33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

Using the Unified Architecture Framework to perform hazard analysis for system of systems

Matthew Hause,
Mhause@SystemXI.com

Lars-Olof Kihlström,
Lars.Olof.Kihlstrom@cag.se

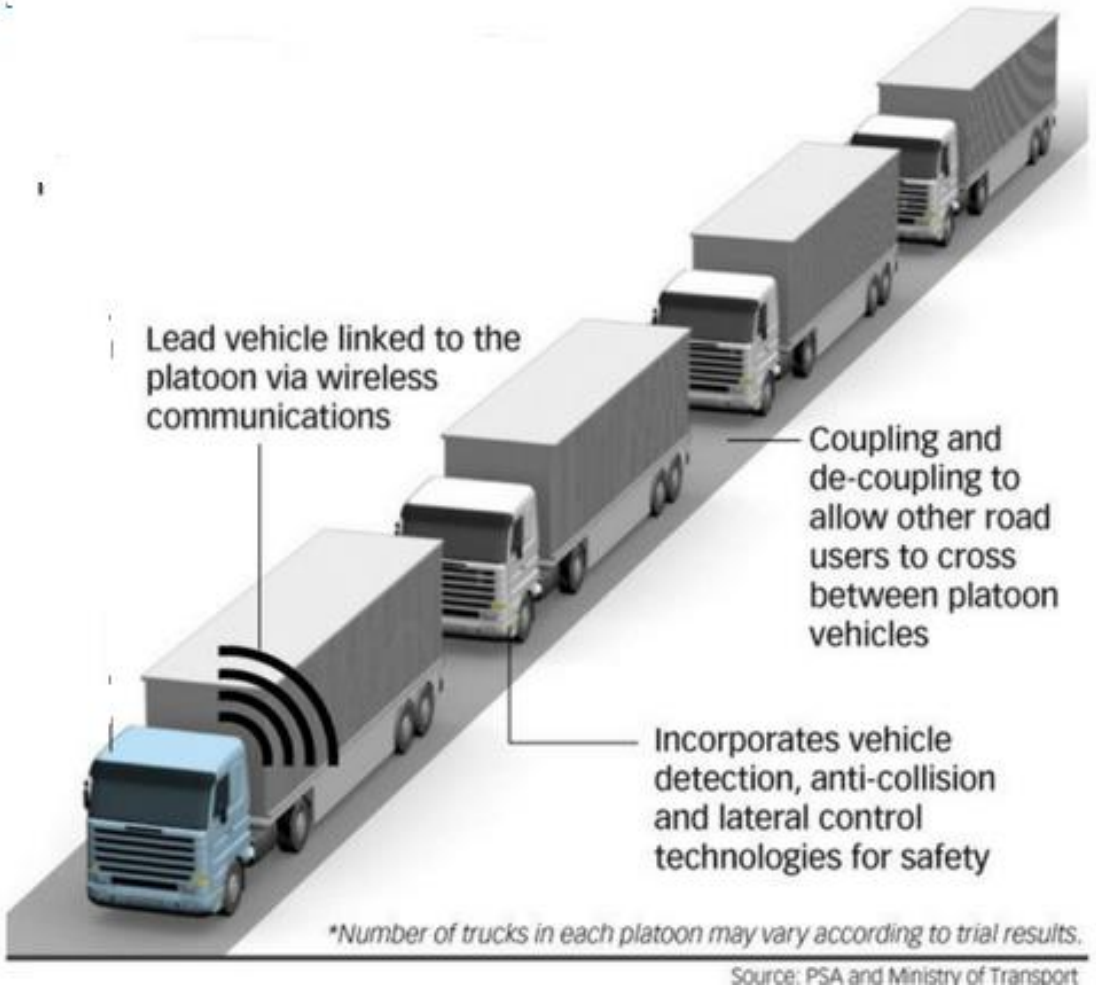
Joakim Fröberg
joakim.froberg@safetyintegrity.se

Hazard analysis for systems

- Hazard analysis is a required task as part of the production of any complex system.
- It is a laborious and expensive task.
- Collaborations between systems, creating systems of systems makes this an even more complex task.
- This presentation presents an approach to manage this by making use of the Unified architecture framework (UAF) in order to create a model that focusses on the system of system aspects.
- During 7 months in 2021 a project named Model-based Risk Assessment and Safety Analysis (MBRASA) was conducted to look at hazard analysis for system of systems and the work presented here derives from the MBRASA work effort.
- This work involved a couple of companies as well as academia and was supported by Swedish government agencies. (TECOSA, 2021)
- The approach is exemplified by using Truck platooning as an example.

Using Truck Platooning as an example of a system of systems

- Platooning implies that trucks combine in a convoy under the leadership of the front truck.
- The trucks will travel very closely together, more so than by just using ACC, thereby relieving congestion, reducing fuel consumption and decreasing Carbon dioxide emissions.

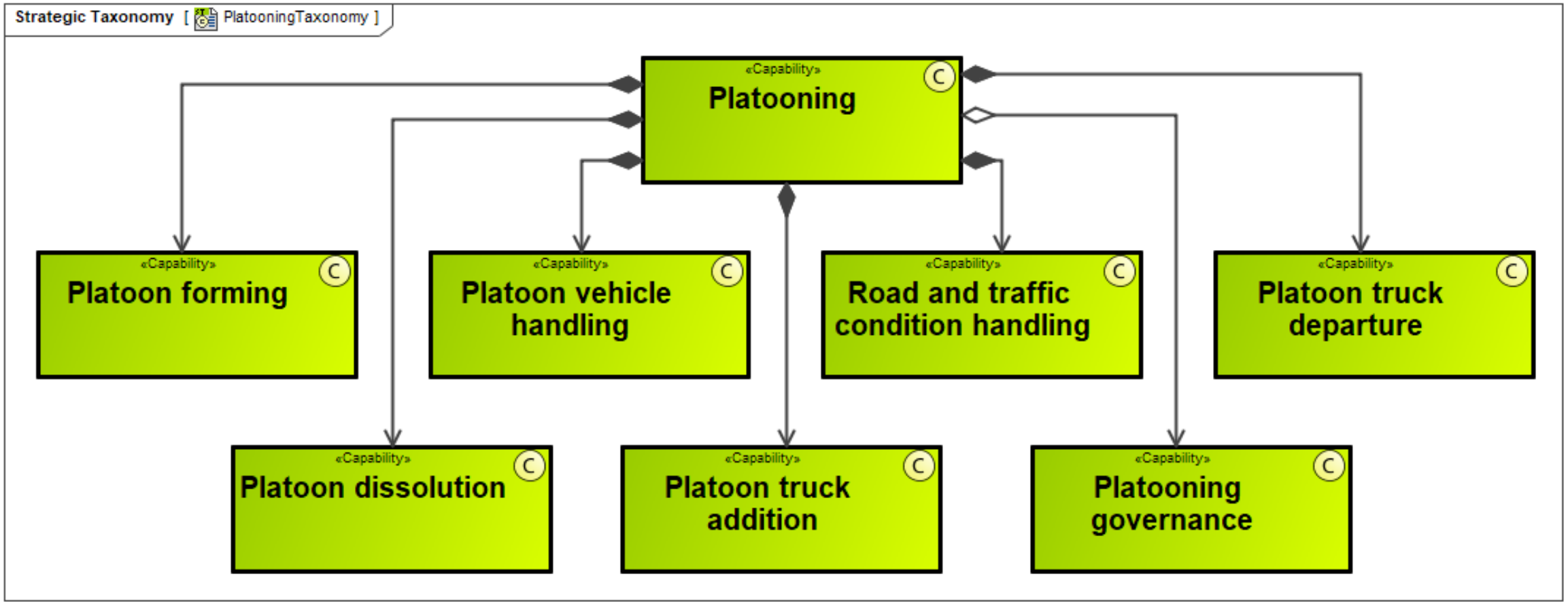


Is truck platooning an example of system of systems?

- A system of systems usually has several levels of different stakeholders with mixed and sometimes contradictory and/or competing interests.
- A system of systems usually has several, possibly contradictory goals and purposes.
- A system of systems usually has several and sometimes different operational priorities and with no defined way escalating any issues.
- A system of systems usually has several lifecycles with elements that are implemented asynchronously.
- A system of systems usually has several owners and drivers that make decisions independently of one another.

- SoS req is met.
- SoS req is met.
- SoS req is met.
- SoS req is met.
- SoS req is met.

Capabilities required for platooning control

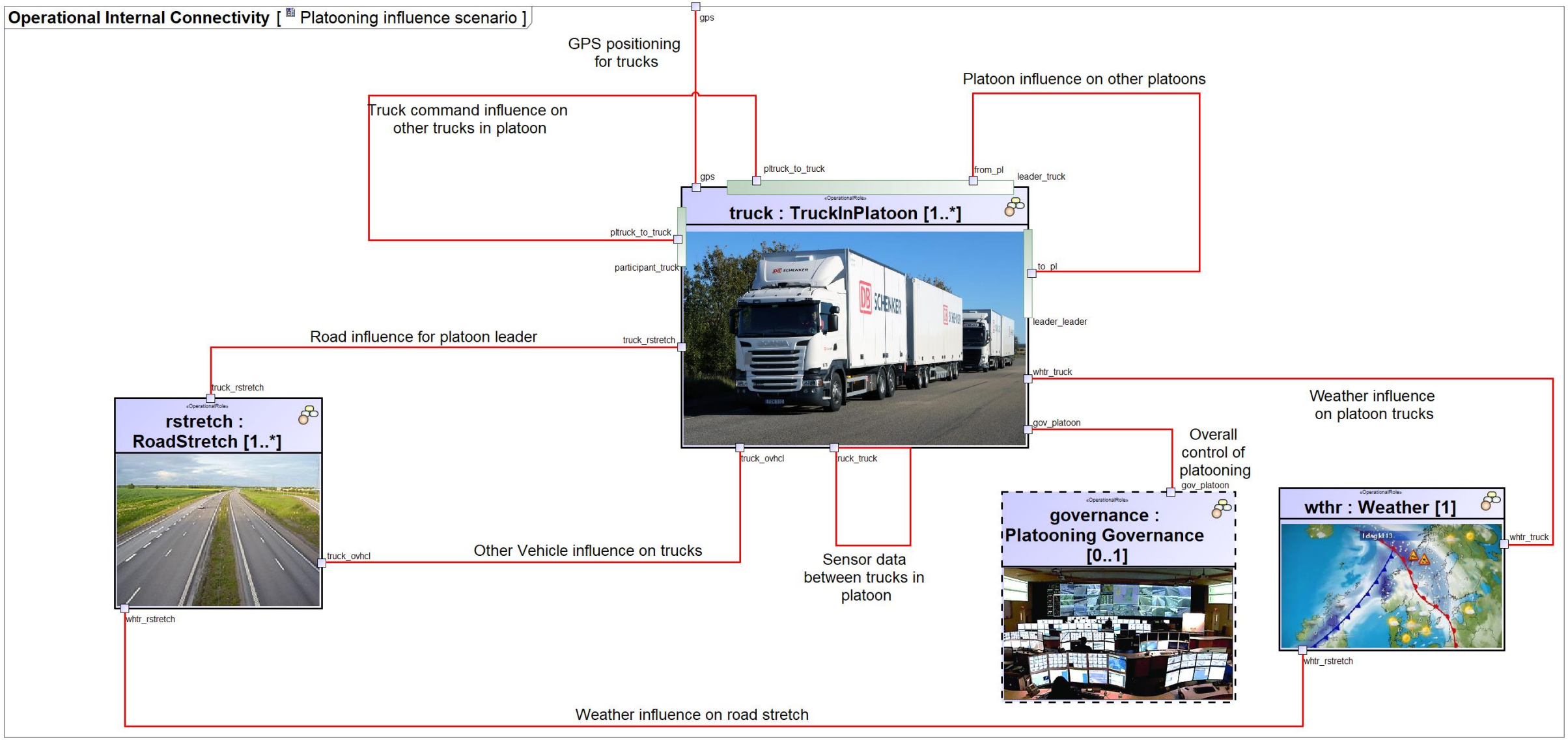


Identifying and dealing with hazards

- Example of type of tables used for hazard analysis
- Combination of different types – created by Safety Integrity
- Potentially can become VERY large

Name	Failure mode	Operational mode	Situation	Consequence	Hazard description	Exposure	Severity	Controllability	ASIL	Safety goal
Brake	Omission	High performance/Differential locks engaged	approaching intersection	Vehicle can not brake	Vehicle can not brake when approaching intersection	E4 Often-always	S3 Life-threatening (survival uncertain) or fatal injuries	C3 Difficult to control or uncontrollable	D	braking shall not fail to deccelerate vehicle

External influences of a platooning trucks



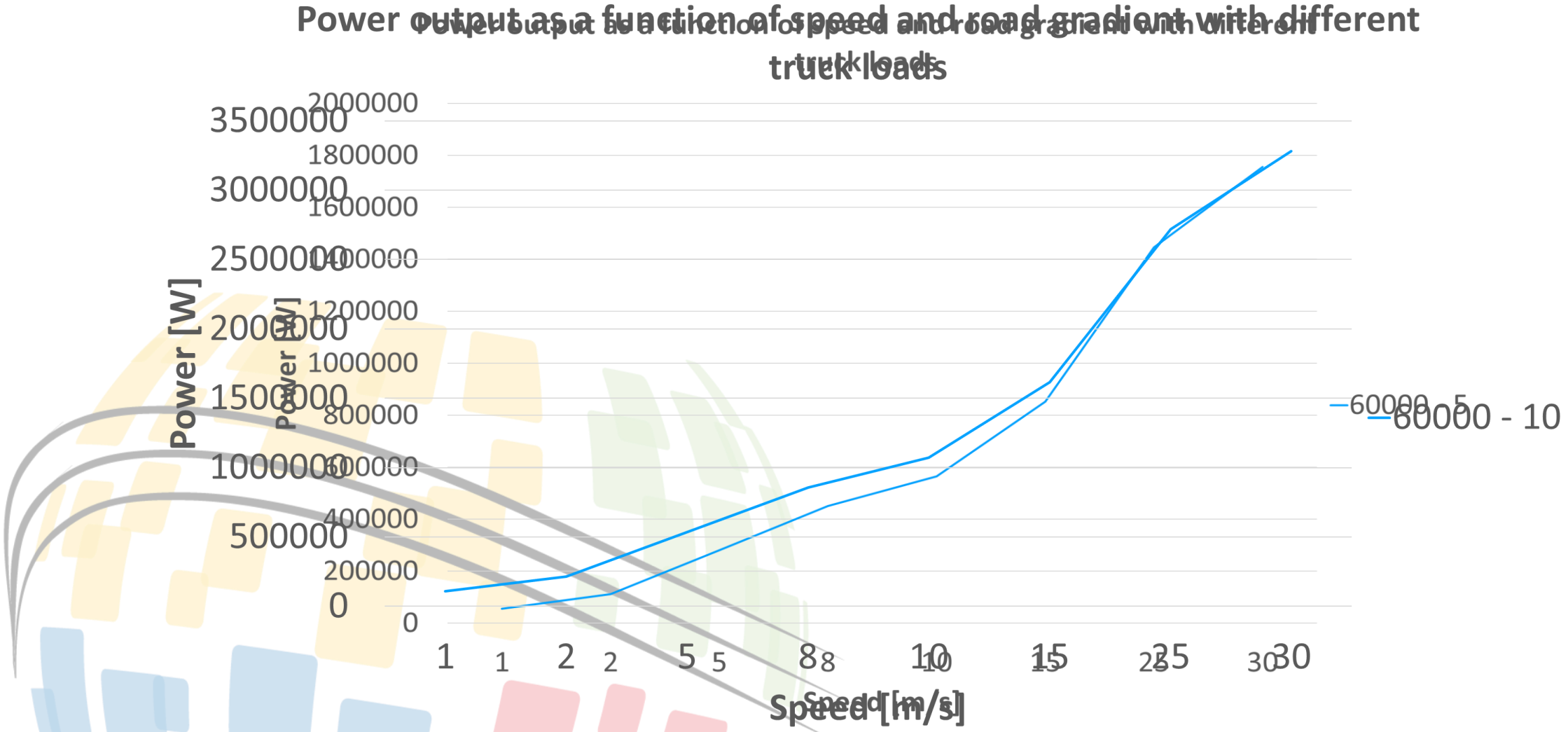
External influences

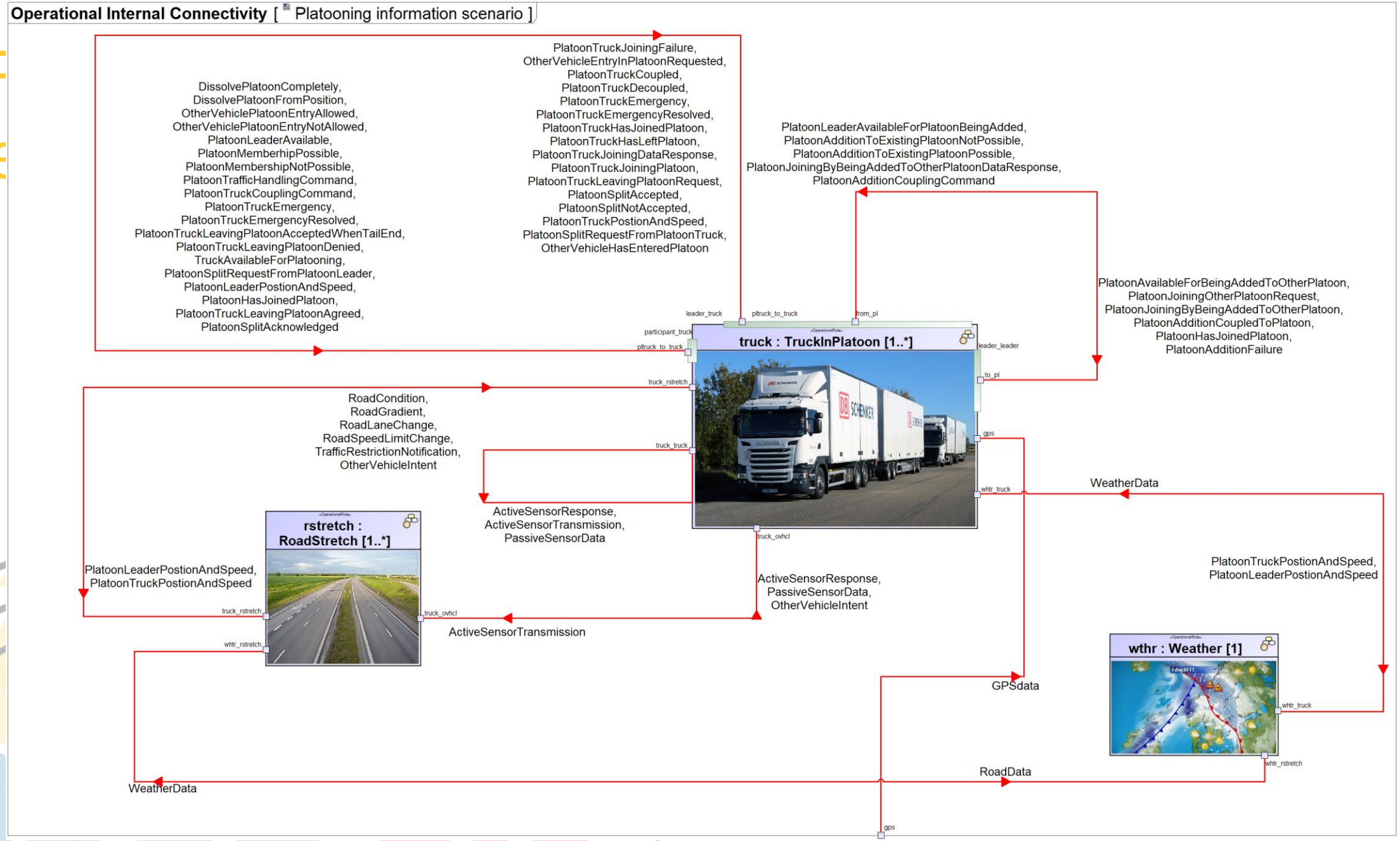
- The weather influences the trucks directly as well as the road on which they travel (snow, rain, ice, fog, heat, cold).
- The road with its changing number of lanes, gradients, speed restrictions and road works will impact of the platoon.
- The traffic that is not part of the platoon will need to be dealt with. The kind of vehicle that interacts with the platoon may well need different handling (police, ambulance, fire brigade, military vehicles, other trucks, civilian vehicles etc.).
- An overall platoon governance entity has been added since there may well be a need for an overall platooning control for a region. It can provide governance for the platoons in the region and provide data regarding conditions beyond immediate line of sight for a given platoon leader.

Constraints that influence platooning

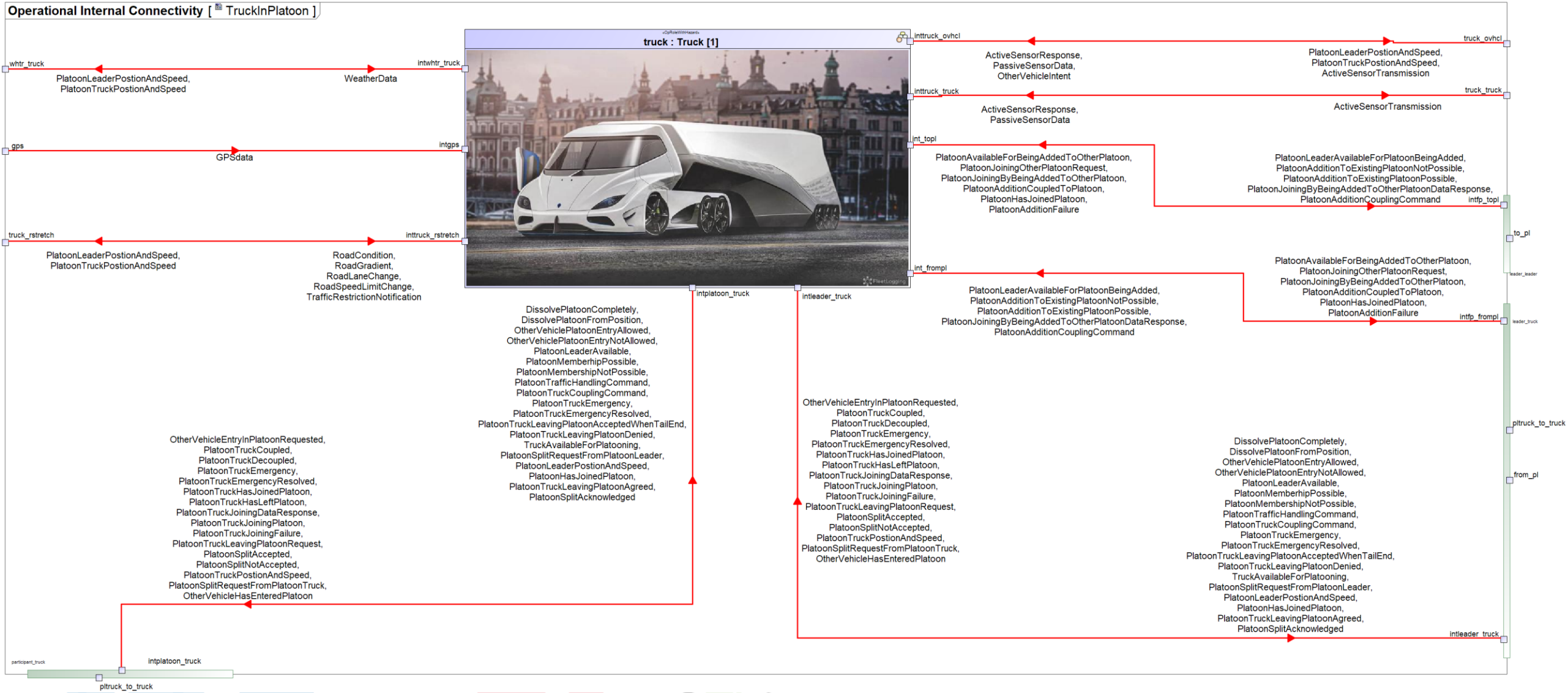
- Trucks have a regulated maximum length. The length differs between different countries, but 25 meters is a reasonable assumption concerning a truck maximum length.
- As the number of trucks in the platoon increase a leader follower approach as regards steering needs to be employed such that steering follows both lanes within the road as well as what the truck directly in front is doing.
- Trucks also have a maximum weight. Also, this can vary between countries and is furthermore subject to regulatory changes. A maximum weight of 60 tons is a reasonable assumption.
- If trucks in a platoon have different maximum power ability, gaps within the platoon may appear as the incline is negotiated. As an example, a 200-meter incline can be negotiated in 8 seconds by a truck capable of maintaining the speed 25 m/s (90 km/h). A truck that is only capable of 20 m/s (72 km/h) will only travel 160 meters in 8 seconds which would yield a gap of 40 meters in between the trucks. A platoon with such gaps appearing will be very difficult to control.

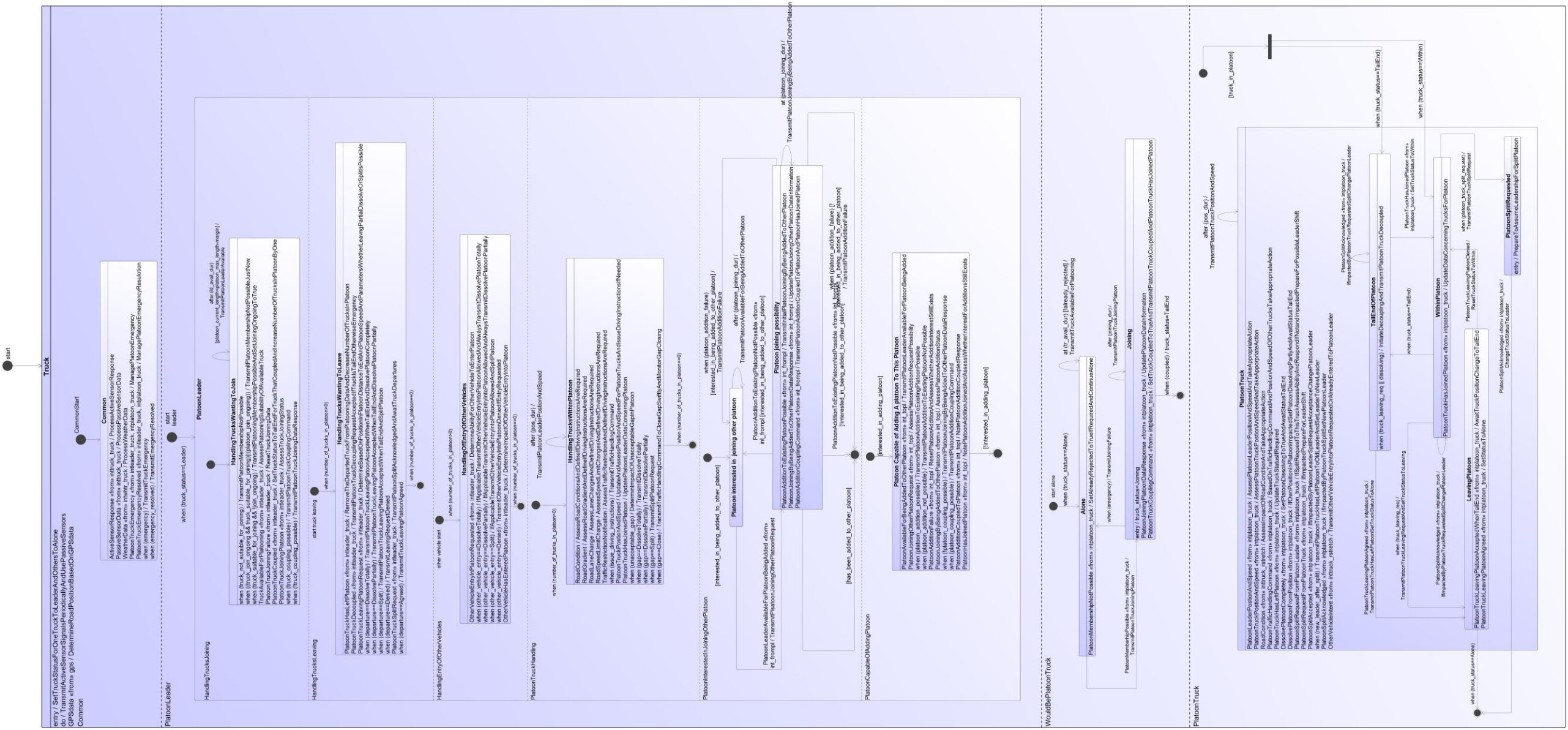
Gradient influence for maintaining the platoon distances




Operational Internal Connectivity [Platooning information scenario]
DissolvePlatoonCompletely,
DissolvePlatoonFromPosition,
OtherVehiclePlatoonEntryAllowed,
OtherVehiclePlatoonEntryNotAllowed,
PlatoonLeaderAvailable,
PlatoonMemberhipPossible,
PlatoonMembershipNotPossible,
PlatoonTrafficHandlingCommand,
PlatoonTruckCouplingCommand,
PlatoonTruckEmergency,
PlatoonTruckEmergencyResolved,
PlatoonTruckLeavingPlatoonAcceptedWhenTailEnd,
PlatoonTruckLeavingPlatoonDenied,
TruckAvailableForPlatooning,
PlatoonSplitRequestFromPlatoonLeader,
PlatoonLeaderPostionAndSpeed,
PlatoonHasJoinedPlatoon,
PlatoonTruckLeavingPlatoonAgreed,
PlatoonSplitAcknowledged
PlatoonTruckJoiningFailure,
OtherVehicleEntryInPlatoonRequested,
PlatoonTruckCoupled,
PlatoonTruckDecoupled,
PlatoonTruckEmergency,
PlatoonTruckEmergencyResolved,
PlatoonTruckHasJoinedPlatoon,
PlatoonTruckHasLeftPlatoon,
PlatoonTruckJoiningDataResponse,
PlatoonTruckJoiningPlatoon,
PlatoonTruckLeavingPlatoonRequest,
PlatoonSplitAccepted,
PlatoonSplitNotAccepted,
PlatoonTruckPostionAndSpeed,
PlatoonSplitRequestFromPlatoonTruck,
OtherVehicleHasEnteredPlatoon
PlatoonLeaderAvailableForPlatoonBeingAdded,
PlatoonAdditionToExistingPlatoonNotPossible,
PlatoonAdditionToExistingPlatoonPossible,
PlatoonJoiningByBeingAddedToOtherPlatoonDataResponse,
PlatoonAdditionCouplingCommand
PlatoonAvailableForBeingAddedToOtherPlatoon,
PlatoonJoiningOtherPlatoonRequest,
PlatoonJoiningByBeingAddedToOtherPlatoon,
PlatoonAdditionCoupledToPlatoon,
PlatoonHasJoinedPlatoon,
PlatoonAdditionFailure
leader_truck
pltruck_to_truck
from_pl
participant_truck
pltruck_to_truck
truck : TruckInPlatoon [1..*]
leader_leader
to_pl
truck_rstretch
gps
truck_truck
whtr_truck
truck_ovhcl
RoadCondition,
RoadGradient,
RoadLaneChange,
RoadSpeedLimitChange,
TrafficRestrictionNotification,
OtherVehicleIntent
ActiveSensorResponse,
ActiveSensorTransmission,
PassiveSensorData
WeatherData
rstretch :
RoadStretch [1..*]
PlatoonLeaderPostionAndSpeed,
PlatoonTruckPostionAndSpeed
truck_rstretch
truck_ovhcl
whtr_rstretch
ActiveSensorTransmission
ActiveSensorResponse,
PassiveSensorData,
OtherVehicleIntent
PlatoonTruckPostionAndSpeed,
PlatoonLeaderPostionAndSpeed
wthr : Weather [1]
whtr_truck
whtr_rstretch
GPSdata
RoadData
WeatherData
gps

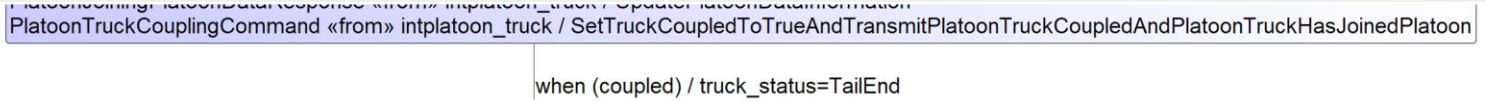
Control handling within a given truck for




Truck
PlatoonLeader
HandlingTrucksJoining
HandlingTrucksLeaving
HandlingEntryOfOtherVehicles
PlatoonTruckHandling
PlatoonInterestedInJoiningOtherPlatoon
PlatoonCapableOfAddingPlatoon
WouldBePlatoonTruck
PlatoonTruck
Common
PlatoonLeader
Alone
Joining
LeavingPlatoon
WithinPlatoon
TailEndOfPlatoon
HandlingTrucksWantingToJoin
HandlingTrucksWantingToLeave
HandlingTrucksWithinPlatoon
HandlingEntryOfOtherVehicles
Platoon joining possibility
Platoon capable of adding a platoon to this platoon
PlatoonTruck
Alone
Joining
LeavingPlatoon
WithinPlatoon
TailEndOfPlatoon

Hazards handling concerning a Truck joining a platoon

Hazard name	Failure/operational mode	Situation	Hazard description
Platoon truck assessment hazard	Incorrect data or assessment of parameters for truck wanting to join.	Truck wanting to join platoon	Platoon access allowed with unsafe safety distance to the truck in front.
Platoon length hazard	Truck joining leading to increase in platoon length	Platoon size increase	The length of the platoon is too long for safe control by platoon leader.



Hazard name	Safety goal
Platoon truck assessment hazard	Inspection handling is required to ensure that the trucks that want to join a platoon deliver correct information to the platoon leader.
Platoon truck assessment hazard	Inspection handling is required to ensure that a platoon leader assessment of truck joining suitability is correct.
Platoon length hazard	The assessment as to maximum length of platoon needs to be made external traffic flow conditions as well as road conditions into account.

Sequ toon


Operational Interaction Scenarios [Joining a platoon]
«OperationalPerformer»
truck : TruckInPlatoon
«OperationalPerformer»
truck : TruckInPlatoon
1: PlatoonLeaderAvailable(platoon_id=1, platoon_leader_truck_id=1, platoon_leader_truck_data=pl_data)
2: TruckAvailableForPlatooning(truck_id=5, platoon_truck_data=truck_data)
3: PlatoonMemberhipPossible(platoon_id=1, platoon_leader_truck_id=1, truck_id=5, joining_distance=sf_dist, position_in_platoon=3)
4: PlatoonTruckJoiningPlatoon(platoon_id=1, platoon_leader_truck_id=1, truck_id=5, current_distance=curr_dist)
5: PlatoonTruckJoiningDataResponse(platoon_id=1, platoon_leader_truck_id=1, platoon_leader_truck_data=pl_data, coupling_distance=c_dist, platoon_slot=3)
{joining_dur}
6: PlatoonTruckJoiningPlatoon(platoon_id=1, platoon_leader_truck_id=1, truck_id=5, current_distance=curr_dist)
7: PlatoonTruckJoiningDataResponse(platoon_id=1, platoon_leader_truck_id=1, platoon_leader_truck_data=pl_data, coupling_distance=c_dist, platoon_slot=3)
{joining_dur}
8: PlatoonTruckJoiningPlatoon(platoon_id=1, platoon_leader_truck_id=1, truck_id=5, current_distance=curr_dist)
9: PlatoonTruckJoiningDataResponse(platoon_id=1, platoon_leader_truck_id=1, platoon_leader_truck_data=pl_data, coupling_distance=c_dist, platoon_slot=3)
{joining_dur}
10: PlatoonTruckJoiningPlatoon(platoon_id=1, platoon_leader_truck_id=1, truck_id=5, current_distance=curr_dist)
11: PlatoonTruckCouplingCommand(platoon_id=1.0, platoon_leader_truck_id=1.0, truck_id=5.0, platoon_slot=3.0)
12: PlatoonTruckCoupled(platoon_id=1, platoon_leader_truck_id=1, truck_id=0.0, distance_to_truck_in_front=dist, platoon_slot=3, speed=t_speed)

Hazards handling for platoon leader dealing with platoon truck

Hazard name	Failure/operational mode	Situation	Hazard description
Road condition handling hazard	Road condition changes (lanes, speed restrictions, traffic lights, traffic flow, gradients)	Platoon moving normally	Changes in road conditions cannot be handled safely by members of the platoon.
Platoon gap hazard handling	Gaps appear inside of the platoon where individual truck members cannot follow the instructions originating from the platoon leader.	Platoon contains gaps that result from inability to manage road conditions	Uncontrolled changes in distance between trucks within a platoon leading to gaps that can be used by other non-platoon vehicles leading to uncontrollability.

when (issue_driving_instructions) / TransmitTrafficHandlingCommand

Hazard name	Safety goal
Road condition handling hazard	Platoon leader shall monitor status of member with a frequency that ensures that road condition changes can be dealt with.
Platoon gap handling hazard	If gaps appear within the platoon the platoon leader shall be able to act to either close the gap, dissolve the platoon, dissolve the platoon partially or split the platoon into two platoons, making the truck with the gap just in front of it the platoon leader for the trucks behind it.

Hazards dealing with truck leaving or entry of other vehicles into platoon.

Hazard name	Failure/operational mode	Situation	Hazard description
Platoon truck departure hazard	Platoon truck leaves platoon	Platoon driving	Platoon truck departure initiated in an uncontrolled manner.
Platoon split request hazard	Platoon leader split request	Platoon should be divided into two platoons	Platoon split into two platoons attempted in an uncontrolled manner.
Other vehicle interested in entry into platoon.	A vehicle attempts to gain entry to platoon	Parts of the platoon has different end destination than other parts.	Other non-platoon vehicle attempting or succeeding in gaining entry into the platoon making the platoon uncontrollable.

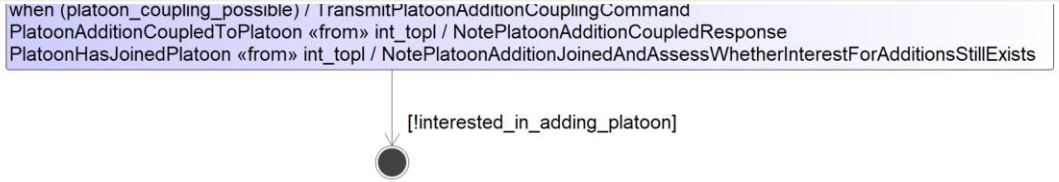
when (number_of_trucks_in_platoon==0)

Hazard name	Safety goal
Platoon truck departure hazard	The platoon leader shall have the ability to respond to a departure request either by agreeing (tail-end truck can easily leave) or by dissolving the platoon completely, partially or by splitting it based on the conditions at the time of the departure request.
Platoon split request hazard	The platoon leader shall be able to manage a split of the platoon either because of a request it generates or after having a platoon truck requesting a split.
Other vehicle interested in entry into platoon.	The platoon leader shall be able to manage a request entry or the fact that another vehicle has already succeeded in entering the platoon by either dissolving it totally or partially or by splitting it making the truck behind the other vehicle platoon leader for the new platoon.

Hazards dealing with platoon joining another platoon

Hazard name	Failure/operational mode	Situation	Hazard description
Platoon joining platoon assessment hazard	Incorrect data or assessment of parameters for platoon wanting to join.	Platoon wanting to be added to another platoon	Platoon addition allowed with unsafe characteristics.
Platoon joining platoon length hazard	Platoon joining leading to increase in platoon length	Platoon size increase	The length of the platoon is too long for safe control by platoon leader.

Hazard name	Safety goal
Platoon joining platoon assessment hazard	Allowing an existing platoon to join another platoon requires assessment of the parameters of all trucks within the platoon wanting to join based on a standardized approach.
Platoon joining platoon length hazard	Adding an entire platoon to an existing platoon shall only be possible if the total length falls within the length safety margin given the external conditions.



Summary

- In this presentation a UAF model has been used to aid in the analysis of hazards for a system of systems.
- Based on the work performed, the use of a logical model to characterize the needed behavior of the system of systems is very useful in determining the hazards that a given system of system will need to deal with.
- The use of a state machine is a very compact way to do this and within it details a very large amount of possible sequence charts that would look at one hazard at the time. If only the sequence charts are used, then the chance of maintaining overall consistency would be much less making the hazard analysis less secure.

Possible future work

- The safety goals added here can be viewed as requirements that the platooning functionality will have to meet and an attempt to create a platooning sub-system to be placed within trucks would have to ensure that these requirements are met.
- Continued work with this application would involve simulation of the model that has been created such that the various functions defined as part of the state machine can ensure the safety goals.
- The UAF security domain should be used to further analyze the need to protect the functionality of platooning from malicious attacks.
- Especially the governance of platoons could benefit from a service approach. The UAF service domain could then be used to describe the functionality of the services that the governance would be able to provide.
- Finally, a real sub-system implementation could make use of the UAF resource domain for a more detailed representation of the system needed to ensure that dynamically creatable and dissolvable platoons consisting of completely different types of trucks could be handled.

Conclusions

- One important conclusion based on the work performed is that the model is a key to the ability to manage a very large combinatory space of situations, fault modes and system states.
- From the example point of view the following conclusion can be drawn.
  - Based on the decisions that the driver of the platoon leader truck will have to make for trucks joining or exiting a platoon it seems clear that it has to be supported by artificial intelligence (AI) applications to perform all the analysis needed in order to present the lead driver with clear cut decisions that will not impact on the driver driving the truck he/ she is driving.

33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

www.incose.org/symp2023
#INCOSEIS