PoC Joining and Splitting

Dieses Dokument ist im Programm smartrail 4.0 in Bearbeitung. Sein Inhalt kann sich noch ändern und hat noch keinen verbindlichen Charakter. Die Vollständigkeit und Korrektheit der Inhalte dieses Dokumentes ist noch nicht gewährleitstet bzw. noch in Überprüfung.

This document is a DRAFT version which is still under construction. Its content may change, is not completely verified and is not yet finalized.

1 Content

Contents

2 Goal

The following project risk was identified:

Trennen und Vereinen - low priority
Für das Vereinen müssen MPs überlagert werden, für das Trennen müssen neue MPs entstehen, die sich überlagern. Überlagerte MPs sind sicherheitskritisch. Es ist unklar, ob Trennen und Vereinen ausreichend sicher realisiert werden kann.

IA-18124 - This document persuades the goal to show that the manoeuvres "Splitting" and "Joining" are safe. Meaning that based on those manoeuvres, which happen numerous times a day, no misinterpretation, false conclusions, violations, human damage, etc. happens. **[**draft**]**

IA-18123 - [draft**]**

3 Assumptions

IA-18126 - The ETCS-Interlocking shall be a safe system and therefore shall not anticipate or retrospectively guess what is happening on the railway network. Hence it is necessary to define assumptions which are basically mandatory or greatly beneficial to the safety during those manoeuvres. **[**draft**]**

IA-18125 - Mandatory:

1. **Acknowledged Joining & Splitting Manoeuvre:** This acknowledgement is necessary so that the SRP-3068 - EI Object Aggregation knows when a joining or splitting takes place and for the latter one if its happening planned or unplanned. The acknowledgement can be in form of a MOB update and does not have to state splitting or joining directly.
2. **Requesting MOB information:** The Staff which gives the acknowledgement (MobUpdate) that a splitting or joining has taken place needs the ability to request the information of the MOB of concern. This shall be done by requesting information about a MOB which the Staff identifies due to certain indicators which are unique to the MOB of interest. How the unique indicators are entered in the information request is irrelevant for the concept. The indicators shall be used to enable OA to determine the correct MOB. Indicators can be for example:
   a. MOB id
   b. Operation Id
   c. MoveableDevice Id
3. **SA Handovers are only necessary if an MP allows the intern MOB to move:** This defines that two MPs as well as their MOBs are allowed to overlap without a safety actor capable of supervising the necessary Safety Responsibilities has taken the responsibility by an SR handover. This is valid as long as no MOB is allowed to move inside its MP (vmax = 0).

Beneficial: Display the MoveableDevices a MOB features: This beneficial assumption is founded on the assembly concept. This would raise the transparency of the MOBs involved in the manoeuvres.

- **Splitting:** A newly created MOB due to splitting can be filled with the correct information of the decoupled vehicle / vehicle groups of the host MOB.
- **Joining:** For Joining the MOB which is extended by additional vehicle / vehicle groups can be updated with the concrete information.

Also the "Validation System" of the concept can be used as the tool to update the MOBs (acknowledgement of joining and splitting).
[draft**]**

4 Manoeuvre Concept

IA-18132 - In this chapter it will be shown, that the manoeuvres Joining and Splitting can be described holistic and that they can be handled with the SR40 Program without provoking safety risks. To do so, the first step is to define the terms splitting and joining as well as setting the frame conditions which are valid during the proceeding of the manoeuvres.**[**draft**]**

IA-18133 - Splitting is defined as a manoeuvre during which a vehicle / vehicle group is detached from its composition. This is done by loosening the couple between two vehicle / vehicle groups.**[**draft**]**

IA-18130 - Joining is defined as a manoeuvre during which a vehicle / vehicle group is attached to another composition. This is done by operating the couple between both vehicles / vehicle groups.**[**draft**]**

IA-18129 - The couples of vehicle / vehicle groups are of different types which show different behaviour. Therefore the type of couples which are considered in this PoC are:**[**draft**]**

IA-18131 -

- **The Automatic Couple**: can be utilized from the engine of a vehicle / vehicle group. This type of couple does not raise the necessity of additional staff to operate the couple locally.
- **The Mechanical Couple**: has to be operated by staff manually. Due to this couple type it is necessary, that a shunter locally operates the couple manually.

Due to the couple types the necessary Staff which is involved during this process is defined for this PoC to be consisting of:

- Engine Driver
- Shunter

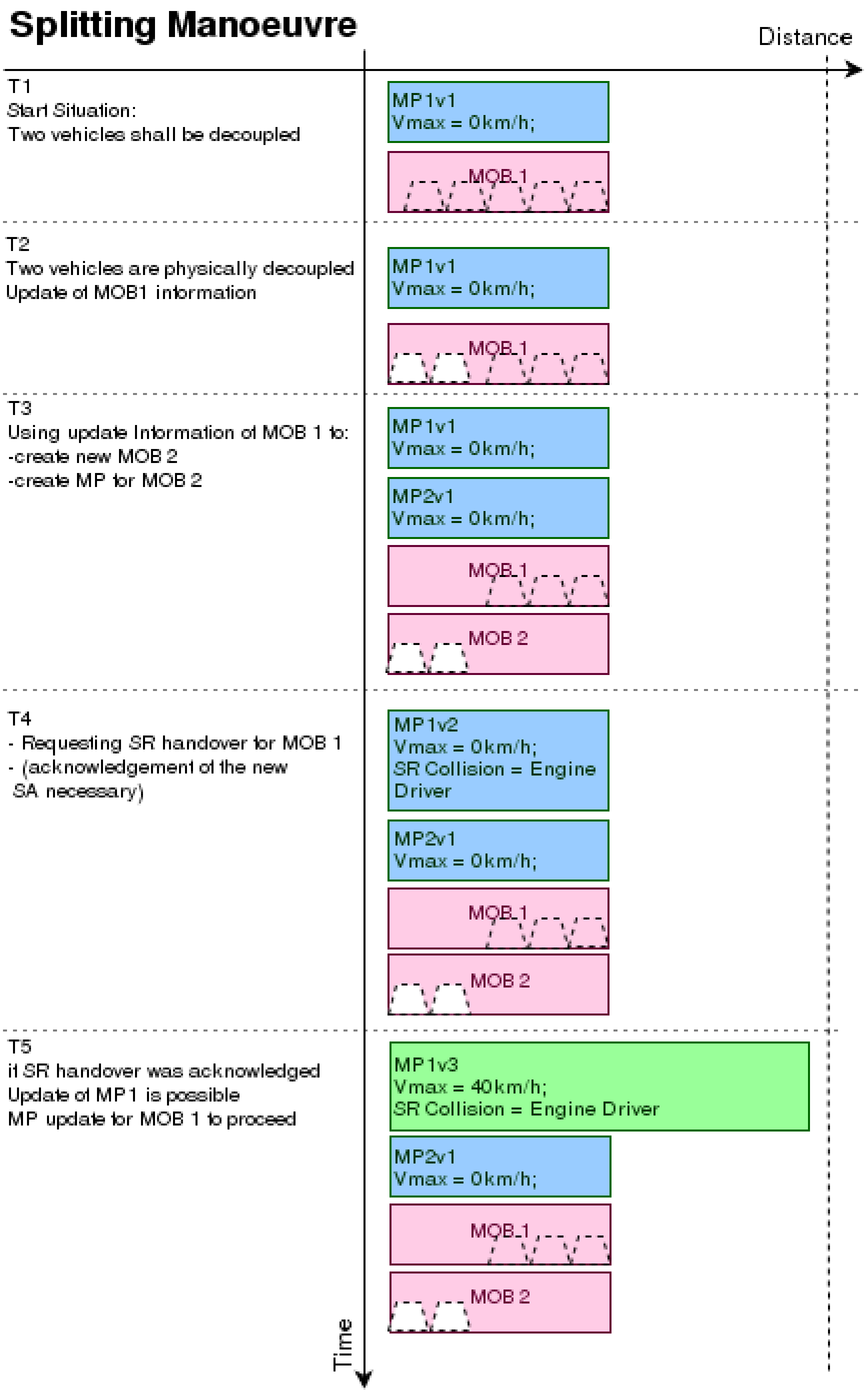
Both staff groups shall be able to be equipped with an system to acknowledge a splitting or joining manoeuvre.**[**draft**]**

IA-18120 - In the following the handling / procedure of the manoeuvres splitting and joining are described.**[**draft**]**

4.1 Splitting

IA-18119 - The planned splitting manoeuvre which is used to prove the functional feasibility and displayability is visualised with an Step-Diagram, where t is the y-axis and the distance the x-axis. The planned splitting which shall act out is described as follows. Two coaches of a MOB, consisting of five MoveableDevices (four coaches and one engine), shall be decoupled.
[draft**]**

IA-18139 -



Splitting Manoeuvre

T1
Start Situation:
Two vehicles shall be decoupled

T2
Two vehicles are physically decoupled
Update of MOB1 information

T3
Using update Information of MOB 1 to:
-create new MOB 2
-create MP for MOB 2

T4
- Requesting SR handover for MOB 1
- (acknowledgement of the new
SA necessary)

T5
if SR handover was acknowledged
Update of MP 1 is possible
MP update for MOB 1 to proceed

[draft]

IA-18180 -

1. A MOB consisting of five MoveableDevices is inside its MP. A splitting manoeuvre requires that movement inside the MP is not allowed otherwise the resulting MP overlap would trigger a safe reaction . Therefore TMS has to be aware of the planned splitting and has to updated the MP, so that all movement inside the MP is prevented. This is done by updating the allowed speed inside the MP to vmax = 0 km/h.

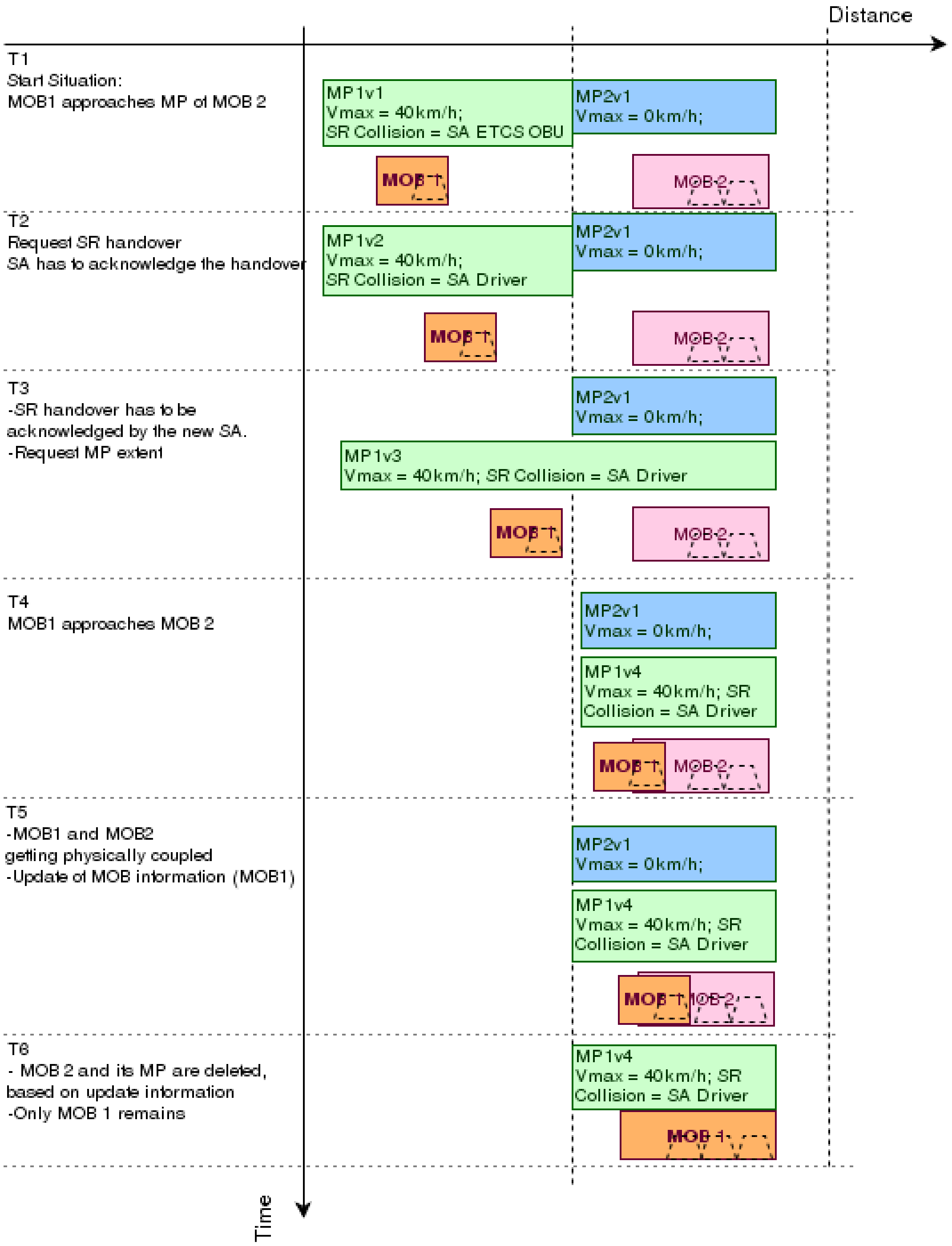
2. The actual act of splitting is executed by staff like for example a shunter or Engine Diver. The Staff has to execute multiple steps to split the planned MoveableDevices. Relevant for this PoC are:
   a. Step 1: The Staff has to operate the couple to detach the MoveableDevices.
   b. Step 2: The Staff has to update the information of MOB 1. Therefore the Staff shall be able to request the necessary information of the MOB from the Object Aggregation via an interface to a validation system. The Staff shall use the MOB information on a validation system to update them by:
      i. Method 1: Choosing the option "split" and enter the MoveableDeviceId of the MoveableDevices between which the splitting is executed and approving the execution to update the information of MOB1 to the Object Aggregation.
      ii. Method 2: Choosing the option "split" and scanning the MoveableDevice badge of the MveableDevices between which the splitting takes part. This will automatically fill in the necessary information (no reading error). The Staff approves them and thereby updates the MOB information to the Object Aggregation.
      iii. Method 3: Choosing the option "split", the MOB of interest and approving the execution of the planned manoeuvre to update the MOB information to the Object Aggregation.
   c. The Object Aggregation uses the information received via a validation system to update MOB1.
3. The update of MOB1s information causes the creation of a new MOB2 by the Object Aggregation. The new MOB2 will automatically get an own MP which is configured by default in a way that no movement inside the MP is allowed. The extent of the MP is the size of MOB2. This is necessary so that the overlap of both MPs and MOBs is uncritical by a safety point of view. The extent of the new created MOB2 is the same as the old MOB1. This is because the exact splitting location is unknown to the Object Aggregation and thus would have to assume a concrete location. This approach was chosen because no assumptions shall be made.
   a. The transparency of the newly created MOB2 is depending on the information which is available inside of MOB1.
      i. Possibility 1: If MOB1 features its MoveableDevices, then MOB2 to can be created featuring the decoupled MoveableDevices
      ii. Possibility 2: If MOB1 does not feature its MoveableDevices or not all, then the new MOB2 will be empty of MoveableDevices.
4. For one MOB to leave the splitting area, it is necessary to handover the responsibility for SR like for example collision to a safety actor which can ensure the compliance to it. In the scenario above the safety actor with fitting capabilities could be the engine driver. If the Engine Driver has acknowledged (mandatory) that the responsibility was taken, the MP can be updated by EI-TMS-ARS.
5. The MP update in the example above enables MOB1 to move away from the splitting area. Thus the splitting manoeuvre is done and resolved.

[draft**]**

4.2 Joining

IA-18184 - The planned joining manoeuvre which is used to prove the functional feasibility and displayability is visualised with an Step-Diagram, where t is the y-axis and the distance the x-axis. The planned joining which shall act out is described as follows. A MOB shall couple with an parked vehicle / vehicle group (MOB 2) which consists of two MoveableDevices.**[**draft**]**

IA-18138 -



[draft]

IA-18183 -

1. MOB1 which shall be coupled with MOB2 is approaching the MP of MOB2. The allowed speed for MOB2 inside its MP is set to vmax = 0 km/h and thus does not allow MOB2 to move.
2. Before EI-TMS-ARS is able to request an MP update which will overlap with the MP of MOB2, a SR handover has to be requested. Via the SR handover the necessary SR shall be taken by a SA featuring the capability to ensure a compliance to the SRs. Therefore in the case above the Engine Driver takes

the SR for e.g. Collision. The Handover has to be acknowledged by the Engine Driver before the next step can be executed.

3. If the requested SA (in this case the Engine Driver) has acknowledged that the responsibility for the concerned SRs will be taken, EI-TMS-ARS can request an MP update. This update will lead to the overlap of MOB1 and MOB2s MP. *Note: Only the MOB which is able to move inside its MP needs a SR handover.*

4. After the MP update was granted MOB1 can approach MOB2. The complete list of which conditions have to be met so that an overlapping of MPs will be granted by the SL is still to be determined.

5. After MOB1 completely approached MOB2 the actual act of joining can be executed. The joining is executed by staff like for example a shunter or the Engine Driver. The Staff has to execute multiple steps for the joining process. For this PoC relevant are:
   a. Operating the couple to join the MoveableDevices.
   b. the Staff has to update the MOB information to the Object Aggregation. Therefore the staff shall be able to request the necessary information of the MOBs via an interface to a validation system. In the case above this means that the information states that MOB1 is joined with MOB2. The Staff shall use the received information to update the MOBs by:
      i. Method 1: Cchoosing the option "joining" and enter the MoveableDevice badges of the MoveableDevices between which the joining takes part. Further the Staff shall approve the execution of the planned manoeuvre and update this to the Object Aggregation.
      ii. Method 2: Choosing the option "joining" on the validation system and scanning the MoveableDevice badge of the MveableDevices between which the joining takes part. This will automatically fill in the necessary information (no reading error). The Staff approves them and thereby updates the MOB information to the Object Aggregation.
      iii. Method 3: Choosing the option "joining", the MOBs of interest and approving the execution of the manoeuvre to update the MOB information to the Object Aggregation.
   c. The Object Aggregation uses the information received via a validation system to update MOB1.

6. Due to the received information MOB1 is updated and MOB2 gets deleted as well as its MP.
   a. The transparency of the joining manoeuvre is depending on the information which is available inside of MOB1 and MOB2.
      i. Possibility 1: If MOB2 and/or 1 feature all/some of their MoveableDevices, then MOB1 to can be updated to feature the joined MoveableDevices
      ii. Possibility 2: If MOB2 and/or 1 does not feature their MoveableDevices, then MOB1 will not feature any further MoveableDevices of the former MOB2.
   b. After both MOBs were joined the remaining MOB can proceed its planned operation.

[draft**]**

5 Definition of Safe and possible measurements

IA-18192 - Both manoeuvres (joining and splitting) are acted out like mentioned above. The chapters above describing only the single steps which are executed to conduct joining and splitting. This shall prove the functional feasibility and grade of displayability. Further more it is to define in this PoC what conditions are considered as safe and which measurements have to be applied to ensure safety. The safety can be divided into multiple categories.**[**draft**]**

IA-18195 -

- Safe Conditions
- Safe Aggregation
- Safe Visualization

[draft]

IA-18194 - Safe conditions define the rule stock to which the joining and splitting manoeuvre is considered safe from a system monitoring point of view. This shall determine under which conditions the ETCS-Interlocking itself defines the process as safe. The ETCS-Interlocking monitores the operating state and applies its safety program to the data available inside the Operating state. Thus the critical situation for which frame conditions have to be set, regards the overlapping of multiple objects in the operating state. Basically objects inside the operating state shall not overlap. As a matter of fact during joining and splitting

- MOBs
- MPs
- RiskBuffer

will be overlapping. This overlap will, under normal circumstances, lead to a safe reaction of the ETCS-Interlocking [Safety Manager]. Therefore conditions have to be defined which lead to a safe overlapping on the real track as well as in the operating state.

- **Overlapping of RiskBuffers** during splitting and joining. During planned manoeuvres the RiskBuffers of both MPs will and have to overlap.
  - **Frame Conditions:** The overlap of RiskBuffers shall be allowed under certain constrains. Those constrains will be defined inside the IA-4319 - Concept Risk Buffer / Distance Function. Basically it can be assumed, that RiskBuffer will feature set of constrains which have to be met so that a RiskBuffer overlap will be considered safe by the ETCS-Interlocking.
- **Overlapping of MPs** which do not allow movement inside them shall be considered as safe. *Note: If movement is allowed or not can be derived from the allowed speed inside the MP. An speed of vmax = 0 km/h represents a state in which no movement is allowed.*
  - **Frame Condition:** MPs which are created based on a newly detected MOB shall not allow movement inside by default [set vmax = 0]. Two MPs which overlap and do not allow movement inside are basically considered safe.

- **Movement inside overlapping MPs** of at least one MOB. Movement of one MOB is necessary to execute the planned splitting or joining.
  - **Frame Condition:** To ensure safety during movement of MOBs, which in the worst case are already overlapping inside the Operating State due to inaccuracy, a safety actor, capable of ensuring compliance to safety responsibilities shall take them. Each MOB which wants to move has to realize such a SR handover. Which safety actor is capable of doing this will be defined by the IA-6231 - Concept Safety Responsibilities as well as which safety responsibilities have to be taken to ensure a safe situation.

- **Overlapping of MOBs** as a result of localisation inaccuracy during splitting and joining. This is a situation which will occur inside the operating state. There are two different cases which have different frame conditions to adhere to.
  - **Case 1:** MOBs are overlapping inside MPs which do not allow the MOBs to move.
    - **Frame Condition:** The overlapping MPs by default shall forbid the MOBs to move inside. If this is the case the overlap shall be assessed as safe by the ETCS-Interlocking.

- **Case 2:** MOBs are overlapping inside MP/s which do allow one or more MOBs to move.
    - **Frame Condition:** likewise to the frame conditions for movement inside overlapping MPs the SR for the relevant responsibilities has to be taken over by a safety actor capable of doing so. This is the case even if the MOBs are overlapping, because the overlap of MOBs is negative product of localisation inaccuracy. As long as a safety actor capable of stating that no collision has happened on the real track, has taken the responsibility for it, the ETCS-Interlocking logic will assume this situation as safe

[draft**]**

IA-18193 - The section of **safe aggregation** deals with the safe processing of input information. This means that due to every information input during the events joining and splitting the Object Aggregation shall be able to update the operating state accordingly and without misconceptions. Therefore safe in this case means that no misinterpretation or false processing due to incorrect addressing of update information is leading to critical situations.

The researched phase of joining and splitting in which wrong addressing of information can originate, is during the updating of the old and/or new MOB. To ensure that update information are always addressed to the correct recipient the IA-12625 - [Core Group decision] Concept :Assembly-; MoveableDevice-; DevicecontrolId introduces a validation system which enables the user to easily request the information of a certain MOB as well as select certain manoeuvres.
The Validation System thus is the key element to chose the correct MOB for the updating process. The MOB can be chosen, by:

- Entering the Operation Id of the MOB
- Entering one MoveableDeviceId
- Scanning one/or more MoveableDevice Badge

One of this indicators would be enough for the Object Aggregation to determine the MOB of interest. But to raise the safety even further, identification methods like for example a two factor identification could be used. This means in this context, that two different indicators shall be entered to determine the MOB. If one of the entered indicators does not correlate with the other, the information request is denied by the Object Aggregation.
Because two MOBs are involved during joining it could be assumed that the order of the entered information is important. But the only difference which resolves from a reversed information entry is, that the other MOB is updated instead of the intended. The resulting information is still correct and safe and thus the joining is independent of the entry order of MOBs. *Explanation: if during joining MOB1 is attached to MOB2 or MOB2 to MOB1 is basically not safety critical. The Result is one single MOB which combines both attributes.***[**draft**]**

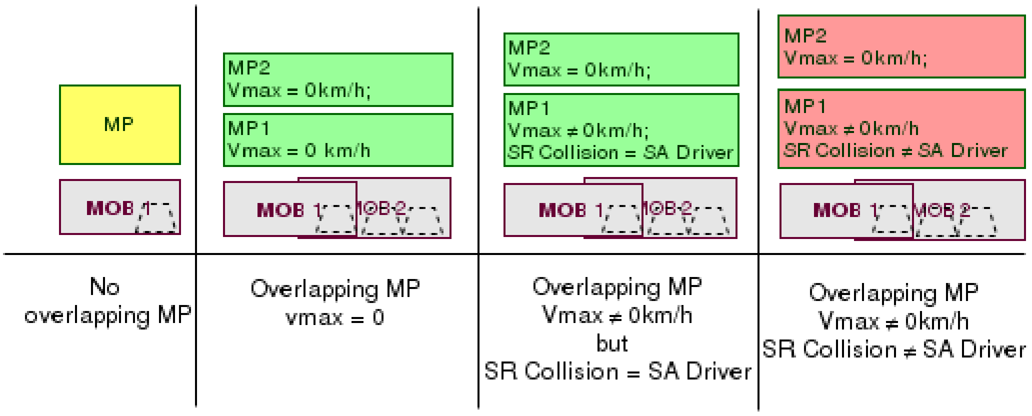
IA-18196 - Safe Visualization summarizes the measurements which have to be made so that an observer of the Operating State can immediately see that a situation on the displayed topology is safe. A situation in which two MOBs potentially collided compared with an joining or splitting manoeuvre shall not be visualized in the same way. This includes multiple aspect which have to be considered.

- **Assessment of the Situation:** A observer of the Operating State has to be able to distinguish both situations and has to be able to contact the safety actor in charge if critical situations occur.
- **time necessary for the Assessment:** In emergency cases a observer has to act as fast as possible, thus the observer shall not have to determine the correctness of the seen situation by researching the relevant information but by merely looking at the situation.

- **Identify Safety Actor in Charge:** if the observer of the operating state recognizes a potential hazard, the observer shall be able to contact the safety actor in charge / capable of intervening as fast as possible.

To ensure that the observer needs a minimal amount of time to decide if a situation is critical or not, the visualization of MPs shall differ based on set attributes. Possible criteria for a different visualization in regard of joining and splitting processes could be the allowed speed inside an MP and the distribution of SR to SA.

For example/proposal:
Color approach:


MP
MOB 1
No overlapping MP
MP2 Vmax = 0km/h;
MP1 Vmax = 0 km/h
MOB 1
MOB 2
Overlapping MP vmax = 0
MP2 Vmax = 0km/h;
MP1 Vmax ≠ 0km/h; SR Collision = SA Driver
MOB 1
MOB 2
Overlapping MP Vmax ≠ 0km/h but SR Collision = SA Driver
MP2 Vmax = 0km/h;
MP1 Vmax ≠ 0km/h SR Collision ≠ SA Driver
MOB 1
MOB 2
Overlapping MP Vmax ≠ 0km/h SR Collision ≠ SA Driver

- Color Set:
  - Not overlapping MPs is visualized with color one
  - Overlapping MPs can have color two [color for safe state] or three [color for unsafe state] depending of the compliance of certain conditions.
- Constrains:
  - MP which does not overlap -> colorone
  - MP which does overlap and fulfills:
    - vmax = 0 -> colortwo
  - MP which does overlap and fulfills:
    - vmax ≠ 0 & SR Collision = valid SA -> colortwo
  - MP which does overlap and fulfills:
    - vmax ≠ 0 & SR Collision ≠ valid SA -> colorthree

with such a color based codification of relevant attributes an observer is able to perceive if a situation is critical/planned or not. Further visual codifications can be applied to enhance the perceivability/transparency of the Operating State.

The time necessary for assessing a situation is minimized with the quality of the visual presentation of objects inside the operating state.

To identify the safety actor who is in charge of the responsibility or the ability to intervene in critical situations shall be accessed easily by an observer.

This could be achieved by displaying always the safety actor capable of intervening at the object of concern.

- directly, so that the SA is visible in the operating state near the object of concern
- by opening the properties of the object of concern.

The SA saved shall be registered with its possible contact methods.**[**draft**]**

6 PoC Summary & Conclusion

IA-18229 - The PoC shows as well as defines mandatory and beneficial assumptions, which have to be made, that a splitting and joining can basically be perceived by the ETCS-Interlocking. The most important assumption is that the ETCS-Interlocking receives information about the splitting and joining in form of a concrete message or an MOB update which embodies the specific manoeuvre. This requires that the staff is able to request MOB information which they can alter afterwards.**[**draft**]**

IA-18228 - The essential process steps of both manoeuvres are illustrated. Proving that the functional feasibility of splitting and joining as well as the displayability is given in its wholeness. Further more it shows which measurements have to be applied that the undertaking of the processes is considered as safe both on the real track as well as inside the operating state.**[**draft**]**

IA-18231 - Finally the PoC shows which safety aspects have to be considered during the splitting and joining manoeuvre. For all three aspects the problem was stated as well as possible solutions or assumption addressed. by considering the stated solutions/assumptions the undertaking of both manoeuvres can be considered as safe. The final style of implementation is to be determined but the overall direction could be shown.**[**draft**]**

IA-18230 - Therefore the final conclusion shall answer the starting question arisen as a project risk. Can joining and splitting be realized acceptable safe. The answer is, that the process is on one hand functional feasible and on the other hand if the proposals/solutions/assumptions are considered in the final ETCS-Interlocking concept also appropriately safe. **[**draft**]**