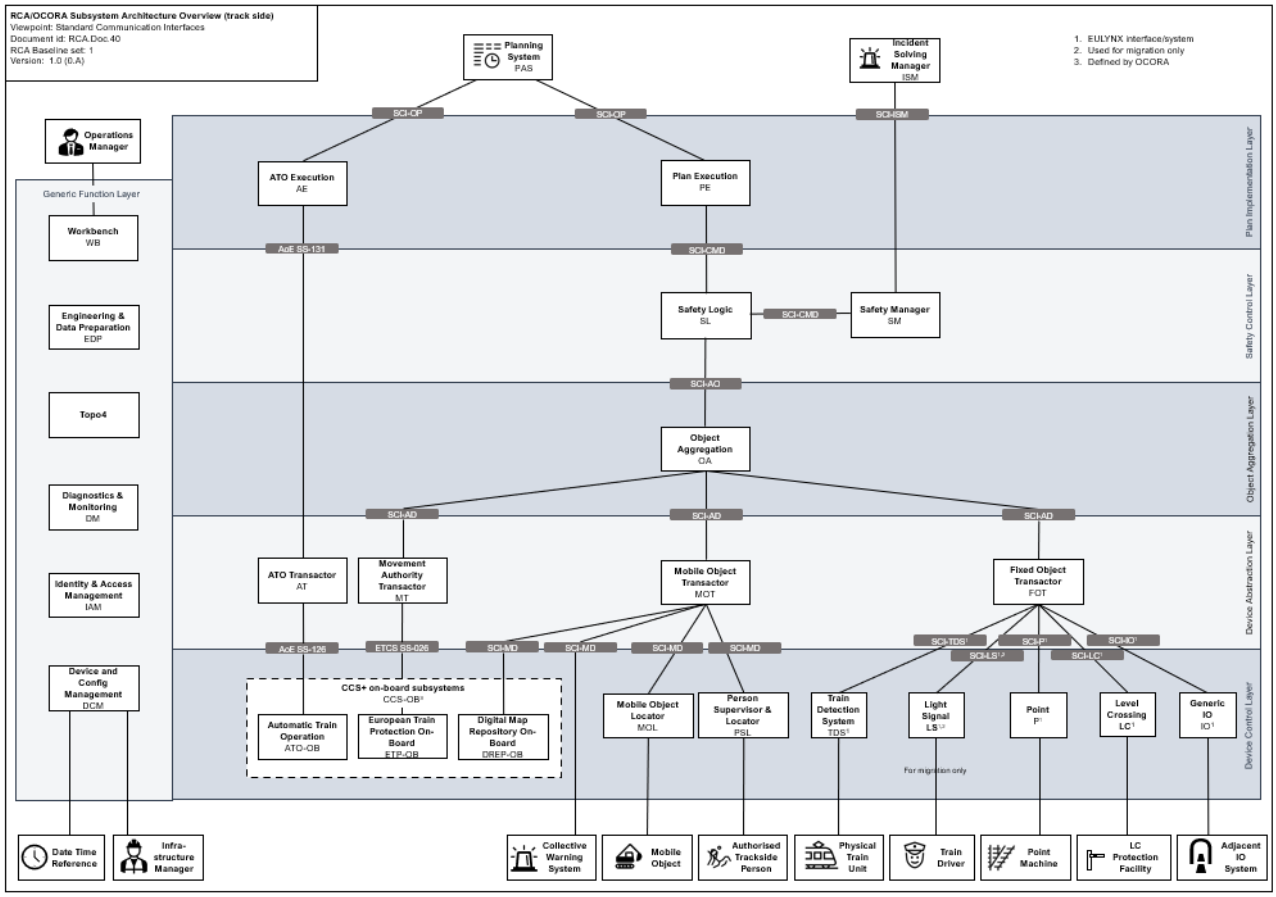

Figure 3: RCA/OCORA Subsystem Architecture Overview (track side)
Refer to RCA Architecture Poster [2]

With regards to train protection and incident management the Safety Control Layer with its allocated components must be pointed out. (Refer also to APS Concept [4])

"Safety Control Layer": Components in the Safety Control Layer ensure a safe future state of the railway network by validating requests and commands, allowing validated requests and commands to reach the Object Abstraction Layer, and reacting to unsafe states of the railway. Components in this layer

- execute combinations of logical functions on strictly abstract representations of real-world elements such as switchable Field Elements and train units,
- publish the aggregated Operating State of the railway especially to the Plan Implementation Layer,
- implement rules only through parameter values in abstract objects, not through IM-specific functions,
- operate in real-time,
- enable modular safety by decoupling the specific behaviour of individual devices from the abstract logic used on this layer.

The main output in this layer is the evaluation and the granting or denying of Movement Permissions requested by the Plan Implementation Layer. Thus, a safe movement path for a train unit is provided including all conditions under which its movement can be performed safely.

Safety Logic (SL) will perform a set of safety checks based on the Operating State to secure a dedicated and safe movement path for a train unit. SL needs the Map Data, the state of all Field Elements, information about existing Movement Permissions, Usage Restriction Areas, Warning Areas as well as the train unit information (capabilities, properties, state) to check reactive, if the requested commands (like the request to extent of a Movement Permission) by subsystems like PE are fulfilling safety constraints

Safety Manager (SM) will provide functionality for a generic risk pattern recognition and implementation of safety measures. SM continuously monitors the Operating State and actively identifies safety incidents and hazardous situations based on configurable risk patterns to mitigate the impact with safety measures.

It is assumed that:

- the Operating State includes the capabilities, properties and state of all Physical Train Units, Field Elements, Authorised Trackside Persons, Mobile Objects, Movement Permissions, Usage Restriction Areas and Warning Areas within the Area of Control.
- SM monitors and evaluates degraded states and failure states as well as safety-relevant alarms to identify safety incidents and hazardous situations related to train protection.
- SM will only respond to safety incidents or hazardous situations which are an immediate threat to the railway system. This means that SM will, for example, only take mitigating safety measures, if the incident concerns a Movement Permission already granted and existing within the Operating State, but not if this is not the case and the incident can be resolved by rejecting requests sent to APS via SCI-CMD (command interface).
- SM can perform the following safety measures (list not extensive):
    - Emergency stop of Physical Train Unit
    - Enforce* shortening / extension of Movement Permission
    - Enforce* downgrade / upgrade of Movement Permission (e.g. speed profile, mode profile)
    - Enforce* creation / removal of Usage Restriction Area

* Enforce means that SM shall be able to demand this action, even if SL would reject the corresponding request.

The current approach of the Open CCS On-board Reference Architecture (OCORA) depicted in Figure 5 does not feature a dedicated Incident Prevention and Management on-board (IPM-OB). According to this architecture ATO on-board (ATO-OB) interfaces with Perception on-board (PER-OB), European Train Protection on-board (ETP-OB) and Localisation on-board (LOC-OB). Perception on-board interfaces with Localisation on-board (LOC-OB) and Digital Map Repository on-board (DREP-OB).

The approach and the benefits to include an Incident Prevention and Management system on-board in OCORA are described in the subsequent section 2.3 as well as in chapter 3 and Annex A.

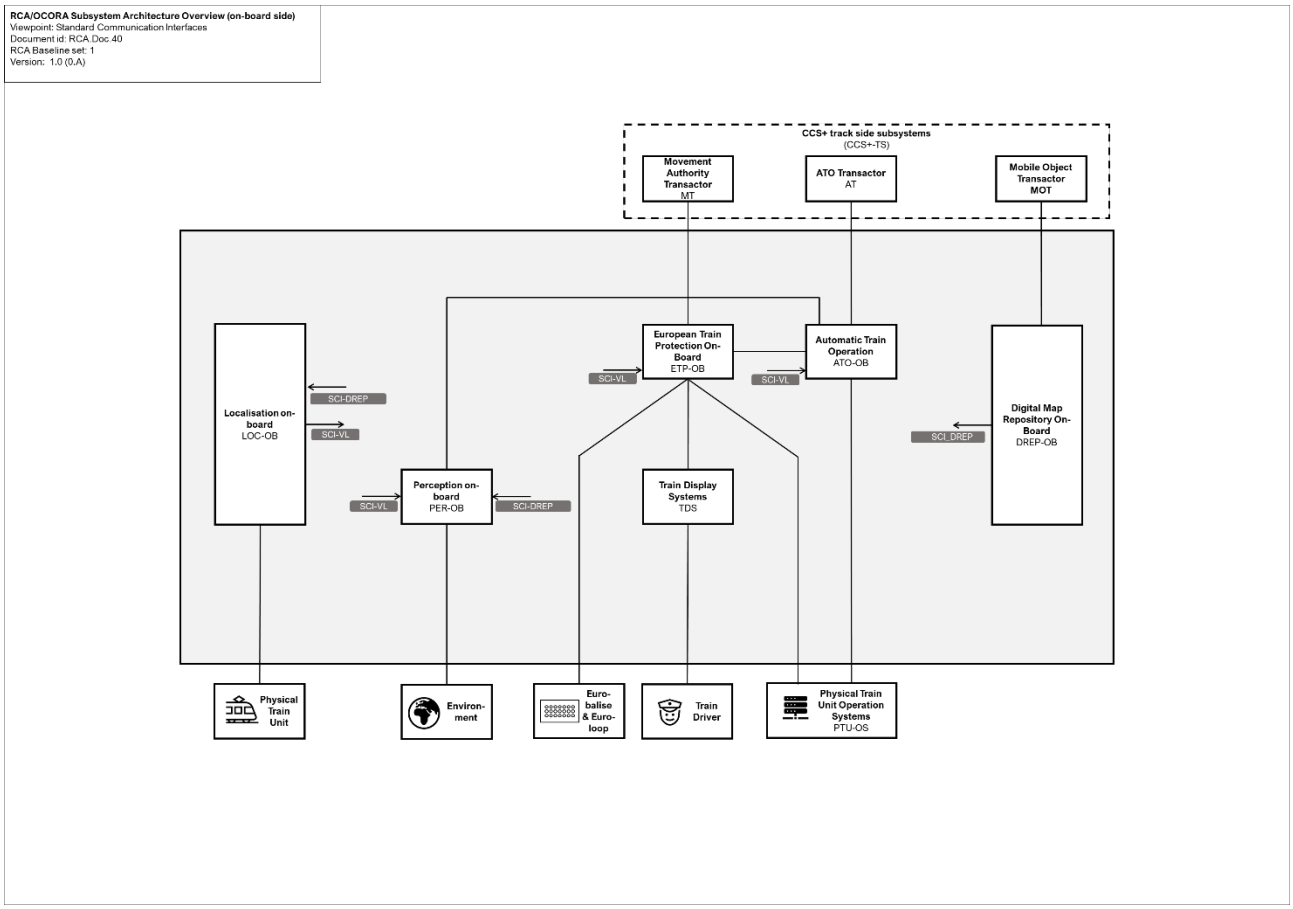

Figure 4: RCA/OCORA Subsystem Architecture Overview (on-board side)
Refer to RCA Architecture Poster [2]

2.2 Principles of Incident Prevention and Management (IPM)

The functional cluster Incident Prevention and Management (IPM) and its related subsystems are responsible for the automated detection and handling of non-regular situations in railway operation. IPM is part of the reference architecture developed by DBS for GoA3/4 operations.

The ambition of IPM is to prevent or mitigate the impact of deviations like low-performance, incidents or accidents as far as possible. The detection of a deviation, the reaction to a deviation as well as the solving of the situation will be part of IPM's scope within the RCA system. Deviations must be handled even before they become a service quality or safety related deviation impacting ongoing or planned train operations. The performance benchmark of IPM are current operational processes and human behaviour of the Train Driver, Operations Manager and all other actors involved who cope with these tasks in a conventional railway system.

On board the train unit, IPM is responsible for the automated detection, continuous monitoring, and handling of abnormal, degraded and emergency situations (e.g. from low performance of entities up to non-regular situations of railway operation) to improve quality and handling of safety related tasks during automated train services. As working hypothesis IPM on-board (IPM-OB) is implementing safety functions, which receive distinct inputs (such as perceived objects, digital map data, localisation data, diagnostic data, etc.), processes these data and derives a safe decision for mitigating the overall risk. This decision is forwarded to executing subsystems such as ETP-OB and TCMS. IPM-OB can be regarded as the planning component of the "sense-plan-act" paradigm of automation.

On the trackside, IPM is responsible for the detection of deviations via systems or actors trackside. The role of IPM trackside (IPM-TS) is to command measures that require balancing and coordination with other systems and actors. It partially handles tasks currently handled by an Operations Manager and other trackside personnel. IPM-TS will cover the detection of deviations and response until solving routines can be initiated by the Incident Solving Manager (ISM). Deviations that are detected via IPM-OB are automatically fed into IPM-TS for further reactions.

Further details about intended scope and functionalities of IPM on-board and trackside are described in chapter 3 as well as in Annex A and Annex B.

Benefits for GoA2

In semi-automated train operations in a GoA2 environment, the Train Driver is responsible for supervising the guideway to prevent or mitigate collision with obstacles or persons on the track, while the ATO-OB controls the acceleration and braking of the train within the limits of a safe speed monitored by the ETP-OB. The Train Driver handles all other train-related failures that can be handled according to skills and responsibilities available. IPM-OB may optionally support the driver tasks here to enhance the quality of services in terms of a timely intervention as well as supporting the driver in tasks requiring documentation or an exchange via radio with trackside entities. IPM-OB paired with a perception system can act as a collision-avoidance warning system informing the driver especially during runs in poor visibility on potential obstacles as well as provide the relevant trackside entities with notifications on obstacles detected on adjacent track to ensure measures are set in place in time.

Furthermore, communication related to deviations occurring on board and in the environment can be transmitted by the system supporting the communication between Train Driver and the operation control centres.

On the trackside IPM-TS can support handling the registration and documentation of deviations reported from train units, occurring in Field Elements or in the tracks supervised ensuring that deviations are handled in time by the Operations Manager or Emergency Control Centre. The increase in network capacity generated by semi-automated train operations as well as the increasing number of train units within this network paired with a higher service quality demand will render every second won as highly valuable. The IPM-TS may therefore act as an automated incident management system proposing steps to be performed by the respective stakeholders and manage the alarms and notifications to the actors.

Necessity for GoA3/4

In driverless and unattended train operations (GoA3/4) the system is supposed to supervise the guideway including the prevention of collision with obstacles or persons on the track. Due to the nature of most heavy rail operations in an open environment there is a necessity for perception systems supervising the guideway and a system to assess the perceived data to identify obstacles and prevent collision or mitigate the impact of the event. IPM-OB is designed to be such a component handling these cases as well as all other train-related deviations such as failures of on-board systems and react accordingly. Furthermore, all communication related to deviations occurring on board and in the environment are registered, documented, and transmitted to the trackside substituting the link between Train Driver and Operations Manager.

In GoA4 operation IPM-OB is responsible to handle (safety-related) validation and verification tasks for automated train preparation and operation which are usually conducted by the Train Driver.

IPM-TS is designed to support the Operations Manager and partly takes over tasks currently done by the Operations Manager in particular regarding the handling of deviations. The system will manage the deviations stemming from both trackside equipment and systems as well as the deviations from all the train units within the Area of Control.

2.3 Integration of IPM in RCA/OCORA and delimitation to current approach

The IPM related subsystems complement the current RCA/OCORA architecture approach for GoA3/4 systems and can optionally be (partly) implemented in GoA2 systems supporting the incident and emergency management and enhancing the resilience of the system in terms of reliability and availability.

IPM is proposed to consist of three (3) subsystems in RCA:

- **Incident Solving Manager (ISM)**, a subsystem not allocated to a specific abstraction layer,
- **Incident Prevention and Management trackside (IPM-TS)** is proposed to be allocated to safety control layer (and/or Plan Implementation Layer)*
- **Incident Prevention and Management on-board (IPM-OB)** as a subsystem on-board within the RCA/OCORA architecture.

*an allocation of IPM-TS to the Plan Implementation Layer appears to be considered as well. The exact allocation on an abstraction layer requires further evaluation in future.

Incident Solving Manager (ISM)

Incident Solving Manager (ISM) comprises the logical component in IPM with the same name (see Annex A). The main task of this subsystem is to manage the recovery from a deviation back to normal operations. The subsystem is supposed to feature only one interface to another RCA subsystem, the IPM-TS. (Refer to Figure 5)

Incident Prevention and Management System Trackside (IPM-TS)

Incident Prevention and Management trackside (IPM-TS) is designed to have interfaces with ISM, IPM on-board (IPM-OB) as well as the Safety Logic (SL). The main tasks are to manage all trackside deviations as well as deviations reported by the train units within the Area of Control. There is no direct interface to the Safety Manager (SM). The SL is reporting deviations to IPM-TS as well as the safety reactions performed by SM (Refer to Figure 5).

Incident Prevention and Management System On-board (IPM-OB)

Incident Prevention and Management on-board (IPM-OB) is proposed to be part of the RCA/OCORA architecture and features interfaces to Perception on-board (PER-OB), European Train Protection on-board (ETP-OB), Automatic Train Operation on-board (ATO-OB), Localisation on-board (LOC-OB) as well as the Digital Map Repository on-board (DREP-OB). The communication to the trackside is realised via an interface with IPM-TS. (Refer to Figure 6)

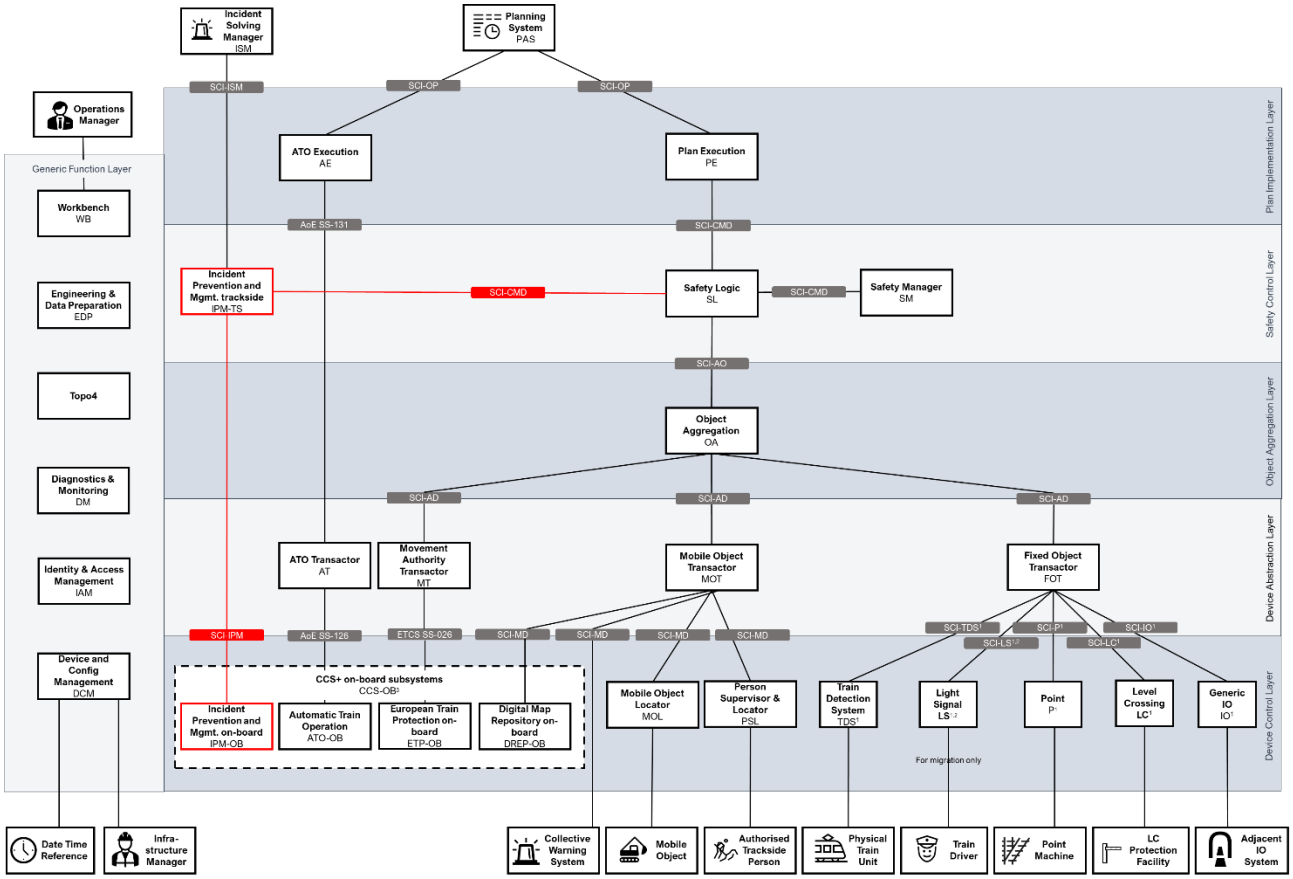

Figure 5: RCA/OCORA Subsystem Architecture Overview (trackside) with IPM-TS

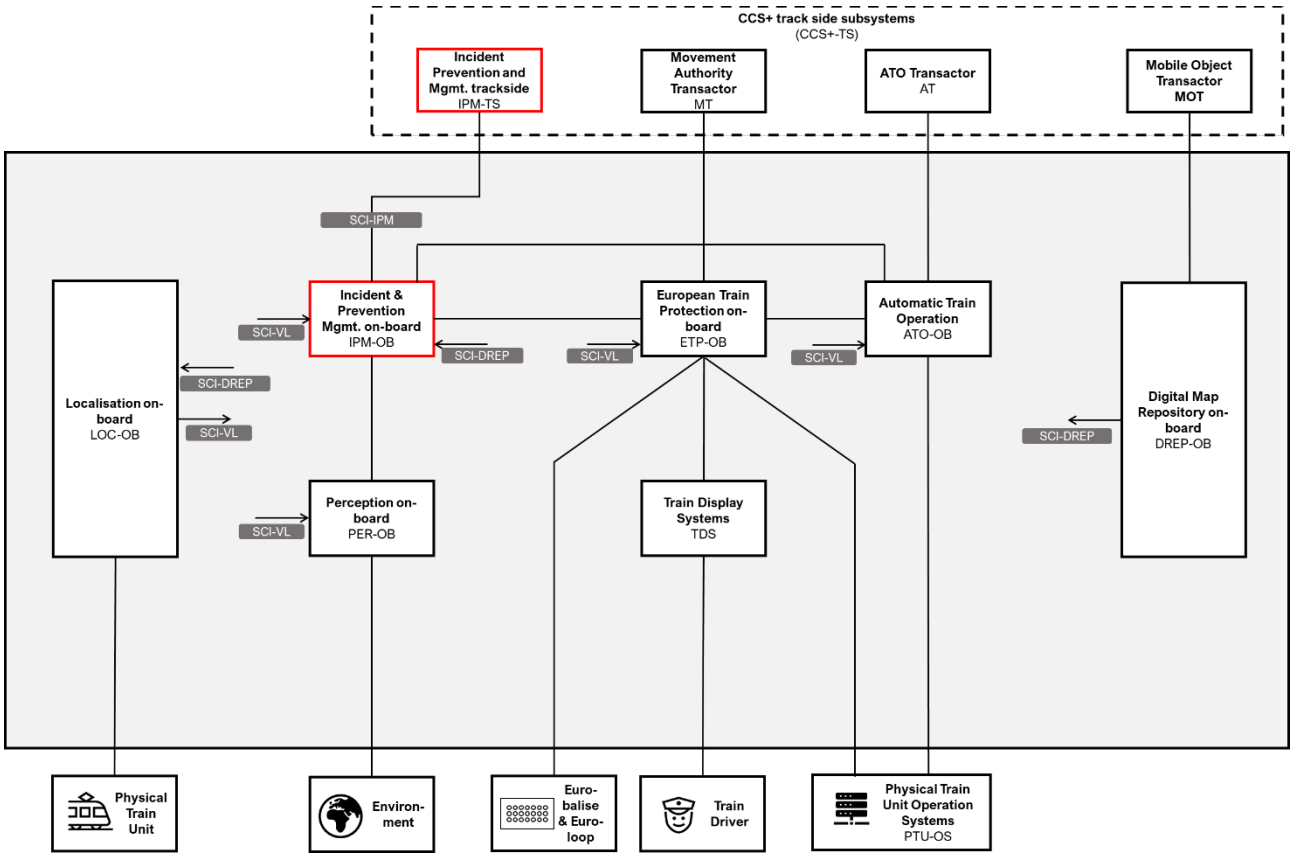

Figure 6: RCA/OCORA Subsystem Architecture Overview (on-board side) with IPM-TS

2.3.1 IPM-TS and Safety Manager (SM)

IPM-TS complements the Safety Manager (SM) on the trackside in GoA3/4 systems, covering the identification, response, and recovery measures outside the scope of SM as well as partly the tasks performed by the Operations Manager and Emergency Control Centre in terms of deviations. The scope of IPM covers safety-related and system performance quality-related deviations. IPM detects deviations before they are becoming an immediate threat to the railway system, when the CCS system is forced to response, thus covering a wider scope than SM to maintain a certain level of availability and reliability in the system.

The SM is supposed to monitor the Operating State of the safety-relevant trackside elements and the positions of train units operating within the Area of Control. Certain safety-related deviations are identified by SM and are then treated independently from IPM-TS. IPM-TS is indirectly informed on measures taken by SM via the interface to the digital map subsystem.

On board train units, IPM is the substitute system for tasks performed in GoA2 systems by the Train Driver and partly the tasks by the Operations Manager in terms of deviations.

2.3.2 IPM-TS and Safety Logic (SL)

After a deviation is detected by IPM-TS a response in form of a reaction is planned and commanded to other systems to perform these. Safety Logic (SL) is one of the subsystems amongst others that IPM-TS utilises to perform a reaction. The reactions IPM-TS commands to SL are Usage Restriction Areas, usage restrictions for tracks. These restrictions can range for instance from a full track closure to restrictions regarding certain train types or speed restrictions.

Safety-relevant failures of wayside equipment are reported by the respective equipment to SL via the Fixed Object Transactor (FOT) and the Object Aggregator (OA). IPM-TS receives the report on a failure from SL. In case of an immediate threat to the system, i.e. train unit immediately exposed to this threat, the Safety Manager will react by imposing a restriction via SL.

2.3.3 IPM-TS and Mobile Object Locator (MOL) / Person Supervisor & Locator (PSL)

The monitoring and warning of Authorised Trackside Persons and Mobile Objects such as track bound machinery in terms of potential conflicts with movements of train units is currently part of the IPM concept. Authorised Trackside Persons are directly warned by IPM if a conflict is identified. Authorised Trackside Persons are then supposed to leave the respective track zone they are currently located in within a specific time subject to the speed and distance of the train unit approaching. If the Authorised Trackside Persons are not leaving the respective track zone to a safe zone, a deviation is registered that may lead to a reaction of the IPM system. The same process applies to mobile objects.

The SM monitors Authorised Trackside Persons as well as Mobile Objects in terms of the Operating State leading to a safe reaction from SM in case that a conflict with a set route for a train unit is detected.

The IPM approach is designed to warn Authorised Trackside Persons or personnel operating Mobile Objects before a conflict is detected by SM. Information on the position within a specific safe zone, where Authorised Trackside Persons and Mobile Objects are safe to dwell but no other (unauthorised) persons or machinery, is passed on to IPM-OB. The Authorised Trackside Persons or machinery is then recognised by the system as an expected object safe to dwell without evoking a reaction by the IPM-OB.

3 Scope and functionalities in IPM

The scope of Incident Prevention and Management (IPM) is the detection, response and recovery from events constituting or leading to a possible deviation in the automated railway system both on board a train unit and within the network.

IPM consists of components both on board a train unit and trackside. IPM on-board substitutes or supports the Train Driver in deviation-related tasks and safety-relevant tasks outside the scope of the ETP-OB and ATO-OB. IPM trackside manages the deviation-related tasks outside the scope of the CCS systems such as but not limited to monitoring the current traction system as well as the mitigation of deviations like overcrowded platforms.

IPM on-board (IPM-OB) will in general cover

- Detection and prediction of deviations by on-board systems affecting the train unit or entities
- Response to deviations in form of reflexive and evaluated reactions by on-board means
- Recovery from deviations by on-board means
- Management of safety-related tasks outside the scope of ETP-OB and ATO-OB.

IPM trackside (IPM-TS) will in general cover

- Detection and prediction of deviations by trackside systems and actors
- Response to deviations in form of evaluated reactions by trackside means
- Recovery from deviations by trackside means (incl. request to actors)
- Collect and update the state for all deviations in a defined Area of Control (operational situation)
- Management of communication to actors for all IPM components
- Warning of Authorised Trackside Persons in case of conflict with train movements

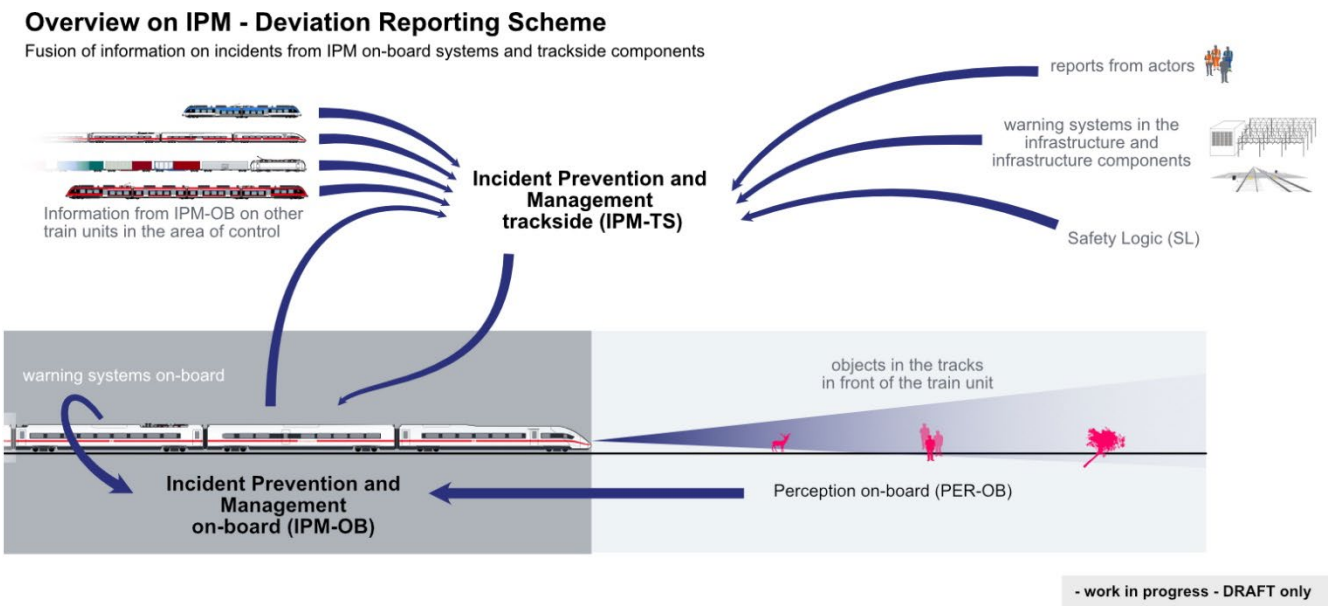

Figure 7: Overview on IPM – Deviation Reporting Scheme

The following list, Table 1, provides an overview of the logical components proposed for IPM on-board and trackside. The logical components detailed here represent the current architecture hypothesis as proposed and elaborated by DBS.

Table 1: Overview of the scope of IPM on-board and trackside components (on-board marked in grey)

Logical component	Abbrev.	Location of log. comp.	Detection functions	Reaction functions	Recovery functions	Auxiliary functions
Incident Register and Monitoring	**IRM**	on-board	✓			
Safe Reflexive Reaction Controller	**SRRC**	on-board	✓	✓		
Evaluated Train Manager	**ETM**	on-board		✓		✓
State and Mode Manager On-board	**SMMO**	on-board				✓
Incident Solving Manager On-board	**ISMO**	on-board			✓	✓
Incident Register and Monitoring Trackside	**IRMT**	trackside	✓			
Authorised Staff Monitoring	**ASM**	trackside	✓	✓		
Evaluated Reaction manager	**ERM**	trackside	✓	✓		✓
Incident Solving Manager	**ISM**	trackside			✓	✓
Actor Communication Platform	**ACP**	trackside	✓	✓	✓	✓

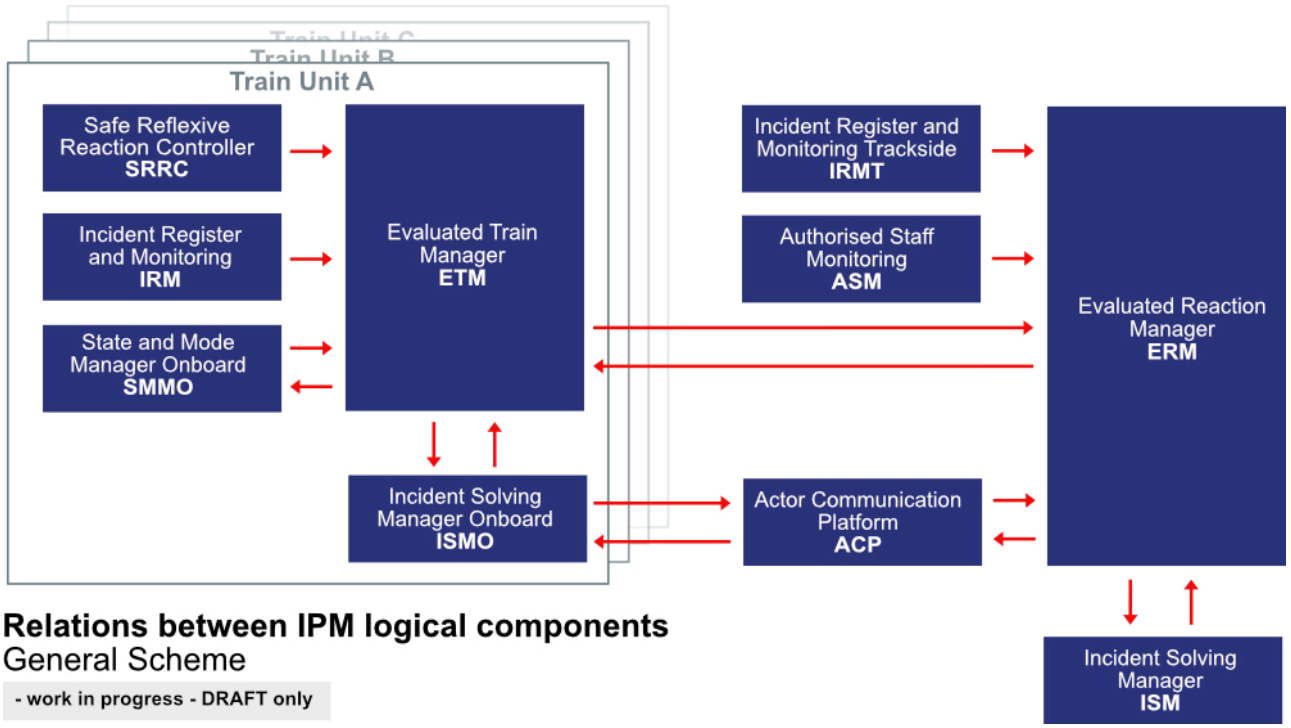

Figure 8: General Scheme on relations between the logical components in IPM on-board and trackside

3.1 Detection of Deviations

The scope of IPM encompasses the detection of deviations impacting or potentially impacting safety of train operations that are not within the scope of SL or SM. IPM will furthermore also detect deviations that have or may potentially have an impact on the service quality of train and network operations which are not covered as part of the TMS. These quality-related deviations include the availability and performance of train units as well as infrastructure components.

Table 2: Scope of deviation detection by IPM on-board and trackside components (on-board marked in grey)

Logical component	Scope of deviations registered
Safe Reflexive Reaction Controller (SRRC)	Registers deviations from perception systems monitoring the environment around the train unit
Incident Register and Monitoring (IRM)	Registers deviations on-board reported by the train unit's TCMS and other systems
Evaluated Train Manager (ETM)	Consolidation of deviation reports from different sources on-board
State and Mode Manager On-board (SMMO)	Registers deviations on-board stemming from other automation-relevant systems.
Incident Register and Monitoring Trackside (IRMT)	Registers deviations trackside reported by trackside systems and sensors
Actor Communication Platform (ACP)	Registers deviations reported by (human) actors
Authorised Staff Monitoring (ASM)	Registers deviations in terms of (potential) conflicts between positions of authorised staff and train movements
Evaluated Reaction manager (ERM)	Consolidation of deviation reports from different sources trackside and the respective systems on train units within an Area of Control. Registers deviations based on pattern analysis of existing deviations.

The deviations and the attributes or circumstances leading to this distinction into a deviation will be registered in form of a deviation report. The deviation report is a unified structure recording the attributes of a deviation. As the nature of the deviation as well as the amount of input data from the reporter might differ not all items in this deviation report might be filled. The deviation report is further enriched with data from database sources than the original reporter sources providing for instance geographical data.

Deviation reports from different reporting sources that register the very same deviation are merged resulting in a consolidated deviation report. This allows the system to enrich the data received from a single reporting source with other sources to increase the comprehension of the nature of the deviation. This more comprehensive view on the deviation allows dedicated bundled reactions taking place to mitigate the impact of the event or prevent a further escalation of the deviation as opposed to reacting to each single deviation report. The consolidation step provides furthermore an overview on all on-going deviations reported, prioritizing the most relevant ones. The consolidation of deviation reports occurs both on-board for deviation reports registered by on-board systems and trackside for deviation reports coming from trackside systems and the consolidated deviation reports coming from the respective train units within an Area of Control. (Refer to Figure 9)

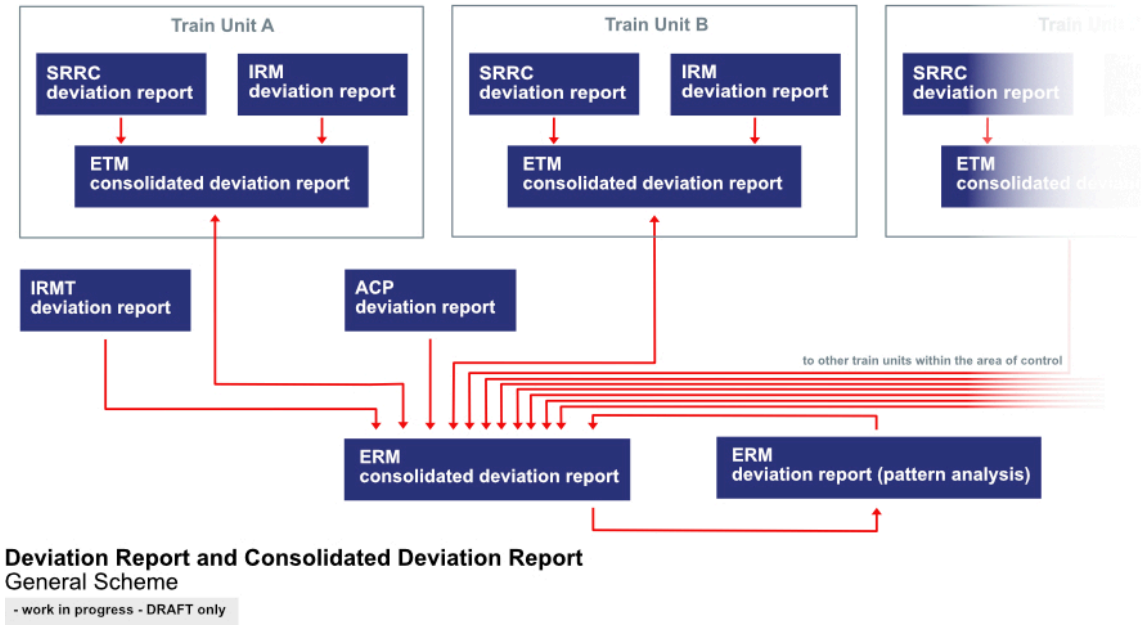

Figure 9: Deviation reports and consolidated deviation reports (general scheme)

3.2 Response to Deviations

Responses to deviations are carried out in form of reflexive reactions and evaluated reactions. Reflexive reactions are planned and commanded by SRRC as an instantaneous response to an obstacle that poses an immediate threat to the train unit itself. Evaluated reactions are planned and commanded by both ETM on board the train unit and the ERM trackside based on the consolidated deviation reports.

On-board reactions both reflexive and evaluated are planned and commanded by the IPM on-board systems using the existing functions of other systems on board, mainly the Train Control and Management System (TCMS) and ETP-OB. Trackside reactions are planned and commanded by IPM-TS using the existing functions of other systems such as SL.

Limited response functions are also incorporated into the State and Mode Manager (SMMO) and the Authorised Staff Monitoring (ASM) components triggering a reaction only for specific deviation.

Table 3: Scope of response to deviations by IPM on-board and trackside components (on-board marked in grey)

Logical component	Scope of responses to deviations
Safe Reflexive Reaction Controller (SRRC)	Reflexive reactions to obstacles on or near the line that pose an immediate threat to the train unit itself.
Evaluated Train Manager (ETM)	Evaluated reactions limited to reactions by the train unit itself.
State and Mode Manager On-board (SMMO)	Reaction in terms of denying departure, if the ready-for-departure state and specific criteria are not met.
Authorised Staff Monitoring (ASM)	Reaction in terms of generated warning to authorised staff in case of conflict between their position and train movements.
Evaluated Reaction Manager (ERM)	Evaluated reactions by trackside means for deviations both detected trackside and on board a train unit within an Area of Control.

3.3 Recovery from Deviations

The recovery from a deviation is planned by the Incident Solving Manager On-board (ISMO) and the Incident Solving Manager (ISM). The ISMO plans, commands, and solves deviations by on-board means for the respective train unit it is installed on. The ISM is the equivalent system on the trackside covering a wider range of measures to solve the deviation.

The ISMO commands and requests solving measures to be performed by resources available on board. These can be both, systems and human actors (e.g. train attendants if available). ISM trackside commands and request resources available trackside to perform the solving measures for both on-board and trackside deviations with access to a higher variety of systems and thus measures as well as a large pool of external actors. The communication between ISMO and ISM to actors is managed via the Actor Communication Platform (ACP). (Refer to Annex B)

The recovery from a deviation can range from solving a non-incident, where an obstacle was detected and a collision prevented due to the obstacle leaving for a safe environment, to solve a large-scale accident involving a variety of stakeholders.

Table 4: Scope of recovery from deviations by IPM on-board and trackside components (on-board marked in grey)

Logical component	Scope of recovery
Incident Solving Manger On-board (ISMO)	Recovery of deviations by on-board means for the respective train unit.
Incident Solving Manager (ISM)	Recovery of deviations by trackside means for both deviations on-board of train units and trackside.
Actor Communication Platform (ACP)	Shares information on the deviation with relevant and authorised actors and channels solving tasks to relevant actors.

3.4 Auxiliary functions

This section lists further supporting functions within IPM apart from the detection, reaction, and recovery from deviations.

3.4.1 State and mode handling on-board

IPM-OB is supposed to substitute safety-relevant tasks of the Train Driver as the ATO-OB is supposed to be designed as a system with a lower safety requirement. Tasks to manage the states and modes of ATO on-board systems as well as engaging ATO-OB to start driving after successfully verifying that all ATO systems are working sufficiently and there are no obstacles ahead in the immediate driving path.

3.4.2 Configuration of systems

The evaluated reaction components (ETM / ERM), recovery components (ISMO / ISM) as well as the actor communication platform (ACP) feature an interface to change the current settings. This facilitates the change of thresholds and patterns for the detection of deviations as well as the reactions for mitigation or prevention by authorised and relevant actors.

These settings shall be configurable by authorised actors or system enabling an adaptation to local / regional conditions, the current state of the network or performance quality-related values.

The actor communication platform features a function to manage the actor profile settings and their rights. The actor profiles should be amendable to reflect organizational changes or changes of responsibilities on behalf of an actor. New actors can be for instance added in case that a new entity is formed with a specific responsibility in case of a deviation.

Table 5: Configuration scope in IPM on-board and trackside components (on-board marked in grey)

Logical component	Availability validations
Evaluated Train Manager (ETM)	Configuration of evaluated reactions, deviation patterns and their respective attributes for the train unit
Incident Solving Manger On-board (ISMO)	Configuration of solving chains and tasks including their allocation to actors on-board
Evaluated Reaction Manager (ERM)	Configuration of evaluated reactions, deviation patterns and their respective attributes for trackside reactions
Incident Solving Manager (ISM)	Configuration of solving chains and tasks including their allocation to actors trackside
Actor Communication Platform (ACP)	Configuration of actor profile settings including rights management

3.4.3 Availability of reactions and solving measures

The availability of reactions and solving measures is monitored by the system based on the capabilities available both for on-board systems as well as trackside systems. This allows the system to adapt and choose another suitable reaction or solving measure available to a deviation in case of unavailability.

Table 6: Availability functions for measures by IPM on-board and trackside components (on-board marked in grey)

Logical component	Availability validations
Evaluated Train Manager (ETM)	Availability of evaluated reactions in terms of resources available
Incident Solving Manger On-board (ISMO)	Availability of solving measures in terms of resources (incl. actors) available
Evaluated Reaction Manager (ERM)	Availability of evaluated reactions in terms of resources available
Incident Solving Manager (ISM)	Availability of solving measures in terms of resources (incl. actors) available
Actor Communication Platform (ACP)	Availability of actors available for reactions and solving measures

The Actor Communication Platform will validate the availability of actors for reactions, notifications and solving measures. This availability information is then transmitted to the relevant functions in ETM, ISMO, ERM and ISM.

3.4.4 Train Capability Report

The logical component Evaluated Train Manager (ETM) features the generation of the Train Capability Report (TCR) providing a comprehensive overview on the operational situation of the train unit. The report contains the health and performance state of the on-board components, static and dynamic train data as well as the list of current on-going deviations related to the train unit registered by the system.

3.4.5 Infrastructure Capability Report

The logical component Evaluated Reaction Manager (ERM) features the generation of the Infrastructure Capability Report (ICR) providing a comprehensive overview on the operational situation of the respective Area of Control. The report contains the health and performance state of the trackside components, data on trains within the Area of Control as well as the list of current on-going deviations registered by the system both from trackside and on-board sources.

4 Conclusion and Next Steps

This document is the first draft of a concept for an Incident Prevention and Management (IPM) system. This concept will in future be refined further if a concept for SM is available to allow a seamless integration.

Open issues that require clarification in future:

- Integration of an IPM system within RCA/OCORA
- Extend of application for IPM
    - IPM as an inherent part of RCA for operations in a GoA3/4 environment or parts of the network with high demand on route capacity
    - Utilisation of an IPM system in a GoA2 environment as an option allowing a future migration to GoA3/4 or seamless interoperability with other systems in GoA3/4
- Distinction of scope between IPM and A.P.M

Annex A: Logical components of IPM On-board

The logical components detailed here represent the current architecture hypothesis as proposed in DBS. *Please note, that the labelling of other logical components or subsystems might differ from the names and abbreviations used for the RCA/OCORA architecture.*

Incident Register and Monitoring (IRM)

The logical component **IPM - Incident Register and Monitoring (IRM)** registers and monitors multiple events and relevant data to compute and classify deviations for the respective Train Unit.

IPM-IRM retrieves evaluated health and performance data from DIA-VEC and DIA-DHM. As DIA-VEC and DIA-DHM are supposed to be a basic integrity system IPM-IRM must retrieve safety related failure and event data directly from TCMS. Based on this data IPM-IRM determines the impact on operation for the Train Unit. The function's output is a failure deviation report which is provided to IPM-ETM as an input for further handling of the deviation.

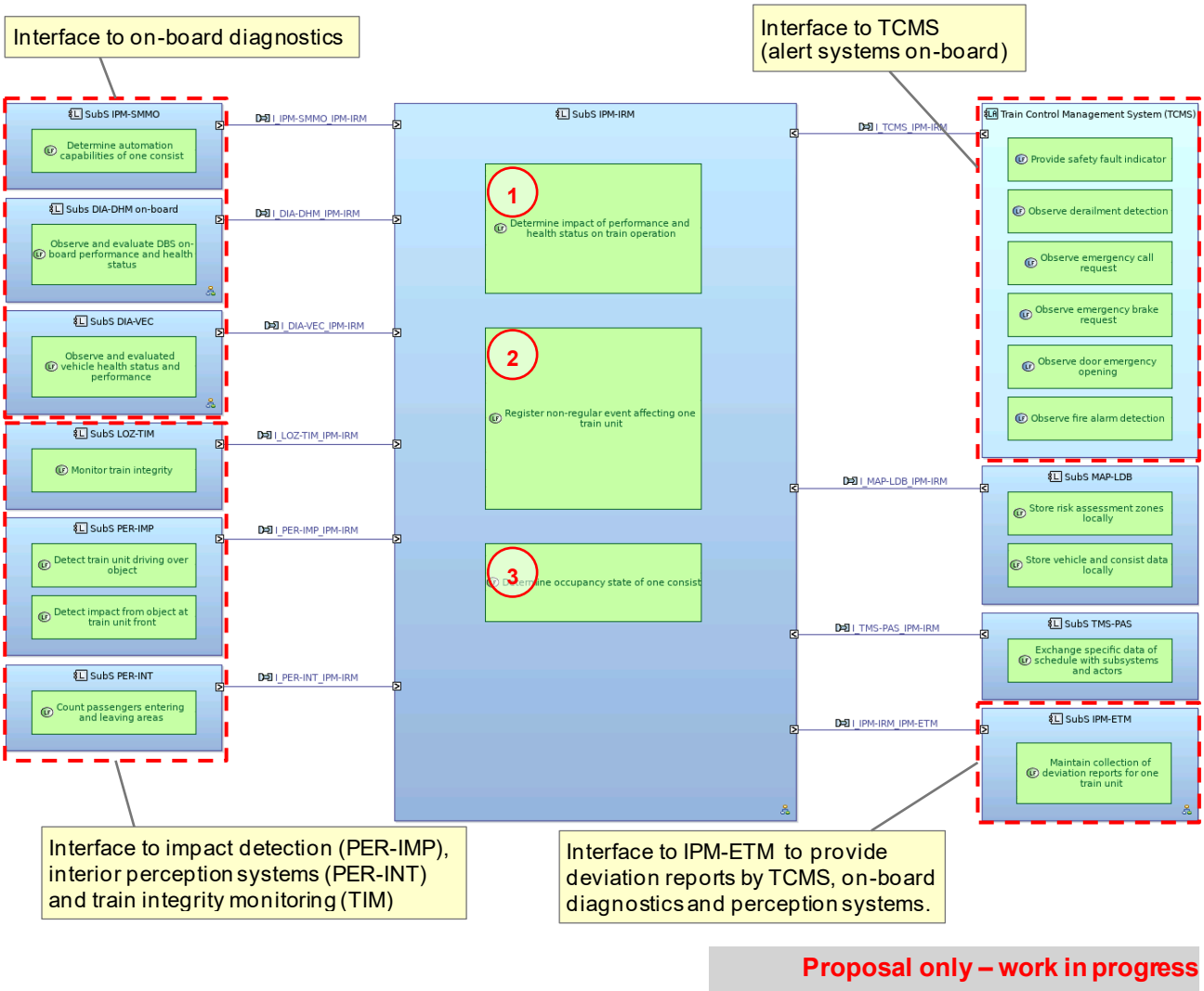

Figure 10: [LAB] IPM-IRM [Conceptual functional context]

(1) Logical Function: Determine impact of performance and health status on train operation

This function determines the impact of the performance and health status, pre-processed by DIA, on operation for one Train Unit taking safety related data from TCMS (safety fault indicator, speed limitation, operating time limitation) into account. Deviations registered are structured into a deviation report and forwarded to ETM.

Based on the available information this function provides (input to) the train capability report (TCR) which is used by the traffic management system (TMS) to optimise the schedule taking actual operational capabilities of the Train Unit into account.

(2) Logical Function: Register non-regular event affecting one train unit

This function registers all receiving non-regular situation (NRS) events that are provided by sensors / on-board subsystems. In case of a deviation, a deviation report is forwarded to ETM to initiate a reaction. The Train Unit composition data and the Train Unit location are used to enrich the forwarded deviation report.

(3) Logical Function: Determine occupancy state of one consist

This function monitors the occupancy state of each consist for a Train Unit to identify overcrowding. The occupancy state is calculated based on the actual number of passengers and the capacity of the consist. A deviation is registered in form of a deviation report and forwarded to ETM.

Safe Reflexive Reaction Controller (SRRC)

The logical component **IPM - Safe Reflexive Reaction Controller (SRRC)** analyses the data within the scene model in front of the Train Unit captured by the on-board perception system to determine if an object is an obstacle for the Train Unit. The objects in the situation model are assigned to risk assessment zones according to their position. If the object was classified (recognised) as a moveable object (object class) the future behaviour of the object will be predicted to identify changes in the risk assessment zone allocation.

Objects within the ego route space in front of the train within an existing track route as defined by a Movement Permission for train, will be forwarded to decide a reflexive reaction. Objects outside the ego route space associated with the track route of the Train Unit are evaluated according to their impact on rail operations by IPM-ETM.

IPM contains several functions to command the execution of immediate measures, the reflexive reactions. While several events might trigger the same reflexive reaction, a single event can trigger none or several (0-n) reflexive SRRC reactions. A deviation report is then generated for the situation that includes the reactions performed.

If the object does not trigger a reflexive reaction as it is not deemed as an immediate threat but a threat to the system or other train units in general, this applies for instance to objects on the adjacent track or that might become a potential obstacle in future, a deviation report is generated. The deviation reports generated are forwarded to ETM.

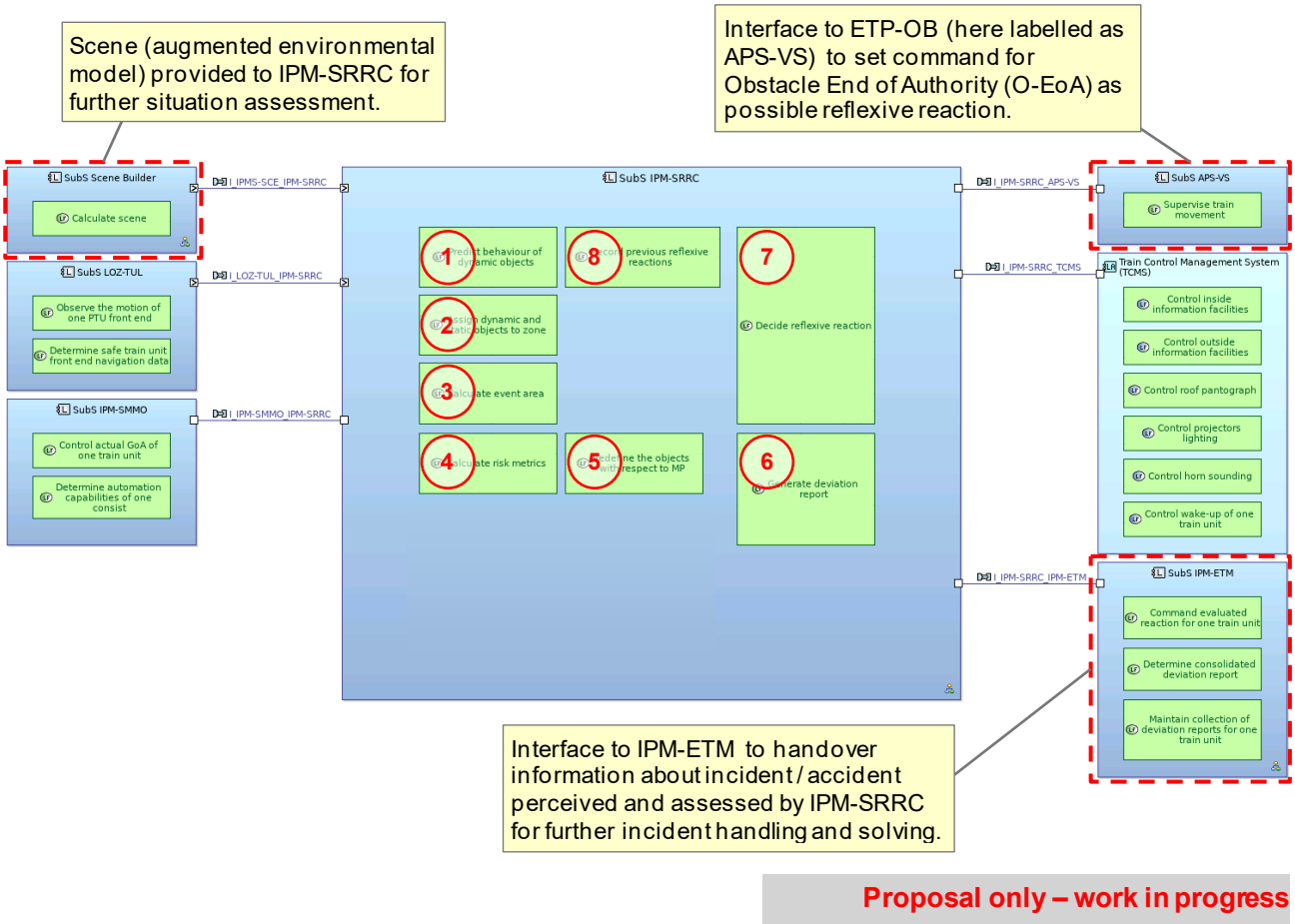

Figure 11: [LAB] IPM-SRRC [Conceptual functional context]

(1) Logical Function: Predict behaviour of dynamic objects

This function analyses the behaviour of an object to predict positions the object might shift in near future. It is provided with information on the object class, data on movement of the obstacle (movement vector), location and precise information on the environment (structures / topography) to estimate if the object is moving to another location.

(2) Logical Function: Assign dynamic and static objects to zone

This function assigns a list of recognised objects to a risk assessment zone (e. g. track zone or overhead line equipment zone). This assignment applies to both static and dynamic objects as well as their predicted positions.

(3) Logical Function: Calculate event area

This function assesses and determines an event area for an object. The event area comprises the object and a safety margin around it. It uses the location (incl. topology), risk assessment zone, object class, data on movement of the obstacle to define the size of the event area.

(4) Logical Function: Calculate risk metrics

This function calculates metrics (TTX and PET) for further assessment of the probability of an impact with the candidate object. Risk metrics are calculated based on the event area for both the current object position (detection) as well as for a predicted future position (behaviour prediction).

(5) Logical Function: Redefine the objects with respect to MP

This function assesses the criticality of candidate objects and forwards them according to their actual and/or predicted location (event area) to either „Decide reflexive reaction“ (SRRC) or IPM-ETM.

static objects

- if the actual position of the candidate object is within the ego route space (MP) of the Train Unit, the object shall be further processed in „decide reflexive reaction“ by IPM-SRRC.
- if the actual event area of the candidate object was generated for an adjacent or neighbouring track or the object position is outside the ego route space (MP), the object shall be further processed by IPM-ETM.

dynamic objects

- if either the actual or predicted positions of the candidate object was or were generated for the ego route space (MP) of the Train Unit, the object shall be further processed in „decide reflexive reaction“ by IPM-SRRC.
- if both the actual and predicted event areas were generated for an adjacent or neighbouring track or both the actual and predicted object positions are outside the ego route space (MP), the object shall be further processed by IPM-ETM.

(6) Logical Function: Generate deviation report

This function generates a deviation report to facilitate transfer of information about static or dynamic objects with event areas inside and outside the MP for further processing in IPM-ETM.

(7) Logical Function: Decide reflexive reaction

This STUB function assesses if one or several reflexive reactions are necessary based on train speed and location, the actual braking distance and the actual situation model which includes recognised object(s) with event area(s) assigned to risk assessment zones and calculated risk metrics (TTX, PET). Furthermore, an inhibition of one or several reflexive rules by IPM-ETM is considered.

For decision making deterministic rules as well as artificial intelligence are applied. Rules and algorithms can be configured and trained. Decisions for reflexive reactions are validated with internal methods.

Reflexive reactions to be commanded include, but are not limited to:

- Control horn sounding
- Control passenger information devices inside the passenger cabin
- Control passenger information devices on the exterior of the train unit
- Control roof pantograph
- Control projector lighting
- Set stopping point (Obstacle End-of-Authority) *

* Obstacle End-of-Authority (O-EoA) refers to a virtual stopping point commanded by IPM-OB to ETP-OB.

(8) Logical Function: Record previous reflexive reactions

This function stores the reflexive reactions commanded for an object based on its ID (object ID / object group ID). Information on previous reactions is considered for objects with the same IDs when commanding another reflexive reaction (decide reflexive reaction) and predicting the behaviour of the object at later timestamp (predict behaviour of dynamic objects).

Evaluated Train Manager (ETM)

The logical component **IPM - Evaluated Train Manager (ETM)** receives deviation reports for the respective Train Unit. In case of a deviation, IPM-ETM decides, which evaluated reaction for the Train Unit is required to prevent a further escalation of the deviation or mitigate the impact of the deviation.

Deviations detected including the situation and circumstances will be reported in form of deviation reports into the ETM from IRM, SRRC as well as the Actor Communication Platform (ACP). The IPM-ETM subsystem is responsible to consolidate deviation reports from different sources on the same deviation and enrich them with relevant data. The consolidated deviation report is then used to prioritise against other on-going deviations in terms of the urgency of reactions required. Reactions commanded by the IPM-SRRC or IPM-ETM are to be part of the deviation report. Based on this consolidated deviation report IPM-ETM is to determine evaluated reactions for the respective Train Unit. A deviation might trigger one or several evaluated reactions or none, in case that another (reflexive or trackside evaluated) reaction is set to be commanded.

Furthermore IPM-ETM must handle safe boarding of passengers at station platforms. For this purpose, additional perception systems installed on the Train Unit (hypothesis) perceive the area beside the Train Unit along the platform, including a monitoring of the gap between platform and Train Unit. IPM-SRRC assesses the scene in the field of view beside the Train Unit (with dynamic and static objects assigned to zone) and provides the situation model with event areas to IPM-ETM for further assessment. A detailed concept must be further developed.

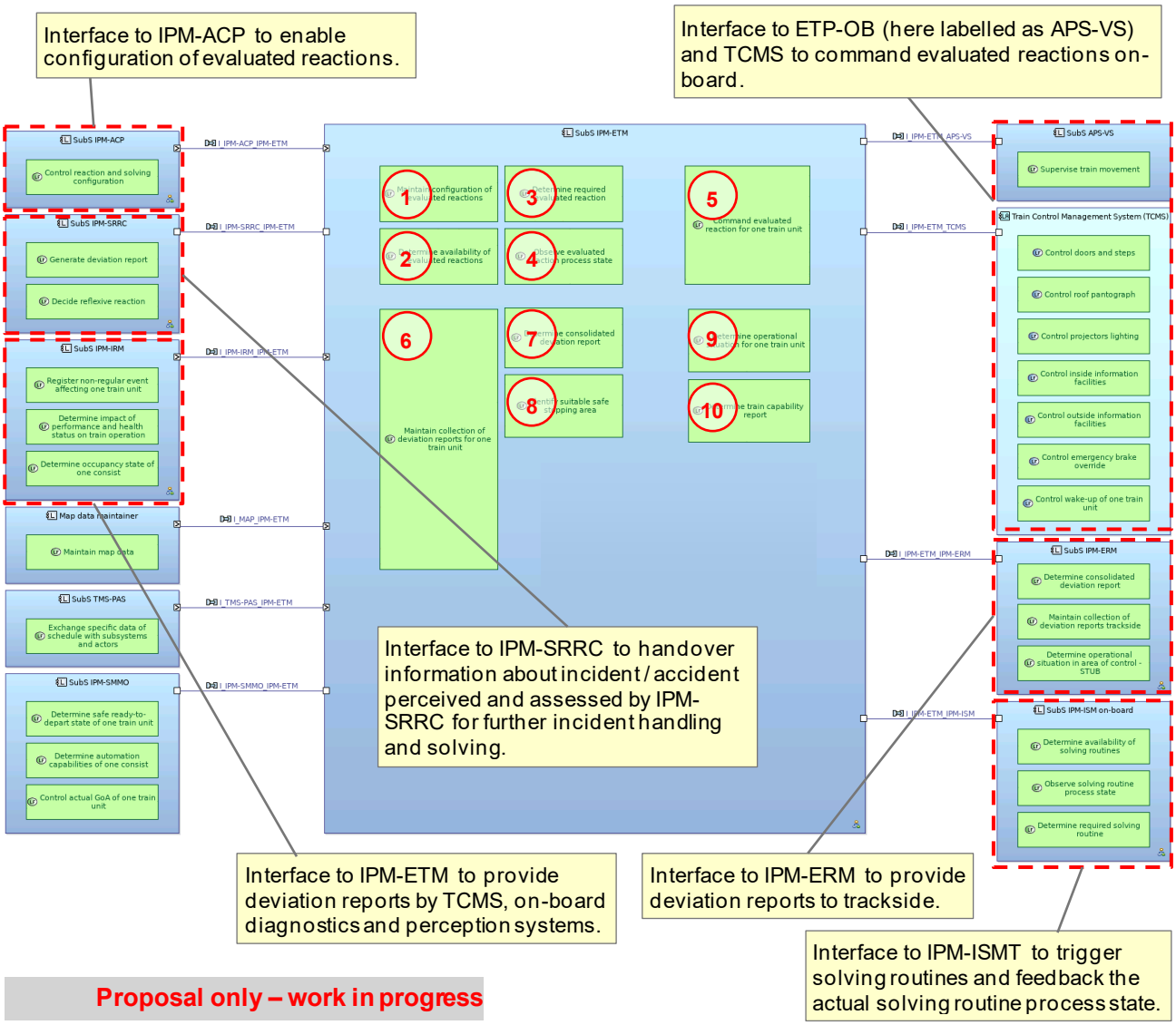

Figure 12: [LAB] IPM-ETM [Conceptual functional context]

(1) Logical Function: Maintain configuration of evaluated reactions

This function maintains the configuration of evaluated reactions depending on the types of deviations.

(2) Logical Function: Determine availability of evaluated reactions

This function determines the availability of reactions as configured and requested within IPM-ETM.

The required evaluated reaction as derived to mitigate a deviation is checked against the actual capabilities of the Train Unit as derived from the Train Capability Report (TCR). As an output this function provides the actual availability state of evaluated reaction which is taken into account for decision making within IPM-ETM.

(3) Logical Function: Determine required evaluated reaction

This function determines the required evaluated reaction based on the deviation type as derived from the actual deviation report, configured reaction chains, and takes the availability of evaluated reactions into account.

(4) Logical Function: Observe evaluated reaction process state

This function observes the progress of each commanded evaluated reaction based on the selected evaluated reaction routine and the acknowledgement signals from the systems or actors.

(5) Logical Function: Command evaluated reaction for one train unit

This function sends dedicated commands to subsystems connected (incl. ETP-OB, IPM-TS, TCMS) to conduct the required reaction(s) as evaluated by IPM-ETM and receives feedback signals to gather acknowledgement.

Evaluated Reactions to be commanded include, but are not limited to:

- Control horn sounding
- Control passenger information devices inside the passenger cabin
- Control passenger information devices on the exterior of the train unit
- Control roof pantograph
- Control projector lighting
- Set stopping point (Obstacle End-of-Authority)*
- Immobilisation of train unit
- Control doors and steps (exterior doors)
- Control emergency brake override function

* Obstacle End-of-Authority (O-EoA) refers to a virtual stopping point commanded by IPM-OB to ETP-OB.

(6) Logical Function: Maintain collection of deviation reports

This function will aggregate and maintain all active deviation reports from different sources for the Train Unit. The deviation reports stemming from different sources will be continuously updated and stored by this function to be further processed as a consolidated deviation report.

(7) Logical Function: Determine consolidated deviation report

This function generates a consolidated deviation report. The consolidated deviation report is based on (single) deviation reports that are merged based on the type of the deviation, its location, time, and date. The aim of this consolidated deviation report is to merge deviations that were registered by different sources and identify a main deviation (if existing) that other deviation reports can be attached to. This means for instance that, if a collision is detected by the system other deviations detected at the same time associated to the event (e.g., broken window), these will be clustered to the main deviation. A single deviation report that cannot be connected to other deviations will automatically result in a consolidated deviation report.

(8) Logical Function: Identify suitable safe stopping area

This function identifies suitable safe stopping areas for the respective train unit. A suitable area will be identified based on topology, topography en-route and the mission information of the train unit. This area needs at least one of the following attributes: planned stop, possibility for evacuation, possibility for self-rescue, access for rescue forces or safe evacuation possible.

(9) Logical Function: Determine operational situation for one train unit

This function will generate a holistic operational situation report for the train unit. The function will analyse the operational situation to identify possible deviations (prevention of possible incidents).

(10) Logical Function: Determine train capability report

This function generates a train capability report (TCR) for the respective train unit providing data on actual performance and health state of train-borne components.

Incident Solving Manager on-board (ISMO)

The logical component **IPM - Incident Solving Manager on-board (ISMO)** determines which solving routine needs to be conducted in order to resolve a feared event for one Train Unit. Solving processes are aligned and prioritised. Specified routines are defined to resolve non-regular situations with a minimal impact on railway operation. Planned routines are executed and assisting entities coordinated.

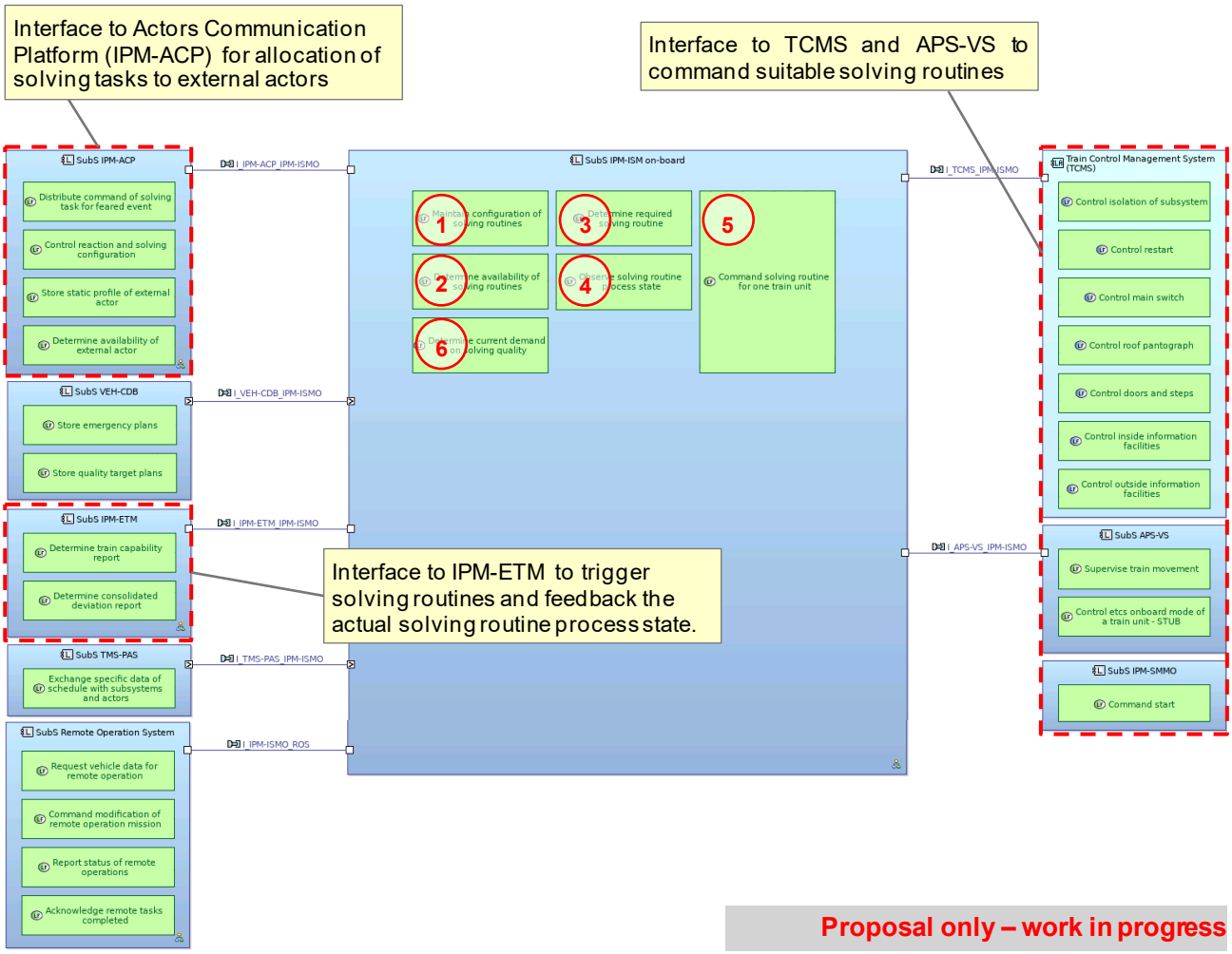

Figure 13: [LAB] IPM-ISMO [Conceptual functional context]

(1) Logical Function: Maintain configuration of solving routines

This function allows a configuration change of the already existing safety solving routines by the competent and authorised actors based upon the procedures set in the safety management system. The changes will be based on authorised emergency and incident plans, failure solving plans and procedures. The solving routines set in in this function will then define the solving for the system. This function therefore contains each solving step for a routine including all parameters leading to the utilisation of a routine. Each routine should be defined with an expected outcome.

(2) Logical Function: Determine availability of resources for solving routines

This function determines the availability of resources dedicated to solving routines as configured and requested within IPM-ETM.

The required resources dedicated to a solving routine as derived to resolve a deviation is checked against the actual capabilities of the Train Unit as derived from the Train Capability Report (TCR).

As an output this function provides the actual availability state of solving routines which is further considered within IPM-ISMO.

If specific resources are not available this can render specific solving routines as unavailable. The previously set ruleset will reflect the resource allocation towards the safety solving routines, i.e. an allocation of resources to solve safety-related deviation is prioritised over quality-related deviations.

(3) Logical Function: Determine required solving routine

This function matches the solving order (identified solving needs) to the relevant available solving routines. This function determines which exact solving routine is utilised to execute the solving order.

Assumption: There is only one specific solving routine for one specific type of deviation. This routine might have branches whereas in the first run, an automated solving is preferred (if available), then a semi-automated solving, then a manual solving.

(4) Logical Function: Observe solving routine process state

This function observes the progress of each solving step (solving commands and tasks) based on the solving order, the specific tasks and the progress reported by the systems or actors.

(5) Logical Function: Command solving routine for one train unit

This function sends dedicated commands to tethered subsystems (APS, IPM, TCMS) or tasks to external actors (via IPM-ACP) to conduct the required solving routine as determined by IPM-ISMO and receives feedback signals to gather acknowledgement.

Note: “Select specific actor for routine” might be included here.

(6) Logical Function: Determine current demand on solving quality

This function determines the current demand for a solving routine dedicated to a deviation report based on schedule information by the Traffic Management System (TMS).

State and Mode Manager on-board (SMMO)

The logical component **IPM - States and Modes Manager on-board (SMMO)** controls and verifies operational states of the automation-relevant components (incl. TCMS) of the Train Unit depending on required capabilities for the current mission. Furthermore, SMMO handles (safety related) validation and verification tasks for automated train operation which are currently conducted by the Train Driver. The SMMO only features limited reaction functionalities in terms of denying departure, if specific automation related functions are not fulfilled.

The current scope of IPM-SMMO, which might extend during further development, is to

- verify the capability of the train unit to operate a current mission in a required grade of automation (GoA),
- control required operational states to automation-relevant subsystems as required for the current mission,
- engage or disengage the ATO-OB to operate in specific train driving modes,
- maintain and provide input data for ETCS "Start of Mission" procedure to the ETCS on-board system.

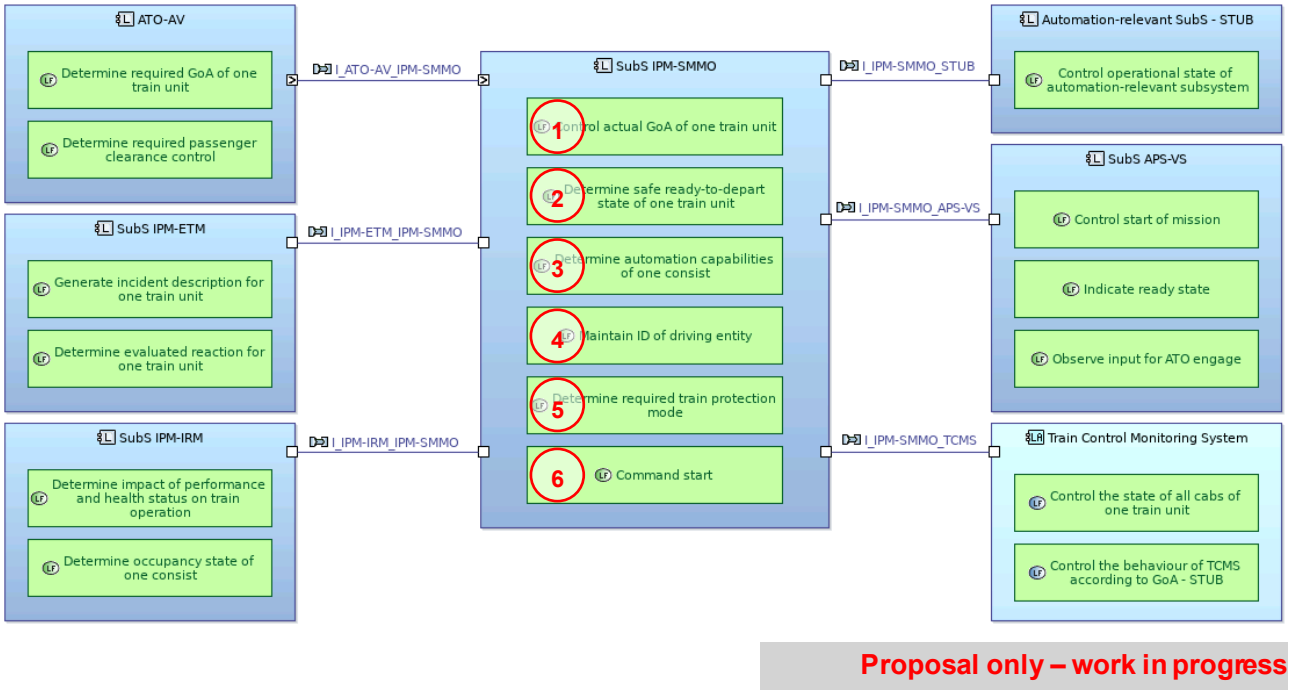

Figure 14: [LAB] IPM-SMMO [Conceptual functional context]

(1) Logical Function: Control actual GoA of one train unit

This function determines the actual grade of automation (GoA) of one train unit. This function receives as an input the required GoA for the current leg of journey as derived from the journey profile. Furthermore, it receives as an input the actual active front end and the actual cab state. Based on these inputs this function controls the required operational state to the dedicated automation-relevant subsystem and receives the actual operational state of the automation relevant subsystem as feedback. If the actual operational state of the automation-relevant subsystem dedicated to the actual active front end and the actual cab state match with the requirements according to the required GoA, then this function sets the actual GoA according to the required GoA.

Note: For safety reasons it might be necessary to set the automation-relevant subsystems to a required operational state based on a dedicated train mode selection via hardware control element in the train unit. Selected train modes are associated with certain grades of automation, such as “fully automatic mode” (FAM) for GoA4 or “supervised automatic mode” (SAM) for GoA2. Nevertheless, verification of actual operational states of the automation-relevant subsystems still needs to be conducted with this logical function by IPM-SMMO.

(2) Logical Function: Determine safe ready-to-depart state of one Train Unit

This function determines the safe ready-to-depart state of one Train Unit. This function receives as an input the ATO ready state (which implies that a Movement Authority is already set), the actual GoA state of the Train Unit (or more likely the verified train operation mode selection) and the actual departure inhibition state from IPM-ETM. This function provides as an output the actual safe ready-to-depart state “True” when the ATO ready state indicates “ready”, the train operation mode selection is “fully automatic mode” (FAM) (for operation in GoA3 or GoA4) and the actual departure inhibition state is “False”.

(3) Logical Function: Determine automation capabilities of one consist

This function uses the health status of the automation-relevant components of each consist in a train unit to determine the actual state of automation capabilities for each consist and for each of the two ends of a consist (for capabilities for which the end is a relevant condition).

To determine the automation capabilities each considered component must identify its consist and, where relevant, also the consist end in a suitable way.

(4) Logical Function: Maintain ID of driving entity

This function maintains the ID of the driving entity, which is not a Train Driver, when the train unit operates in GoA4. This ID is provided for ETP-OB.

Note: Alternatively, it could be decided that in GoA4 no driver ID is needed, neither for ETP-OB nor for ATO-OB.

(5) Logical Function: Determine required train protection mode

This function determines the required train protection mode the train unit should adhere to.

(6) Logical Function: Command start

This function provides the command to ETP-OB for ATO-OB engagement, when the train unit operates in GoA4.

Annex B: Logical components of IPM trackside

The logical components detailed here represent the current architecture hypothesis as proposed in DBS. *Please note, that the labelling of other logical components or subsystems might differ from the names and abbreviations used for the RCA/OCORA architecture.*

Incident Register and Monitoring Trackside (IRMT)

The logical component **IPM - Incident Register and Monitoring Trackside (IRMT)** is responsible to register and monitor deviations (related to safety, security, and service quality) affecting usage of infrastructure. IPM-IRMT pre-processes incoming alarms, health and performance status and provides a unified handover of the deviation related information in form of a deviation report to IPM-ERM.

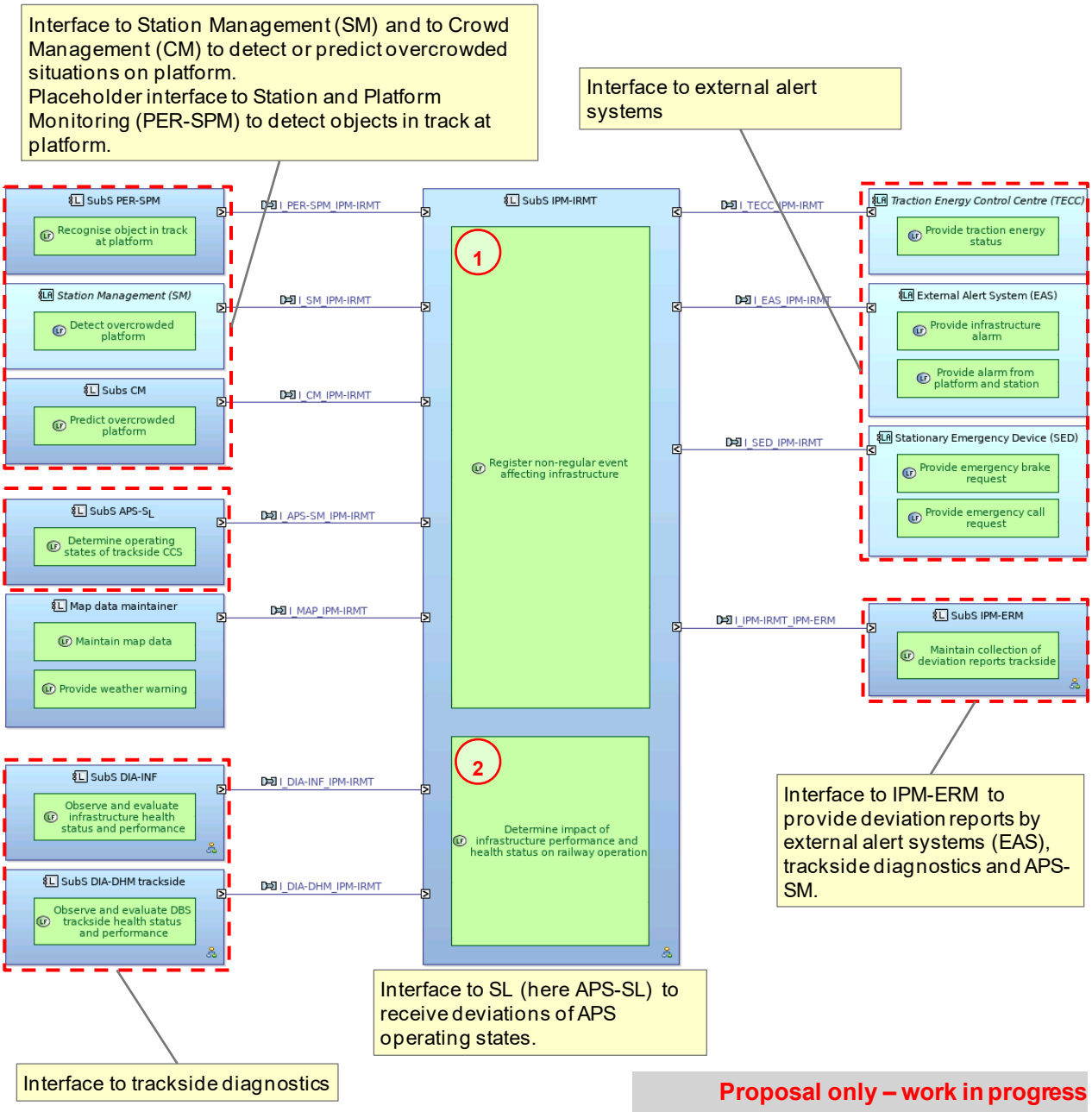

Figure 15: [LAB] IPM-IRMT [Conceptual functional context]

(1) Logical Function: Register non-regular event affecting infrastructure

This function registers all receiving non-regular situation (NRS) events that are provided by external actors and trackside DBS subsystems. In case of a deviation detected, a deviation report is generated and forwarded to IPM-ERM to consolidate similar deviation reports and initiate a reaction. Actual weather data, the platform and station model and the track topology are used to enrich the forwarded deviation report.

Safety-related deviations are detected based on:

- Reports on deviations from SM (monitoring the Operating State)
- Alarms from external alert systems detecting deviations
- Failure messages of safety-relevant trackside equipment
- Failure messages of safety-relevant functions of ATO systems and other automation-relevant systems trackside.
- Reports from systems such as
    - Weather forecast
    - Traction energy control
    - Detection systems trackside (e.g., crowd management systems, CCTV)

(2) Logical Function: Determine impact of infrastructure performance and health status on railway operation

This function analyses the health and performance information related to infrastructure elements provided by DIA-INF and DIA-DHM trackside. When the performance of infrastructure elements is reduced, this function determines the impact on the railway operation and provides an infrastructure failure report to IPM-ERM.

As DIA is supposed to be basic integrity, the infrastructure failure description cannot be processed by IPM-ERM for safety related use cases. Possible use cases for using the information based on DIA inputs are:

- Infrastructure capability report (ICR) or a situation overview for a certain Area of Control indicating the actual performance and health status of trackside elements
- Determine an appropriate solving routine matching to the specific type of failure / reduced performance.

Note: The safety related supervision of Field Elements (such as level crossing, points, etc.) is in the scope of APS.

Quality-related deviations in terms of availability not covered by TMS are detected based on input from DIA systems trackside such as

- Failure and low-performance messages of non-safety-relevant trackside equipment
- Failure and low-performance messages of quality-related functions of ATO systems and other automation-relevant systems trackside.

Evaluated Reaction Manager (ERM)

The logical component **IPM - Evaluated Reaction Manager (IPM-ERM)** aggregates, maps, and monitors multiple events and relevant data and classifies deviation with deterministic rules. In case of a deviation it decides, which evaluated reaction is required to prevent a further escalation of a deviation or mitigate the impact of a deviation detected. Apart from the functions to consolidate deviation reports and initiate reactions, ERM features a function to detect deviations based on patterns of existing deviations registered.

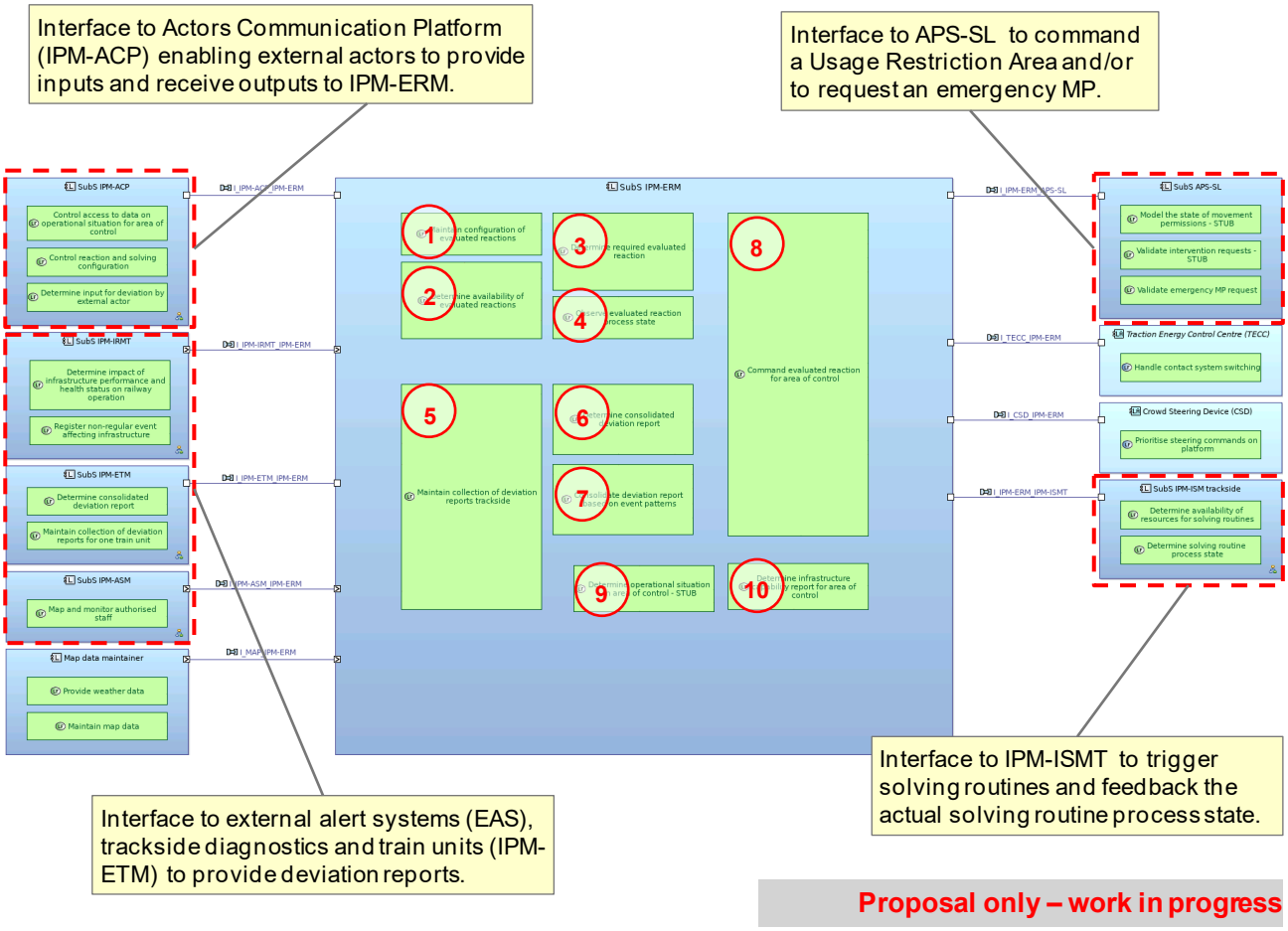

Figure 16: [LAB] IPM-ERM [Conceptual functional context]

(1) Logical Function: Maintain configuration of evaluated reactions

This function allows a configuration change of evaluated reaction routines by the competent and authorised actors based on operational rules. The changes will be based on authorised emergency and incident plans and failure handling procedures. This function therefore contains all parameters leading to the utilisation of an evaluated reaction. Each reaction should include a value that defines when the performance of the reaction is finished (i.e. the desired effect is fulfilled).

This function also sets the parameters for the quality and safety-related evaluated reactions based on the definitions entered. It will automatically readjust tasks and allocate functions for it as well as check for logical inconsistencies or discrepancies.

(2) Logical Function: Determine availability of evaluated reactions

This function monitors the current (temporary) availability of resources to operate evaluated reaction routines. If specific resources are temporary not available this can render specific evaluated reaction routines as unavailable. The previously set ruleset will reflect the resource allocation towards the safety evaluated reaction routines, i.e. an allocation of resources to react to safety-related deviation is prioritised over quality-related deviations.

(3) Logical Function: Determine required evaluated reaction

This function matches the deviation report to the relevant available evaluated reaction routines. This function determines, which exact evaluated reaction routine is utilised to prevent or mitigate the impact of the deviation.

(4) Logical Function: Observe evaluated reaction process state

This function monitors the progress of each commanded evaluated reaction based on the selected evaluated reaction routine and the acknowledgement signals from the systems or actors.

(5) Logical Function: Maintain collection of deviation reports trackside

This function will store and maintain all active deviation reports from different sources for the train unit. The deviation reports stemming from different sources will be continuously updated and stored by this function to be further processed as a consolidated deviation report.

(6) Logical Function: Determine consolidated deviation report

This function generates a consolidated deviation report. The consolidated deviation report is based on (single) deviation reports that are merged based on the type of the deviation, its location, time, and date. The aim of this consolidated deviation report is to merge deviations that were registered by different sources and identify a main deviation (if existing) that other deviation reports can be attached to. This means for instance that, if a collision is detected by the system other deviations detected at the same time associated to the event (e.g., broken window), these will be clustered to the main deviation. A single deviation report that cannot be connected to other deviations will automatically result in a consolidated deviation report.

Documentation of all available information on a detected non-regular situation with an impact or potential impact on service quality and safety based on

- Data from the reporting system or entity, which includes at least
    - Type of event
    - Location of the event
    - Reporter of the event
    - Time and date

The data documented may include further, but is not limited to:

- Impact of the event
- Potential affected infrastructure and train units by the event itself
- Safety reactions performed
- Affected infrastructure and train units by safety reactions
- Event solving status

(7) Logical Function: Consolidate deviation report based on deviation patterns

This function identifies (potential) deviations using patterns based on the consolidated deviation reports currently registered by the system. The consolidated deviation reports will be analysed based on their (regional) locations, type of deviations, time, and date.

(8) Logical Function: Command evaluated reaction for Area of Control

This function assesses, if a command to impose a Usage Restriction Area and/or a command to power down a traction current section and/or a command to steer passengers are needed to prevent further deviations, based on the received deviation descriptions or the current operational situation in the Area of Control (AoC). This function also determines the size of the Usage Restriction Area and which kind of track restriction deeds to be imposed (e.g. closure, speed restriction, weight restriction, type of train restriction, mixed traffic with different GoA level not allowed).

(9) Logical Function: Determine operational situation in Area of Control

This function determines the operational situation in the Area of Control (AoC). The operational situation represents a holistic overview for a certain AoC for operating states of infrastructure elements (tracks, level crossings, catenaries, etc.) and moveable objects (train units, authorised staff, etc.).

(10) Logical Function: Determine infrastructure capability report for Area of Control

This function generates an infrastructure capability report (ICR) based on the operational situation in a certain AoC**.**

Incident Solving Manager (ISM)

The logical component **IPM - Incident Solving Manager (IPM-ISM)** predicts the geographical, temporal and resource-related impact of events on scheduled railway operation. Solving processes are aligned and prioritised. Specified routines are created to resolve non-regular situations with a minimal impact on railway operation. Planned routines are executed and assisting entities coordinated. A deviation is monitored and managed during his whole lifecycle from the first recognition to the dissolution.

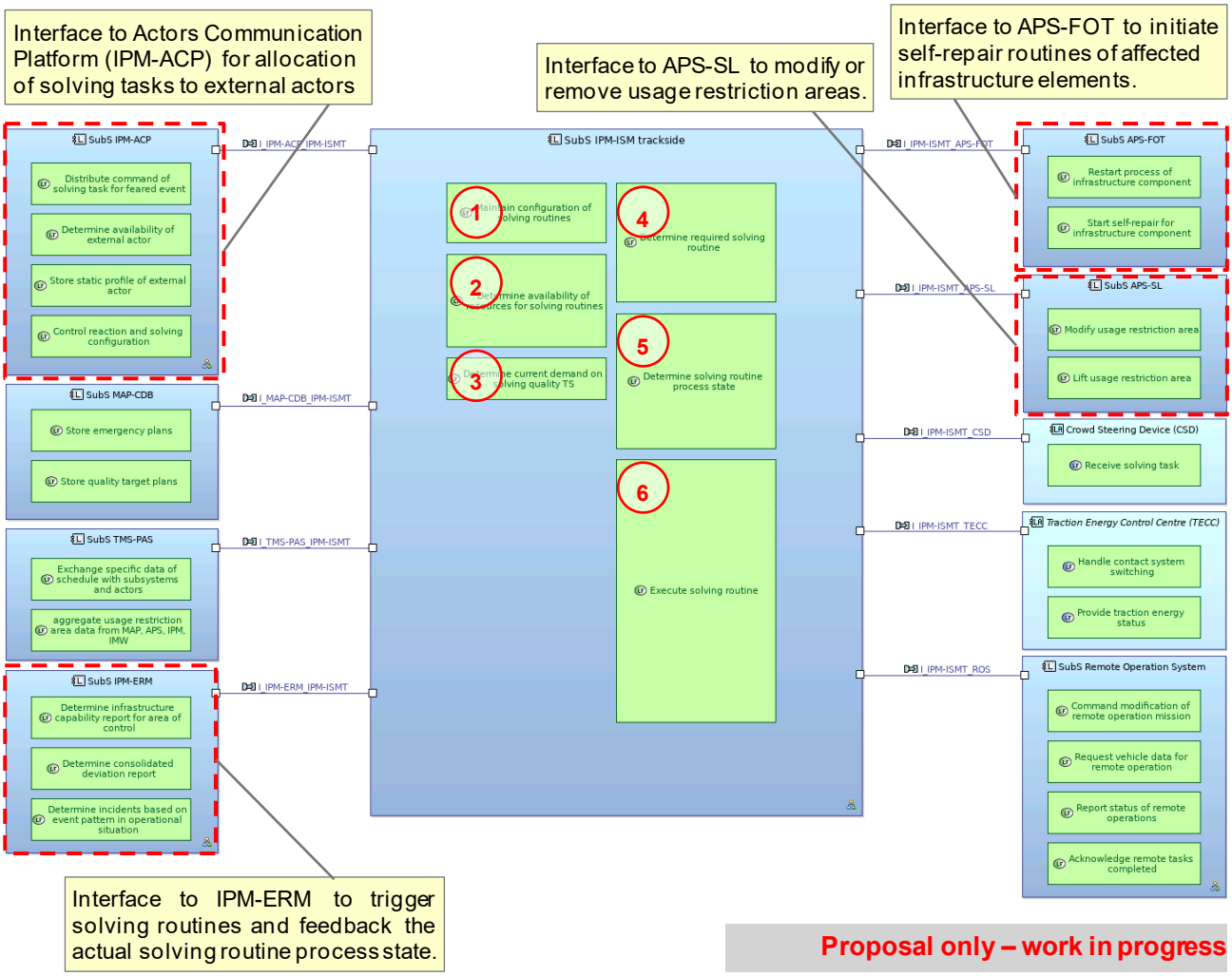

Figure 17: [LAB] IPM-ISM [Conceptual functional context]

(1) Logical Function: Maintain configuration of solving routines

This function allows a configuration change of the already existing safety solving routines by the competent and authorised actors based upon the procedures set in the safety management system. The changes will be based on authorised emergency and incident plans, failure solving plans and procedures. The solving routines set in this function will then define the solving for the system. This function therefore contains each solving step for a routine including all parameters leading to the utilisation of a routine. Each routine should be defined with an expected outcome.

(2) Logical Function: Determine availability of resources for solving routines

This function monitors the current (temporary) availability to operate the solving routines. If specific resources are temporary not available this can render specific solving routines as unavailable. The previously set configuration of the solving routines will reflect the resource allocation towards the solving routines for safety-related deviations, i. e. an allocation of resources to solve safety-related deviations is prioritised over quality-related ones.

(3) Logical Function: Determine current demand on solving quality

This function determines the priority for solving based on scheduling information.

(4) Logical Function: Determine required solving routine

This function matches the solving order (identified solving needs) to the relevant available solving routines). This function determines which exact solving routine is utilised to execute the solving order.

(5) Logical Function: Determine solving routine process state

This function monitors the progress of each solving step (solving commands and tasks) based on the solving order, the specific tasks and the progress reported by the systems or actors.

(6) Logical Function: Execute solving routine

This function sends out the specific solving commands for the systems and specific solving tasks for the actors.

Actor Communication Platform (ACP)

The logical component **IPM - Actor Communication Platform (ACP)** manages the communication between all other IPM subsystems and external actors. The group of external actors encompasses but is not limited to relevant railway infrastructure personnel or entities and personnel or entities from the respective railway undertakings as well as third entities such as police entities, fire brigades among other relevant stakeholders.

These actors can be notified and requested depending on the nature of the deviation. The ISMO and ISM generate the solving requests and allocate specific tasks according to their profiles to the actors and provides them with the relevant information to perform their tasks. At the same time the ACP can provide the ISMO and ISM with a list of actors for the Area of Control and their availability status, if obtainable. The actors can then update the progress status of their tasks, availabilities, and other necessary information for solving via this component back to the ISMO and ISM.

Actors can report deviations to the system via this logical component which will transfer the information into a deviation report. Other stakeholders such as members of the public or passengers can report deviations through one of the relevant actors to the system.

The deviation reports are forwarded to the ERM component trackside and if a specific train unit is affected to the respective ETM on-board.

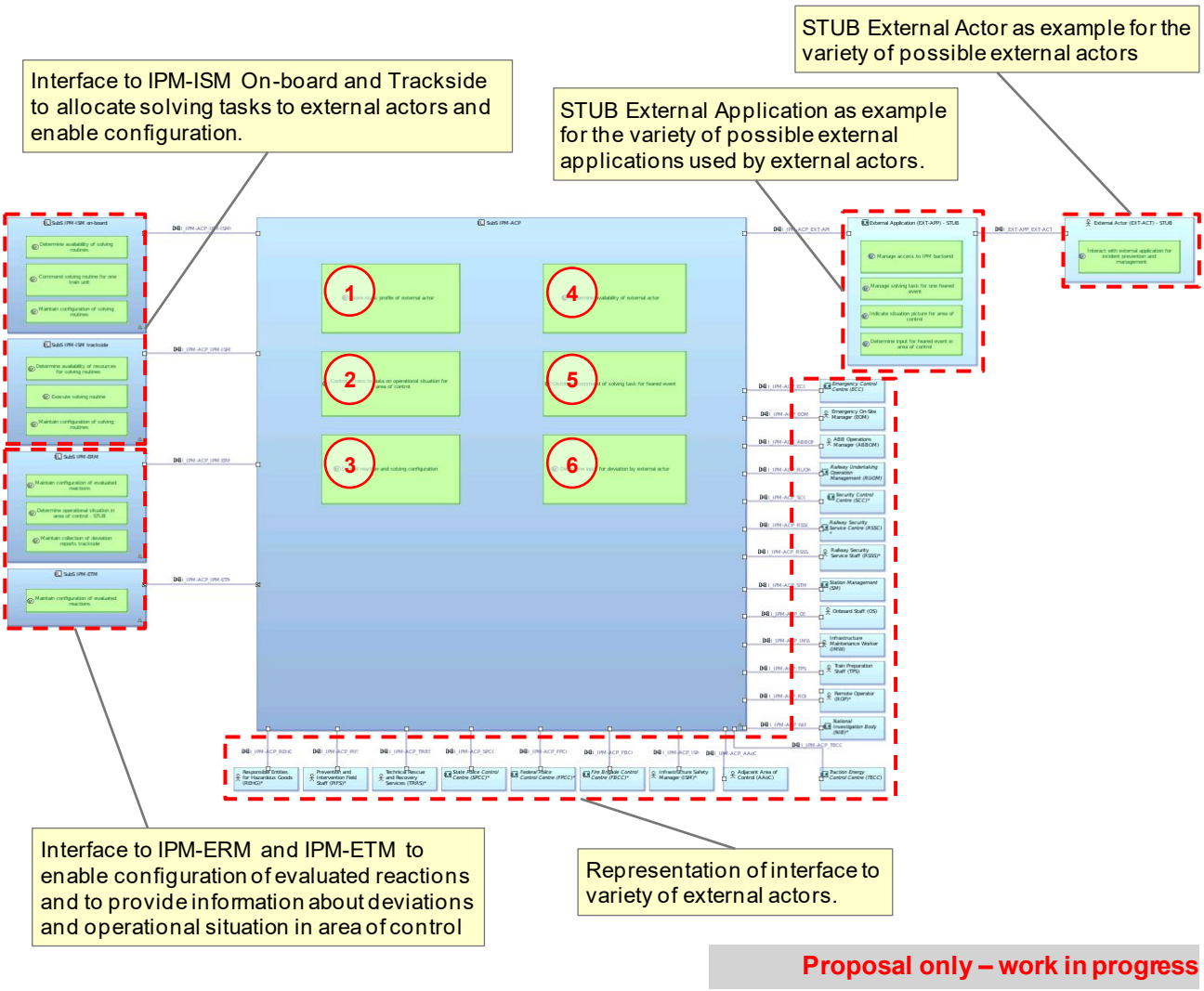

Figure 18: [LAB] IPM-ACP [Conceptual functional context]

(1) Logical Function: Store static profile of actors

This function provides configuration of profiles to manage rights and duties of actors for access to Incident and Prevention Management - Actor Communication Platform (IPM-ACP).

(2) Logical Function: Control access to reaction and solving configuration

This function receives input for IPM reactions (response) and solving (recovery) routine configuration and distributes the information to the respective routine configuration functions in the IPM subsystems.

(3) Logical Function: Control access to data on the operational situation for Area of Control

This function indicates incident information related to the situation picture for the dedicated Area of Control.

Depending on the defined rights, an external actor may be informed about incidents and the situation picture with customised data depth.

This function receives input for IPM reactions (response) and solving (recovery) routine configuration and distributes the information to the respective routine configuration functions in the IPM subsystems.

(4) Logical Function: Determine availability of external actor

This function registers and monitors the availability of external actors to the Incident and Prevention Management – Actors Communication Platform (IPM-ACP).

When an external actor connects to IPM-ACP, the actual availability state for this actor changes from FALSE to TRUE. Some external actors an update their exact availability status (e.g. occupied/vacant). Thus, the external actor is regarded as available and can be considered, if applicable, for reaction and solving routines in case of a deviation.

This function receives input for IPM reactions (response) and solving (recovery) routine configuration and distributes the information to the respective routine configuration functions in the IPM subsystems.

(5) Logical Function: Distribute command of solving task for feared event

This function receives and distributes solving tasks an acknowledgement between IPM and external actors vice versa.

Solving tasks from IPM-ISM (trackside) will be forwarded to the relevant external actors. Notifications on the current state of the execution of the assigned solving tasks from the external actors are received by this function and distributed back into IPM-ISM.

This function receives input for IPM reactions (response) and solving (recovery) routine configuration and distributes the information to the respective routine configuration functions in the IPM subsystems.

(6) Logical Function: Determine input for deviation by external actor

This function provides the interface to external actors observing their inputs dedicated to the deviation. The extent of possible inputs is controlled based on configuration data for actors' rights and duties.

External actors have the possibility to provide inputs for a new deviation to be registered or to provide inputs for an existing deviation to be updated in the IPM backend.

Authorised Staff Monitoring (ASM)

IPM - Authorised Staff Monitoring (ASM) is responsible to localise, monitor and warn authorised staff within the Area of Control via Person Supervisor and Locator (PSL). ASM is designed to send out warning messages directly to the affected authorised track personnel if there is a potential or immediate conflict between their position within the zone model and the movement of a train unit.

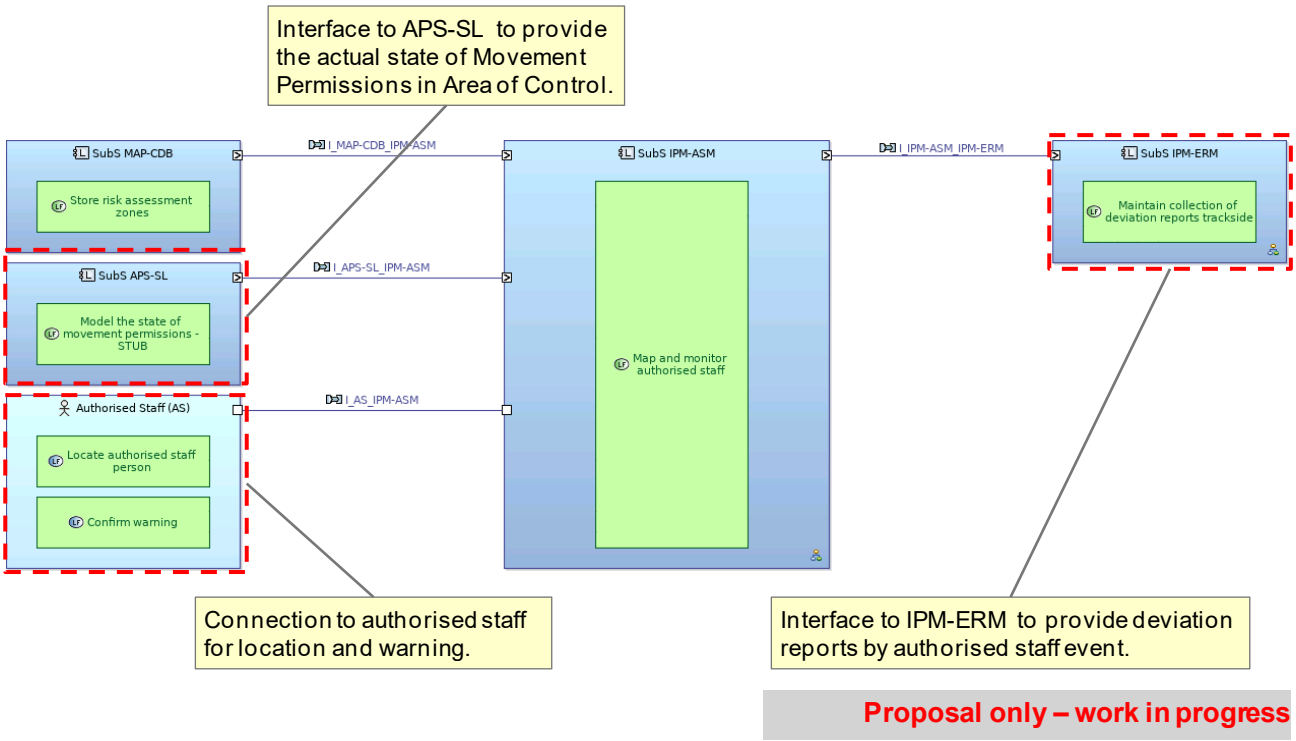

Figure 19: [LAB] IPM-ASM [Conceptual functional context]

Logical Function: Map and monitor authorised staff

This function maps and monitors authorised staff on or near the line within the Area of Control. The position of authorised staff is mapped with the zone model to identify potential conflicts with Movement Permissions set for train units. If authorised staff is in a track zone or near track zone with Movement Permission, the authorised staff will get a request to leave the zone. In case that the authorised staff is not leaving their position a deviation report is generated to initiate a reaction by IPM-ERM.